GSA U.S. General Services Administration

GOVERNMENT SMART CARD HANDBOOK

PREFACE

This guidance Handbook is the result of Government experience gained over the past several years with smart card programs that include many smart card implementations, pilots, and projects conducted throughout the Federal government. The Handbook includes very significant input from industry and academic resources. The purpose of this Handbook is to share lessons learned and to provide guidance to Federal agencies contemplating the development and deployment of smart card or integrated circuit card-based identity and credentialing systems.

At this writing there is a project under way to make this Handbook as web friendly as possible. Any suggestions on how to make this Handbook more useful and convenient would be appreciated. Please e-mail comments to Jim Hunt (jim.hunt@gsa.gov) and Bill Holcombe (bill.holcombe@gsa.gov).

Bill Holcombe,

Office of Governmentwide Policy
General Services Administration

February 2004

ACKNOWLEDGEMENTS

This '*Government Smart Card Handbook'* has been developed under the joint sponsorship of the General Services Administration Office of Governmentwide Policy and the Smart Card Interoperability Advisory Board (IAB). It would not have been possible to produce this Handbook without the contributions of knowledgeable people from government, industry, and academia. We acknowledge their contributions and give special thanks to the following direct contributors:

Tim Baldridge – National Aeronautics and Space Administration
Ralph Billeri – BearingPoint Inc.
Dallas Bishoff – Veterans Affairs AAIP Team
Joseph Broghamer – Department of Homeland Security
Michael Brooks – General Services Administration
Michael Butler – DoD Common Access Card Program
Fred Catoe – Veterans Affairs AAIP Team
Pamela Corry – Department of Homeland Security
Patty Davis – Department of Agriculture
Russ Davis – Federal Department of Insurance Corporation
Peter Dauderis – General Services Administration
Portia Dischinger – National Aeronautics and Space Administration
Mary Dixon – Department of Defense
Bob Donelson – Department of Interior
Ron Dorman – Defense Information Systems Agency
James Dray – National Institute of Standards and Technology
John de Ferrari – General Accounting Office
Keith Filzen – Central Intelligence Agency
Jack Finberg – General Services Administration
Liz Fong – National Institute of Standards and Technology
George Fortwengler – Department of Health and Human Services
Damon Goddard – General Services Administration
Scott Glaser – General Services Administration
David Hauge – BearingPoint Inc.
Peter Han – General Services Administration
Gordon Hannah – BearingPoint Inc.
Daryl Hendricks – General Services Administration
Barbara Hoffman – Department of the Navy
Bill Holcombe – General Services Administration
Lee Holcomb – Department of Homeland Security
Keith Hughes – Department of Homeland Security
Paul Hunter – Transportation Workers Identification Credential
Joel Hurford – United States Patent and Trademark Office
Kevin Hurst – Office of Science and Technology Policy
Lisa Kalinowski – BearingPoint Inc.
Jeff Kindschuh – Veterans Affairs AAIP Team
July Kresgi – Department of Agriculture
Lolie Kull – Department of State
Steven Law – General Accounting Office
Greta Lehman – Department of Defense – Army
Graham MacKenzie – Department of Treasury
Amin Magdi – World Bank Group
Eugenia McGroarty – DoD – Defense Logistics Agency
John Mercer – Department of State
Carey Miller – BearingPoint Inc.
Mary Mitchell – General Services Administration
Martin Monahan – World Bank Group
John Moore – General Services Administration
William Morrison – National Aeronautics and Space Administration
Trung Nguyen – Department of Treasury
Steve Parsons – Transportation Security Administration
Sonya Pee – General Services Administration
Arthur Purcell – United States Patent and Trademark Office
Ronald Pusz – BearingPoint Inc.
Fred Riggle – United States Geological Survey
Teresa Schwarzhoff – National Institute of Standards and Technology
John G. Sindelar – General Services Administration
Judith Spencer – General Services Administration
Dario Stipisic – BearingPoint Inc.
Michael Sulak – Department of State
David Temoshok – General Services Administration
Janel Valverde – BearingPoint Inc.
Martin Wagner – General Services Administration
Dr. Jim Wayman - National Biometric Testing Center, San Jose State
William Windsor – General Services Administration
James Zok – Department of Transportation – Maritime Administration

We also recognize and give thanks to the Smart Card Alliance and their industry members for their assistance in providing commentary and editorial advice to this Handbook:

Randy Vanderhoof – Executive Director, Smart Card Alliance
Cathy Medich – Government Smart Card Handbook Committee Chair, Smart Card Alliance

Bob Beer – Datacard Group
Linda Brown – Infineon Technologies
Alex Giakoumis – Atmel Corporation
Kevin Kozlowski – XTec, Incorporated
Bob Merkert – SCM Microsystems
Neville Pattinson – Axalto
Joe Pilozzi – Philips Semiconductors
James Russell – MasterCard International
Carlos Santos – IBM
Rick Uhrig – Gemplus
Bob Wilberger – Northrop Grumman IT

TABLE OF CONTENTS

TABLE OF FIGURES

Executive Summary

When the first edition of the 'Smart Card Policy and Administrative Guidelines' was published in 2000, it was presented to an audience of smart card managers as a primer on the technology. Managers were offered a resource that enabled them to evaluate the technology, reflect on relevant policy issues, and develop an implementation strategy.

Since the publication of the original Guidelines, the government's acceptance of smart cards has transformed from an enterprise interested in the technology to one in which the technology is being readily implemented. Specifically, over four million smart cards have now been issued to government employees. Smart cards are being used across several government agencies and at varying levels of functionality. Hence, there is a strong need within government to have access to a resource that can provide current, up-to-date information regarding smart cards. One of the most significant lessons learned in early smart card programs has been the need to incorporate a team that includes all the stakeholders including the program manager, physical access personnel, and information technology support staff. Through the development of the team, will come the knowledge and understanding necessary to assign roles and responsibilities for a successful program. Furthermore, as the underlying technologies such as public key infrastructure and biometrics that make smart cards more robust and versatile have continued to converge and mature, the publication of this Handbook becomes even timelier.

The goals of this Handbook are to offer a valuable, hands-on resource that will facilitate the reader's understanding of smart cards, cite case studies of smart card engagements in government, and map the process for implementing smart cards through the careful consideration of task order criteria and key decisions. It is intended that readers return to the Handbook's pages frequently and be presented with an opportunity to reinforce their knowledge of smart cards or discover an entirely new facet of the technology.

Several years removed from the first government installation of multi-application smart card technology, we can conclude with confidence that the technology is no longer experimental. Instead, the application of smart cards within government has developed into a proven asset with a quantifiable return on investment that has facilitated and secured the process employees use to access government facilities and resources.

Finally, the Handbook presents tremendous value to a reader because its content is an amalgamation of the experiences of many of the leading smart card users working in government, industry, and academia. The recent efforts of smart card project managers, policy makers, and manufacturers to further the adoption of smart cards have been consolidated here in an effort to offer an all-encompassing perspective on the current state of smart cards in government.

Government Smart Card Handbook

1. INTRODUCTION

The Clinger-Cohen Act (CCA) of 1996 and the Defense Reform Initiative of 1999 committed that certain government agencies improve innovation through the reformation of business processes and exploitation of technology to achieve efficiencies and improve readiness. The core ideologies for this reform were to: focus the enterprise on a unifying vision, commit leadership to change, focus on core competencies, streamline organizations, invest in people, exploit information technology, and eliminate barriers between organizations.

Reforms in electronic business, travel re-engineering, and expanded use of government-wide commercial purchase cards have presented new opportunities to use smart card technology as an enabling tool. Smart card technology offers an additional layer of electronic security and information assurance for user authentication, confidentiality, non-repudiation, information integrity, physical access control to facilities, and logical access control to an agency's computer systems. To facilitate this effort, the Smart Card Program was established and composed of representatives from the Federal civilian, defense, and intelligence communities as a co-operative effort under the leadership of the General Services Administration (GSA) and the Smart Card Project Managers Group. The President's Management Agenda (PMA) released in fiscal year 2002, also called for the following:

- Expand and improve the FirstGov web site (www.FirstGov.gov) to offer citizens a convenient entry to government services;
- Establish a Federal Public Key Infrastructure (PKI) to be adopted by agencies to promote digital signatures for transactions within the Federal government, between government and businesses, and between government and citizens; and
- By the end of 2002, use a single e-procurement portal, www.FedBizOpps.gov, by all agencies to provide access to notices of solicitations over $25,000.

This Government Smart Card Handbook was developed to assist agencies in the development of a smart card program to harness the technologies currently available to:

- Obtain a secure identity management solution.
- Accomplish the objectives of government initiatives.
- Remain consistent with government regulations, directives, and applicable standards.

This Handbook is intended to serve as a reference document providing government agencies with guidance for implementing an interoperable smart card program within their organization. This Handbook was originally conceived and published in 2000. As a result of significant advances in smart card technology, an effort was initiated in 2003 to bring the information in the Handbook current. In addition, many government agencies have significantly increased their internal knowledge of smart card technologies and related systems. This information is reflected in the current version of the guide. The implementation of smart cards can be complex. The intent of this guide is to provide the high level reasons for **why** to implement a program as well as provide practical guidance for **who** should be involved and **how** to begin.

1.1 Smart Identification Card Vision and Goals

In order to help achieve the vision of using smart card technology to streamline administrative processes, a role of GSA is to provide assistance to Federal agencies in the implementation of smart card technologies for a wide range of purposes including personal identification, physical and logical access, digital signatures, travel, and small purchases. It is GSA's intent to assist Federal agencies, via the Smart Access Common ID contract, in reengineering their business processes to achieve streamlined operations and cost savings through enhanced operational efficiency.

In creating a common identification card for Federal government employees, the three goals of the Smart Identification Card program are to:

- Develop smart card interoperability;
- Establish a set of mandatory requirements with optional value-added services; and
- Build in the capability to add new applications and migrate to advanced technologies.

To provide a common, interoperable identification card that can be used similarly across agencies, this project has defined the following objectives for this card program:

- Interoperability across Federal agencies;
- Open government system framework;
- Flexibility; and
- Interentity cooperation.

Each of these objectives is described in further detail in the following sections.

1.1.1 ACHIEVING INTEROPERABILITY ACROSS FEDERAL AGENCIES

INTEROPERABILITY – What Is It and Why Do We Need IT?

Interoperability refers to the cooperative processing of an application by distinct software, hardware, firmware, various generations of cards and terminals, operating policies and administrative procedures. Thus, this term describes a system or product that can operate with another system or product directly without additional development effort by the user. In an interoperable environment, there is sufficient flexibility to accommodate cards from multiple issuers and provide access to multiple services. Interoperability ensures that there is flexibility at all levels of service delivery, that investments by consumers and service providers are protected, and that customers have vendor-independent access to services.

Interoperability, however, entails more than just the technical capability of a card to operate in any terminal. In an environment in which the card is to be used for physical access in non-"home" agencies, the card issuer for the receiving agency may be different from the card issuer for the originating agency. Business agreements must be in place between originating and receiving agencies if the card is to be accepted for physical access across agencies. If the Smart Identification Card includes financial applications, the issue of interoperability may become even more complex. In such an environment, there may be no direct relationship between the card issuer and the acquirer of the financial transactions. To achieve interoperability, both the card issuer and the acquirer must agree to a common set of operating rules.

Technical specifications, operating rules, and business arrangements are interrelated in the achievement of interoperability. Technical specifications ensure hardware, software, and data compatibility by configuring system components to interoperate to pass data and transactions.

While technical standards ensure “physical” compatibility, operating rules provide the management and administrative framework to ensure that transactions are properly handled. These rules define procedures for exception processing and security and build on technical specifications by defining data flows and procedural standardization. Most importantly, the rules allocate responsibilities and liabilities within the system. Within an open system, operating rules constitute the components of binding business arrangements among the system participants and stakeholders. Formerly, there were few if any operating agreements across government agencies that addressed common procedures for card management or interagency access to facilities, systems, or data. GSA continues to work to achieve interoperability across agencies.

A key goal for government agency smart card credentialing systems is interoperability. Accomplishing this goal throughout the government requires general e-authentication policies, specific identity management policies and detailed technology roadmaps and interoperability specifications. A number of federal initiatives and groups are collaborating on deliverables that are setting the directions for interoperability for new government smart card credential programs. Vendors and manufacturers are also working collectively to achieve solutions that work in concert with one another.

One of the largest barriers agencies face is the ability to authenticate one another’s identification credentials. Going forward, agencies will continue to develop a level of trust for credentials provided by other organizations. There is a dedicated focus on a trusted government credentialing system in which one credential is recognized and accepted government-wide.

The following are current initiatives that are focused on achieving government smart card interoperability.

Federal Identity and Credentialing Committee (FICC). A committee of the E-Authentication Initiative**,** FICC has goals to simplify and unify identity authentication for Federal employees, to create requirements for credentials used for physical and logical access as well as for credential issuance, and to develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture. FICC participants include smart card and public key infrastructure (PKI) managers, human resource managers, physical security managers, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). The group has completed a draft policy framework that includes policies for smart cards and PKI and guidance for establishing employee identity.

Smart Card Interoperability Advisory Board (IAB). The IAB is composed of multiple government agencies and is chartered to set the technology roadmap for interoperable smart card implementations. The IAB in cooperation with the FICC is developing a policy statement on the use of smart cards for identification and credentialing of Federal employees.

Government Smart Card Interoperability Specification. Developed by GSA and NIST, the Government Smart Card Interoperability Specification (GSC-IS) provides technical solutions to a number of interoperability issues associated with contact and contactless smart card technology implementation. The specification was defined to provide the ability to develop secure identification smart cards that can operate across multiple government agencies or among federal, state and local governments. Version 2.1 of the specification was released by NIST in July 2003. It provides guidance for system planners, both in and out of government, and the tools necessary to ensure that they have smart card and smart card reader interoperability. Products will be certified via conformance and security test programs established by NIST, providing organizations with a ready supply of certified products and the assurance that information technology (IT) investments will have a broader opportunity to generate a return.

Federated Identity Cross-credentialing System (FiXs)/Defense Cross-credential Identification System (DCIS). The Department of Defense (DoD) and a coalition of private industry partners has launched a proof-of-concept project that implements an identity management and credentialing system between DoD and industry participants that have a need for employee identification and authentication as part of their joint working environment (e.g., providing DoD employees with authenticated access to private industry facilities with DoD-issued credentials and strongly authenticating contractor personnel who present contractor-issued credentials). The baseline of credentialing will be to establish an environment for government-to-government, business-to-government, government-to-business and business-to-business identification processes, with biometrics held at the visitor's home site. Interoperability of credentials is established through a set of policies, operating rules and technical specifications that allow participants to act and exchange information on an equal basis. This pilot is being conducted under the direction of the Federated Electronic Government Coalition (FEGC) and will demonstrate how multiple organizations can collaborate to achieve interoperable, trusted credentials. The Department of Defense will be using the ***Common Access Card (CAC)*** as their identity token, while individual contractors will be using a token developed by them, which is in most cases a smart card. This FiXs/DCIS pilot could provide valuable lessons learned that may be applied throughout all government agencies, thus reducing development time and expenditures.

In addition to the efforts described above, commercial labs offer services for evaluating products and the interoperability of products. Since identity management systems are complex and include multiple products and technologies, use of such a lab may be beneficial in assessing the interoperability of products.

1.1.2 OPEN GOVERNMENT SYSTEM FRAMEWORK

It is an objective to develop the Smart Identification Card project within an open government system framework that is vendor independent and encourages open competition. The smart card industry has embraced a number of initiatives to enhance system openness. Achieving an open system configuration and maintaining the ability to easily transition to new and emerging technologies in the future are key objectives. Therefore, a critical enabling strategy for this effort is compliance with an open framework including:

- Open Card Framework (OCF) or Personal Computer/Smart Card (PC/SC) Work Group specifications for PC application programming interface (API);
- Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC) for databases;
- Generic APIs for biometrics;
- Open operating systems such as Java-based systems; and
- Other industry initiatives to achieve openness in system architecture, open source code, and platform transparency for applications.

1.1.3 FLEXIBILITY

There is a spectrum of agency security characteristics across the government. Some agencies, including those that comprise the intelligence community, have far more intensive security needs. Civilian agencies, with different security requirements, will have less need (though not "no need") to implement an intensive access control program. Closely related to these varying levels of need are the corresponding levels of resource availability. Agencies have different priorities and, therefore, different levels of ability to implement security-related systems. ID systems must provide the flexibility to enable agencies to customize a solution to their individual needs while continuing to focus on interoperability.

Government agency characteristics and needs can be diverse. It is the intent of the Smart Identification Card project to respect agency diversity and encourage solutions that are customized to meet the needs of specific circumstances. While GSA encourages adherence to recognized industry standards and actively promotes efforts to achieve interoperability, the agency's intended role is not to mandate "one size fits all" solutions. Rather, through the concept of value-added requirements, GSA is striving to achieve maximum flexibility by providing the appropriate building blocks to assemble smart card solutions that work effectively to meet the needs of individual agencies.

1.1.4 INTERENTITY COOPERATION

Another factor that will affect the success of a smart card implementation is the ability to develop the necessary management structure to achieve a multi-application card platform. It will be necessary to rethink traditional strategies for card issuance and management. A new paradigm for distributing cards to the cardholder population may have to evolve to address the complex structure needed to accommodate multiple applications or functions on the card.

The smart card management structure may vary from agency to agency. Interagency cooperation as well as ongoing interaction with private entities will become critical to the smooth operation of a multi-application smart card issuance process. Thus, GSA believes that the smart card program must be flexible enough to support many forms of interentity cooperation in order to accommodate divergent approaches to card issuance and management.

1.2 GSA's Role

To help achieve the vision of using smart card technology to streamline administrative processes, enhance security, and support electronic commerce across the Federal government, GSA was tasked to facilitate the transition to this emerging technology. GSA's Office of Smart Card Initiatives and Office of Government-wide Policy teamed to develop the smart card program to respond to this tasking. The original purpose of this initiative was to establish a contract vehicle available for all Federal agencies to use that would allow government agencies to acquire a standard employee identification/building pass card. It was envisioned that agencies would be able to choose a card that would have a standard appearance but also have a distinctive agency identity, including logo/mark and agency/bureau name. The card would also provide unique functionality as defined by the implementing agency. The card would carry a mark or icon indicating that it met the Federal government standards being set for such a card under the smart card program.

The card system and card services were intended to provide uniform physical and logical access control functions for participating Federal agencies based on a set of common requirements. The intent was for the card to be used for physical access control to buildings, offices and restricted areas and logical access control to Federal systems, networks, and servers. The goal was to achieve a standardized card, which could be read by multiple types of readers in government facilities with basic and enhanced identification attributes. The card would carry identification and authentication information and provide the optional capability of multiple technologies as required by the agency.

The first step to achieving this vision was to organize the Common Access ID Steering Committee representing the various stakeholders for the Smart Identification Card. This group was tasked with determining card attribute specifications, card technical standards and common operational requirements for government-wide use. Under the auspices of this work group, GSA surveyed a wide range of Federal agencies, developed a Common Requirements Document, and, based on the Common Requirements Document, prepared a Statement of Work for the Smart Identification Card Request for Proposals.

As part of the requirements-gathering initiative, GSA met with representatives from the Federal civilian, defense, and intelligence agencies and documented individual agency requirements. Additionally, GSA surveyed the vendor community to determine the state of available technology. Based on the input obtained from these interviews, GSA completed an exposure draft of the *Smart Identification Card: Preliminary Requirements Document* that was released on December 14, 1998.

The Common Access ID Steering Committee reviewed this document initially and a second draft, Exposure Draft 2.0, was developed that incorporated the comments of this work group. Exposure Draft 2.0, dated March 23, 1999, was then widely distributed to government agency representatives for comment. The resulting updated document, Exposure Draft 3.0, incorporated the agency comments and was presented to the wider vendor community for comment at the CardTech/SecurTech Conference in May 1999. Industry-submitted comments and suggestions for the document were incorporated into the *Smart Identification Card: Final Requirements Document* released July 2, 1999. Additionally, a synopsis of vendor comments and GSA's response was posted to GSA's web site.

Based on the final requirements document, GSA developed a Statement of Work. This Statement of Work was submitted to the Federal Computer Center (FEDCAC), which released the Smart Identification Card (GS-TFF-99-203) solicitation for the Smart Identification Card on January 7, 2000. A number of companies competed to qualify for delivering on the statement of work. In May 2000, the Smart Access Common ID contract vehicle was awarded to four qualifying vendors, BearingPoint, EDS, Maximus and Northrop Grumman IT.

The current Handbook was updated as a result of the General Accounting Office (GAO) report, GAO-03-144, dated January 2003. This report recommended that GSA update the previous version of the 'Smart Card and Administrative Guidelines' to reflect current smart card technology and standards.

1.3 Handbook and Smart Access Common ID Contract Purpose and Organization

While adoption of a multi-application smart card offers the potential for cost savings and streamlined operations, it also raises a number of issues of concern to agencies contemplating the use of this emerging technology. In order to promote the adoption of smart card technology, it was found necessary to provide technical support and management assistance to those agencies lacking that expertise.

The intent of the Smart Access Common ID contract is to provide assistance to those agencies seeking to implement smart card technology. By documenting common requirements, resolving standards, and offering a government-wide contract vehicle, Government sought to streamline the procurement process, reduce the cost of card acquisition, achieve economies of scale, and encourage conformance to agreed-upon standards.

1.3.1 PURPOSE

The purpose of this Handbook is to provide guidance for those agencies that want to use the Smart Access Common ID contract vehicle to procure and implement an interoperable employee identification card. This Handbook presents and discusses the issues and lessons learned during the implementation of a multi-application smart card platform.

1.3.2 ORGANIZATION

This '*Government Smart Card Handbook'* is organized into the following sections:

- **Section 1: Introduction.** This section introduces the Smart Identification Card Project and presents the organization of this Handbook.

- **Section 2: Smart Card Technology.** This section introduces and describes smart cards and related technologies. It discusses the benefits of smart cards and presents the relative merits of smart cards vs. related technologies. This section also includes a discussion of the different smart card functions and applications that can be implemented, including a detailed description of PKI, digital signatures and biometrics.

- **Section 3: Agency Implementations.** This section highlights the importance of an agency's role in understanding its own specific smart card requirements and goals for a successful smart card implementation. This section also describes the current status of major smart users and departments throughout the federal government.

- **Section 4: Key Decisions.** This section walks agencies through making the key decisions that will affect procurement and implementation of their smart card platform.

- **Section 5: Planning & Implementation Issues.** This section assists agencies in planning and developing procedures for their smart card program implementations. It addresses the re-engineering and implementation planning that should accompany the procurement process.

- **Section 6: Writing the Task Order.** This section describes the role of GSA as it relates to implementing a smart card project. It introduces the process by which an agency can use GSA's expertise for requirements definition, RFP development, and other activities up through system implementation.

- **Section 7: Summary and Recommendations.** This section summarizes lessons learned from the different smart card implementations and presents technical, management/organizational, legal, cost, and standards/interoperability recommendations for agencies implementing a Smart Identification Card.

Additionally this Handbook contains appendices that are meant to provide a "tool kit" for practical assistance to agencies in their smart card implementation efforts. These appendices include:

- **Glossary of Terms.** Appendix A provides a glossary of technical terms used throughout this Handbook.
- **Survey of Federal Smart Card Projects.** Appendix B describes some key smart card programs that have contributed to the body of "lessons learned" in the introduction of smart card technology in the government environment.
- **Index of Smart Card Web Sites.** Appendix C provides a listing of key web sites that are good sources of information on smart card technology and policy.
- **References.** Appendix D presents key references considered to be of use to agencies developing smart card programs.
- **Interoperability Standards.** Appendix E presents the most current version of the Smart Card Interoperability Specifications developed by the Interoperability Committee.
- **Agency Profile Questionnaire.** Appendix F assists an agency in developing a profile that will impact whether or how a smart card will be implemented.
- **Agency Profile.** Appendix G presents the agency profile that is used by agencies to determine their specific characteristics and needs.

2. SMART CARD TECHNOLOGY

Goal: Understand smart cards and how they could benefit your agency.

2.1 Smart Cards and Related Technologies

This section discusses basic concepts about smart cards and defines key smart card terms. This section also reviews the common smart card technologies that are available through the Smart Access Common ID contract.

2.1.1 OVERVIEW

A smart card is a credit card-sized device that contains one or more integrated circuits (ICs) and also may employ one or more of the following machine-readable technologies: magnetic stripe, bar code (linear or two-dimensional), contactless radio frequency transmitters, biometric information, encryption and authentication, or photo identification. The integrated circuit chip (ICC) embedded in the smart card can act as a microcontroller or computer. Data are stored in the chip's memory and can be accessed to complete various processing applications. The memory also contains the microcontroller chip operating system (COS), communications software, and can also contain encryption algorithms to make the application software and data unreadable. When used in conjunction with the appropriate applications, smart cards can provide enhanced security and the ability to record, store, and update data. When implemented properly, they can provide interoperability across services or agencies, and enable multiple applications or uses with a single card.

Smart card technology can enable an organization to become more secure, efficient, and interoperable while delivering strong authentication and security, identity management, data management, customer support, and communications. The ICC, the technology on a card that makes it a "smart card," provides a number of functions. Smart card technology is commercially active and therefore provides additional benefits through commercial off-the-shelf (COTS) products and well-established technology standards.

Smart card technology can address issues surrounding identity management and can also provide the means to eventually re-engineer inefficient processes with a high return on investment (ROI). In the identification of inefficient processes, outdated business practices, and low ROI programs, an organization can eliminate deficiencies, unnecessary costs, and under-used resources through the implementation of smart card technology. The combination of smart card technology with web-based applications, electronic commerce, and other business uses of the Internet can improve the quality of life for citizens and employees.

Smart card technology provides a toolbox of enhanced capabilities that can be used to implement a smart identification card, including functions, such as: [1]

Access Control Tools. Smart cards can provide significantly enhanced security features that allow the card to operate as an authentication token for secure logical access to terminals and networks

[1] Catherine Allen, "Smart Cards Part of U.S. Effort in Move to Electronic Banking," in *Smart Card Technology International: The Global Journal of Advanced Card Technology*, ed. Robin Townsend (London: Global Projects Group, 1995), 193-194.

(such as local area networks (LANs) and the Internet), as well as for physical access to buildings, rooms, parking lots, transit and other facilities.

Payment Tools. Smart cards can serve as credit, debit, or stored-value payment and/or payment token instruments and provide the capability to access financial accounts and transfer funds between accounts.

Information Storage and Management Tools. Depending upon the size of the ICC, smart cards can store and manage data to assist with various applications. For example, medical information stored on a smart card can be accessed by an authorized medical official in the event of an emergency or on a routine medical visit. On-card information availability can reduce the amount of time spent locating hard-copy paperwork. If the medical event were a life-threatening emergency, the information would be immediately accessible, possibly saving critical time.

Enhanced Secure Access Capabilities. The use of sophisticated technologies such as biometrics and PKI further enhances the security of identity verification in granting physical and logical access. PKI uses public and private keys for digital signatures and email encryption and decryption. If the digital signature is verified using the signer's public key, then the recipient knows that it was signed by the owner of the public/private key pair and that it has not been changed in any way since it was signed. This assures both the sender and recipient that the information has not been altered. Biometrics use physical characteristics (e.g., fingerprint, hand geometry, iris scan and voice/facial recognition) to authenticate an individual's identity. PKI and/or biometrics can be used to more accurately identify an individual.

2.1.2 TYPES OF CHIP CARDS

Often the terms "chip card," "integrated circuit card" and "smart card" are used interchangeably, but they can mean different things. Cards are distinguished both by the type of chip that they contain and by the type of interface that they use to communicate with the reader.

There are three different types of chips that can be associated with these cards: memory only, which includes serial-protected memory, wired logic and microcontroller. The terms "memory only," "wired logic" and "microcontroller" refer to the functionality that the chip provides. The following further discusses the types of chip cards. [2, 3]

- **Memory-Only Integrated Circuit Chip Cards (including Serial Protected Memory Chip Cards).** Memory-only cards are "electronic magnetic stripes," and provide little more security than a magnetic stripe card. The two advantages they have over magnetic stripe cards are: a) they have a higher data capacity (up to 16 kilobits (Kbits) compared with 80 bytes per track), and b) the read/write device is much less expensive. The memory-only chip cards do not contain logic or perform calculations; they simply store data. Serial-protected memory chip cards have a security feature not found in the memory-only chip card; they can contain a hardwired memory that cannot be overwritten.

  Early versions of memory-only cards were read-only, low capacity (maximum of 160 units of value), prepaid disposable cards with little security. New versions include prepaid disposable

[2] Jack M. Kaplan, *Smart Cards: The Global Information Passport* (New York: International Thomson Computer Press, 1996), 69-75.
[3] Jose Luis Zoreda and Jose Manuel Oton, *Smart Cards* (Boston: Artech House, Inc., 1994), 5-6.

cards that use read/write memory and binary counting schemes that allow the cards to carry more than 20,000 units of value. Many of these cards also have advanced logic-based authentication schemes built into the chip. Other memory-only cards have been developed for re-loadable stored value applications. The cards contain a purse, which can be protected through the use of a personal identification number (PIN) and counters, which limit the number of times the purse can be reloaded.

- **Wired Logic Integrated Circuit Chip Cards**. A wired logic chip card contains a logic-based state machine that provides encryption and authenticated access to the memory and its contents. Wired logic cards provide a static file system supporting multiple applications, with optional encrypted access to memory contents. Their file systems and command set can only be changed by redesigning the logic of the IC. Wired logic-integrated chip cards include contactless variations such as I-Class or MIFARE.

- **Secure Microcontroller Integrated Circuit Chip Cards**. Microcontroller cards contain a microcontroller, an operating system, and read/write memory that can be updated many times. The secure microcontroller chip card contains and executes logic and calculations and stores data in accordance with its operating system. The microcontroller card is like a miniature PC one can carry in a wallet. All it needs to operate is power and a communication terminal. Contact, contactless and dual-interface microcontroller ICs are available. Unlike memory-only products, these microcontroller ICs have been designed (and can be verified) to meet security targets, such as Common Criteria (for example, the Department of Defense Common Access Card IC). The secure microcontroller chip card is normally the version referred to as the “smart card.”

Today’s chip card market offers a range of memory-only and microcontroller chip cards; however, only microcontroller chip cards will be addressed in this report. Because of their limited storage capacity and low level of security, memory-only chip cards are not suitable as multi-application or multi-purpose cards in support of government requirements.

There are two primary types of chip card interfaces—contact and contactless. The terms “contact” and “contactless” describe the means by which electrical power is supplied to the ICC and by which data is transferred from the ICC to an interface (or card acceptance) device (reader). Cards may offer both contact and contactless interfaces by using two separate chips (sometimes called hybrid cards) or by using a dual-interface chip (sometimes called “combi” cards).

- **Contact Smart Cards.** A contact smart card requires insertion into a smart card reader with a direct connection to a conductive micromodule on the surface of the card[4].

- **Contactless Smart Cards.** Contactless smart cards must only be in near proximity to the reader (generally within 10 centimeters or 3.94 inches) for data exchange to take place. The contactless data exchange takes place over radio frequency (RF) waves. The device that facilitates communication between the card and the reader are RF antennae internal to both the card and the reader.

[4] Charles Cagliostro, *Smart Cards Primer* , (December 1999)

- **Hybrid Smart Cards.** A hybrid card contains two chips on the card, one supporting a contact interface and one supporting a contactless interface. The chips contained on the card are generally not connected to each other.

- **Dual-Interface Chip Smart Cards.** A dual-interface chip card contains a single chip that supports both contact and contactless interfaces. These dual-interface cards provide the functionality of both contact and contactless cards in a single form factor, with designs able to allow the same information to be accessed via contact or contactless readers.

2.1.3 THE SECURE MICROCONTROLLER CHIP

A secure microcontroller chip has:

- An 8-bit to 32-bit central processing unit (CPU);
- Read Only Memory (ROM) or flash memory that contains the chip's operating system and, optionally, application software;
- Random Access Memory (RAM) that serves as a temporary register for data;
- Other non-volatile memory that is used for storage of user data (e.g., Electrically Erasable Programmable Read Only Memory (EEPROM), ferroelectric RAM, flash memory);
- Features that integrate countermeasures against known and foreseen security threats to achieve Common Criteria or FIPS 140-2 certification;
- Environmental sensors (e.g., voltage, frequency, temperature);
- At least one serial communication port;
- A random number generator;
- Timers;
- Optional cryptography engine(s) (e.g., providing support for DES, 3DES, RSA, ECC);
- Optional other dedicated peripherals (e.g., checksum accelerator, Serial Peripheral Interface (SPI) communication port).

The following further discusses the types of memory used on smart cards:[5, 6,7]

- **ROM. Read-Only Memory** contains the chip's operating system. The operating system or command set controls all communication between the chip and the outside world. The operating system controls the access to the file system or applets. The ROM is masked or written during production by the semiconductor manufacturer and, once written, cannot be altered.

- **EEPROM. Electrically Erasable Programmable Read-Only Memory** is non-volatile memory (i.e., it does not lose its data if power is shut off) and is read/write memory for the storage of data. Access to the EEPROM memory is controlled by the chip's operating system. EEPROM can currently contain 128 kilobytes (Kbytes) of memory with the potential for more than 256 Kbytes. EEPROM may contain data such as a PIN that can only be accessed by the operating system. Other data, for example, a card's serial number, can be written to EEPROM during card

[5] Jose Luis Zoreda and Jose Manuel Oton, *Smart Cards* (Boston: Artech House, Inc., 1994), 56-60.
[6] Jack M. Kaplan, *Smart Cards: The Global Information Passport* (New York: International Thomson Computer Press, 1996), 72-75.
[7] WhatIs.com, http://whatis.techtarget.com/.

manufacture. EEPROM is typically used for application data and for certain filtered functions. Most of the EEPROM memory is used to store user data such as a biometric, purse balance, special use authorization or payment tokens, loyalty tokens, demographic information, and transaction records. EEPROM can be rewritten from tens to hundreds of thousands of times and can be programmed or erased in either blocks or bytes.

- **FRAM** (ferroelectric RAM, also called Fe-RAM) is another non-volatile memory technology. FRAM can read data thousands of times faster at far lower voltage than other non-volatile memory devices. FRAM is random access memory that combines the fast read and write access of dynamic RAM (DRAM)—the most commonly used memory in personal computers—with the ability to retain data when power is turned off (as do other non-volatile memory devices such as ROM and flash memory). Because FRAM is not as dense as DRAM and static RAM (SRAM) (i.e., it cannot store as much data in the same space), it is not likely to replace these technologies. However, because it is fast memory with a very low power requirement, it is expected to have many applications in small consumer devices such as personal digital assistants (PDAs), handheld phones, power meters, smart cards, and security systems. FRAM is faster than flash memory. It is also expected to replace EEPROM and SRAM for some applications and has the potential to become a key component in future wireless products. However, unlike EEPROM or flash memory, FRAM is not yet a proven high-density mass production technology for smart cards.

- **Flash Memory** (sometimes called "flash RAM") is a type of constantly-powered, non-volatile memory that can be erased and reprogrammed in units of memory called *blocks*. Flash memory is often used to hold control code such as the basic input/output system (BIOS) in a personal computer. When the BIOS needs to be changed (rewritten), the flash memory can be written to in block (rather than byte) sizes, making it easy to update. Since flash products are generic and applications can be downloaded at the last step of the production flow, they add flexibility and can provide faster time-to-market. While features vary among different products, flash memory is usually lower cost than EEPROM but current products generally can't be programmed and erased as many times and usually can't program or erase single bytes of memory.

  Flash memory gets its name because the chip is organized so that a section of memory cells are erased in a single action or "flash." The erasure is caused by Fowler-Nordheim tunneling in which electrons pierce through a thin dielectric material to remove an electronic charge from a *floating gate* associated with each memory cell. A form of flash memory is available today that holds two bits (rather than one) in each memory cell, thus doubling the capacity of memory without a corresponding increase in price.

  Some chip manufacturers provide components with a combination of ROM, flash memory and EEPROM.

- **RAM. Random Access Memory**, which is volatile, is used as a temporary storage register by the chip's microcontroller. For example, when a PIN is being verified, the PIN sent by the terminal or PIN pad is temporarily stored in RAM.

The following example will further explain the functions of the memory types listed above. A commonly used microcontroller chip card would have its operating system stored in ROM. The operating system or command set would respond to commands, such as "read a record," "write a record," and "verify PIN," sent to the card by a terminal or reader. Information such as fund balances, card serial number, and demographic information are stored in EEPROM. The CPU performs all processing functions, such as encryption, while RAM serves as a temporary register for information. During PIN verification, the PIN is temporarily stored in RAM. Since RAM memory is volatile, as soon as a card is powered off, all information stored in RAM is lost.

When evaluating card types for a particular application, the amount of memory in various components is important. The EEPROM capacity of a card is critical because a larger capacity EEPROM can store a greater number of application records and transaction files. The amount of ROM is also important because a larger capacity ROM can contain a more sophisticated operating system, which facilitates complex card and system operations. There is also a relationship between ROM and EEPROM in some cards because several vendors allow custom code extending the ROM's operating system to EEPROM. While this technique increases the card's functionality, it decreases the amount of EEPROM available for application and transaction storage. Conversely, more established and accepted applications can be included in ROM in future chip versions, freeing up EEPROM space for additional applications and expansion.

2.1.4 SMART CARD READ/WRITE DEVICES

Smart card read/write devices provide the physical link between the smart card and the host system or application. The host system can be a PC, a network device, or a stand-alone access control device such as a turnstile controller. The read/write device delivers power, initializes the card, and acts as the mediator between the smart card and the host. Power is delivered to the smart card by making a physical contact on the contact smart card micromodule or by inducing current through the antenna of contactless designs. Initialization is a specified protocol that must be performed on all smart cards and is supported by compatible readers. Therefore, from an implementation standpoint, one should be certain that the reader selected is compatible with the chip's protocol. This can be accomplished by testing card and reader compatibility before they are purchased in bulk quantities.

Smart card read/write devices can be either transparent, requiring a host device to function, or they can be standalone devices functioning independently. Transparent read/write devices require a host for all signaling functions, including initialization and application delivery. This type of hardware has no internal logic except for a line driver to condition the signal between the card and the host. A transparent reader is similar to a PC soft modem; a host drives the reader and the card. This requires more support from the software, which must understand the design of the reader and the card communication requirements.

A standalone read/write device has all of the logic required to initialize a card and to act as a mediator between a smart card and the host. For example, the host may deliver a large packet of information to the reader to pass on to the card. The reader checks the packet and sometimes breaks it into smaller packets before sending the information to the smart card. This means that the host is only concerned with communication to the reader and not to the smart card. Standalone hardware functions as a pass-through for microcontroller cards. The operating system defines all of the commands that a microcontroller card understands, so the reader is not required to intervene.

Transparent readers require more drivers than standalone types, but are cheaper to manufacture and easier to change. Standalone readers, although more expensive than transparent devices, have generic driver sets that define the communication between a reader and a host. This is an important distinction because the design of a system's architecture will determine the ease of adding future applications and performing software upgrades.

Individual smart cards and some smart card readers are relatively inexpensive when compared with deploying an entire system. However, when deploying smart cards and smart card readers to hundreds or even thousands of users, equipment cost can become an important consideration. Evaluation of smart card hardware is necessary to select devices that best meet the needs of your application and budget. The smart cards, readers, and applications that you deploy are likely to be used many times per day; therefore, it is important that hardware be as reliable as possible and that service level agreements defined during requirements definition and proposal acceptance provide objective methods for measuring and documenting satisfactory performance.

A number of different smart card read/write devices and interface mechanisms are now available that meet various application needs. Smart card read/write devices can provide a single function or they may be integrated into a variety of other devices such as a personal computer keyboard. Purchasing an integrated smart card reader within a PC keyboard ensures compatibility with the host system to which it is connected, eliminates the need to purchase a single function plug-in reader at a later time, and also avoids any compatibility issues. A good use for this type of reader is enabling secure logical access to a computer system or network. Single function readers are also available with various host interface connections, including keyboard plug-in wedge, USB port, PCMCIA, serial port, and direct-wired such as with a door controller for physical access control.

Smart card readers can be mounted in a variety of ways including free-floating desktop and door-mounted units. Readers designed for secure physical access control applications are usually mounted at a convenient height on a door or turnstile with wiring hidden from view to prevent tampering. Smart card read/write devices can be integrated into other specialized devices and applications (e.g., a PDA). This type of application can provide secure access and portability.

Smart card writing devices or encoders are also used during the card personalization step. Most card personalization systems have smart card-encoding logic that enables the card’s chip to be initialized with personalization data in the same operation as the card’s visual data and text (i.e., personalization) are applied. This helps to ensure that the software application matches the user data and avoids the need to encode at a later step. Most commercial ID card printer systems can be fitted with an in-line smart card encoder. Figure 1 shows examples of common smart card read/write equipment.

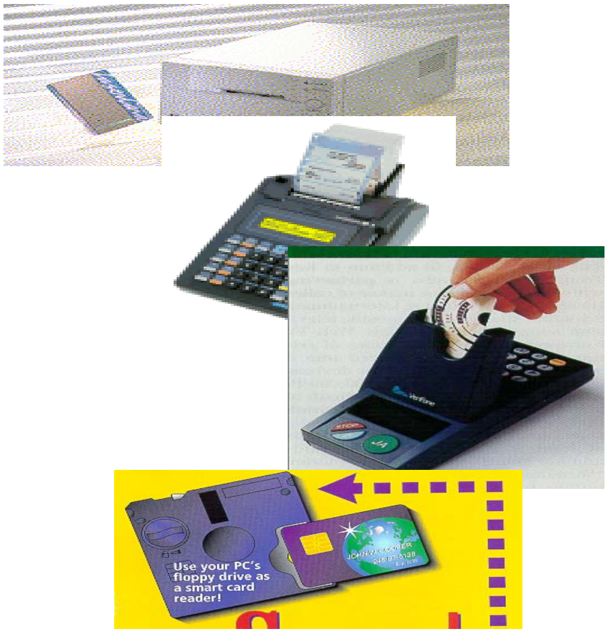


Figure 1: Smart Card Read/Write Equipment

2.1.5 SMART CARD INTERFACES: CONTACT AND CONTACTLESS CARDS

Smart cards may interface with read/write devices either through direct electrical contact with the card or through wireless data transfer (i.e., contactless interaction) using radio frequency or induction coupling techniques. The contact interface requires the card to be inserted into a card reader so that the reader can establish a direct electrical contact with the chip. A contactless smart card contains a chip and an antenna sandwiched between two layers of plastic. Communications are facilitated using RF technology. The chip is powered through the card's antenna when the card is placed within 10 centimeters (3.94 inches) from the smart card reader. Contact cards are generally used for a wide variety of applications, including financial transactions and logical access control. Contactless chips are typically used for functions that require greater speed or ease of throughput (e.g., high volume transit automated fare collection systems or office building access). They also eliminate concerns over reader wear when compared to their contact chip counterparts. Contactless chips have become increasingly accepted as the ID credential of choice for controlling physical access.

Contact, contactless and multiple interface smart cards can support multiple applications, offering advantages to both the organization issuing the card and the cardholder. The issuing organization can consolidate an appropriate mix of technologies and support a variety of security policies for different situations. Applications such as logical access to computer networks, electronic payment, electronic ticketing, and transit can be combined with physical access on a multi-application and multi-technology ID credential. Issuers can also record and update appropriate privileges from a single central location. For physical access, the organization as a whole can incur lower maintenance costs over the system life, due to the elimination of mechanical components and reader resistance to vandalism and harsh environmental conditions. With hybrid and dual-interface cards, issuers can also implement systems that benefit from multiple card interfaces.

There are three primary contactless technologies considered for physical access control applications: ISO/IEC 14443, ISO/IEC 15693 and 125 kHz technologies.

ISO/IEC 14443 and ISO/IEC 15693. 13.56 MHz contactless smart card technology is based on either ISO/IEC 14443 or ISO/IEC 15693 standards. Cards that comply with these standards are intelligent, read/write devices capable of storing different kinds of data and operating at different ranges. Standards-based contactless smart cards can securely authenticate a person's identity, determine the appropriate level of access, and admit the cardholder to a facility, all from data stored on the card. These cards can include additional authentication factors (such as biometric templates or PINs) and other card technologies, including a separate contact smart card chip to satisfy the requirements of legacy applications or applications for which a different technology is more appropriate.

ISO/IEC14443 was developed to be compatible with ISO/IEC 7816, the contact smart card standard. Smart cards meeting ISO/IEC14443 (parts 1 through 4) provide an interoperable means of transferring commands and data between the card and reader. Part 4 of ISO/IEC14443 ends with a statement that the card edge commands can be as defined in ISO/IEC7816-4. While the electrical interface is contactless instead of contact, the format for exchanging information between card and reader is the same.

ISO/IEC14443 has also been designed specifically to function poorly beyond the 10 centimeter specified range. It is not possible to "listen to" the card from a distance that is far enough away that the extremely large antenna needed to energize the card and IC would go undetected. It is important to note that if the IC uses authentication and encryption, the card contents could not be accessed in any case.

ISO/IEC15693 was developed for logistics, labeling and agriculture applications where small amounts of data need to be transferred a longer distance. While it also has 4 parts, like ISO/IEC14443, the protocol layer has not been designed for compatibility with ISO/IEC7816. Part 4 of ISO/IEC15693 allows vendor-specific implementations of the protocol and, therefore, does not provide the same level of interoperability as ISO/IEC14443.

Cards complying with these standards are developed commercially and have an established market presence. Multiple vendors are capable of supplying the standards-based components necessary to implement a contactless physical access system, providing buyers with interoperable equipment and technology at a competitive cost.

125 kHz. 125 kHz read-only technologies are used by the majority of today's RFID access control systems. These systems are based on de facto industry standards rather than international standards. 125 kHz technologies allow for a uniquely coded number to be transmitted and processed by a back-end system. The back-end system then determines the rights and privileges associated with that card.

Contactless Technology Comparison[8]

Features	**14443**	**15693**	**125 kHz**
Standards	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810	None[9] (de facto)
Frequency	13.56 MHz	13.56 MHz	125 kHz
Read range	Up to10 centimeters (~3-4 inches)	Up to 1 meter (~3.3 feet)	Up to1 meter (~3.3 feet)
Chip types supported	Memory Wired logic Secure microcontroller	Memory Wired logic	Memory Wired logic
Encryption and authentication functions[10]	MIFARE encryption, DES/3DES, AES, RSA[11], ECC	Supplier-specific, DES/3DES	Supplier-specific
Storage capacity range	64 to 72K bytes	256 and 2K bytes	8 to 256 bytes
Read/write ability	Read/write	Read/write	Read only[12]
Data transfer rate (Kbytes/second)	Up to 106 (ISO) Up to 848 (available)	Up to 26.6	Up to 4
Anti-collision	Yes	Yes	Optional
Card-to-reader authentication	Challenge/Response	Challenge/Response	Password
Hybrid card capability	Yes	Yes	Yes
Contact interface support	Yes	No	No
GSC-IS compliant	Yes	No	No

Figure 2: Contactless Technology Comparison

Figure 2 presents a comparison of the different contactless technologies and shows examples of the features available with each (such as memory size and encryption methods).

Physical Access Application Solutions. Contactless devices were developed and the technology was standardized to provide a fast, reliable interchange of data for physical access applications. Physical access applications typically require a user to present a valid credential at an entrance guarded by a checkpoint. If the credential is authentic, the user is permitted to access the area.

For physical access applications, contactless technology offers reliable and fast throughput. If another authentication factor is introduced, such as fingerprint recognition, the throughput

[8] Source: "Using Smart Cards for Secure Physical Access," Smart Card Alliance, July 2003.

[9] The Security Industry Association (SIA) has published the industry specification, SIA AC-01 (1996.10): Access Control: Wiegand Card Reader Interface Standard. This industry specification covers electrical specifications for the transfer of data between Wiegand card readers and security, access control, and other related control panels. The specification also defines power requirements and limits, as well as electrical control of devices contained in the reader.

[10] The ISO standard does not specify security functions.

[11] RSA-based encryption and authentication may not be available on all cards due to power consumption, execution time or key length constraints.

[12] While the majority of the installed 125 kHz technology is read only, cards are commercially available that support read/write.

advantages offered by contactless technology are decreased, but the strength of security and authentication is increased.

Where hostile environmental conditions exist, such as when the reader is exposed to heavy rain or when contaminants are present, contactless technology offers a significant advantage over any contact technology. Contactless readers are also more resistant to tampering and vandalism, and the lack of moving mechanical parts (e.g., landing pins or read heads) significantly reduces maintenance.

Logical Access Application Solutions. Currently, contact technology provides a convenient and cost-effective way to transfer significant amounts of data between a card and a reader and host system and to perform complex cryptographic operations for authentication applications. In addition, contact chips have microcontrollers while contactless chips may or may not. For these reasons, contact smart cards have been a prominent solution for network security implementations.

To accommodate the user's desire for a single ID credential, using a contactless card for both physical and logical access could be attractive. Depending on system requirements, a contactless smart card can now be used to provide the required level of security for logical access, while providing a reliable and easy to use solution for physical access. There have not been any FIPS 140-2 approved contactless chips to date.

2.1.6 GSC-IS 2.1: CONTACT AND CONTACTLESS INTEROPERABILITY

In July 2003, the NIST released version 2.1 of the Government Smart Card Interoperability Specification, or GSC-IS 2.1[13] (also referred to as NISTIR 6887). A major goal of GSC-IS 2.1 was to lay the foundation for interoperability for contact and contactless cards and to allow use of the same smart cards for several purposes but different smart cards for the same purpose. To assure interoperability, contactless cards must adhere to parts 1 through 4 of the ISO 14443 standard. Any cryptography must use algorithms approved under Federal Information Processing Standard 140-2. GSC 2.1 specifies ISO 14443 for the contactless interface but does not specify Type A or B[14].

To address a growing demand, GSC-IS 2.1 defines a common interface for contactless smart cards. The specification holds smart card vendors to interoperability requirements for the application program interfaces that communicate a smart card service to the client application on a host computer. The purpose of this capability is to ensure agencies will no longer be tied to a single vendor's proprietary smart card software or hardware.

Furthermore, GSA is leading an effort to strengthen the process in which smart cards are authenticated. The goal of this initiative is to establish guidelines for the protection of data stored on the smart card's microcontroller chip and to enable the card reader to verify the authenticity of a smart card as it is being presented to the card reader.

[13] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

[14] The ISO/IEC 14443 standard defines a way to provide power and communicate between a reader and a contactless smart card. The standard specifies 13.56 MHz as the frequency and also defines a communication protocol between the card and the reader. Type A and Type B are the two communication methods defined by the standard. Differences include the modulation of the magnetic field used for coupling, the coding format and the anticollision method (i.e., how the cards and readers respond when more than one card responds at the same time to a reader's request for data

2.1.7 MULTIPLE TECHNOLOGY AND MULTIPLE INTERFACE CARDS

Organizations now have a number of choices when implementing smart ID card technology, including the use of multiple technology and multiple interface cards. A common challenge for project managers in developing a system is ensuring that the new system is interoperable with existing legacy applications. For example, the user may want a newly-issued smart card to interface directly with an existing physical access control system that uses a legacy technology. To accommodate this, the new card can be produced with contact or contactless smart chip technology, magnetic stripe, bar codes, optical stripe and/or 125 kHz proximity antenna. A card containing several types of read/write media is generally called a multiple technology card.

Multiple technology cards are also available that can combine either of the ISO/IEC standard contactless smart card technologies with 125 kHz proximity technology. This enables the card to operate with legacy physical access control systems, as well as new ISO/IEC-compliant systems. Providing multiple read/write capabilities on a card can often assist in providing the tools needed to enable a transition from legacy to new technology applications over time. In addition, readers are available that can support legacy card systems and aid in a transition from one card-based technology to another.

Each technology incorporated on the card serves a purpose; however, it can represent a potential problem as well. In considering a multi-technology smart ID card, it is important to remember that combining a small number of compatible ID technologies may be a practical solution, while other combinations may be impossible or impractical to implement. While it is technically possible to mix various technologies on one card, care must be taken to consider the overall impact. Multi-technology card constraints include: inclusion of multiple contactless technologies that operate at the same frequency, card thickness, embossing location, printing issues, card cost, card manufacturability and availability, and card failure rate. The combination of a small number of compatible ID technologies into a single card is easier and can be more cost-effective than combining many technologies. While multi-technology cards may provide solutions for accommodating legacy access control systems, organizations must carefully consider the added complexity of implementing and maintaining multiple technologies.

Multiple interface smart cards are also available. Smart cards can include dual-interface chips to provide a single card solution for contact and contactless applications. When using a dual-interface chip, both contact and contactless technologies are incorporated on a single ICC on the smart card. This configuration enables the smart chip and its applications to interact with either contact or contactless readers. A user might select this configuration when both contact and contactless readers exist within a single facility.

Hybrid cards are also available in the market today. These cards usually have two ICCs – one contact chip and one contactless chip. A user may select this configuration to enable each chip to contain different applications or to provide additional processing capability. These products allow organizations to use a single credential to satisfy both contactless physical access control applications and applications requiring a contact interface, such as logical access to computers and networks.

Use of these different technologies can provide powerful security benefits as well as cost benefits. Organizations can link physical and logical access privileges to increase security. For example, requiring the use of a smart ID card to exit a facility can reduce unauthorized access and improve emergency management response in the event of a facility catastrophe. The use of multiple technologies on a single ID card can reduce card issuance and administrative costs and provide users with the convenience of a single access ID credential.

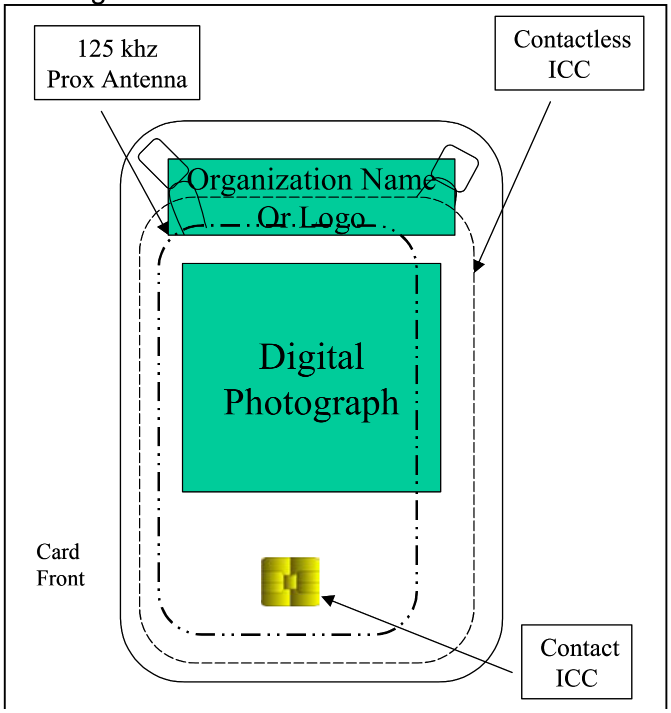


Figure 3: Multi-Technology Smart Card - Front

Figure 3 shows an example card front of a multiple technology smart card that has color digital photograph, and other personalization graphics. The card also has a contact integrated circuit chip, contactless chip and 125 kHz proximity antenna.

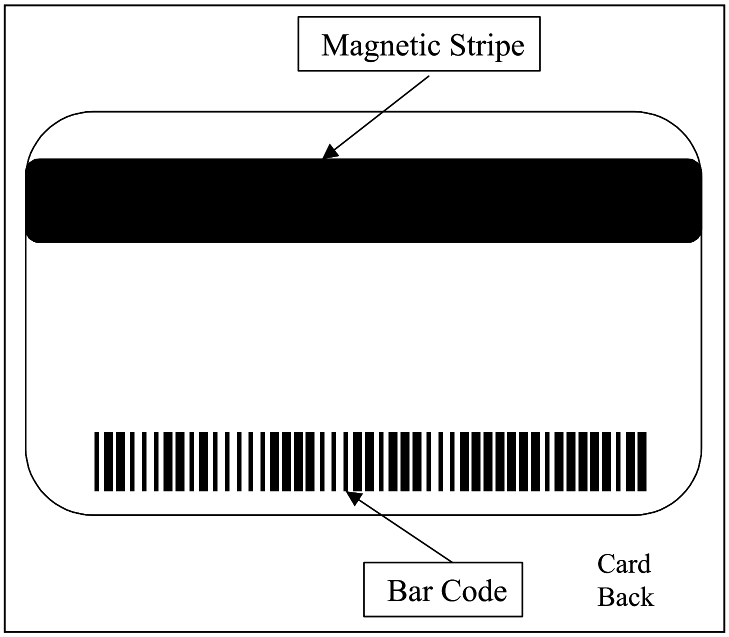


Figure 4: Multi-Technology Smart Card - Back

Figure 4 shows an example of the card back on a multiple technology smart ID card with a magnetic stripe and bar code. The magnetic stripe could be used to access legacy financial systems and the bar code could be used in an inventory or legacy provisioning application.

2.1.8 MULTI-APPLICATION CARDS

Smart card technology provides an opportunity to include multiple applications on one card. A multi-application card may serve as an identity authentication token and may also provide the cardholder with additional capabilities, such as digital signatures for email, email encryption, payment using an electronic purse, physical access to controlled buildings, logical access to computer systems, and data storage for medical information for use by authorized personnel. Both contact and contactless smart cards can support multiple applications.

When using a multiple application card, each application may be managed by a different group within an organization or even by an external application provider (for example, a third-party electronic purse for cafeteria use). While requiring more complex organizational coordination, implementation of multiple applications can enhance the business case supporting the adoption of smart cards.

One example of a multi-application card is the student campus ID card. A student at a university may use the university ID card as a basic form of identification to gain access to the university's facilities, obtain educational references and books from the university library, purchase meals or decrease value from a meal plan, purchase materials and supplies from the university store, or use university's vending machines. Additionally, the card may also be used to access the university's computer systems, network and intranet or Internet, as long as the capability has been incorporated into the card design. Figure 5 provides an overview of potential uses for multi-application cards.

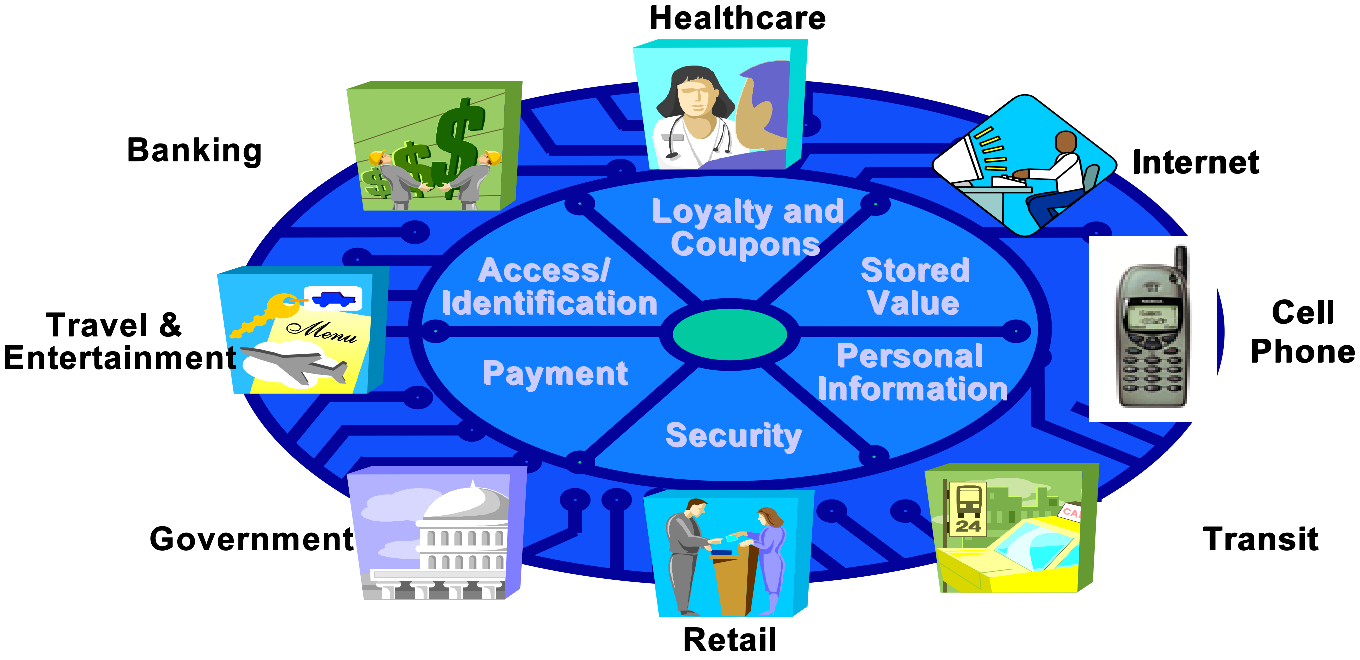


Figure 5: Potential Uses for Multi-Application Smart Cards

As the development of industry standards for smart cards expands, many cards will be designed to support both open and closed system applications. Building upon the previous example of the university ID card, the same university may choose to have local merchants accept the card as a standard (open) debit, credit or stored value purse, while the closed-system campus applications also remain on the card. Indeed, there will likely be a standard migration path from closed to open system applications. A closed environment of people with similar needs (e.g., campus, corporation, government.) will issue a card to meet those needs within the closed system; the card issuer will add open system or public applications to include other stakeholder interests, as required, within a wider community. In this environment, the convergence of international standards requirements is critical to develop interoperability, where government, industry and the public can accept each other's credentials and grant privileges based on that credential.

Card issuers have a variety of options available when designing a multi-application smart card. Differences may be physical such as the use of company logos, digital photos, and printed information on the card. Other variations may include differences in the technologies incorporated such as contact and contactless chips, bar codes, and a magnetic stripe.

When designing an ID card, the technologies incorporated on the card should meet the current and future anticipated requirements. An implementation effort will require close collaboration of the IT, security, and human resource (HR) departments among others. Using the existing infrastructure whenever possible during the implementation effort can also provide time and cost advantages. Part of the challenge in deploying a multi-application and multi-function card system is the development of the card support infrastructure. Additionally, organizations must consider other issuance and card management requirements, including: central issuance versus decentralized issuance, re-issuance, location of the cardholder and card management information, and management of credentials and lost or stolen cards.

For example, the ID holder of the university card in the previous example may require the card to be re-issued to incorporate senior privileges that are not available to other classmates. The re-issuance of the university card becomes increasingly complex if the card is used for multiple applications. Prior to issuing a new university card, the individual's identity and eligibility must be verified. Balances remaining on any accounts must also be transferred to the new ID card, in addition to the individual's information.

The selection of an appropriate operating system can be critical to card success. Choosing the correct operating system increases the functionality of the card by supporting reconfiguration of applications after the card is issued. In many instances, an issuing organization initially deploys a card with a single application; as card acceptance grows and market opportunities arise, the issuer can increase the functionality of the card by adding new applications. Applications can be added efficiently when an operating system supports secure dynamic loading and unloading of applications. An open operating system allows any card deployment to migrate to more functionality as market and consumer acceptance increase. The two most standardized operating systems in the smart card industry are Java Cards and MULTOS[15]. The Global Platform specifications also provide standards for an open smart card infrastructure that enables service providers from many industries to deploy and manage multiple applications for their customers through a variety of devices[16].

[15] For more information, see Java Card Forum, www.javacardforum.org and MAOSCO, www.multos.com.

[16] For more information, see www.globalplatform.org.

The strength of the multi-application card lies in its ability to store and process data, therefore enabling secure access to multiple applications and functions through a single card in either a closed, open or federated system environment. Designated applications must have access to a common set of shared data and services (including identification and the principal security functions) that support smart card interoperability independent of unique applications. Additionally, each application must maintain logic and data that are protected from access by any another application or user. It is through the support of multiple applications and adherence to common standards such as GSC-IS 2.1, Global Platform, ISO/IEC 14443, EMV and others (discussed in section 2.1.9) that a convincing business case can be made for smart card technology. In most instances, agreement on a common data model that provides a required set of shared attributes and a technology design that allows for versatility is the only clear path to achieving cost economies of scale and true interoperability for multiple application cards. When developing or implementing smart card systems, agencies should evaluate how alternatives support common standards, interoperability and cost economies and should conduct a short versus long-term analysis prior to requesting approval for funding.

2.1.9 SYNOPSIS OF TECHNICAL STANDARDS

Over the past several years, industry groups implementing smart cards have developed a number of standards and specifications. These standards are voluntary, but are generally adhered to in the interest of achieving conformity and interoperability.[17, 18] Organizations implementing smart card-based systems should review the standards and specifications that are relevant to the applications being implemented and determine where compliance is needed.

Going forward, adherence to smart card usage and system design standards should significantly enhance the ability to achieve the following:

- Providing a clear and concise definition of terms so that all agencies have a common understanding and common criteria for evaluation.
- Providing the standards and specifications that are required for a trusted multi-agency credential and for credential information to be used across a defined infrastructure.
- Driving requirements and recognition of the total cost of ownership of a complete ID system architecture.
- Allowing convergence of disparate identity and authentication media (e.g., cards) to a common credential token that can be used and trusted across the defined enterprise.
- Providing the flexibility to meet additional agency needs to use legacy tokens, as well as safeguarding the individual’s right to privacy.

A brief synopsis of the various smart card standards and specifications is presented below to illustrate the progress that has been made in standardizing smart card technology and usage. Additional information can be found in the body of work referenced with each smart card standard or specification.

- **Government Smart Card Interoperability Specification version 2.1[19] (GSC-IS v2.1, also known as the NIST Interagency Report 6887 – 2003 edition).** The GSC-IS v2.1

[17] Jack M. Kaplan, *Smart Cards: The Global Information Passport* (New York: International Thomson Computer Press, 1996), 209-214.

[18] *Smart Card Forum Standards and Specifications of Smart Cards - An Overview*, March 1996, Technology Committee -- Standards Subgroup.

[19] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

interoperability standard was issued by NIST, with assistance from the Government Smart Card Interagency Advisory Board (composed of members from the Federal sector and industry). GSC-IS v2.1 was designed to provide solutions to interoperability challenges that arise while developing an identity-based, multi-application smart card program. The specification defines certain criteria that must be met in order for a smart card implementation to claim compliance with the GSC-IS v2.1. These criteria are broken into several sections in the GSC-IS v2.1. These sections are the Architectural Model, the Access Control Model, Basic Services Interface, Virtual Card Edge Interface, Card Capabilities Container, Container Selection and Discovery, and Data Model. These sections contain information that, if adhered to, will lead to an interoperable smart card solution.

- **International Standards Organization (ISO)/International Electrotechnical Commission (IEC) Standards.** ISO/IEC is the worldwide standard-setting body for technology, including plastic cards. These standards set minimums, but also include many options and tend to leave some issues unaddressed. As a result, conformance to ISO standards alone does not necessarily ensure interoperability – nor does it ensure that cards and terminals built to the specifications will interoperate. The main standards that pertain to smart cards are ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 10536, ISO/IEC 15693 and ISO/IEC 7501.
  - ISO/IEC 7816 is broken into eleven parts. Part 1 describes the specifications for the physical characteristics of integrated circuit cards with contacts. Part 2 defines the dimensions and location of coupling areas. Part 3 explains electronic signals and mode switching. Part 4 specifies transmission protocols between the card and the interface device (e.g., reader).
  - ISO/IEC 14443 describes the standards for “proximity” cards. Specifically, it establishes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for proximity cards that operate within 10 centimeters (3.94 inches).
  - ISO/IEC 10536 describes standards for “close-coupled” cards. Specifically, it establishes standards for the physical characteristics, dimensions and location of coupling areas, and electronic signals and reset procedures.
  - ISO/IEC 15693 describes standards for “vicinity” cards. Specifically, it establishes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for vicinity cards that operate within 1 meter (approximately 3.3 feet).
  - ISO/IEC 7501 describes standards for machine-readable travel documents and has made a clear recommendation on smart card topology.

- **American National Standards Institute (ANSI) Standards.** ANSI recommends standards directed to the needs of the U.S. and supervises standards-making activities. It does not write or develop standards itself. Thus, in the U.S., any group that participates in ISO must first participate in ANSI. The International Committee for Information Technology Standards (INCITS) serves as ANSI’s Technical Advisory Group (TAG). Working groups within INCITS – such as B10 (Identification Cards and related devices), T6 (Radio Frequency Identification Technology) and M1 (biometrics) contribute directly to ISO groups (specifically, the ISO/IEC Joint Technical Committee 1/Subcommittee 17 (JTC 1/SC 17)).

- **Security Equipment Integration Working Group (SEIWG) Specification 012.** This specification establishes the requirements for the performance, design, manufacture, test and acceptance for the Magnetic Stripe Credential (MSC) prime item. The SEIWG-012 specification states that a 40-digit credential or “unique identifier” should be encoded on all access control cards that contain a magnetic stripe. The unique identifier is in the form of a 40-digit numbering scheme. This specification initially only pertained to magnetic stripe cards because these cards were the only cards that had sufficient storage capacity to comply with the specification. As smart card technology became more prevalent, the SEIWG-012 specification was applied to it as well. Smart card technology is capable of securely storing the 40-digit credential and smart card readers are capable of securely reading the information from the card.

- **Biometric Standards.**
  - The Biometric Application Program Interface (BioAPI) provides a high-level generic biometric authentication model. The body responsible for developing biometric API standards is the BioAPI Consortium. The BioAPI Consortium was formed in 1998. In 1999 the consortium merged with the Human Authentication Program Interface (HA-API) Working Group. By developing a standard biometric API, interoperability can be achieved among a wide range of applications and biometric technologies. BioAPI v1.1 became an ANSI standard, ANSI INCITS 358-2002, on February 13, 2002.
  - The Common Biometric Exchange File Format (CBEFF) was published by NIST on January 3, 2001 as NISTIR 6529. The CBEFF describes a set of data elements necessary to support biometric technologies in a common way.
  - Efforts towards biometric interoperability are progressing.

- **Federal Information Processing Standards (FIPS).** FIPS standards are developed by NIST, specifically the Computer Security Division within NIST. FIPS standards are designed to protect Federal computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.
  - Digital Signatures
    - FIPS 186-2 specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm.
    - ANSI X9.31-1998 contains specifications for the RSA signature algorithm. The standard specifically covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry[5].
    - ANSI X9.62-1998 contains specifications for the ECDSA signature algorithm.
  - Advanced Encryption Standards
    - FIPS 197: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.
  - Security Requirements for Cryptographic Modules
    - FIPS 140 (1-3): The security requirements contained in FIPS 140 (1-3) pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.7

- **Global Platform (GP) (formerly Open Platform).** Global Platform is an international, non-profit smart card association. Its goal is to create and promote global smart card technology specifications, including specifications for smart cards, smart card devices, and smart card systems. Throughout the world there are currently approximately 20 million individuals use smart cards that are implemented using Global Platform specifications. Global Platform serves the following industries: retail, health care, government, transit, financial, and mobile telecom. Global Platform's strategy is to create systems that are interoperable, backwards-compatible, and standards-based. For more information on Global Platform, see http://www.globalplatform.org.

- **Common Criteria (CC).** Common Criteria applies to security evaluation for IT products and systems. CC's goal is to provide a common or standardized way to evaluate IT products and services, thus producing a certain assurance level for those products and systems. CC was developed by organizations that sponsored previous criteria from the United States, Canada, and Europe. These organizations came together and developed the Common Criteria in 1993. In 1996, Common Criteria v1.0 was produced; in 1998, v2.0 was produced; and in 1999, the most recent version, v2.1, was produced. CC v2.1 complies with ISO/IEC 15448.

- **International Airline and Transportation Association (IATA).** The IATA develops standards for recommendation to the airline and transportation industry. IATA has formed a task force to develop interoperability standards for smart card-based ticketless travel. Its mission is to ensure easy and convenient negotiation of electronic airline tickets. In addition, credit card companies such as American Express, MasterCard, and industry groups are providing support to facilitate interoperability with other companies in the travel industry.

- **G-8 Health Standards.** The G-8 countries have come together to develop a standard format for populating data on a health card. This standard attempts to create interoperability across health cards from the G-8 countries. It addresses file formats, data placement on the card, and use of digital certificates in health care.

- **Global System for Mobile Communication (GSM) Standards.** GSM is a standard for cellular telephone systems, primarily offering international compatibility. The specifications tie a telephone number to smart card, called a Subscriber Identification Module (SIM) or User Identity Module (UIM), rather than to a telephone handset. The SIM is inserted into a telephone to activate it.

- **EMV 2000 Specifications.** To expedite the issuance of globally interoperable smart cards, Europay, MasterCard, and Visa (EMV) published the first version of standard card and transaction terminal specifications in 1995.[20][21] The specifications are built on the ISO/IEC 7816 standard and serve as an expansion to accommodate debit and credit transactions. An updated version of this specification, EMV 2000 version 4.0, was published in December 2000. EMV v4.0 consists of 4 books.
  - Book 1, *Application-Independent ICC to Terminal Interface Requirements*, describes the minimum functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability independent of the application to be used.

[20] Andrew Tarbox and John Tunstall, "EMV Specifications Update," in *Smart Card Technology International: The Global Journal of Advanced Card Technology*, ed. Robin Townend (London: Global Projects Group, 1996), "M" pages.
[21] Europay International, MasterCard International Incorporated, and Visa International Service Association, *EMV '96 Integrated Circuit Card Specification for Payment Systems*, Version 3.0, June 30, 1996.

  - Book 2, *Security and Key Management*, describes the minimum security functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability. Additional requirements and recommendations are provided on online communication between ICC and issuer and the management of cryptographic keys at terminal, issuer and payment system level.
  - Book 3, *Application Specification*, defines the terminal and integrated circuit card procedures necessary to effect a payment system transaction in an international interchange environment.
  - Book 4, *Cardholder, Attendant, and Acquirer Interface Requirements*, defines the mandatory, recommended, and optional terminal requirements necessary to support the acceptance of integrated circuit cards in accordance with Books 1, 2 and 3[10].

- **Personal Computer/Smart Card (PC/SC) Workgroup Open Specifications.** The PC/SC Workgroup was formed in 1996 and included Schlumberger Electronic Transactions, Bull CP8, Hewlett-Packard, Microsoft, and other leading vendors. This group has developed open specifications for integrating smart cards with personal computers. The specifications are platform-independent and based on existing industry standards. They are designed to enable application developers to create smart card-based secure network applications for banking, health care, corporate security, and electronic commerce.[22] The specifications include cryptographic functionality and secure storage, programming interfaces for smart card readers and PCs, and a high-level application interface for application development. The specifications are based on the ISO/IEC 7816 standard and support EMV and GSM application standards.

- **OpenCard™ Framework.** The OpenCard Framework is a set of guidelines announced by IBM, Netscape, NCI, and Sun Microsystems, Inc., for integrating smart cards with network computers. The guidelines are based on open standards and provide an architecture and a set of application program interfaces (APIs) that enable application developers and service providers to build and deploy smart card solutions on any OpenCard-compliant network computer.[23] Through the use of a smart card, an OpenCard-compliant system will enable access to personalized data and services from any network computer and dynamically download from the Internet all device drivers that are necessary to communicate with the smart card. By providing a high-level interface, which can support multiple smart card types, the OpenCard Framework is intended to enable vendor-independent card interoperability. The system incorporates Public Key Cryptography Standard (PKCS) - 11 and is expandable to include other public key mechanisms.

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191).** This law states that the Secretary of Health and Human Services (HHS) is to adopt national standards for implementing a secure electronic health transaction system. Examples of these transactions include: claims, enrollment, eligibility, payment, and coordination of benefits. The goal of HIPAA is to create a secure, cost-effective means for individuals to efficiently accomplish electronic health care transactions. HHS has designated the Centers for Medicare and Medicaid Services the responsible entity for enforcing HIPAA. All applicable entities must be in compliance by October 16, 2003.

- **International Civil Aviation Organization (ICAO), Passport Guidelines.** The ICAO is responsible for issuing guidance on the standardization and specifications for Machine Readable

[22] Blair Dillaway, "PC/SC Workgroup Specification for PC-ICC Interoperability," Presentation at CardTech/SecurTech '96 West, December 1996.
[23] OpenCard^{TM} Framework Website, http://www.nc.com/opencard/

Travel Documents (MRTD) —i.e., passports, visas, and travel documents. Although current specifications do not include guidance on the use of smart card technology, the ICAO is in the processing of researching the possibility of adding this functionality to MRTD. The ICAO has produced a technical report on the possibility of including contactless integrated circuits in MRTD, titled "*Use of Contactless Integrated Circuits In Machine Readable Travel Documents*, Mike Ellis, Version 3.1, 16-April-2003."

2.1.10 CURRENT LEGISLATION AND OMB GUIDANCE

- **E-Government Act of 2002.** The E-Government Act of 2002 contains a number of provisions relevant to smart card implementations. The E-Government Act also delegates authority to OMB to issue guidance on how agencies are to move from paper to electronic transactions. This list does not exhaust all relevant legislation or guidance, but is meant as an overview of some of the major areas that a smart card implementation could affect.

  - **Section 203.** The stated purpose of Section 203 of the E-Government Act is to ensure an appropriate level of security for Federal electronic transactions. OMB issued guidance on how Section 203 should be implemented in M-04-04, "E-Authentication Guidance for Federal Agencies." This memorandum creates a framework to assist agencies in determining appropriate levels of identity assurance for electronic transactions that require authentication. M04-04 also updates OMB guidance on the Government Paperwork Elimination Act of 1998 (GPEA). GPEA engages the Federal government to use electronic transactions in order to promote internal efficiencies as well as efficiencies in dealing with citizens.

  - **Section 208.** Section 208 of the E-Government Act ensures that agencies maintain proper privacy protections, regarding the use of IT to collect new information or the procurement of new IT that processes personally identifiable information. OMB has issued M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002." This memorandum requires that agencies report compliance with Section 208 as well as requiring privacy impact assessments on applicable IT projects. This legislation is in addition to the requirements imposed by the Privacy Act of 1974.

  - **Federal Information Security Management Act (FISMA).** FISMA is set forth in Title III of the E-Government Act of 2002. FISMA recognizes that importance of keeping Federal networks secure and making sure that controls on Federal operations and assets are evaluated and maintained.

  - **Electronic Signatures in Global and National Commerce Act (E-SIGN).** E-SIGN allows for electronic signatures to be legally effective. OMB issued M-00-15 "Guidance on Implementing the Electronic Signatures in Global and National Commerce Act" to aid agencies in complying with E-SIGN. The Department of Justice also issued guidance in this area entitled "Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies" in November of 2000.

- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT).** USA PATRIOT requires the implementation of an integrated entry and exit data system for all border ports of entry. USA PATRIOT instructs the implementation to focus on biometrics and tamper-resistant, machine-readable travel documents. The act designates certain leadership roles and reporting requirements.

- **Enhanced Border Security Act of 2001.** The EBSA lists development considerations for the implementation of an integrated entry and exit data system. Biometric identifiers, machine-readable visas, and passports are listed as aspects to be considered.

- **Privacy Act of 1974.** The Privacy Act governs the collection and use of records by federal agencies. It imposes procedural and substantive duties on federal agencies. It gives individuals certain rights with regard to records covered by the act. Violations of the act can result in civil and criminal penalties.

- **Policy Issuance Regarding Smart Cards Systems For Identification and Credentialing of Employees.** In February 2004, the Federal Identity and Credentialing Committee (FICC) released guidelines for developing interoperable federal identification systems based on smart cards. The FICC guidelines lay out the minimum requirements for smart-card credentials:
  - Standard electrically readable format for data
  - Tamper and counterfeit resistance
  - Support for three means of authentication, such as passwords, credentials and biometrics
  - Automated use monitoring for audit trails
  - Digital certificates on each card for identification, encryption and digital signatures
  - Ability to be updated after issuance
  - Certification of applications carried on the cards.

It should be noted that certain types of information are treated differently by legislation and guidance. For example, personally identifiable health information may have to comply with the Health Insurance Portability and Accountability Act (HIPAA). OMB issued guidance on the sharing of personal information between agencies (M-01-05). The Office of Personnel Management issued regulations on applying the Privacy Act to personnel records (5 CFR 297). Certain financial transaction may have to comply with the Graham-Leach-Bliley Act (GLBA). The types of information used and collected will vary and determine the level of care that a smart card implementation must exercise.

2.1.11 SMART CARD IMPLEMENTATION CONSIDERATIONS

The implementation of a multi-application smart card program requires the resolution of a number of issues, which includes technical, management/organizational, legal/regulatory, cost, and standards/interoperability considerations. The issues are outlined below in their respective categories.

- **Management/Organizational.** Management and the organization will face issues that are associated with administrative and operational structures and procedures such as: card ownership, customer education and support, and card administration. Customer buy-in is critical in any implementation and often involves a change in management's philosophy. A top-down emphasis to drive the implementation is vital to success. Demonstrating and/or explaining how the new concept will better the lives of those that use it aids in customer buy-in, which is a critical factor in program success. Developing a well-organized communications campaign to promote the implementation will help set the stage for each phase of the effort and create user awareness. It is essential for an organization to define an implementation strategy and decide whether to provide for a centralized or de-centralized issuance process. As the implementation progresses, certain processes may become obsolete or redundant and should be reengineered to gain efficiencies that improve performance.

- **Technical.** Accurately defining the infrastructure requirements for the implementation effort is one of the most critical steps in designing and deploying an effective system. The minimum requirements for a common smart card credential token, as defined by the FICC, are the following[24]:

  1. Identity data must be in a standard electronically readable format and use an active authentication process.
  2. Information contained both on the visible surface of the Federal Identity Card and within the chip or chips will be tamper resistant and counterfeit-resistant. A tamper-resistant card contains features both making it difficult for persons to alter the information, and making alterations readily apparent to a qualified person or validating system. A counterfeit-resistant smart card contains features making it difficult for persons to produce illegitimate tokens that could be incorrectly accepted by a qualified person or validating system.
  3. Cards should support multiple authentication methods to protect the credential token from unauthorized use or theft. Factors may include something you know (e.g., a password), something you have in your possession (e.g., a digital certificate), and something you are (e.g., a biometric such as a fingerprint or iris scan). Agencies are encouraged to provide support for all these technologies in their architecture and planning.
  4. Smart cards must be supported by an infrastructure providing automated administration and maintenance of audit trails of smart card usage and must be in accordance with Electronic Records Management systems requirements
  5. Every smart card should have the capability to carry digital certificates for identity, encryption and digital signature. Credential requirements should be standards based meeting the certification requirements of the Federal Bridge model including all NIST recommended and approved standards and specifications such as FIPS 140-2: Security Requirements for Cryptographic Modules.
  6. Cards should have the capability to carry certificates needed to sign and encrypt sensitive mail as defined by the agency and be supported by Agency applications.
  7. The card should allow post-issuance updating of data in a secure fashion and using a multi factor means of authentication.
  8. Compliance with NISTIR 6887 – 2003 Edition, identification formal standards, and other standards as appropriate.
  9. Applications carried on the Federal Identity Card will be subjected to a certification process to ensure they are downloaded to the card in a secure and trusted manner and may require FIPS 140-2 validation. All applications or data downloaded to the Federal Identity Card are the responsibility of the issuing agency both at initial issuance and post issuance. The card should allow post-issuance updating of data in a secure fashion and using a multi factor means of authentication.
  10. For security purposes agencies need to establish and enforce work policies and business processes that report a stolen or lost Federal Identity Card and revocation of privileges based on the Federal Identity Card credentials as soon as possible. Agencies will also need

[24] Federal Identity and Credentialing Committee, *Policy Issuance Regarding Smart Cards Systems For Identification and Credentialing of Employees*, February 2004. http://www.smart.gov/smartgov/whats_new.cfm.

to enter into agreements with other cooperating entities on procedures and methods to be developed for cross-agency notification when a credential is revoked or suspended.

As an organization defines specific requirements, questions concerning the hardware, software, card architecture, infrastructure and system must be addressed. Cross-organizational planning and team involvement in the definition of system requirements and design are critical to promoting agreement and cooperation on the new system implementation[25]. It is important that implementations evolve and not wait for the perfect solution, as evolution is critical to developing a solution that best fits current needs while also allowing the organization to move forward. Waiting for a perfect solution at each stage of implementation will cause severe delays and increase the potential for project failure and cost overruns. Organizations need to remain flexible during implementation and plans may have to be re-evaluated to accommodate a changing environment.

- **Legal/Regulatory.** As technology evolves, so do the laws and regulations that govern the use of card technology in electronic commerce. Interpretation and application issues can arise when taking into account laws and regulation that relate to an individual's right to privacy in an ID system. An important component of privacy is the security of the information – both during collection and during use of the credential in the ID system.

- **Cost.** Adequate planning and well-defined requirements will significantly aid an organization in estimating the costs associated with widespread smart card issuance. Without well-defined requirements and planning in place, an implementation can experience significant delays that, in turn, cause cost overruns. Additionally, organizations must budget for maintenance of the smart card program once the initial issuance has been completed. Costs for card re-issuance (i.e., for cards that are lost, stolen, expired or damaged) and system and application support and maintenance should also be considered.

  While smart cards are not inexpensive, they offer substantial labor and resource savings over time. Despite the large up-front investment required, smart cards can prove to be more cost-effective than other ID technology approaches.

- **Standards and Interoperability.** Critical to the widespread acceptance of card technology is the ability to achieve interoperability among diverse card systems. The development of standards is critical to achieving interoperability, with the importance of standards increasing as technology evolves and smart card programs are rolled out. Government and industry must work together to develop and advance standards in order to achieve interoperable solutions. The ability to remain vendor and product-neutral is key to achieving interoperability. For example, Bank A's automated teller machine (ATM) card can be used in any ATM around the world regardless of the ATM manufacturer or bank supplier. The same must be true for smart cards. An organization should and must be able to use any smart card in any smart card reader. Agreed-upon industry standards and specifications are key to achieving interoperability.

- **Privacy**. It is important to note that the U.S. has no standard body of privacy laws and regulations, and that there is no central authority to enforce privacy laws, regulations, controls, or policies. Laws and regulations covering privacy protection come from a variety of sources including the U.S. Constitution, state constitutions, and various statutes with regulations. The

[25] Smart Card Alliance, *Contactless Technology for Secure Physical Access: Technology and Standards Choices, September 2002.*

result is that the information permitted to reside on a card can vary greatly from one area to another, posing challenges for any open system.

2.2 Components of a Smart Card System

The configuration of the smart card platform will vary substantially from project to project depending upon the card management approach, card personalization and issuance procedures, card capabilities and applications, and technical environment selected by the project. However, the following generic components will typically comprise an employee smart identification card platform that includes PKI:

- **Cards.** Smart cards contain an ICC that provides computational power similar to that of a PC. Smart cards have the capability to implement multiple authentication technologies such as PKI and biometrics. They also have a certain amount of storage capability. Smart cards are generally used for both physical and logical access, and are available with both contact and contactless interfaces.

- **Central Card Management System.** The central card management system should function as the core of the smart card system, and as such, requires connectivity and interfaces with all other system components. It houses the central cardholder database that supports the capture, storage, retrieval, retention, integrity, and management of data necessary for the Life Cycle Management (LCM) of smart cards. LCM includes: pre-issuance, issuance, status, replacement, renewal, post-issuance capabilities and audit of smart cards for each agency.

- **Smart Card Equipment and Software.** Smart card equipment and software includes the computers, peripherals, and software needed to capture the information used to enroll a cardholder, personalize the card, load the card with any necessary PKI certificates, issue the card to the cardholder, and perform post-issuance capabilities such as PIN reset and certificate updates on the card. Card issuance equipment typically includes:
  - Enrollment Workstation. The enrollment workstation is used to capture enrollment information and route it to the central card management system and to the equipment actually personalizing and issuing the cards (if not the enrollment workstation itself). At agency discretion, attachments to the enrollment workstation may include a digital video camera to capture the cardholder’s digitized photo, a digitized signature capture device, a biometric capture device (most commonly a fingerprint capture device but could include a wide variety of biometric capture devices), and a key pad used for generating a user’s PIN. Depending on the procedures for capturing demographic data (e.g., through manual entry or legacy system upload), the enrollment workstation may be used to collect demographic data for card personalization. In some implementations, the biometric data and/or public keys captured through the enrollment workstation could be directly routed to the certificate/attribute authority workstation as part of a certificate request.
  - Key Generation Workstation. Although key pairs generally will be generated by a cryptoprocessor on the smart card, some agencies may choose to use a separate workstation to generate keys (i.e., using software-generated keys rather than token-generated keys). Once keys have been generated, they are securely transmitted (using mutual authentication protocols and encryption (symmetric or asymmetric)) and loaded onto the card at the point of card personalization and issuance. A related concept is key management, which will be discussed in section 2.3.

  - Card Personalization System. The card personalization system is used to personalize the card with data, photos, key pairs (if not generated on the card itself), and digital or attribute (i.e., biometric) certificates. Attached to the card personalization workstation is a card reader that is used to load information to the chip on the card and a card printer that is used to print information and photos on the face of the card. In some scenarios, the card personalization workstation and enrollment workstation may be the same device, depending on whether a centralized (i.e., bulk personalization) or decentralized (i.e., on-site issuance) process is used for card personalization and issuance.
  - Registration Authority System**.** In some scenarios, if an agency has a designated registration authority, a separate workstation may be used to read public keys from the card (or verify biometric data), document identity proofing, and generate a digital certificate (or attribute certificate) request. In turn, the registration authority system may receive signed certificates from the certificate authority (or attribute authority) and place them on the card. The registration authority workstation could be the same as the enrollment workstation and the card personalization system in an on-site card issuance location.
  - Certificate/Attribute Authority System. The certificate and/or attribute authority system is a trusted computer system that receives certificate requests (that would contain public keys and data or a biometric template) from the entity acting as a registration authority, and, in turn, signs and issues certificates that are returned to the registration authority (or enrollment workstation/card personalization system) for loading onto cards. The certificate or attribute authorities typically will maintain their own repositories (i.e., Lightweight Directory Access Protocol (LDAP) servers) that are used to publish certificates.
  - Card Reader. A card reader is used to communicate with the smart card during a transaction. It is the interface between the card and the host system. Card readers provide power and timing to the ICC and can operate with either contact or contactless interfaces.

- **Applications.** Smart cards be used to implement physical and logical access control applications, as well as other applications that are components of an agency's card system. Depending on the card management approach, these applications may communicate with the central card management platform to upload back-up transactions and/or to download hot lists.

- **Interfaces to Legacy Databases.** Many agencies will choose to personalize their smart cards with data from existing legacy systems. Thus, important components of the platform architecture are the interfaces from legacy systems to the central cardholder database or to the card issuance workstation.

2.3 Card Life Cycle Management Architecture

In any card system, roles and responsibilities must be assigned and policies and procedures developed for all facets of card management including card procurement, inventory control, personalization, card issuance, card replacement, and application management. The three phases in the life cycle management of a smart card program that must be considered in the card management process are pre-issuance, issuance and post-issuance. Recommended card management functions for agencies implementing a smart identification card platform are the following:

- **Card Procurement.** The agency or its designated card issuer may procure cards from one or more card manufacturers. It is to the agency's advantage to remain vendor-neutral to obtain competitive pricing. Vendor neutrality is possible due to the evolution of standards in the smart card industry. If undecided, the agency could work with GSA, the card manufacturer or a system integrator to identify the card handling and security procedures desired to protect card and system integrity (also known as a smart card pre-issuance specification). Agencies may find it beneficial to leverage the DoD pre-issuance specification, which is a comprehensive specification that governs all of the steps from card manufacture to delivery. Card procurement will occur during all phases of smart card program life cycle.

- **Card Initialization.** Initialization is the process of programming chips in a batch of cards with identical data for a batch (e.g., a file structure). Initialization may also include printing identical information, such as a logo, on a batch of cards. It is usually performed by the card manufacturer prior to the shipment of cards, but can also be performed at the same time as personalization during card issuance. During the card initialization process, the card vendor can perform functions such as:
  - Loading the operating system into ROM;
  - Allocating memory zones on the chip (e.g., for photo, for digital signature);
  - Loading the unique card serial number into ROM;
  - Generating security keys; and
  - Performing other card initiation tasks as requested by the agency.

- **Card Personalization.** Personalization occurs at the end of the manufacturing process and is the process of printing data on the surface of the card, encoding the magnetic stripe on the card (if applicable), and programming data into the chip that will uniquely associate the cardholder to the smart card. Agencies may employ different approaches to obtain data for the card personalization process, depending upon individual agency requirements. Downloads from existing legacy systems, web-based applications to collect data, or employee interviews are examples of techniques that may be used to obtain necessary card personalization data. Once the information is collected, interfaces may be built to efficiently enter the data into a master or legacy database. An automated interface will reduce the potential for manual errors. Security is a also factor to be considered, as the secure transmission of data is critical, particularly if automated interfaces will be used to transport card personalization data from master or legacy databases. Encryption may be used to protect sensitive data transmitted across open networks. Depending on the applications being loaded on the card, the personalization processes may include some combination of the following:
  - Encoding the magnetic stripe;
  - Encoding the bar code;
  - Loading application software, basic demographic information and/or keys on the chip;
  - Printing card graphics;
  - Printing a photo and signature image on the card;
  - Printing demographic data on the card; and
  - Printing other agency-specific information on the card.

  As part of the enrollment and card personalization process, the agency or its designated card issuer will perform some combination of the following functions depending on the specific capabilities and implementation strategies required by individual agencies:
  - Capture the digital photograph of the employee using a photo imaging system;
  - Capture the digitized signature of the employee using a signature capture device;
  - Capture the biometric of the employee using a biometric capture device;

  - Capture demographic data to be maintained in the cardholder database and write this demographic data to the chip; and
  - Populate the card with digital and attribute (i.e., biometric) certificates.

- **Card Issuance.** The process of distributing personalized cards to cardholders is called card issuance. Depending upon the agency's organizational structure and smart card program requirements, a vendor may personalize and print the smart identification cards at a central location to support mass card distribution. Agencies that are geographically dispersed may want to consider a decentralized card issuance approach; however, security should be the driving factor in determining the agency's approach to card issuance. Prior to authorizing the issuance of a card, the potential cardholder should be required to present documentation that verifies identity and employment status and that can be compared to an agency personnel database. As an additional security measure, the agency should compare the presented application with a picture and/or biometric that has previously been collected in the personnel database. The applications that will be loaded onto the smart identification card will vary depending on the cardholder's role and responsibilities. All cardholders will require a card for visual identification and physical access to their relevant duty station or area of responsibility. Not all employees will require a digital signature or attribute certificate, as this will be determined by individual agency program requirements. The card personalization, card issuance, and card management solutions should provide the capability to capture and maintain records on the privileges associated with each employee's card.

- **Card Replacement.** The card replacement process is used to provide replacement cards to individuals reporting a lost, stolen or a malfunctioning card. When a card is reported to be lost, stolen, or malfunctioning, the issuance office will deactivate the card by revoking the certificates on the card and by placing it on a list of invalid cards (also known as a "hot list"). When a replacement card is issued, it must carry all the privileges, data, and system access keys that resided on the original card that is being replaced. It should also indicate that it is a replacement card. Typically, either the agency or its designated card issuer takes responsibility for the replacement process. The card replacement process includes:
  - Procedures for re-issuance;
  - Procedures for checking hot-listed cards;
  - Procedures for revoking certificates;
  - Time frame for hot-listed cards being deactivated in the card database;
  - Personnel responsible for locking and unlocking cards;
  - Procedures for removing hot-listed cards from the list;
  - Procedures for generating new keys or biometric templates if the card has digital or attribute certificates;
  - Time frame for reissuance and reactivation of cards; and
  - Procedures for restoring value if the card has an electronic purse.

- **Card Block/Unblock.** When a card is reported as lost or stolen, it must be deactivated to ensure that an unauthorized individual cannot use the card. An agency or its designated card issuer should have the capability to hot list any card that has been reported as lost, stolen or malfunctioning and to revoke certificates on the card. Additionally, the departments who have an application on the card or other agencies that could grant access privileges to cardholders on the hot list should receive immediate notification of the deactivated card(s). In addition, agencies must take into consideration the ability to unblock cards upon issuance. For example, if a cardholder blocks their card by entering an invalid PIN, the cardholder should have the capability to unblock the card. When the cardholder's card is initially setup, a special unblock code should be generated, encrypted and then stored in the card management system.

- **PIN Reset.** The cardholder must have the ability to securely reset the PIN on the card without requiring the cardholder to return to a smart identification card issuance facility. Depending on the deployment strategy, the mechanism to deploy a PIN reset solution may vary. One option may be a graphical user interface (GUI) to the system that allows a user to change the PIN by providing the old PIN for authentication and then the system allows a new PIN to be established. Another approach may be a web-based portal in the card management system; using this approach, the user can authenticate to the web site and then navigate to a PIN reset screen where the old PIN is required and validated using the rules set on the smart card during the chip personalization process. The ability to change the PIN via the desktop utility can be disabled as desired. Ultimately, agencies must determine the best method to service cardholders to ensure customer convenience and satisfaction.

- **Certificate Management.** Certificate management is both an issuance and post-issuance function in a smart card-based ID system using PKI. Technology can be used by organizations to build ways to develop trust in electronic transactions and rely on digital signatures. The certificate authority or certification authority (typically called a CA) brings together two parties who may have never met and uses public key technology to facilitate digital business transactions. The CA builds confidence in the transaction by acting as a well-known, trusted third party that vouches for the authenticity of a public key. The role of the department certificate authority is to maintain the PKI certificates and keys that are injected into the smart identification card from the issuance system or portal. The CA constructs, signs, and publishes a digital certificate using the CA's private key. The digital certificate is an electronic credential that can be used to verify another person's signature, encrypt documents, and protect the integrity of the transaction. In order to construct the digital certificate, the CA must identify the person, verify that the person possesses the associated private key, and know other information about the person that is required to construct the certificate. Certificate management is a post-issuance function as well. Cardholders must have the ability to request new or updated certificates after the initial issuance in the event that: the CAs were unavailable at initial issuance; the card recipient did not have an email address at initial issuance; or the card recipient's email address has changed after initial issuance.

- **Key Management.** Key management is an integral and significant part of a card management program. Anyone planning to implement a smart card program should have the resources available to ensure a complete and thorough understanding of card keys. It is important to understand how keys will be used, especially if the card system plans to work with more than one organization or entity. Keys hold the secret to the system. If not managed properly, the integrity of the entire system can become questionable and thereby useless.

  Key management is an application that is used for generating and maintaining cryptographic keys. An interface between the card management system and the key management system makes it very easy to import keys into the card management system where they can be used to secure smart cards. Key management is the procedure to control key generation, key storage, key distribution, key usage, and key destruction. Key management functions include those shown in Figure 6.

Function	Tasks
Registration	- Verifying Official (VO) - Application - Chip registration and enablement
Key and certificate generation requests	- Request application load and delete certificates - Request certificates from CA - Request key pairs from hardware security modules (HSMs) with security server
Key and certificate storage	- HSM has specific security requirements, which must be taken into consideration

There are also a number of key types. Keep in mind that smart card keys are not the same as PKI keys.

Card Key Type	Function
Open Platform (OP) Key	- OP keys are used to protect key management operations on Java based interpretive cards and regulate card operations
Container Key	- Control read and write access to data contains
Transport Keys	- Temporary keys used to secure cards during transfer from manufacturer to card issuer
PIN Unlock Key	- Enables resetting of PINS

Figure 6: Key Management Functions

During the pre-issuance phase of life cycle management, the card manufacturer should generate three key sets known as the transport key, master key, and the OP master key, which is injected into the smart card. The card manufacturer's OP master key set is wrapped with the transport key to send to the card issuer for the key ceremony. The key ceremony initializes the key sets into the card issuer's hardware security module (HSM) and generates card issuer keys. During the card issuance phase, key pairs in the smart card are produced with the generation of the ID and email signature key, if required. Other activities, which may need to be considered in the card life cycle management, are not to be confused with the generation of the ID and email signature key (if required). Following the issuance of the smart identification card, the agency must provide a method to update the smart card keys, replace PKI certificates (e.g., for email), regenerate the PKI signature and encryption key pairs, and allow PIN reset. Following the issuance of the smart identification card, the agency must provide a method to update the smart card keys, replace certificates (e.g., for email), regenerate the signature and encryption key pairs, and allow PIN reset.

- **Cardholder Database Management.** The agency should maintain an archive of all cards issued. This record should link the card serial number or unique identifier to the cardholder and maintain the cardholder's digital photograph, signature image, digital and attribute certificates, and other pertinent information for all applications carried on the card. This will allow a replacement card to be issued containing all initially authorized privileges and data in the event that the cardholder's card is lost or stolen or malfunctions.
- **Card Inventory Control.** Smart card stock should be maintained in a secure environment. The agency or its designated card issuer records the serial numbers of cards received in inventory, as defined by the agency's pre-issuance specification. Cards must be stored in a secure

location with access limited to authorized individuals. The diagram in Figure 7 depicts the card order life cycle.

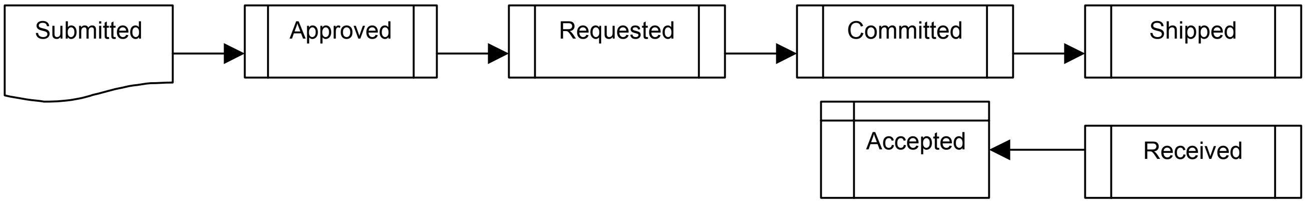


Figure 7: Card Order Life Cycle

The card manufacturer is generally responsible for all cards until they are delivered to or accepted by the agency at designated over-the-counter card issuance locations (in the last stage of the card order life cycle). Agencies must have the ability to track card inventory levels and control their availability to designated card issuers. In addition, the agency or its designated card issuer should be responsible for the following:

- Recording serial numbers received into inventory and issued from inventory;
- Monitoring inventory levels and requesting additional card stock from the card manufacturer;
- Processing returned or damaged cards for inventory log update and chip failure testing; and
- Maintaining a distributor card database that details the number of cards issued monthly and annually by agency and includes the collection status of card and chip failures.

During the card life cycle, inventory information can be transmitted from the vendor system to the agency's system. The card inventory system can be incorporated into the card management system. This will allow the creation of key reports for additional card requirements and for card vendors to ship directly to the site where the cards are required. Other card inventory approaches can also be negotiated between the vendor and the agency.

- **Cardholder Services.** The agency or its designated card issuer must provide customer service support for the smart card platform. Typically, a help desk is established that provides a toll-free number for cardholder's inquiries. To serve cardholders, the agency or the designated card issuer should provide an automated response unit (ARU), in addition to customer service representatives. Anticipated client customer services via either the ARU or a customer service representative include:

  - Reporting a lost, stolen, damaged, or inoperative card;
  - Reporting a malfunctioning card;
  - Reporting unauthorized card use or other breach of security;
  - Reporting an update in demographic data (e.g., name change, change of address);
  - Providing information support for card applications and services; and
  - Ordering card replacements.

  Additionally, the agency will need cardholder training materials for the following topics:

  - Basic card usage;
  - Card application usage;
  - Card security and key protection procedures; and
  - Privacy safeguards.

2.4 Capabilities of the Smart Identification Card for Agencies

The expanding capabilities of smart cards offer agencies the opportunity to issue a portable ID technology that enables users secure access to multiple applications. Figure 8 provides examples of smart card functions and applications. As Figure 8 shows, the primary functions performed by the smart card include identification, record storage and retrieval, secure physical and logical access, financial services delivery, and unit tracking and inventory. Examples of specific applications associated with these functions are also listed.

Smart Card Functions and Applications		
	Function	Application
Store and Process Data	Identification: Verifies identity by displaying stored demographic data, photograph, or biometric; enables the automatic population of standard forms; allows implementation of automated identity verification processes through machine-readable cardholder data; provides for multi-factor authentication of identity.	• Basic identification • Extended identification • Licenses • Permits
	Physical Access Control: Authenticates individuals and permits access to physically secure areas.	• Parking • Building • High security areas
	Logical Access Control: Authenticates individuals and permits access to accounts and networks.	• Internet • PC personalization • Mobile phone • Authentication – Digital signature – Biometrics – Passwords/single sign-on
	Digital Signature and Biometrics: Provides strong authentication for high-value financial transactions and high security physical and logical access control.	• High value financial transactions • High security network or Internet access • Physical access to high security areas
	Value Added Services: • Unit tracking & inventory: Keeps tracks of units accumulated and used for "in-kind" services.	• Loyalty • Meal plans • Phone • Library
	• Record storage and retrieval: Stores data files and records, which can be displayed on a terminal or used to populate standard forms.	• Medical records • Insurance forms • Eligibility information • Service provider
	• Financial services: Calculates data associated with financial transactions and maintains balance record.	• Debit • Credit • E-check • Stored Value – Vending – Tolls – Fare collection

Figure 8: Smart Card Functions and Applications

2.4.1 IDENTIFICATION

The smart card can be used as an identity card, allowing a number of security features to authenticate identity. First and foremost, it can be used as an employee card. Card personalization may include printed identification on the card including name, agency and other basic identification data such as height, weight, eye color, date of birth and/or social security number. The cardholder's digitized photo and digitized written signature may also be printed on the card. Demographic data, including data such as the digitized photo, may be stored on the card chip and accessed through authorized terminals. Cardholder information and data (e.g., digitized photo, name) may be stored on the chip, accessed through authorized terminals and provide support for automated identity verification processes.

The smart card also enables multi-factor authentication. For example, the chip can provide more secure authentication of the cardholder’s identity by maintaining the cardholder’s digital certificate containing the cardholder’s public key. The digital certificate binds the cardholder’s identity to his/her public key. The smart card also holds the cardholder’s private key, which can be used to digitally sign electronic documents and transactions.

The smart card can also be used to maintain a biometric template, which can be used to authenticate the identity of the cardholder by matching a live scan of a biometric feature (such as a fingerprint or iris scan) to the template on the card. Thus, the card can provide highly secure and portable authentication of the cardholder’s identity.

2.4.2 SMART CARDS AND BUILDING SECURITY: PHYSICAL ACCESS CONTROL

The smart card can be used as part of an automated system that controls an individual's ability to access a physical location such as a building, parking lot, office, or other designated physical space. Although the technical implementation may vary across different physical access control systems, physical access control systems typically include the following functions:

- Enroll employee;
- Assign access privileges;
- Conduct the access control transaction;
- Authorize access;
- Update and revoke access privileges;
- Provide for temporary credentials;
- Track or audit accesses;
- Generate access reports;
- Manage the card hot list;
- Maintain the access database; and
- Manage visitor control;

In some cases, if the physical and logical access control databases are integrated, there may be some overlap in the functions provided by these two applications. The smart card can be used in a number of ways to identify the cardholder to the physical access control system:

- To carry a number that can be used to retrieve the cardholder’s access privileges from the physical access control system’s files;
- To carry access control privileges on the card;
- To carry a digital certificate to verify the cardholder’s identity; and

- To carry a biometric template against which the cardholder's live biometric scan is compared to verify the cardholder's identity.

2.4.3 SMART CARDS AND IT SECURITY: LOGICAL ACCESS CONTROL

The smart card can be used as part of an automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application or database. Computer system security generally encompasses three functions:

- Data Security. Data security schemes use mechanisms such as data encryption to protect information;
- Authentication. Authentication techniques are used to prove the identity of an individual before providing access; and
- Access Control. Access control techniques are used to manage and control an individual's privileges to access workstations, databases, applications, host systems, and other networks.

Although the technical implementation may vary, the basic functional capabilities of the logical access control function are standard across systems. These basic functions include:

- Enroll employees;
- Assign access privileges;
- Update privileges;
- Authenticate individuals;
- Conduct access control transactions;
- Track and audit access; and
- Generate access reports.

The tremendous expansion of interest in Internet access has generated increased concern over the security of data transmission and user authentication. Secure access is of interest for other secure remote access applications, such as home banking, wireless systems, cellular, and satellite-based systems. Smart cards provide a secure and portable authentication token for secure remote access.

2.4.4 DIGITAL SIGNATURES

Recently, the United States Code was amended to mandate the electronic submission of information and the acceptance of electronic signatures. To assist in the implementation of this U.S. Code amendment, the Government Paperwork Elimination Act was passed as part of the Omnibus Appropriations Bill. The Government Paperwork Elimination Act directs the Director of the Office of Management and Budget to develop procedures for the use and acceptance of electronic signatures by Executive Departments within 18 months. There has been increasing interest in the use of digital signatures at the state level as well. A number of states have adopted electronic signature legislation and have developed the necessary public policy to support public key cryptography.

Public key cryptography is the use of a cryptographic method that relies on pairs of cryptographic keys, of which one is private and one is public. If encryption is done using the public key, decryption requires application of the corresponding private key (and vice versa). Public key cryptosystems make possible authentication schemes in which a secret can be verified without needing to share the secret. Digital signatures are generated with the private key component of the public/private key pair. The corresponding public key is used to verify the signature. Given that a user's private key is never shared with another party, there can be a strong association between the user's identity and the use of the private key.

A digital signature on electronic documents functions like a handwritten signature on printed documents. The signature is an unforgeable (i.e., computationally impossible or very difficult to forge) piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a higher degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming that the signature was forged. The digital signature enables "authentication" of digital messages, assuring the recipient of a digital message of both the sender identity and the message integrity.

Digital signatures rely on public key cryptography and make use of the public key infrastructure (as defined below). For example, when Alice digitally signs a document, she puts her private key and the document together (or the document alone) and performs a hash computation on the composite to generate a unique number called the digital signature. When an electronic document uses this method, the output is a unique digital signature of the document.

Verification of the signature requires only knowledge of the public key. So Alice can sign a message by generating a signature only she can generate, and other people can verify that it is Alice's signature, but cannot forge her signature. This process is called a signature because it shares with handwritten signatures the property that it is possible to recognize a signature as authentic without a person being able to forge it.

The use of digital signatures provides the basis for secure electronic commerce, the foundation of electronic service delivery.

The steps for creating and successfully transmitting a digitally signed document using public key cryptography are described below:

Bob, the message sender, through his computer system:

- Creates a message to send to Alice;
- Applies a hash function to create a message digest (digital signature);
- Encrypts the original message as well as the message digest with his private key; and
- Sends the encrypted message and digital signature to Alice's system.

- Alice, the message receiver, through her computer system:
- Decrypts the message using Bob's public key;
- Decrypts the digital signature with Bob's public key to recover the message digest;
- Applies the same hash function that Bob used to the original message to obtain a message digest; and
- Compares the message digest that her system obtains with the message digest received from Bob's system. If they match, the digital signature is verified. Alice can be sure that a) the message came from Bob's computer, and b) the message was not altered during the transmission.

It is important to note that in most smart card systems, the entire document would not be encrypted using the PKI public key (since this is a computation-intensive process). Typically a "secret" key (e.g., using the Data Encryption Standard (DES) or Triple Data Encryption Standard (3DES)) is used to encrypt the entire document. The "secret" key is then encrypted with the "private" public key and sent with the encrypted document and the digital signature. The "secret" key that is used can be a one-time key derived using a random number and a smart card "secret" key.

Digital signatures are self-authenticating; that is, if a single byte of the digitally signed message has been altered, the decryption process will reveal that alteration. The message is retrieved twice; once from the decrypted digital signature and again by recomputing it directly from the input data. If the two messages do not match, the text has been altered. Thus, digital signatures are highly secure and robust.

In order to use public key cryptography for identity authentication, encryption, and digital signatures on a large-scale, it is necessary to establish a PKI infrastructure to support the generation and distribution of keys. Digital certificates can then be used to authenticate the identity of the owner of a specific public key. The implementation of this infrastructure to support public key cryptography requires a defined set of services that must be provided by some entity. Entities that use certificates, as well as other parties who contribute in various capacities, are key stakeholders that participate in the certificate environment and are affected by the public policy decisions made for a PKI. Key stakeholders include:

- **Certification Authority (CA)**. A person or entity that issues a certificate. In a hierarchical PKI, there can be issuing CAs (i.e., a CA who has elected to apply a policy to itself and its subjects including other CAs and end entities) or subject CAs (i.e., a CA that is certified by the issuing CA and hence complies with the certificate policy of the issuing CA). Depending on the PKI in question, CAs could be government agencies, banks, vendors, or other organizations.

- **Registration Authority (RA)**. A person or entity that is responsible for the identification and authentication of subjects of certificates, but is not a CA, and hence does not sign or issue certificates. An RA is trusted to register other entities and assign them a relative distinguished value such as a distinguished name, hash or certificate. Generally, an issuing authority approves an RA to assist persons in applying for certificates, revoking (or where authorized, suspending) their certificates, or both. The RA may also be given authority to approve applications.

- **Subscriber.** A person or entity (e.g., corporation, employee or consumer) who is the subject named or identified in an issued certificate and who holds a private key that corresponds to a public key listed in that certificate.

- **Relying Party**. A person or entity (e.g., merchants or their acquirers) that has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them. The recipient is a relying party who acts in reliance upon receiving a certificate and digital signature.

All of these parties may be in a direct relationship with each other in some portion of the certificate issuance and usage process. The "ground rules" governing the relationships of these parties must specified either in contracts among the parties or by operating rules that specify roles, responsibilities, and liabilities of the participants.

In addition to these key stakeholders, there are other potentially interested stakeholders in the certificate environment. These other stakeholders may vary depending on the certificate implementation environment. Potential additional stakeholders include:

- **Ancillary Service Providers.** A person or entity offering or performing a service, other than issuance of certificates, in support of digital signatures and other related areas of secure electronic commerce including:
    - **Archival Service.** A person or entity that keeps records for a certification authority, repository, or another person involved in electronic commerce.
    - **Confirmation Service.** A person or entity aiding a certification authority in performing its duty to confirm certain information.
    - **Directory Service.** A person or entity who locates and furnishes certificates and other information about persons, such as distinguished names, online addresses and identifying or descriptive information, either directly or through links to third party directories of such information.
    - **Technical Due-Diligence Service.** A person or entity that reviews the technical compliance of a number of messages, time stamps, digital signatures, and certificates related to a particular transaction or series of transactions. The person documents the results of such review to relying parties in electronic form suitable for deposit online in a repository and/or offline in an archival service.
    - **Financial Assurance Service.** A person or entity that aids a certification authority in satisfying the financial responsibility requirements such as surety issuing a bond or a liability insurance carrier.
    - **Key Pair Generation Service.** A person or entity that creates key pairs to be used by others.
    - **Message Corroboration Service.** A person or entity that creates a hash result to fix the content of the message, and then associates a time stamp with the message and/or hash result. Message corroboration provides assurance of message integrity and the time the message was created, but provides no authentication of the signer's identity.
    - **Key Escrow Service.** A person or entity who holds the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber.
    - **Private Key Trust Service.** A person or entity who holds the private key of a subscriber pursuant to an express trust, letters testamentary, or similar legal arrangement which is voluntarily created by the subscriber.
    - **Time Stamping Service.** A person or entity time-stamps the digital signatures, messages, or records of others.
- **Policy Approving Authority (PAA).** A management entity associated with a root CA in the Federal PKI who evaluates CA policies and determines the level of trust (i.e., federal assurance levels) provided by each CA. The PAA also performs periodic reviews (or audits) on the operations of each Federal PKI CA to assess conformance with its policies.

- **Auditors.** An independent entity such as a CPA or other designated person or organization that is charged with periodically reviewing the policies and operations of a CA to indicate compliance with established CA guidelines or audit methodologies.

- **Notaries.** A person or entity that confirms the association between the public key and the subscriber's identity by notarizing the certificate application form, which facilitates the issuance of the certificate by a certification authority. Notaries act as trusted third parties, granting the association the special legal status a notarization brings, enhancing the proof and enforceability of certain digitally signed records, and bolstering both the real and perceived trustworthiness of the digital signature environment. The notarization supports the later verification and proof of transactions created under the signer's digital certificate.

- **Guarantors.** A person or entity (e.g., United States Fidelity and Guaranty Company in the NetSure Protection Plan) who provides warranties for subscribers to protect them from unauthorized use, unauthorized disclosure, and compromise of their private keys, as well as unauthorized revocation and loss of use, delay in requesting revocation, erroneous issuance, and impersonation.

- **National Associations.** An entity convened for the purpose of establishing and enforcing operating rules surrounding the working of the certificate environment (e.g., the National Automated Clearing House Association (NACHA) Electronic Benefits and Services Council, a CA trade association or consortium of companies).

Public key cryptography offers agencies a secure means to authenticate the identity of employee cardholders, as well as a mechanism to sign documents to ensure non-repudiation. Agencies needing highly secure identity authentication mechanisms or contemplating electronic service delivery using digital forms should consider this technology.

2.4.5 BIOMETRICS AND SMART CARDS

Secure access, whether to buildings, information, bank funds, or other resources, has long been based on a combination of two concepts: what you have and what you know. Basic bank debit card security is based upon what you have – the debit card – and what you know – the PIN. This type of security is considered insufficient for securing access to areas of high value since PINs can be recorded, lost or stolen. In situations requiring higher security, the requirements expand to include "what you are"—which can be substantiated by the use of a biometric. Biometric technology involves the measurement of a distinctive biological feature to verify the claimed identity of an individual through automated means.

A **biometric** is a measurable physiological or behavioral trait of a living person, especially one that can be used to identify a person or verify a claimed identity. As a biometric is uniquely bound to a person, it can provide the strongest single factor for user authentication. A biometric can be used in conjunction with a password or a token (such as a smart card) to provide strong, two-factor authentication. Although biometric systems have been commercially available since 1968, the commercial use of biometrics has experienced significant growth only in the last five years. Biometrics are increasingly used in time and attendance systems, customs and immigration, physical access control systems, ATMs and point-of-sale (POS) systems, and information system access control.

A **physiological biometric** (also called *physical biometri*c, *static biometri*c) is a biometric based on data derived from measurement of a part of a person's anatomy. Examples of physiological biometrics include fingerprint, hand, face, iris and retina. A **behavioral biometric** (also called *dynamic biometri*c) is a biometric based on data derived from measurements of an action performed by a person and, distinctively, incorporating time as a metric; that is, the measured action has a beginning, middle, and end. Examples of behavioral biometrics include voice and signature.[26] Physiological biometrics are unchanging (barring severe physical injury) and unalterable without significant duress, but are perceived as more invasive and raise privacy concerns more quickly. Behavioral biometrics are less stable than physiological traits, changing with stress and sickness and, generally, are less secure.

This section describes different types of biometrics that can be used with a smart identification card, including information about biometric uniqueness, image capture method and template definition and size.

- **Fingerprint Scan**. The fingerprint is one of the most widely used biometrics in the government today. It is currently the only authorized biometric for the Department of Defense, and then only for specific purposes disclosed to the individual.

  Fingerprint scanners have been commercially successful biometric devices over the last several years, accounting for nearly 50 percent of the 2001 worldwide biometrics market (according to the International Biometric Group). A wide variety of devices are available. Because of the association of fingerprints with criminal forensics, these biometric technologies are also called *fingertip* or *finger scan* technologies.

  *Distinctivenes*s: It has been estimated that the chance of two people having the same fingerprint is less than one in a hundred billion (even for monozygotic siblings— "identical" twins or triplets). While this is difficult to prove empirically, in over a century of the use of fingerprinting, no two fingerprints have ever been found to be identical. In addition, it is now known that fingerprints form in the womb at around five months and remain constant even after death. Fingerprints have even been successfully taken from well-preserved mummies more than 2,000 years after their death.

  *Image captur*e: A fingerprint image can be captured using one of four technologies: optical, capacitive (silicon), thermal (silicon), and ultrasonic. The majority of companies use optical technology, but the trend is toward silicon.

  - Over the past decade, optical scanners have been the most widely implemented fingerprint technology. Optical fingerprint technology is proven but is relatively expensive and not always reliable due to environmental conditions. To operate, a user places a finger on a platen of glass or hard plastic (proprietary to each company). The fingerprint is illuminated by an internal light source and a charge-coupled device (CCD) converts the image of the fingerprint into a digital signal.
  - Capacitive (silicon) technology has gained considerable acceptance since its introduction in the late 1990s. Most silicon, or chip, technology is based on direct current (DC) capacitance: the silicon sensor acts as one plate of a capacitor and the user's finger is the other. The capacitance between platen and the finger is converted into an eight-bit grayscale digital image. An exception to this is a technology, which employs alternating current (AC) capacitance and reads to the live layer of skin. Capacitive imaging generally produces better

[26] FIPS Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, National Institute of Standards and Technology (NIST), September, 1994, p. 32.

[17] A majority of Section 2.4.5 can be attributed to the Smart Card Alliance White Paper, 'Biometric Authentication: Perspective'; July 19, 2002.

image quality from a smaller surface area than optical. The chips have a resolution of about 0.05 millimeters (0.002 inches) and are small enough to be integrated into many devices that cannot accommodate optical technology. Many major companies have recently moved into the silicon field.

- Using thermal (silicon) technology, the finger is swept across a rectangular array of pixels, which are sensitive to heat transfer due to the application of a pyroelectric layer above the silicon. A slice of the fingerprint is captured, and multiple slices are reconstructed into a full fingerprint image. This technology has a thick surface coating, providing high levels of mechanical robustness (e.g., resistance to abrasion and corrosion) and electrostatic discharge (EDS) protection. Power consumption is low. Thermal technology provides a high quality image and is able to capture poor fingerprints (i.e., those with little topography) very well. The swiping method is self-cleaning and, combined with the thermal technology, enables the sensor to operate in challenging environmental conditions. Resolution is 0.05 millimeters (500 dots per inch). Due to the swiping method and the resulting small silicon area, thermal technology offers a small and low cost solution.
- Ultrasound technology is not yet widely used. The sensor transmits acoustic waves and measures the distance based on the impedance of the finger, platen, and air. Preliminary uses of the products indicate that this technology promises to be the most accurate fingerprint technology.

*Template*s: Systematic approaches to matching fingerprints to certain individuals were introduced in the 19th century. One such approach, the Henry Classification System, is based on patterns such as loops, whorls and arches and is still used today to organize fingerprint card files. The most common method of generating a template emulates the traditional police method of matching **minutiae** (literally, “small details”): bifurcations, divergences, enclosures, endings and valleys in the ridge pattern. Each minutia is described by a set of numeric variables. A typical fingerprint image can show between 30 and 40 minutiae. Approximately 80 percent of biometric fingerprint sensors use minutiae in some fashion. Other methods include “traditional” pattern matching techniques and moiré fringe patterns.

The fingerprint has one of the largest biometric templates, ranging from 250 bytes (minutiae) to over 1,000 bytes (pattern matching). Note that, as with any other biometric technology, the template holds only particular data about the features, not the image of the fingerprint itself, and the image cannot be reconstructed from the template.

- **Hand Geometry**. Hand geometry is currently being used in several government agencies including the Department of Energy and the Department of State. Hand geometry systems use optical technology to map key geometrical features of hand topography to verify an individual’s identity. Hand geometry technology uses a number of different measurements to create the template. These readings may include measuring finger length, skin translucency, hand thickness, and palm shape. Different products use diverse methodologies to construct the hand geometry template, so there is currently no standard template that can be used for smart cards. Live scans of the hand are compared against the template to verify a person’s identity.

  *Distinctivenes*s: Virtually every person’s hands are shaped differently, and the shape does not significantly change over time. A biometric template can be built from measurements of geometrical characteristics of a person’s hand.

*Image captur*e: Hand geometry scanning devices use either mechanical or image-edge detection. In either case, a charge-coupled device is used to record the hand's three-dimensional shape. One variant uses the shape and characteristics of just the index and middle fingers.

*Template*s: Over 90 measurements of the length, width, thickness, and surface area of a person's hand and/or fingers are used to generate the template. This is one of the smallest templates, generally 10 to 20 bytes.

- **Facial Recognition**. Several state motor vehicle departments are currently using facial recognition to provide identity authentication in issuing driver's licenses. Facial recognition is based on comparing the characteristics of a live scan of a face against a stored template of facial characteristics. Various technologies may be used to perform facial recognition. Some products use off-the-shelf video/digital cameras. Such products employ algorithms to create a set of numbers related to the face rather than the facial image itself. One method uses spatial measurement, recording such distances as the center of the eye to the bottom of the ear, to the tip of the chin, and to the high cheek feature. Another method uses two cameras to record a stereo view of the face. This method evaluates the entire face, not just key features. Other products use infrared technology. Because the technology for creating facial templates varies from product to product, there is no standard facial recognition template.

  *Distinctivenes*s: An obvious limitation of face verification is that, because it generally disregards changeable characteristics like hair color and style, it cannot differentiate between monozygotic siblings.

  *Image captur*e: The system locates the human face within an image captured by a video camera, isolating it from the other objects captured within the image. Software then analyzes the captured images for general facial structures (such as eyes and nose) and measures and determines the rest of the face. Other imaging methods include three-dimensional mapping (using a laser range scanner, instead of a camera) and thermal imaging of blood vessels under the skin.

  *Template*s: Templates may be generated by one of several methods:

  - Eigenfaces. Eigenface (from the German eigen, 'own') is an MIT-patented technology that uses two-dimensional, global grayscale images representing distinctive characteristics of a facial image. Variations of eigenface are frequently used as the basis of other face recognition methods.
  - Eigenfeatures. The system combines facial metrics—measurements of the distance between specific facial features, such as the eyes, nose and mouth—with the eigenface approach.
  - Local feature analysis. In this derivative of the eigenface method, the system selects sets of blocks, or features, in each face that differ from other faces in the database. The most common points used are the nose, eyes, mouth, and areas of definite bone curvature differences, such as the cheeks.
  - Neural networking technology. This system employs artificial intelligence and "learns" from experience. Features from both faces—the enrollment and trial face—"vote" on whether there is a match.
  - Curvature measurements. This method is used with three-dimensional mapping.

  - Thermogram. This method is used with thermal imaging.

- **Iris Scan.** The iris consists of a trabecular meshwork of connective tissue, collagenous stromal fibers, ciliary processes, contraction furrows, rings, and coloration. In the 1960s ophthalmologists proposed that the iris might be used as a kind of "optical fingerprint," based on clinical results that showed that every iris is unique and unchanging. John Daugman, Ph.D., O.B.E., an academic at the Computer Laboratory, University of Cambridge, U.K., developed the mathematical algorithms behind iris recognition (Internet: www.cl.cam.ac.uk/users/jgd1000/).

  *Distinctivenes*s: The uniqueness of eye identification is well-established. The iris is a robust biometric as it remains unchanged throughout a person's life and is not subject to wear and injury, although damage to the cornea or disease might obscure the iris. The iris has 6 times as many distinct, identifiable features as a fingerprint. Like fingerprints, no two iris patterns are alike, even among monozygotic siblings.

  *Image captur*e: The iris presents a number of challenges. It is a small target (one centimeter or half an inch) that must be acquired from a distance (one meter or one yard), and is often prone to movement. Moreover, the iris is located behind a curved, wet, reflecting surface, is obscured by eyelashes, lenses, and reflections, and is partially occluded by eyelids that are often drooping. This accounts for the higher capture device cost as compared to some other biometric systems. Iris image capture can be passive or active. With active iris image capture, the user must be between 15 and 35 centimeters (6 and 14 inches) from the camera lens. Passive iris image capture incorporates a wide-angle lens, automatically determines the position of the eye, and zooms in on the eye to capture the image. The user can be between 30 and 100 centimeters (1 and 3 feet) away from the cameras. This method is more user-friendly, but also more costly.

  *Template*s: The template or "IrisCode" is constructed by "demodulation" of the iris pattern. This mathematical process is unchanged by the size of the iris (and hence unaffected by the imaging distance and the optical magnification factor) and by the dilation diameter of the pupil within the iris. It is also insensitive to contrast, camera gain and illumination level. The description is very compact, requiring only 256 bytes to represent each iris pattern. (The other 256 bytes of a 512 byte IrisCode control the comparison process.) The recognition of irises by their IrisCodes is based on the "failure of a test of statistical independence." Any given IrisCode is statistically guaranteed to pass a test of independence against any IrisCode computed from a different eye; however, it will uniquely fail this same test against the eye from which it was computed.

- **Retina.** Research into eye recognition technology began in 1935 when an article appearing in the New York State Journal of Medicine suggested that the pattern of blood vessels on the retina were unique from person to person and so could be used to identify an individual. The first commercial product to use retinal scans, EyeDentify 7.5, appeared in 1985. Today, the retina segment of the biometrics market comprises a very small market share.

  *Distinctivenes*s: Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. Research has shown that retinal patterns, even between monozygotic siblings, are unique. With the exception of some types of degenerative eye diseases, severe head trauma, damage to the cornea, glaucoma, cataracts, and other factors that might obscure the retina, retinal patterns can be used throughout a person's life.

*Image captur*e: Retina scan devices read through the pupil, with the user putting his or her eye within 1 to 2 centimeters (approximately 0.5 to 0.8 inches) of the device and holding still while the image is captured. The user looks at a rotating green light as a low-intensity infrared light is projected through the eye and onto the retina.

*Templat*e: The patterns of the retinal blood vessels are measured at over 400 points to generate a 96-byte template.

- **Voice Recognition**. Voice identification technology was pioneered in the 1960s. Voice identification has since undergone aggressive research and development to bring it into the mainstream. Voice verification is possible because every person has a unique set of voice characteristics and speech patterns. Voice verification extracts specific and unique features from a person's speech, such as pitch, tone, cadence, harmonic level and vibrations in the larynx, and stores and uses them to differentiate that person's voice from other voices. All voice recognition systems require speech samples from each user to associate with the user's profile or account. A person using a voice verification system begins by claiming to be an enrolled user. This is generally accomplished by speaking or otherwise inputting an identification code. The spoken input is compared with a stored sample of the enrolled user's speech. This stored sample is called a voiceprint. If the voiceprint and spoken input samples match, then the person is accepted. If they do not match, the person is rejected and denied access. Voice is a very convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access, so it is particularly popular for logical access control applications.

  *Distinctivenes*s: Voice is less accurate than other biometrics. Its main attraction is its suitability for telephone applications and interactive voice response (IVR) systems, where it can be deployed with no additional user hardware costs.

  *Image captur*e: Voice "images" can be captured with conventional microphones used in telephones and PCs.

  *Template*s: There are different methods or processes to analyze a person's speech pattern, but all systems are developed using broader-based speech processing technology. Voice systems incorporate several variables or parameters in the recognition of the voice or speech pattern, including pitch, dynamics, and waveform. Voice scan templates commonly require 1,500 to 3,000 bytes.

- **Signature**. Signature-based authentication, also known as *dynamic signature verification* (DSV), is another instinctive biometric as authentication by signature occurs during many everyday transactions. It is popular in document authentication applications that have traditionally used written signatures.

  *Distinctivenes*s: Signature identification systems analyze two different areas of a person's signature: the specific features of the signature itself (the visual image) and the specific features of the *process* of signing. Features that are taken into account and measured include speed, pen pressure, directions, stroke length, and the points in time when the pen is lifted from the paper. With sufficient practice, a person might be able to duplicate the visual image of someone else's signature, but it is difficult, if not impossible, to duplicate the dynamics.

*Image captur*e: Signature identification is an inexpensive biometric solution. Tablet-based systems that operate using off-the-shelf digitizers cost as little as US$99, but suffer from limited accuracy.

*Template*s: The major technological hurdle for signature identification involves the method of trying to differentiate between the parts of the signature that are habitual (consistent) and those that vary from time to time. Systems must also be able to adapt to any slight variations over time.

Biometric Systems

Although biometric technologies differ in what and how they measure, all biometric systems work in a similar way. The user submits a **sample**—that is, an identifiable, unprocessed image or recording of the physiological or behavioral biometric—via an acquisition device (for example, a scanner or camera). This biometric is processed to extract information about distinctive features to create a **trial template** (or *verification templat*e). Templates are essentially large number sequences; it's impossible to reconstruct the sample from the template. The trial template is the equivalent of the user's "password."

Verifying a memorized password or a one-time password (such as a password that is generated by an authentication token) is a yes/no decision. However, verifying a trial template is not. A trial template is compared against a **reference template** (or *enrollment templat*e) that was created from multiple images when the person enrolled in the biometric system. No two templates are ever exactly alike, so the biometric system must judge whether or not there is a "close enough" match: i.e., the matching score must exceed a configurable threshold.

Thus, biometric systems can err. A trial template might be matched incorrectly against another person's reference template, or it might not be matched even though the user is enrolled. The accuracy of a biometric system is measured by:

- **False match rate (FMR)**, also known as Type I error or *false acceptance rate* (FAR), and

- **False non-match rate (FNMR)**, also known as Type II error or *false rejection rate* (FRR).

Both methods focus on the system's ability to limit entry to authorized users. The lower a system's FMR, the better its security. The lower a system's FNMR, the easier it is to use. In general, for a given system and as the threshold is varied, the lower the FMR, the greater the FNMR. Therefore, there is often a trade-off between security and ease of use when using biometric systems.

The Role of Smart Cards with Biometrics

The role of smart cards with biometrics is as a powerful one-to-one verification/authentication technique for cardholder identity.

Depending on the biometric system, the role of the smart card can be quite varied. Two main uses for the smart card are discussed below.

- **Match off-card**. For this type of implementation, the enrolled template is initially loaded onto the smart card and then dispensed from the smart card via either contact or contactless interface when requested by the external biometric system. The external equipment then compares a new live scan template of the biometric with the one being presented from the smart card. This implementation clearly has some security risks associated with transmitting the enrolled template off the smart card for every biometric challenge. Appropriate security measures should be implemented to ensure the confidentiality and integrity of the released template. With this technique, the smart card is storing a template (or multiple templates), but has no significant knowledge of the type of biometric information, nor the ability to process it in any way. This implementation method is appropriate for all types of smart cards; this technique will work with memory, wired logic or microcontroller-based smart cards.

- **Match on-card.** This implementation technique initially stores the enrollment template into the smart card's secure memory. When a biometric match is requested, the external equipment submits a new live scan template to the smart card. The smart card then performs the matching operation within its secure processor and securely communicates the result to the external equipment. This method protects the initial enrollment template since it is maintained within the smart card and never transmitted off-card. Cardholder privacy is also maintained with this technique since the cardholder's biometric template information is not readable from the smart card. With this technique, the smart card must be a microcontroller-based device and be capable of computing the one-to-one match. One such implementation of match-on-card for fingerprint patterns is commercially available and has been implemented on several smart cards. It is also important to note that Java Card API V2.2 supports the notion of a Biometric Manager that can use the on-card API to facilitate the secure match-on-card functionality.

Business Use

There are three general applications of biometric systems:

- User authentication for information system access control (including financial services usage);
- Physical access control;
- Monitoring (for example, time and attendance).

Physical access control and monitoring applications of biometric systems already in use or in trials include:

- Airline passenger processing systems at European and U.S. airports.
- Other border or passport control systems, to allow enrolled citizens to bypass long immigration queues.
- Prison visitor systems, to stop visitors and inmates from swapping identities.
- Junior school and child care facilities, to allow entry only to enrolled adults (staff, parents, and guardians) as a defense against child abuse and kidnapping.
- Driver's licenses, to stop drivers (particularly truck drivers) having multiple licenses or swapping licenses among themselves when crossing state lines or national borders.
- Time and attendance, to stop "buddy punching."
- Benefit payment systems in several U.S. states, to stop multiple claims ("double dipping"). In states using these systems, the number of individuals claiming benefits has dropped dramatically.

Biometric Technology Benefits

Increased Security

- Biometric information cannot be lost, stolen, or forgotten. It cannot be written down or discovered by social engineering. It cannot be shared with other users. In some biometric systems, it cannot, without duress, be used by anyone other than the individual. (See discussion on capture and replay attacks below.)

- By installing biometrics, organizations can positively verify users' identities, improving personal accountability (through positive identification of users in audit trails) and allowing high-value transactions to be offered at remote terminals and over the Internet.

- In conjunction with smart cards, biometrics can provide strong security for PKI credentials held on the cards, thus providing greater trust in PKI services, especially digital signatures for non-repudiation.

- A user is not required to present a card or remember a password or PIN. Since biometric information cannot be lost, stolen or forgotten, it is always available to the individual.

- Organizations can eliminate the overhead of password management and improve customer service.

- Organizations can implement recognition systems rather than simple authentication systems, so that users no longer have to manually logon to information systems.

Biometric Technology Risks

Privacy Concerns

Users, especially consumers rather than corporate users, are concerned about the storage and distribution of biometric data. If an organization holds a central repository of templates, users have no control over the distribution of this data and are wary of:

- Misuse of the data (for example, illicit exchange with other organizations).
- Use for purposes other than the purpose for which it was originally collected ("function creep").

In the European Union, established data protection legislation might apply to biometric data as it does for other personal data for a living person. In the U.S. and elsewhere, regulatory statutes are required to provide safeguards. Holding the user's reference template on a smart card is a way of mitigating this concern, but may give rise to manageability issues.

Other privacy concerns include fears about the ability to search records about a person and to monitor a person in real-time. This is a particular concern for consumer applications; however, corporate users also may see the specter of "Big Brother" if, for example, an organization places a video camera on every desk (to implement iris or face recognition biometric systems).

When considering using smart cards with biometric systems, the smart card should be viewed as a privacy-enhancing technology. The smart card is able to augment the identity/biometric system, providing a secure container for the biometric template and having the ability to compute the biometric match within the card rather than on external equipment. The smart card can be viewed as the "local security officer" of the issuer for the day-to-day use of the ID by the cardholder.

Personal, Cultural and Religious Concerns

Fingerprint systems face user opposition because of the stigma of its criminal connotation, since the use of fingerprints in criminal forensics is well known. There are also concerns over hygiene (e.g., would a hand geometry scanner have to be sprayed with an antiseptic after each use) and over the possibility of actual harm (e.g., with retina systems where light is shone into the eye). There is also the perception that users run the risk of harm from criminals—from copying or using a biometric under physical duress to the loss of a hand or finger.

Some cultural and religious taboos can inhibit the use of biometrics systems. For example, people of Japanese origin may resist the use of fingerprint or hand systems that others have touched.

Some Christian groups have associated biometrics with "the mark of the beast" described in Revelation 13:16-17. Some ministers have preached that biometrics herald the coming of the Apocalypse. This continues to worry some consumers.

Suitability for All Users

Between 1 and 3 percent of the general public does not have the feature required for mapping any one biometric. Users who are mute cannot use voice systems. Users lacking fingers or hands from congenital disease, surgery or injury cannot use fingerprint or hand systems. A biometric system that is, or is seen to be, socially regressive—in that it excludes the disabled and the old—may meet with principled resistance. A biometric system might be defeated by legal challenges on a number of grounds and may also be vulnerable to attackers who are or pretend to be disabled.

Any organization that wants to employ a biometric system must address this issue by providing a "fallback" system, not necessarily using another biometric. If these are less secure, then their use may yield an attack.

If Compromised, a Biometric Cannot Be Reissued

Biometric authentication is, in principle, vulnerable to capture and reply attacks—between the scanning device and client software, or between client and database server (possibly over an open network). If an attacker can capture the image or trial template of a user's biometric, then the attacker can replay that data to masquerade as that user. Once a person's biometric is compromised, that user can no longer make use of that trait on that system, or on any other similar system, for life. Unlike a password or token, a biometric cannot be reissued. In order to participate in the biometric system again, the user must re-enroll.

A system can store and match reference templates on smart cards to reduce this risk, as the biggest vulnerability for compromise comes from communications over a network. Some systems might also embed the scanner on the card, so the image and templates never leave the smart card. In these cases, tamper-resistance must be strong enough to ensure that an attacker cannot recover a template from a lost or stolen smart card.

Where biometric authentication is used over a networked system, some type of dynamic encryption is indicated. Such encryption, however, must be stronger than would be required for other authentication credentials. Because a biometric trait is "issued" for life, the data must be protected against attacks for the next 30 years or more. Symmetric encryption with 90-bit keys might well provide communications security for a decade or so, but organizations must use longer keys to extend this lifetime to protect biometrics data.

Biometric Systems Are Not Foolproof

In theory, and sometimes in practice, biometric systems can be compromised by a variety of attacks, including:

- Submission of another person’s biometric (e.g., if the system has a high FMR).
- Submission of the enrollee’s biometric with the user under duress or incapacitated (for example, using some type of drug).
- Submission of an enrollee’s biometric using a severed body part (in a physiological biometric system).
- Submission of a facsimile or recording of an enrollee’s biometric. Successful fingerprint facsimiles can be created not only directly from the enrollee’s finger but also from prints left on a drinking glass or other surface.
- Submission of a latent image on a fingerprint sensor, for example, by placing a small plastic bag filled with warm water on the sensor.
- Electronic attacks, such as the transmission of a reference template, replay of a captured trial template, or replay of a captured sample to recreate a new trial template.

Biometric Selection Guidelines

Organizations should determine the level of security needed for the specific application since this will have the most bearing on which biometric, technology, and vendor are most appropriate. Generally, a behavioral biometric is sufficient for low-to-moderate security applications; a physiological biometric is appropriate for medium-to-high-security applications. Organizations must take into account the size and composition of the user population, the number of acquisition devices that will be needed (i.e., “many” desks or “few” kiosks), and the environment for the devices (e.g., indoors or outdoors, supervised or unsupervised).

One of the key barriers to biometric technology adoption has been the scalability and manageability of biometric systems, particularly in large heterogeneous enterprise networks. In the past few years, a number of vendors, mostly with roots in the biometrics industry, have brought A*uthentication Management Infrastructure* (AMI) products to market. Like other authentication middleware, such as single sign-on (SSO) products, AMI products support multiple authentication methods, not just biometric technologies. Unlike SSO products, however, an AMI product provides a single management framework and authentication service for multiple target systems and lets the organization use different authentication methods singly or in combination.

In the long run, an organization is likely to derive more benefit from its choice of a good infrastructure product than its choice of any particular biometric. In the short term, when selecting one biometric over another, organizations should consider:

- User acceptance
- Effortlessness—ease of use
- Security—accuracy, reliability and resistance to attack
- Cost
- Template storage—location, capacity planning

Biometric Insights

Biometrics are uniquely bound to individuals and offer organizations a method of user authentication that is more secure against attacks and abuse than passwords or tokens alone. Biometric technology has matured over the years but still faces barriers in user acceptance and complexity. Privacy concerns may force biometrics to remain a niche technology for consumer and public applications: the use of biometrics in law enforcement raises the specter of “Big Brother” and overshadows the privacy-enhancing uses of biometrics for information security. Lack of scalability can also be a barrier to adoption for medium and large enterprises.

Lack of robustness (resistance to attack) is another concern and organizations should seek independent confirmation of vendors' claims. For ATMs and other kiosk-style applications involving multiple users, organizations should consider iris, fingerprint, hand, or face. For information system security, fingerprint or iris is more appropriate. Two types of biometrics lend themselves to particular applications: voice for telephone applications (including mobile devices) and IVR systems, and signature for document-centric applications. Medium and large organizations will also be best served by adopting authentication middleware that allows biometrics to be used alongside and in combination with other authentication methods and offers better manageability and scalability than "single-engined" solutions.

2.4.6 OTHER VALUE-ADDED SERVICES

In addition to the identification, physical access, and logical access control applications, agencies may use their smart card platforms for a variety of other applications and services including:

- **Property Management.** A chip-based application that provides the capability to enter, update, and delete asset information from the employee's card. This asset information can then be manually read and verified by a guard when the employee enters or exits a building or read automatically through RF tags in assets when the employee passes through a portal.

- **Exchange of Clearance Information.** A chip-based application that allows clearance information to be transported on the smart card between agencies and used to grant the visiting employee access to high-security facilities.

- **Rostering.** A chip-based application that allows data residing on the smart identification card to be retrieved, date or time stamped, and transferred to a database that is then used to generate a variety of specialized reports and to provide positive proof of attendance.

- **Medical.** A chip-based application that allows basic medical and insurance data to be stored on the card, read when appropriate by authorized providers, and used to populate claim forms.

- **Training/Certification.** A chip-based application that allows training and job-specific certifications to be entered on the card.

- **Electronic Forms Submission.** By combining the use of data maintained on the card with the ability to digitally sign an electronic form, this application can populate and submit a wide range of standard administrative forms used by virtually all Federal agencies.

- **Electronic Purse.** A chip-based application where cash or value is recorded on a chip and is available for use in vending machines and at participating merchants, typically for small transactions. Through this application, merchants can replace labor-intensive cash transactions (counting, sorting, bundling, and transporting) with electronic transactions vending service providers can eliminate loading and emptying coins from machines, as well as eliminate the incentive for vandalism. Customers are able to reduce the need to carry and make payments with cash, particularly when exact change is required.

- **Credit/Debit.** A magnetic stripe application used to access information through an online system for travel, fleet, and purchase card commercial credit applications.

In addition to these suggested administrative applications, agencies may choose to develop their own customized applications for use on the smart identification card platform.

2.5 Benefits of Implementing a Smart Card System

Because of the previous lack of an extensive infrastructure and the costs generally associated with procuring smart card systems, agencies had been reluctant to consider transitioning to this technology. However, the following changes have made smart cards increasingly of interest to agencies:

- **Number of Chip Cards Increased.** Chip cards are becoming increasingly popular in the U.S. With the American Express issuance of the Blue Card and Visa and MasterCard following close behind, the commercial sector is beginning to generate interest in chip cards. Similarly, the advent of the GSA Smart Access Common ID contract has resulted in a substantial increase of smart card implementations throughout the Federal government. With states moving to electronic commerce solutions, state governments are also showing increased interest in smart card technology. As an increasing number of cards are issued, it becomes easier to achieve the card infrastructure critical mass that is needed to make smart cards viable in the commercial world.

- **Price per Card Decreased**. As the volume of smart cards issued goes up, the price for cards is coming down. Depending on the card capabilities required, prices now often average between $3 and $10 per card when purchased in volume. As usage continues to increase, it is anticipated that card prices will continue to decline.

- **Response Time Reduced.** With the advent of improved operating systems (such as Java Card) and faster processors, the time to read data from and write data to the chip has been reduced substantially. This reduction in response time has added to the move toward smart cards.

- **Memory Capacity Increased.** Memory capacity has steadily increased from 1 Kbyte to 64 Kbytes or more, with 32 Kbytes now the average capacity. This increase in memory capacity makes the cards far more practical since it allows cards to host multiple applications, reducing the cost for each application on the card.

- **Move to Multi-Application.** With improved security, increased memory and enhanced card capability, there is an increasing move to multi-application cards. These cards not only provide substantial convenience for cardholders, but also allow cost sharing that makes card platforms affordable for each individual program. Perhaps more than any other factor, the shift to multi-application cards has encouraged the use of smart cards across many entities that could not afford separate card platforms for their individual program.

- **Interoperability Encouraged through Legislation and Developing Standards.** A number of new laws have promoted the concept of interoperability. Additionally, standards bodies have made great strides in issuing and propagating standards to promote interoperability of cards and card readers. The government has also actively promoted standards, with its Government Smart

Card Interoperability Specification v2.1[27] and the interoperability work being conducted under the Smart Access Common ID contract.

With these changes in the smart card market, agencies are beginning to take a closer look at this technology. The following section is meant to help agencies evaluate whether or not they are good candidates for smart cards.

2.5.1 WHY IMPLEMENT A SMART CARD SYSTEM?

Although smart cards themselves are more expensive than plain plastic cards, sharing a multi-application platform can reduce the overall expense of a card program. Issuers and application owners are expected to experience card issuance and administration cost savings from sharing overhead processes, including:[28]

- **Consolidation.** Processing of data and information supporting the core services is shared among the applications loaded on the card. This results in cost sharing and consolidation for application owners.

- **Data Collection.** The task of gathering and storing data common to multiple applications is shared among the application owners.

- **Personalization**. The card may be personalized and issued once for multiple applications, rather than needing a different personalized card for every application. This results in overhead cost savings to individual application owners.

- **Infrastructure Sharing.** For many applications, the infrastructure deployment or retrofit costs can be shared among application owners.

- **Card Reliability.** Smart card performance and durability have improved in recent years, resulting in improvements in cost performance figures.

Of course, these cost savings must be balanced against the benefits of issuing a single-function card and the upfront investment in infrastructure. When considering the costs of smart card implementation, agencies must consider the total baseline costs of doing business. If the study assumes the costs of cash and paper handling, fraud loss, and claims are free, then the cost study is inaccurate. Rather, the cost-benefit analysis needs to compute the full cost of the business process in the paper world versus cost in a multi-application smart card environment.

Cost savings, however, are only part of the picture. In assessing smart cards, agencies must understand their role in transforming business to electronic commerce and/or electronic government. If the agency is going to limp along with paper, there are less expensive alternatives to smart cards. Rather, smart cards must be considered within the context of their power to re-engineer business processes. Smart cards provide the following benefits:

[27] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

[28] Stephen Lee, "The Case for Multifunctional Smart Cards," in *Smart Card Technology International: The Global Journal of Advanced Card Technology*, ed. Robin Townend (London: Global Projects Group, 1996), 66-70.

- **Enhances Security.** A key smart card benefit is its ability to carry either a digital certificate or a biometric template to enhance authentication of the cardholder's identity. Smart cards provide the tools to enable more secure access to buildings, secure areas, and electronic systems. The smart card provides a secure token to hold the key pairs that enable the authentication of the recipient and originator of transactions across public networks, and if desired, that can be used to encrypt transactions.

- **Simplifies Access to Buildings, Meetings, Computers, Phones, Email, and the Internet.** By hosting PINs, biometrics, or digital certificates, smart cards allow the cardholder to have more convenient access to physical facilities and electronic systems. Smart cards carry the cardholder's identification with him/her wherever he/she goes. Individuals no longer have to remember multiple passwords or fill out redundant paper forms to gain access to buildings, meetings, communications, or systems. The reduction in staff time can be substantial considering the hours required to process all of the paperwork associated with these administrative tasks.

- **Consolidates Personal Identity Requirements.** Smart cards provide a single, central credential that is the individual's digital identity and that is the local agent of the issuer. This eliminates the need for individuals to carry multiple cards and to remember multiple PINs and login information.

- **Eliminates the Need to Write the Cardholder Name and Address Repeatedly.** Because the smart card can populate forms, it keeps the cardholder from having to repeatedly supply the same information in multiple locations, thereby streamlining application processes and reducing clerical time for multiple tasks.

- **Provides Private and Secure Access and Payments for Internet Services and Purchases.** One of the factors keeping agencies from moving to electronic transactions is the fear of loss of privacy and security for payments across the Internet. While consumer losses associated with credit card fraud may be acceptable, agencies conducting high value transactions across the Internet are particularly vulnerable. Those agencies most interested in moving to electronic commerce are most likely to need a mechanism to secure large electronic transfer of funds.

- **Enables Electronic Forms and Reduction of Paper Files.** Although many agencies are slowly moving to electronic forms, particularly in the administrative area, the need to maintain paper signatures for legal purposes makes redundant paper files necessary. By enabling non-repudiation, digital signatures are increasingly enabling electronic documents to replace these paper files, moving agencies closer to total electronic offices. Digital signatures are made transportable and more convenient by the smart card token.

- **Automates Accounting.** The use of the smart card enables end-to-end electronic purchasing so that accounting information can be transferred electronically. Administrative forms can be electronically completed by the employee and then easily transmitted to accounting systems. The ability to automatically populate back-end accounting systems saves substantial time and money.

- **Improves Employee/Vendor Convenience.** Employees are able to carry their data with them wherever they go, thereby having convenient access to data that is needed to populate necessary forms. Smart cards provide employees greater flexibility in using computer systems, allowing them to more securely access remote systems. Smart cards can also maintain demographic and medical data, making it less likely that employees will receive redundant services. The smart card is particularly appropriate for agencies that have a large percentage of traveling employees. If financial and travel applications are maintained on the card, employees have convenient access to purchasing capability when they travel. Additionally, vendors can more easily accommodate electronic orders.

- **Enables Significant Productivity Gains.** The use of a multi-application card eliminates the need to perform redundant card management processes for multiple cards. Card issuance and maintenance can be performed once, freeing staff for other activities. Additionally, card information can be kept in a single database, reducing the need to maintain multiple separate systems. Smart cards can securely hold multiple application usernames and passwords, providing the user with convenient access through a single PIN (or biometric) and reducing or eliminating the cost of help desk calls.

- **Supports Business Process Re-engineering.** Smart cards can help organizations achieve productivity gains if they are used to support the streamlining of business processes. The card can be used to share data across entities and to consolidate redundant processes. For example, the badging process can be re-engineered so that issuance of employee identification cards and population of the card with all access privileges (whether to buildings or systems) are combined in a single location and maintained in a single system.

- **Enables Secure Update of Legacy Databases**. By using the PKI certificates on the smart card, legacy databases can be PKI-enabled and access granted to only authorized people. Rather than carrying a lot of data on the smart card that now must be kept synchronized with a database, the smart card can enable direct, secure update of the database. Various Federal agencies have been exploring two different concepts of secure data sharing: network-based and card-based. Both concepts could be useful to Federal agencies in different circumstances, depending on the environment and the requirements of a particular program. For example, while some agencies have well-established network-based systems and would like to link these with other programs' systems, other agencies (e,g,, DoD) have a particular need for a portable, offline information carrier that is viable when telecommunications are not available. Both smart card-based approaches may have utility and save data sharing costs for the agencies.

    - **Web-Based Virtual Account**. The Virtual Employee Account is a web-based application that provides secure access to cardholder information from multiple legacy applications viewed through a web browser application. This application tests the concept of network-based data sharing. The card in this case carries a digital certificate that authenticates the identity of the employee seeking access to confidential records, common demographic information used across programs, and information about the programs in which a employee participates. The web-based application first verifies the identity and access privileges of the cardholder by checking the status of the digital certificate on the card and the card-based access privileges. Once the identity and access privileges of the cardholder have been verified, the application reads from the card the system record identifiers for the programs in which a cardholder participates. The application would then go to these legacy systems and pull specified data from the system and display it through a virtual employee account. Thus, the most up-to-date data from multiple legacy systems could be securely shared across a network. The virtual account could provide a variety of data including medical, financial, or personnel records.

- **Card-Based Employee Account**. In addition to the data described above, the card could also carry information necessary for circumstances in which network-based access is impractical. For example, such data may include a limited amount of emergency medical data. These data would be accessed offline through card readers at provider offices or, in the case of the DoD, in battlefield conditions.

Agencies evaluating the use of smart cards for employee identification should consider not only the cost of the cards, but rather the full cost of paper versus re-engineered smart card processes. Some agencies' business lines and missions may lend themselves to achieving economies from streamlining operations through smart card applications, while other agencies' business processes may be less likely to benefit from smart cards. Therefore, these costs should be evaluated within the context of the potential applications for which smart cards could be used within the specific agency performing the cost-benefit analysis.

2.5.2 RELATIVE MERIT OF SMART CARDS VS. ALTERNATIVE TECHNOLOGIES

A number of commercially available technologies can be considered in the design of a personal identification or credentialing system. Government agencies and private entities have adopted different combinations of identification methods and media for secure identification purposes. The General Accounting Office (GAO) has recommended that NIST continue its work on developing smart card interoperability specifications to include optical stripe media, biometrics and other technological advances. This section discusses the various types of ID technologies that are currently available and their relative advantages and disadvantages in the implementation of a privacy-sensitive ID system.

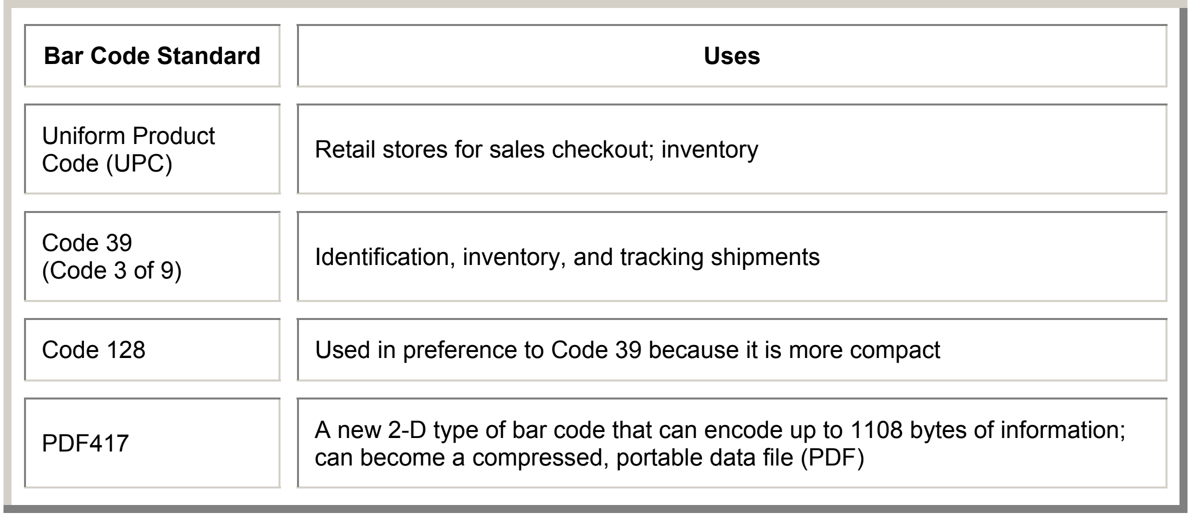
- **Credential Documents and Authentication Tokens.** In accordance with the Department of Homeland Security (DHS) Federal Protective Service and Interagency Security Committee on Federal Building Security, the standard Federal ID credential is required to contain a machine-readable credential. Security standards for Federal buildings require that the credential consist of an authentication token such as a contact and contactless smart cards and biometric technologies where indicated by Federal buildings of the stipulated security level.

- **Plastic Cards or Paper Cards.** Simple plastic or paper cards with printed visual identification information (e.g., individual name, address, photo) are used in numerous applications where information is visually verified when the card is presented for identification. Because visual identification is highly dependent on a security officer's ability to recognize images and relies more on individual judgment, visual identification is considered to be one of the least secure identification methods.

- **Bar Codes**. A bar code is an image of varying width lines (bars) and spaces that can be affixed to retail store items, identification cards, and postal mail to identify a particular product number, person, or location. The code uses a sequence of vertical bars and spaces to represent numbers and other symbols. A bar code symbol typically consists of five parts: a quiet zone, a start character, data characters (including an optional check character), a stop character, and another quiet zone. Bar codes can store personal information and can be printed on plastic cards. Linear bar codes are used to store simple alphanumeric data (e.g., in retail applications).

Two-dimensional bar codes can now store significantly more data in a small amount of space (up to 1108 bytes). Data is translated into a bar code and embedded on the card during the printing process. The card is then scanned by a bar code reader at the point of interaction. The reader uses a laser beam that is sensitive to the reflections from the line and space thickness and variation. Bar codes can be easily copied using a standard photocopier. This fact may prohibit the use of bar codes for some secure applications. Masking is a method that is sometimes used to cover a bar code to increase its security. Printing a bar code with a high carbon-content printing ribbon and then masking the bar code with a non-carbon black ink will prevent a bar code from being successfully duplicated but will still allow it to be read with an infrared wand or scanner. This method may increase a bar code's security somewhat.

Figure 9 summarizes barcode standards and the applicable barcode uses.



Bar Code Standard	Uses
Uniform Product Code (UPC)	Retail stores for sales checkout; inventory
Code 39 (Code 3 of 9)	Identification, inventory, and tracking shipments
Code 128	Used in preference to Code 39 because it is more compact
PDF417	A new 2-D type of bar code that can encode up to 1108 bytes of information; can become a compressed, portable data file (PDF)

Figure 9: Bar Code Standards and Uses

- **Magnetic Stripe Cards.** Magnetic stripes have been used on cards since the 1970s for a wide range of applications – from financial credit cards to transit cards to driver's licenses. The magnetic stripe on the back of an ID card is composed of iron-based magnetic particles encased in plastic-like tape. Each magnetic particle in the stripe is a tiny bar magnet about 20-millionths of an inch long. When all of the bar magnets are polarized in the same direction, the magnetic stripe is blank. Information is written on the stripe by magnetizing the tiny bars in either a north or south pole direction with a special electromagnetic writer, called an encoder. Identification information is written to the magnetic media during the personalization process and then read by swipe or insertion readers at the point of interaction. A new magnetic stripe standard for cards will provide more memory capacity than available with previous cards. The user data encoded on magnetic stripes can easily be copied and interpreted using a standard magnetic reader. The data can also be easily transferred to another card. This fact makes magnetic stripe technology most applicable for low security applications. New technology is available, however, that determines the magnetic "fingerprint" of a magnetic stripe card; by adding this as a component of the card data and verifying the fingerprint with a compatible reader, the magnetic stripe card can be made more secure.
- **Optical or Optical Stripe Cards**. Optical stripe cards are a proprietary static technology that relies on proprietary external equipment to read, write and process information stored on the compact disk (CD)-type material. It is recommended that optical stripe cards be kept within a

protective paper jacket or cover to reduce the damage to the optical storage material in normal use. Optical stripe cards use a technology that is similar to the one used to read and write CDs. Cards with an optical stripe use Write Once Read Many (WORM) recording technology, allowing data to be read and added, but not deleted or erased. Optical stripe cards have a relatively high non-volatile memory capacity (multiple megabytes) and are used in identification, health care, logistics management and other applications requiring storage of a large amount of data.

- **Smart Cards – Contact or Contactless Cards**. A smart card includes an embedded computer chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are used worldwide in financial, telecommunications, transit, health care, secure identification and other applications. Today's production microcontroller smart cards can store up to 128KB of usable data. Future versions will surpass this. Through the use of locking mechanisms and encryption, data stored on smart card chips can be made very secure. Smart cards can perform powerful complex operations within their secure internal computing environments including the ability to perform match-on-card biometric operations.

- **USB**. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to a computer without having to add an adapter card or even having to turn the computer off. USB supports a data speed of 12 megabits per second. This speed can accommodate a wide range of devices, including MPEG video devices, data gloves, and digitizers. It is anticipated that USB will easily accommodate plug-in telephones that use ISDN and digital PBX. Since October, 1996, the Windows operating systems have been equipped with USB drivers or special software designed to work with specific I/O device types. USB is integrated into Windows 98 and later versions. Today, most new computers and peripheral devices are equipped with USB. A different plug-and-play standard, IEEE 1394, supports much higher data rates and devices such as video camcorders and digital video disk (DVD) players. However, USB and IEEE 1394 serve different device types. USB security tokens are available that can be used to authenticate users to a computer or network (e.g., providing storage for usernames, passwords, biometrics or cryptographic keys).

The use of **biometric technology** is widely believed to be essential in any secure ID system design. As discussed in Section 2.4.5 - Biometrics and Smart Cards, biometrics are identification and authentication techniques based on the physical characteristics of a person such as fingerprints, hand geometry, iris scan or voice. Biometrics can be used with the card technologies discussed above (e.g., smart cards), where biometric information is stored on the card and then verified with the received biometric at the point of interaction. By securely recording and then checking an individual's unique biometric information (e.g., fingerprints, hand geometry, retinal or iris patterns, facial patterns or voiceprints), the system can validate the individual's identity. The verification process may be done by a smart card (i.e., with an on-card biometric match) or by a biometric-specific reader. Alternatively, a central database of biometric information can be used, with an online screening device. Figure 10[29] shows a detailed comparison of dynamic versus static ID technology with relation to memory and security.

[29] Russell, James, *Comparison of Dynamic versus Static Technology with Relation to Memory and Security*, MasterCard International, September 2003.

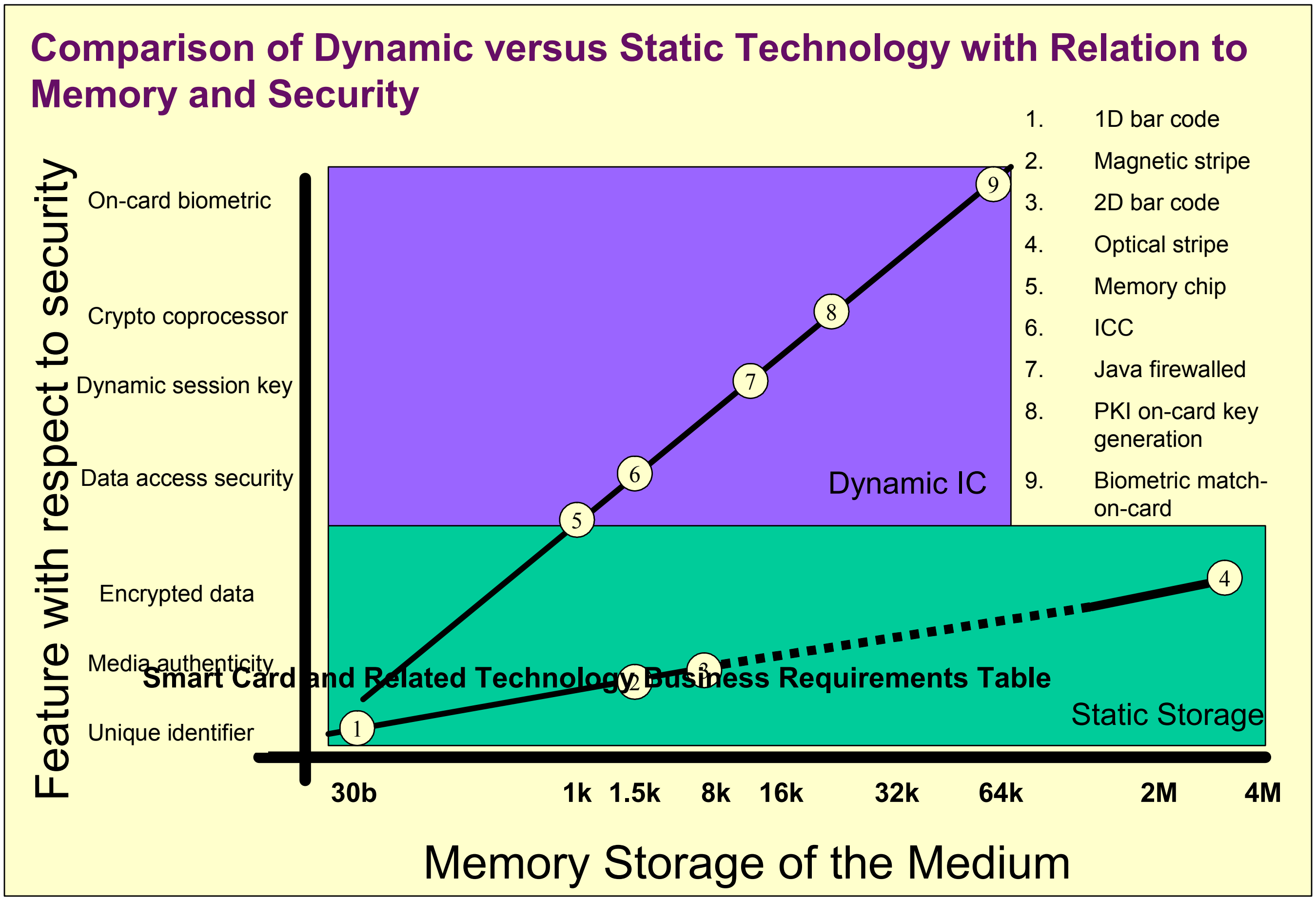


Figure 10: Comparison of Dynamic and Static ID Technology

Smart Card and Related Technology Business Requirements Table

The table below summarizes key business factors that may be considered when selecting a technology or media for an agency's smart card program. An "X" indicates that the technology supports or applies to the business requirement. Relative ratings (high, medium and low) are assigned for some business requirements to illustrate differences between technologies.

Business Requirements	**Technology/Media**								
	Bar Code 1D	Bar Code 2D	Magnetic Stripe	Optical Stripe	Memory Chip	Contact Chip	Contactless Chip	Dual Interface Chip	USB
Usage in new government ID deployments	**X**	**X**	**X**	**X**	**X**	**X**	**X**		
Manufacturers	Multiple	Multiple	Multiple	Few	Multiple	Multiple	Multiple	Few	Multiple
Post issuance modification			**X**	**X**	**X**	**X**	**X**	**X**	**X**
Support for logical access (LA) and physical access (PA)	Both - PA preferred	Both - PA preferred	Both	Both - PA preferred	Both – LA preferred	Both – LA preferred	Both – PA preferred	Both	LA Only
Cost of ID device	L	L	L	M	L	M	M	H	H
Cost of readers	M	M	M	H	L	L	M	H	N/A
Storage capacity	L	L	L	H	M	M	M	M	H
Security	L	L	L	M	M	H	M	M-H	M
Support for multiple applications	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Financial applications			**X**			**X**	**X**		
Standards support	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**
Support for multiple operating systems					**X**	**X**	**X**	**X**	
On-card biometric storage		**X** Select vendors	**X** Select vendors	**X**		**X**	**X**	**X**	**X**
On-card biometric match						**X**		**X**	
On-card key generation						**X**		**X**	

Figure 11: Smart Card and Related Technology Business Requirements Table

Smart Card and Related Technology Comparison Table

The table below depicts a variety of smart card specifications and requirements that are relevant to ID system applications as well as the applicable media/technologies. This table is not all encompassing but provides a general overview of how various media adhere to the current technical specifications and requirements.

MEDIA	SPECIFICATIONS/REQUIREMENTS															
	FIPS 140-2 (1-3)	Open Card Frame Work	ISO 7816	ISO 14443 A/B	ISO 10536	ISO 15693	GSC-IS 2.1	SEIWG 012	BioAPI V 1.1	FIPS 186-2	ANSI X9.31	ANSI X9.62	FIP 197	GP	Common Criteria V 2.1	EMV 2000
Bar Codes																
1 D																
2D																
Magnetic Stripe								X								
Optical Stripe																
Memory Chip			X											X		
Contact Chip	X	X	X				X	X		X	X	X	X	X	X	X
Contact-less Chip	X	X		X		X	X	X		X	X	X	X	X	X	X
Dual Interface Chip	X	X	X	X			X	X		X	X	X	X	X	X	X
USB																
125 kHz					X											

Note: An 'X' indicates that it is possible for the technology media to comply with the applicable specification/requirement but compliance is not guaranteed for every product within a specific technology media.

Figure 12: Smart Card and Related Technology Comparison Table

3. AGENCY IMPLEMENTATIONS

Goal: *Understand the characteristics and develop a "profile" of your individual agency that will impact whether or how you will implement a smart card.*

The decision to implement a smart card program may come from a multitude of sources. It may be in response to a federal mandate or it may be championed by the Chief Information Officer or the Chief Security Officer. A vital first step is the choice of a champion for the agency. Also though, it is essential to develop an integrated team to consider the options, scope, opportunities and impacts of the smart card program the agency develops. The team should include individuals representing the diversity of smart cards. Personnel from physical security, information security, business applications, network management, human resources and financial management are essential to the team. Other areas such as privacy and labor unions should not be overlooked. One of the most significant lessons learned in early smart card programs has been the need to incorporate a team that includes all the stakeholders including the program manager, physical access personnel, and information technology support staff. Through the development of the team, will come the knowledge and understanding necessary to assign roles and responsibilities for a successful program.

The GSA Smart Access Common ID contract has many options, and often the selection of one option affects another. Therefore, it is important that the agency develop a general profile regarding its requirements prior to completing one or more task orders. For example, if an agency requires strong security and encryption to be generated from the card, this will affect the chip cryptographic capabilities and memory capacity. Or, if an agency has the need for secure and authenticated exchange of information electronically, this will affect its choice of PKI services. Toward that end, Appendix F provides a questionnaire that will enable the agency to develop a profile of the agency type. Appendix G includes five "models" of agencies to provide examples for how to translate the profiles into a model. The creation of a good integrated team will ensure the profile is as accurate as possible.

3.1 Agency Smart Card Requirements

Prior to initiating a task order for smart cards, it is critical that each agency understand its own specific requirements and goals for the smart card platform. The technology procured must be driven by these goals and agency characteristics. While it is important that agencies consider future requirements when designing their card platforms, it is equally important that the program not incur unneeded expense to obtain technologies that are beyond the agency's basic implementation needs. The smart card program specifically aims to ensure maximum flexibility by accommodating a wide range of divergent needs across agencies. The GSA contract vehicle enables acquisition of a broad spectrum of platform capabilities and accompanying services. Because the contract meets such a wide range of needs, however, it is imperative that agencies be able to more narrowly define their specific needs within this broader context.

The first step in focusing on an agency's needs is to determine the goals for the card platform. Agencies should consider the following "big picture" questions before embarking on any further analysis:

- What are the primary goals that the agency is attempting to achieve through the implementation of its smart card platform?
- At what level (e.g., agency-wide, bureau/division, geographic area, campus, set of buildings, single building) is the employee identification card targeted?
- Is there a Program Management Office for the agency or Department? Are there other related smart card programs in development or production?

- Will the Department's card be required to work with a smart card program outside of the Department (e.g. DHS must coordinate efforts with U.S. Coast Guard's DoD issued CAC card)?
- What potential impact can smart cards have on the agency's core businesses?
- What potential impact can smart cards have on reducing the agency's costs?
- What potential impact can smart cards have on improving the agency's efficiency?
- What potential impact can smart cards have on improving the agency's security?

Key agency decision makers should participate in an initial goal-setting session. The vision, goals, and scope for the smart card project will provide a framework that guides all subsequent decisions about the card platform. All stakeholders sharing in the implementation of a multi-application card platform should be represented at this framework defining session.

Once the card platform analysis framework is in place, the agency can proceed through the agency questionnaire (in Appendix F) to help establish its own agency profile. Through answering the questions regarding specific characteristics and needs (i.e., How large? How important is security? Centralized or distributed?), agencies will build their profile. Agencies can use the agency profile to help differentiate among the various levels of technology and card capabilities offered and determine what actually will be needed for their own specific implementation.

The agency profile can be used to categorize agencies and develop representative models of smart identification card applications and solutions. These representative models provide a guide for agencies to see how technological and management choices can be derived from specified characteristics. Agencies can then determine the extent to which they share characteristics with or diverge from these general models. It is hoped that these models will provide a starting point to help agencies understand how to choose among the various alternatives and to adopt the technologies and applications that will best meet their business goals.

Agencies should understand that there are no "right" or "wrong" choices. Selecting a card platform will require trading off multiple factors and conflicting priorities. For example, what may be a logistically preferable solution may be cost prohibitive or may be inadequate to support security requirements. The questionnaire in Appendix F is intended to help agencies document and better understand their own needs and priorities, so that they are better prepared to make informed tradeoffs in selecting a card platform.

An agency profile is divided into 7 areas: security, current architecture, interoperability, size and geographic distribution, card management, applications, and resources. These are discussed in Appendix G. In each section of the appendix, relevant questions from the questionnaire are presented and the analysis surrounding alternative answers to the question follows.

3.2 Current Status of Smart Card Development of Major Users and Departments

3.2.1 INTRODUCTION

Smart card technology is a powerful enabling tool that can greatly improve the effectiveness and efficiency of modern government and industries. A smart card implemented as an ID credential can provide the basis for new levels of trust, more effective physical access to buildings and transportation, and more secure logical access to information systems with enhanced information assurance. With such systems, access to buildings and information systems can be much faster for trusted entrants, while much more effective in preventing unauthorized access. These benefits can be achieved through the use of full-featured life cycle card management systems that adhere to recommended enrollment, issuance, usage, monitoring and deactivation processes and link to identify proofing, background checking, liability and risk mitigation processes

Additionally, smart card technology helps to:

- Facilitate electronic commerce (by providing more secure authentication and non-repudiation),
- Reduce paperwork through PKI and the Internet,
- Decrease transaction and business process time,
- Provide strong system security and authentication,
- Improve business processes,
- Improve the security of physical access, and
- Improve the security of unclassified networks.

The integrated security, data management, and process improvement capabilities that are delivered by smart card-based systems streamline core business practices and result in an enhancement of overall business processes, an increase in customer satisfaction, substantial cost savings, and a better quality of life for cardholders. In order to provide some of the most effective end-to-end smart card solutions, agencies and industry can learn from each other and work with one another to focus on interoperability across the entire enterprise. Toward that end, many agencies in the Federal government are working to define common policy and standards for identity proofing and smart card implementation.

3.2.2 CURRENT AND PLANNED SMART CARD IMPLEMENTATIONS

Since the 1990s, the U.S. government has considered smart card technology and related chip-based technologies as a solution for improving the security for access to buildings and computer systems. The President's Budget for Fiscal Year 1998 called for adoption of "…smart card technology so that, ultimately, every Federal employee will be able to use one card for a wide range of purposes, including travel, small purchases, and building access." This strong guidance, plus guidelines and contracts put in place by the GSA has promoted the development of numerous smart card programs throughout government agencies, providing a wide range of benefits and services.

There are numerous smart card credentialing projects ongoing, including the Departments of Interior, Treasury, Homeland Security, Defense and State; the National Aeronautics and Space Administration (NASA); GSA; and the Transportation Security Administration. Examples of applications being deployed in smart card programs include:

- Secure physical access through turnstiles and card readers to buildings, secure areas and transportation.
- Secure logical access through card readers and proximity sensing devices to computers, networks, storage, phones, and PDAs (enabling virtual private network access, desktop security, network logon)
- Encryption and signing of emails and other electronic forms and documents
- Deployment platform for biometric-based authentication
- Support for PKI implementation or alternative authentication tokens
- Access to and protection of financial systems
- Property control
- Support for secure payment applications
- Secure information storage (e.g., emergency medical information, travel orders, human resources information)

This section discusses a few prominent agency smart card programs to highlight key applications and the breadth of smart card deployment. While the section is not meant to be all-inclusive, it is meant to present a summary of the efforts of several major users and departments. Figure 13 summarizes the status of U.S. government agency smart card initiatives. For a more complete list of current and archived U.S. government smart card projects, please go to http://www.smart.gov and click on 'Smart Data' or use the following direct link http://estrategy.gov/smartgov/smart_carddata.cfm. Appendix B also provides a summary of US government smart card initiatives.

Department of Defense (DoD). One of the most advanced smart ID card programs in the U.S. is the DoD Common Access Card (CAC), a smart card that will serve as the DoD standard identification and physical access credential as turnstiles are installed for machine-readable authentication and access at DoD facilities over the coming years. The card is currently used for secure authentication and network access. The card is issued to active duty military, selected reservists and National Guard, DoD civilian employees and selected DoD contractors. As of September 2003, DoD had issued 3.5 million smart cards on the way to over 4 million, a goal that they expect to achieve by Spring 2004. This 4.5 million serves all active military and reserves, their contractors and visitors. DoD has deployed an issuance infrastructure in over 900 sites in more than 15 countries around the world, and is rolling out more than 1 million card readers and the associated middleware. A key goal of the CAC program is to meet DoD's mandate to digitally sign all electronic mail and other electronic documents.

Future plans include: using the CAC for signing and encrypting email; expanding the number of portals capable of doing web-based e-business using PKI authentication tools; adding a biometric to the cards to provide three-factor authentication; and expanding the use of the cards for physical access by adding a contactless chip. Contactless chip pilots are underway and DoD will begin rollout in early 2004, using ISO/IEC 14443 Parts 1-4 with a FIPS-approved algorithm.

DoD is developing a comprehensive identity management system that provides strong authentication for identity credentials at the front-end, secure smart card credentials and strong identity binding to the back-end system using biometrics. DoD is working with industry on the Federated Identity Cross-credentialing System (FiXs)/Defense Cross-credential Identification System (DCIS) proof-of-concept project. This project implements an identity management and credentialing system between DoD and industry participants that have a need for employee identification and authentication as part of their joint working environment. An initiative is being pursued under the Federated Identity Cross-credentialing System to extend the cross-credentialing efforts to Federal agencies outside of DoD.

As the CAC identity credential is now in the final stages of issuance to all active military, DoD is beginning to concentrate on incorporating the CAC into many other applications as they are renewed, to exploit the benefits of machine-readability into other DoD applications.

DoD is also in the early stages of planning to serve other large communities that are closely tied to Defense, including the DoD military dependents, DoD recipients of health care services from the Tri-Care medical system, and veterans.

Department of State. The U.S. Department of State is in the process of implementing smart ID cards to function as an individual's identification card throughout the government enterprise. The Bureau of Diplomatic Security will issue smart ID cards for physical access to all U.S. Department of State employees, contractors, and affiliates who work within the Department. The Bureau of Information Resource Management (IRM), which oversees logical access, will use the smart ID card as a token for PKI. The Department of State is one of the first Federal agencies to use a smart card for physical access, as well as logical access and PKI.

Approximately 35,000 users will use the new card for facility access to State Department buildings. The smart ID cards and physical access readers adhere to the Government Smart Card Interoperability Specification (GSC-IS). The majority of Department of State users (80 to 90 percent) will use their smart ID cards to secure

PKI applications, including desktop security and encryption, secure email, and virtual private network (VPN) access. Future plans include integrating biometric readers for logical access and possibly physical access into sensitive areas. The State Department plans to store other data on the smart card, including emergency medical information, HR data, and travel orders.

Department of Homeland Security (DHS). DHS is establishing a common trust model across the enterprise, formally composed of 22 separate entities. The 22 DHS component entities (which include the Transportation Security Administration (TSA), Immigration Naturalization Service, U.S. Secret Service, and Coast Guard) have approximately 200,000 employees, including contractors. The DHS identification and credentialing effort will be implemented using a hybrid cryptographic smart card using a public key infrastructure for logical access and a contactless chip for physical access. The cryptographic chip will be compliant with Java 2.1 and Global Platform 2. The contactless chip will adhere to ISO/IEC 14443 Type A specifications. Authentication of the individual to the card will employ biometrics, with a PIN as a backup. These cards will be totally interoperable within DHS as well as with the U.S. Department of Defense smart card program and the NIST/GSA smart card specifications.

- **Transportation Security Administration.** TSA is mandated by federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system. The Transportation Worker Identification Credential (TWIC) is intended for each worker requiring unescorted physical or logical access to secure areas of the nation's transportation modes (maritime, aviation, transit, rail, and other surface modes).

  The TWIC will allow implementation of a nationwide standard for secure identification of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the TWIC to gain access to secure transportation sites. Each individual enrolled in the TWIC system will be positively matched to his or her credential via a reference biometric (or multiple biometrics) and will have undergone a standard background check.

  The program infrastructure carefully balances security, commerce, and privacy requirements. The TWIC is to be universally recognized so that workers will not require redundant credentials or background investigations to enter multiple secured work sites and will allow facilities to better manage site access. Additionally, the credential will have the capability to be used within a facility to meet multiple levels of secure access requirements.

  The TWIC system will contain sufficient technologies to be compatible with Government Smart Card Interoperability Specification while maintaining access to and within local facilities. This will enable the TWIC to leverage existing access control system investments, rather than require replacement of these systems at considerable expense. Additionally, the TWIC system will serve as the standard platform for future technology purchases at transportation facilities.

National Aeronautics and Space Administration (NASA). NASA is planning to implement a multi-application, multi-technology smart card program with a user base spread across the agency. The NASA smart card deployment will provide users with a single identification credential to use for visual identification, physical access control, and logical access control.

The first phase of the NASA smart card program includes adopting the GSC-IS v2.1 specification, which includes a specification for contactless smart cards to be used in physical access applications. The NASA smart card will include both contact and contactless proximity technologies. In the initial phase, the principal development activities will include engineering integrated solutions for current physical access control systems and integrating logical access control for multiple platforms including Windows®, Macintosh®, UNIX®, and Linux. A distributed-issuance, centralized card management system modeled after the DoD CAC RAPIDS stations and issuance portals will be deployed in the initial phase. New identification cards that include both contact and contactless smart card technologies are planned.

Food and Nutrition Service (FNS). In October 2003, the FNS completed the 'WIC Smart Card Interoperability Specification for Offline Grocer and Clinic Electronic Benefit Transfer (EBT) Systems' for the Special Supplemental Nutrition Program for Women, Infants and Children (WIC) Program. This program defined the card-to-reader interface for use in the implementation of an offline EBT system for the WIC program.

Department of the Treasury. The Treasury smart card implementation goal is to have a common smart card for every Treasury employee. The Department presents interesting challenges in that there are nine bureaus as well as the Departmental offices performing a variety of functions from manufacturing to international commerce. As of September 2003, the Department completed issuing cards to over 2,000 employees for use with PKI, biometrics, and physical access. Bureau involvement continues to increase. The Treasury smart ID card includes a 32K contact chip, Java operating system, and magnetic stripe and supports single sign-on (SSO).

Department of the Interior (DOI). The DOI is another smart card implementation effort incorporating the use of PKI for physical access interoperability. Interoperability, as described by DOI, is the ability for any agency to present their card at any reader and the reader will be able to read the published common data string (SEIWG). The DOI website will have a visitor's site that provides the ability to read the visitor's SEIWG and have authorization on the backend. A temporary visitor PIN will be PKI-encrypted, time-stamped (valid for meeting duration) and sent back to the visitor via email.

Smart Card Program	Sponsoring Agency or Department	Project Status	Expected Completion Date	Number of cards issued or planned	Applications Supported (Initial and Future)
DoD Common Access Card	DoD	Production	April 2004	3.5 million, with 4.5 million planned	• Physical access • Logical access • PKI applications • Ebusiness applications
Dept. of State ID	Dept. of State	Production		35,000 planned	• Physical access • Logical access • PKI applications • Secure data storage
Department of Homeland Security Employee ID	DHS	Pilot	Conclude pilot by Feb. 2004; implementation by May 2004	40,000-90,000 planned	• Physical access • Logical access
TWIC	TSA	Pilot		12-15 million planned	• Physical access • Logical access
NASA ID	NASA	Pilot	Conclude pilot by mid 2004	90,000 planned	• Physical access • Logical access
GSA ID	GSA	Production	End of 2003		• Physical access
Dept. of Treasury ID	Treasury	Planned			• Physical access • Logical access (single sign-on) and PKI applications

Smart Card Program	Sponsoring Agency or Department	Project Status	Expected Completion Date	Number of cards issued or planned	Applications Supported (Initial and Future)
Dept. of Interior ID	Dept. of Interior	Planned		5,000 cards issued of 100,000 total planned	• Physical access using PKI
US Passport	Dept. of State	Planned	Pilot by Oct. 2004; implementation by end 2005	7.1 million passports issued per year	• Contactless chip with data and biometric for identity authentication
Entry/Exit	INS	Pilot			• Physical access
VA ID Card	Veterans Affairs	Planned	Sept 2007	500,000 planned	• Physical access • Logical access • PKI applications
Department of the Treasury Electronic Treasury Enterprise Card (E-TREC)	Treasury	Production	Completed Sept 2003	2000	• Physical access • Logical access with biometrics
Dept. of Treasury Cash Management Projects (EZpay, Marine Cash, Eagle Cash, Navy Cash)	Treasury	Production	Complete	1 million issued	• Epurse for payment on bases and ships and on overseas bases

Figure 13: Summary of Current and Planned Government Agency Smart Card Programs

3.2.3 IDENTITY MANAGEMENT SOLUTIONS

Smart cards are being implemented as a critical component in new government identity management solutions. Issues in identity management, however, go beyond issuing a secure ID token and include system and process requirements for:

- Determining the organization's risk profile and developing the appropriate security policies and procedures that mitigate the risks.
- Specifying the data that is collected and used for identity proofing and identity verification.
- Verifying the authenticity of the data collected.
- Specifying how identity information is kept secure and private.
- Developing the overall trust model that is needed, both within an organization and with other organizations who will be part of the identification system.
- Proving identity (i.e., ensuring a person is who they say they are) and developing the processes and procedures for enrollment.
- Developing an architecture and selecting technologies that meet the identity system requirements and accommodates legacy systems.

Choosing the appropriate technology solution should map to the overall organization requirements. For example, the perception is that smart card technology, biometrics, and/or public key infrastructure can assure strong identity authentication; however, when each of these technologies is used alone they may not be totally adequate for organizations that need the strongest security. The security of physical and logical access solutions can be optimized by using multi-factor authentication, where one factor is a secure ID token (the smart card), a second factor is a PKI certificate or PIN, and a third factor is a biometric.

An example program using smart cards and PKI is the DoD Common Access Card. The ***Defense Information Systems Agency (DISA)*** has teamed with the ***Defense Manpower Data Center (DMDC) and the Access Card Office (ACO)*** to integrate PKI on the DoD smart card, also known as the ***Common Access Card (CAC)***. Some custom software development was necessary for the PKI program. As of October 2003, there are three certificates on the CAC:

- Identity credential
- Email credential to sign email
- Email credential to encrypt email

The CAC and PKI certificates will be used for various applications such as the ***Defense Travel Service*** and the ***Army Online Portal***. The medical community previously relied on Federal Express to deliver MRI and x-ray films, but now images are sent electronically and use certificates. The goal is to have all DoD applications use the CAC and certificates. One of the major upgrades that DISA and the PKI program are working on is to enable users to go to a kiosk to get new certificates or reset passwords. The next step is to allow users to get new certificates at their desktop.

As discussed earlier, biometric technology uses physical characteristics of an individual to authenticate an identity. A biometric such as fingerprint can be used to identify an unknown identity or to verify a claimed identity of an individual. Biometric technology helps to support non-repudiation and can provide a high level of security. Multiple biometrics relying on voice, fingerprint, facial scans, or other physiological or behavioral characteristics can be used for identification. The advantages of biometrics are that they:

- Offer positive proof of identity, and
- Cannot be borrowed, lost and/or forgotten.

As technology and standards develop, many agencies are considering the incorporation of biometrics into their smart card programs. One such program is the ***Transportation Worker Identification Credential,*** mentioned previously. The TWIC will use a biometric to tie all technologies together. An upfront background check will be required and a reference biometric as well as an operational biometric will be obtained to ensure that persons requesting access are who they claim to be. On a similar note, the ***Centers for Disease Control (CDC)*** are considering using biometrics for identity authentication in high-risk areas. They will store the biometric on a server and not on the card. Additionally, the ***Department of State*** is exploring the use of a facial image as the primary biometric for identity authentication in the passport project.

As of calendar year 2003, biometrics are collected enterprise-wide in ***DoD,*** but are not currently used for physical or logical access. The lack of a privacy policy and standards relating to the collection and use of biometrics for identity management is currently creating a barrier for using biometrics in smart card implementations. The ***Federal Deposit Insurance Corporation (FDIC)*** is considering the use of biometrics, but feels they are not ready due to the lack of standards to regulate an effective and secure smart card implementation. Many agencies are waiting for biometric standards development from the ANSI B10 and International Committee for Information Technology Standards (INCITS).

3.2.4 USER SUPPORT

Although the size of current and planned smart card implementations vary, a common theme expressed by many government agencies is that a smart card implementation must be transparent to the end users (i.e., cardholders), or at least have minimal impact on them. Agencies expressed that the technology used to implement and sustain a smart card program is important, but equally important, if not more so, is educating and supporting the end user. As such, the end user experience is critical and training sessions and information awareness initiatives are recommended by several government agencies. Many government agencies have developed training materials for users. For example, the ***Department of Interior*** has developed an informational DVD for user education. The DVD serves three main functions: 1) it educates employees; 2) it educates managers; and 3) it provides a technical overview of the smart card system.

For many government organizations, a smart card program implementation brings with it a cultural change. Users need to be taught how to use their cards. Specifically, users will need to know such things as: what functions their cards will perform (physical and/or logical access); how the cards interact with the readers; how secure their cards are (i.e., not susceptible to identity theft); and how many chances they will get to enter their PINs before their card is locked. Agencies that have implemented smart card programs or that are considering an implementation realize that not all users will be satisfied and that, at some level, will push back. Agencies stated that every attempt should be made to educate and inform users of all facets of the smart card implementation. Since end users are so important, agencies that are issuing smart cards need to make every effort to educate and inform individuals prior to, during, and after an implementation.

In most cases it is not possible to support all of the functionality that users or departments may want in a smart card. Smart card programs should include a sufficient amount of time to write a User Requirements Definition document. Many agencies expressed that a document of this type can significantly aid in user support by clearly defining the user impact of a smart card implementation. The document should be dynamic and clearly define and outline all of the requirements of a smart card implementation as they relate to the end user. The User Requirements Definition document should define program features, such as the population that will be receiving the card, the functionality of the card, the security of the card, the method for issuance, as well as other specifications defined by the agency that will be administering the smart card program.

Ease of use and user functionality is very important. Some examples of user support are: ease and speed of initial card/credential issuance, the ability for users to reset their PINs via a web interface, and the ability for users to perform post-issuance functions easily and in a timely manner.

If users are not satisfied with initial issuance of a smart card, subsequent deployments can experience severe push back by the end users. Therefore, every attempt needs to be made by the issuing agency to make initial issuance as effective as possible. Many organizations will be issuing smart cards to a diverse and disparate population. In such circumstances, the agency should provide issuance capabilities that are close to the user. An example of this can be found in the ***Department of Defense***, within the ***U.S. Department of the Navy (DON).*** The Navy has three remote issuance trailers (Mobile Card Issuance Labs) that are used to issue smart cards to individuals. The benefit of these trailers is that they can travel to the users in order to issue cards, thus reducing the time required by the user to receive their cards and generally improving the issuance experience of the end user.

Users forgetting their PINs can be a major expense in a smart card program. Generally, users have a preset number of opportunities to enter their PIN before a card is locked out of the system. And, if users forget their PIN, a trusted agent must reset it for them. A host of agencies, including ***DMDC***, ***DISA***, ***the U.S. Department of the Army, and NASA,*** are currently researching ways that users can reset their PINs via a web interface. Not only would developing a web interface for PIN reset save money, it would save time for the end user because they would not have to go to an issuance station to reset their PIN.

The discussion above illustrates some examples of how agencies can support the end user. All agencies realize that user support is a major factor in the success of a smart card implementation and have stressed the importance of ensuring proper communication, education, and functional support before, during, and after a smart card implementation.

3.2.5 SUMMARY

Numerous government agencies are implementing secure identification systems, which require new policies, processes, architectures and technologies both within their organization and with organizations that will need to work with the new identification system. Smart cards are a critical component of these new systems and are being used in conjunction with PKI and biometrics to provide secure multi-factor authentication of an individual's identity. New ID systems are both in production and in pilots. Lessons learned in early ID system implementations can provide other agencies with an excellent starting point for new programs.

The deployment of Federal Enterprise Architecture (FEA) is in the early stages, carrying with it requirements that affect Federal smart card projects. The FEA requirements direct that Federal smart card programs are described as a standardized architectural component. Smart card deployments are expected to be more effective and efficient as the standardized architectural components for Federal smart card programs are developed.

4. KEY DECISIONS

Goal: Make sound key decisions as they apply to the procurement and implementation of your agency's smart card initiative.

Some key decisions must be made prior to the development of the task order under the Smart Access Common ID contract. The models found in Appendix G of this document provided examples of how sample agencies, with the characteristics described, made some of these same decisions. This chapter discusses these decisions and presents information to help your agency successfully decide on key issues, thus enabling a seamless procurement and implementation of a smart card platform.

4.1 Deciding on a Smart Card

The very first question your agency will face is whether or not it makes sense for your agency to migrate to a smart card-based employee identification card at all. The following section discusses the salient characteristics of a smart card platform that can help you evaluate the practicality of this card technology for your agency.

Smart cards are inherently more complex and expensive than other technologies used for an employee identification card. Agencies considering smart cards will find them more costly than other card types. However, smart cards have specific capabilities that other technologies do not provide, including security features that help to thwart identity theft, which has become a growing concern. Smart cards, if implemented properly in an overall identity management scheme, can provide a higher level of assurance of an individual's identity than can just a "flash pass". Therefore, to evaluate if your agency should implement smart cards, you must determine which smart card characteristics provide sufficient added value to justify the expense and opportunity costs associated with implementation. Card capacity is finite, although it is improving. Card implementers should know that they may not be able to accomplish all of the possible options.

- **Portability.** One of the most fundamental smart card characteristics is its data portability. By adopting smart cards, an agency is able to maintain data on a form factor (i.e., the smart card token) that can be transported to any physical location. The smart card portability allows data to move with the client between providers. Data on the card can be accessed wherever and whenever it is needed. Therefore, agencies with a mobile workforce that needs to transport information to various locations should consider smart cards. Smart cards can provide various levels of security to ensure data integrity. When considering the portability of data you should also consider how the data is going to be protected from illicit interception, modification or substitution. Smart cards are designed to address all these concerns.

  - **Information Sharing.** Smart cards enable the sharing of data across disparate systems. The smart card can move information between applications. Data can be written to the card from one legacy system at the first provider's office and be read from the card to update a legacy application in the second provider's office. Agencies that work closely with other organizations and need to frequently share data across systems are good candidates for smart cards.

  - **Processing Capability.** Smart cards are able to perform data manipulation and calculations in a variety of locations. Also, smart cards can securely maintain data on the card. The processing capability of a chip can be used to protect the data on the card. For example, the card can require a PIN to access data or use encryption to protect data and to enhance the security of the information. Agencies that need to be able to transport, store, process and update data securely would find smart cards useful.

- **Identity Authentication/Information Security.** As a result of the ongoing problem of identity theft, the fact that agencies are moving increasingly to electronic commerce and/or electronic service delivery, and the growing use of web-based applications, it is becoming increasingly important to verify the identity of the transaction originator and receiver. By providing a mechanism for secure identity authentication (through a digital certificate and/or biometric template), the smart card provides a means for the cardholder to identify himself/herself in cyberspace. Agencies that are contemplating the use of electronic transactions with other agencies, businesses, or the general public should consider the smart card as a token to secure these transactions.

  - Identity authentication has also become increasingly important for physical access to facilities, buildings, and bases. Because of the storage capability of smart cards, a biometric template or an electronic image can be stored on the card and then checked against the individual attempting to gain access to the facility. When the smart card itself is used to perform the one-to-one identity verification rather then external equipment, a high degree of confidence and security of the credential's verification is achieved.

- **Automatic Forms Population.** Most government agencies spend substantial amounts of time processing an abundance of paper forms. Moving to electronic form submission could save significant staff time. The smart card provides the capability to populate forms with demographic data carried on the card, thereby reducing the redundant capture of data.

- **Multi-Application Enabler.** Because of the technical limitations of other card technologies, card platforms have traditionally supported single applications. By leveraging the robust technology associated with smart cards, more than one application can reside on the card platform. Some examples of applications are time and attendance, physical and logical access, and e-purse. Agencies that have a number of related card-based applications, as well as programs willing to share a platform, should consider smart cards.

- **Updateable Applications.** Other card technologies require static applications. Once a card is issued, any changes require the card to be re-issued. Smart cards built on an open platform are dynamic and can accept new applications and data structures even after the card has been issued. Agencies that contemplate frequently changing needs and addition of new applications should consider smart cards.

- **Support for Multiple Technologies.** Smart cards support different technologies and interfaces including contact and contactless RF. Further, chips can be embedded in proximity cards and can also be combined with magnetic stripe or bar code technologies. Biometric and PKI technologies can also be added to the smart card functionality for a layer of added security. Agencies with different legacy systems that require different technologies should investigate multi-technology cards.

- **Cost Sharing.** Agencies have the potential to experience substantial economies of scale when implementing multi-application cards. Rather than have each program pay for card issuance, management, and customer service, multiple programs can share these fixed costs. The cost of the applications residing on the chip card platform can also be shared among the programs using the application. Thus, although smart cards themselves are more expensive than other types of cards, the total implementation cost could be absorbed by multiple organizations or agencies.

4.2 Determining the Applications, Capabilities and Options of the Card Platform

Once your agency has determined that it is interested in a smart card-based employee identification card, the next step is to select the applications and platform capabilities that will best suit your agency's needs. The agency profile, described in detail in Appendix G, provides an excellent starting point to identify your agency's requirements. By examining the models in Appendix G, the reader can begin to understand how the characteristics of their agency mandate widely disparate approaches in different environments. The sections that follow explain the key decisions your agency must make in order to plan its smart card platform.

4.2.1 TECHNOLOGY CAPABILITY

An agency's business requirements, as well as its existing technical environment, will drive the technical capabilities required by its platform. There are three main areas that will impact the size of the chip, the types of technologies included as part of the platform, and the supporting hardware and/or software needed to use the card:

- Existing legacy environments;
- PKI strategy; and
- Biometric strategy.

4.2.1.1 EXISTING LEGACY ENVIRONMENT

The technology of your agency's current physical access, logical access, property management, and financial systems will have a significant impact on the card technology selected. A key issue to be decided is which legacy systems will be retained and which will be replaced. If, for example, your agency has legacy physical access control systems, it is important to decide whether or not the agency requires backward compatibility with these systems. Your agency has several options in this area.

- **Replace the Legacy Systems.** This option does not require any backward compatibility and allows your agency maximum flexibility in selecting a technology for physical access control. However, if your agency operates from many different locations throughout the country and the world, this may be a project to undertake a step at a time. Although this option is the most expensive initially, it may provide cost savings in the future.

- **Maintain the Legacy Systems but Swap Out Old Readers.** This option allows the legacy physical access control systems to remain in place, but by replacing card readers and modifying the legacy system software, the old system can be adapted to use the new card technology. This is less expensive than full system replacement, but there are certain difficulties that can arise when pursuing this option. For example, it can be a complex and time-consuming process.

- **Use Multi-Technology Cards to Address Backward Compatibility.** In this option, some legacy systems are replaced by the chip standard, but many of the legacy physical access control systems within an agency are left in place. Alternatively, all legacy systems may be left in place and the card platform may use the chip for logical access control only and continue to use the technology of the existing physical access control system. The smart card platform can include different technologies to allow the card to be read by different legacy systems. For example, if an agency had multiple proximity and magnetic stripe systems, but wanted to move to a contact chip standard, the agency may opt for a card platform with a contact chip embedded within a proximity card as well as have a magnetic stripe on the back of the card. This option avoids the expense of replacing legacy systems, while providing the agency with a migration path to a standard environment in the future. However, it requires a more expensive multi-technology card platform.

- **Retain the Old Systems and Issue Multiple Cards.** This option assumes that the older systems will be retained and that separate physical access cards will be issued in addition to the smart card employee ID card. Although this option is the least expensive in terms of the system replacement costs, it defeats the purpose of a multi-application employee identification card. In some cases, the long term costs of issuing and maintaining multiple cards can be greater than the cost of moving to a single card platform. The economies to be gained by sharing the cost of card issuance and management, as well as maintaining an integrated card management database are eliminated with this option. Further, the employee convenience of a single card is also lost.

The decision on the approach to achieving backward compatibility with existing legacy systems, whatever they are, will impact the configuration of the card platform. If, for example, an agency decides to replace the legacy physical access control system with a contactless chip system, the card may need to be a hybrid or dual-interface card to support both contact and contactless interfaces. Alternatively, if the agency decides to replace some systems but retain some of the old systems in different buildings, the card platform will have to include multiple technologies (e.g., contactless chip, magnetic stripe, bar code) to accommodate the range of options in different buildings. The decision on what type of system will be implemented can also affect what card readers and software will be implemented.

Similar decisions will have to be made for legacy logical access control systems, property management systems, financial systems, and any other existing agency systems that must provide data to or receive data from the new card system. If other types of legacy systems are linked to the card platform, interfaces will have to be built. The cost of these interfaces should be considered in the implementation strategy of the card platform and requirements for integration services should be included in the task order.

One important consideration in this area is the degree of security that must be deployed. Older physical access technologies (such as magnetic stripe or proximity technologies) are very weak in security terms. They are easily broken into or compromised by such tricks as cloning a card or replaying the card communications. Smart cards can offer much higher degrees of security to counter typical attacks of the legacy systems. Agencies should consider requiring the use of security practices that are commensurate with the asset being protected, and not assume that the legacy system in use meets today's increased security demands.

4.2.1.2 PKI STRATEGY

Your agency's PKI strategy will substantially impact the configuration of the card platform. The infrastructure and man-hours needed to support PKI can be significant in terms of cost and labor, therefore a number of questions must be answered about the PKI strategy before writing your agency's task order. The most basic question is whether or not your agency has need for PKI. Agencies that have completed the agency profile and have identified that they possess one or more of the following characteristics should consider PKI:

- Requirement for a high level of security for its facilities and systems;
- High percentage of employees performing high-value electronic purchase or monetary transactions;
- Interest in the use of electronic forms;
- High percentage of employees who often travel or telecommute, requiring remote access to your computer system;
- High percentage of employees who transmit and/or receive data across open networks;
- High percentage of employees who transmit confidential or high-security data or information through email;
- Interest in providing services or information to citizens via the Internet;
- Interest in providing services or information to businesses or other government agencies via the Internet;
- Need to encrypt transactions sent over open networks or via the Internet;
- Need to exchange clearance information with other agencies; and
- Need to exchange other confidential information (e.g., visa information, immigration information, passport information) with other agencies.

Once your agency has determined that it needs PKI, the next question is how to provide PKI services. PKI services can be provided entirely in-house, totally through outsourcing, or with a combination of the two approaches. Providing PKI services in-house requires substantial resources including: staff; a trusted computing environment to generate certificates and house the certificate repository; and substantial hardware and software to perform enrollment, certificate issuance, verification, and revocation. Generally, only those agencies with the highest level of security needs and that already have secure computing environments will find a total in-house implementation strategy cost beneficial and practical. Agencies using the in-house approach will have to decide whether to build their own PKI system or to procure a “turnkey” solution from a PKI vendor.

Agencies choosing to outsource their PKI must determine the level of outsourcing. Some agencies may choose to outsource the entire PKI operation including registration, certificate issuance, certificate verification, and certificate maintenance (e.g., suspension, revocation, and renewal). Other agencies may decide to outsource the certification authority (CA) functionality and customer service, while performing registration authority functionality in-house. Still other agencies may opt for a vendor-supplied “turnkey” system staffed by agency personnel. The PKI strategy can be customized to fit the individual situations within the agencies, depending upon the required level of security, the availability of in-house staff resources, the agency’s ability to secure hardware and software, the availability of facilities to house a certificate repository, the degree of geographic dispersion for enrollment, and other factors that are identified by the agency that is implementing PKI.

The agency’s PKI strategy must also address the issue of enrollment and how it can most effectively be handled. Some agencies will opt to perform local, in-person identity proofing to enable employees to come to a convenient location to show documented proof of their identity. Other agencies will require in-person identity proofing, but set up a centralized registration authority location to which employees would be referred. For agencies with less stringent security requirements, a centralized online registration process could be setup in which participants register for a certificate online and activation information is sent via the mail or another "out-of-band" procedure to verify the registrant's address. Finally, some agencies may decide that no identity verification is needed for their own employees, so that the certificates may be issued automatically during the employee ID card issuance process. The agency's level of security needs, degree of geographic dispersion, and available resources should all be considered when determining its enrollment strategy. The chosen enrollment strategy, in turn, will influence the equipment and software that must be acquired for the platform.

The final issue centers around the degree of interoperability required among different agencies in recognizing each other's digital certificates. As PKI has evolved in the Federal government, there has been a movement from totally disparate PKI systems to more interconnected systems. The Federal government has been researching and developing ways in which one credential can be recognized by several different agencies. PKI is one factor in this development. Figure 14 shows the path along which PKI within the government has been evolving. In planning PKI strategy, your agency should determine where along the spectrum—from closed to totally open—its needs lie. The business line and missions of some agencies will require little need to exchange certificates with other agencies, while others will require interoperability not only with other Federal agencies, but also with commercial partners.

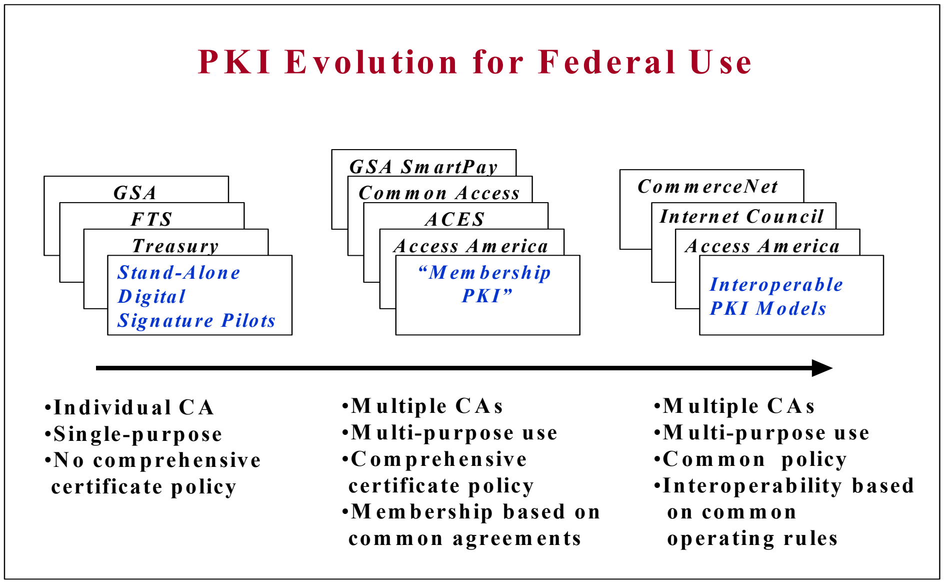


Figure 14: Federal PKI Evolution

Initially, a number of standalone digital signature pilots, with an individual CA, supported distinct government-only applications. Many agencies will choose to initiate PKI implementations in this closed environment. This approach offers far less complexity in that only a single CA must validate digital certificates — the CA that issued the certificate. It also requires far less sophisticated equipment and processes for certificate validation. Similarly, no interoperability agreements or certificate policy must be put in place.

In the next phase, a set of government-sponsored "closed" PKI models have evolved in which a set of designated participants exchange certificates. In this phase, multiple CAs participate in government (and potentially commercial) applications. The growing complexity of this type of implementation demands a comprehensive certificate policy that allows public and private sector participants to agree on the policies and procedures that will form the basis of their "closed membership" PKI. Within these closed systems, cross-certification must occur between the various CAs. To achieve interoperability among the defined participants, consistent business practices are needed, as are contractual relationships that define the roles and responsibilities of all of the parties. In such an environment, a framework is needed to ensure that all necessary elements of policy are in place so participants can agree upon common workable procedures and practices. Agency's whose business requires interaction with a limited number of partners, whether those partners are other government agencies or commercial entities, are likely to be interested in this "membership" PKI model. These agencies must develop interoperability agreements and operating rules among themselves. They must also acquire the hardware and software needed to enable cross-certification between different CAs.

As PKI evolves to more complex interoperable models, the discrete certificate policies of the closed membership PKIs must begin to converge. Agencies that have deployed different PKI models must be able to achieve cross-certification (i.e., interoperability) across their models. To do this, they must agree on a common framework and a common set of standards and rules. While one solution may have been acceptable within a closed environment, different solutions may need to emerge to accommodate the varying needs of increasingly diverse participants. Interested agencies must work together to establish solutions to policy issues that support varying models, so that similar certificate policies can be developed to provide the basis for interoperability. In this stage, an "open but bounded" PKI emerges, in which agencies may exchange certificates with a broader range of governmental and commercial partners.

In the final phase, a universal PKI, a common certificate policy and CA standards will be critical to allow numerous CAs to interact. While the need for standardization will be particularly acute in such an environment, the diversity of players will make such standardization increasingly difficult to achieve. The challenge will be to incorporate the needs of several agencies with different PKI implementation schemes into one agreed-upon standardized policy. Together, these interested agencies must achieve consensus on dynamic operating rules upon which common business practices can be built. Agencies providing electronic commerce solutions to their employees and/or electronic service delivery to the public that require certificate validation across a broad range of CAs will need to evolve to this totally open PKI. In this environment, hardware and software such as a certificate arbitration module will be needed by agencies to properly route certificate validation transactions. Comprehensive interoperability agreements will also be required.

Another set of decisions centers around the digital signature algorithms that the agency is to use. Two commonly used algorithms are RSA and the Digital Signature Algorithm. Another technology available is elliptic curve technology, which does not require a co-processor; this technology is increasingly popular because it can be implemented on a less expensive smart card. Similarly, the format of the X.509 certificate may vary from implementation to implementation. The number of fields used in the X.509 certificate can impact the size of the chip needed for the card. Such decisions, which can affect the memory size and characteristics of the chip, can influence your agency's selection of a card and/or affect the card specifications included in your agency's task order.

Only after these key decisions have been made will agencies be able to formulate their comprehensive PKI strategy. Once that strategy is in place, agencies will be in a better position to develop their card platform requirements to support PKI. Finalizing PKI requirements is essential prior to issuing your agency's task order.

4.2.1.3 BIOMETRIC STRATEGY

As with your agency's PKI strategy, your biometric strategy will substantially impact the configuration of the card platform. A number of questions must be answered about the biometric strategy before writing your agency's task order. The most basic question is whether or not your agency has a need for biometrics. In many cases, PKI and biometrics may be used for the same identity authentication purposes. For example, agencies may choose to use a contactless chip for perimeter control that requires quick throughput, while adding biometrics for access to special areas within the building that require added levels of security. Agencies with several of the following characteristics should consider biometrics:

- Requirement for a high level of security for its facilities and systems;
- Requirement for a strong mechanism for identity authentication;
- High percentage of Sensitive Compartmentalized Information Facility (SCIF) areas within the facilities;
- High percentage of employees who work with confidential or high-security information;
- High risk of hacker attack on agency systems; and
- Significant adverse consequences if systems or facilities are compromised.

Once your agency has determined that it has valid uses for biometrics, the next question is what biometric to select and what criteria to use to make that selection. The following is a list of biometrics, described in greater detail in Section 2.4.5:

- **Fingerprint Scan.** This is a convenient, relatively low-cost biometric, generally considered non-intrusive by employees. It may have a negative connotation, however, because of its association with law enforcement.
- **Hand Geometry.** This is an accurate, relatively non-intrusive biometric. However, there is currently no standard template used with smart cards.
- **Facial Recognition.** This biometric is captured through the use of a video/digital camera. There are several different methods for facial recognition so there is no standard template.
- **Iris Scan.** The iris is a robust biometric but presents challenges for image capture. Iris image capture is generally considered non-intrusive because this method merely takes a picture of the iris.
- **Retina Scan**. Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. Because of the method of image capture, retina scan is considered much more intrusive by users than many of the other technologies.
- **Voice Recognition.** Voice is a very convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access so it is particularly popular for logical access control applications. However, voice recognition is subject to replay attack and can easily be fooled; as such, it should only be considered for recognition of the speech and not for voice identification of the speaker.
- **Signature.** Signature identification is an inexpensive biometric solution and is popular in document authentication applications that have traditionally used written signatures. The major technological hurdle for signature identification involves differentiating between the parts of the signature that are consistent and those that vary from time to time.
- **Others.** There are currently other types of biometric methods that are in different states of maturity and development.

A number of factors must be considered by agencies in selecting the right approach to use in biometric authentication. It is critical that agencies understand the application, the user base, and the characteristics of the biometric device itself. Agencies must also consider the conditions under which biometrics will be used. Finally, agencies must also plan what fallback authentication methods, such as passwords or tokens, will be instituted when biometrics are not available (e.g., for persons with disabilities). When choosing among biometrics, agencies should take into account user, implementation, and product considerations, as recommended in the *Guidelines for Placing Biometrics in Smartcards*.[30]

User considerations include the following:

- **Public Acceptance.** Collection of biometric information may be the subject of privacy concerns among the target audience. Among the public, certain biometrics engender a greater perception of privacy invasion than others do. There are also cultural and religious factors that have to be considered.
- **User Acceptance.** Both public perception and degree of intrusiveness can impact user acceptance of biometric devices. For example, while retinal scans may have greater accuracy than other biometrics, the invasiveness of the capture device has resulted in public reluctance to routinely use this biometric.
- **Target Clientele Characteristics.** Some biometric verification products may have better characteristics for a given target audience. For example, race and gender, occupation, age, and color of eyes can affect the error rate and success of certain biometrics.
- **User Difficulties.** Some populations have difficulty using certain biometric capture devices. Difficulties may be based on alignment in the image capture area or characteristics of a given target population.
- **Ease of Use.** The scanning method, false non-match rate, and speed of a product can greatly influence user acceptance. Less intrusive biometric systems are more likely to be successful.

The following implementation issues should be considered by the agencies:

- **Enrolled Image Quality.** Enrollment image quality is very important to achieve high operational performance. Feedback on poor enrollment quality can be important to a successful implementation. Balancing software enrollment feedback mechanisms with an understanding of acceptable quality by the enrollment officer may be important for implementing a particular biometric.

- **False Match/False Non-Match.** The False Match Rate (FMR) is the rate at which the system incorrectly recognizes an individual as a valid user. The False Non-Match Rate (FNMR) is the rate at which a valid user is rejected by the system. The FMR and FNMR are inversely related, meaning when the FMR goes down the FNMR goes up and (vice versa). Therefore, system administrators must balance the FMR against the FNMR to ensure adequate security while still being convenient for users.

- **Uniform Testing.** There is a need for a uniform or standard testing approach to ensure that FMR and FNMR are calculated uniformly across products so that agencies can use these rates to assist in the selection of products.

- **Circumvention.** No biometric system is 100 percent foolproof. Certain biometric systems are more vulnerable to being compromised by individuals wishing to defeat the biometric system. Therefore, when

[30] National Security Agency, Central Security Service, *Guidelines for Placing Biometrics in Smartcards*, Version 1.0, September 11, 1998, p. C-2-7.

choosing which biometric system to implement, agencies must be aware of the risks and benefits associated with each.

- **Cost.** The cost of implementing a biometric system may profoundly affect an agency's choice of which system they will implement. While the costs associated with implementing biometric programs generally are falling, the cost of building the infrastructure can be a barrier for many agencies. Standardization, user acceptance, and technology development are having a positive effect on biometric pricing. Consequently, it is important to ensure that modularity at the application interface is in place to allow interchange of commercially developed hardware components. This will allow agencies to take advantage of positive pressure on product pricing in the commercial biometrics market.

- **Template Storage.** The size of a template and the number of templates may be a factor for agencies selecting biometrics. For example, multiple templates may be needed to achieve the necessary levels of accuracy, driving the amount of storage needed by agencies. Multiple templates may influence the viability of card storage and/or processing capabilities.

- **Computer Resources.** The complexity of matching algorithms may vary from product to product. Currently, there is no standardized algorithm for biometric devices. Agencies are more likely to consider biometrics that have a reasonable performance characteristic using a workstation with a medium range processor.

- **Calibration/System Performance.** The complexity of the calibration effort needed to support accurate use of a biometric may affect the viability of the biometric for an agency. The frequency and intrusiveness of periodic adjustments needed to ensure correct reading must also be considered.

Agencies may have to contemplate the following product considerations when selecting a biometric to use with the Smart Identification Card:

- **Applicable Standards.** Many biometric solutions use their own proprietary algorithms and processes. The implementing agency must ensure that the biometric solution that they implement follows applicable standards to the greatest extent possible.

- **Processing Time**. The time required to scan a live image, process the data into a template, and verify the result may vary from product to product. This time component may be used by agencies to differentiate among biometric products. The maximum processing time to scan, process the image, and verify it against a biometric should be 1 second.

- **Biometric Upgrade/Obsolescence**. The ease with which a given biometric product can be updated or improved over time may impact an agency's selection. As many biometric vendors are start-up companies focused on establishing profitability, it would be prudent for an agency considering the deployment of a biometric system to evaluate the financial status of the vendor. This is suggested as a means with which to protect the agency's biometric system from technology obsolescence in the event that the vendor ceases operations.

Once your agency has determined what biometric solution(s) satisfies your needs, the next question is how to provide biometric services to the end users. Biometric services can be provided entirely in-house, totally through outsourcing, or through a combination of the two approaches. Agencies can opt to purchase their own biometric system and operate it in-house. In this case, the hardware and software are purchased from a vendor, but the agency staff provides all services (including verification of attribute certificates if this approach is used by the agency). Providing biometric services in-house requires substantial resources including: staff trained in the use of biometric equipment; a trusted computing environment to generate attribute certificates and house the certificate repository; and substantial hardware and software to perform enrollment and template creation, capture, translation, and verification.

Agencies can also opt to totally outsource the biometric system. The easiest approach for an agency is to contract for turnkey biometric services. In this case, the agency contracts not only for the equipment and the software, but also for the services required to operate the system including taking live scans in the enrollment process, maintaining the biometric database (if applicable), and assisting with instances of false matches. In a combination situation, the agency can, for example, rent equipment but use its own staff to enroll employees and take live biometric scans.

Another decision is whether to perform centralized or decentralized enrollment. This issue concerns not only the place of enrollment but also the timing of enrollment. If enrollment is performed locally, card personalization and distribution can be performed over-the-counter, while if it is performed at a central location, the template must be downloaded to the card issuance facility. Local enrollment is often faster than centralized enrollment, but requires the purchase of more equipment.

Perhaps the most controversial issue surrounding biometrics is how to provide a secure means to bind the biometric to the smart card and to ensure that the biometric is properly attributed to the correct individual. Although a variety of techniques are available to create this binding, the Smart Access Common ID contract vehicle suggests the approach presented in the *Guidelines for Placing Biometrics in Smartcards*.[31] This approach advocates placement of authentication information, including the biometric template in an attribute certificate (i.e., the "biometric certificate") on the Smart Identification Card when the user is enrolled in the system and issued the card.

The attribute certificate can be retrieved by any system component or application to authenticate the user after a mutual authentication protocol has been successfully completed. The system component or application verifies first the signature of the certificate, and then the authentication information via the means specified in the certificate (depending on the type of biometric template contained in the certificate). An attribute authority must be established to support the creation and maintenance of authentication certificates. At an agency's option, the same authority may or may not create both the public key certificate and the attribute certificate.

Although the use of the attribute certificate to bind the biometric template to the smart card is clearly the most secure means of implementing biometrics, it also requires substantial overhead to maintain the attribute authority, perform attribute certificate validation each time the biometric is used, and manage the attribute certificate revocation process. Because of its substantial cost, some agencies may choose to implement their biometric projects without the use of the attribute certificate. The degree of security required and resources available should guide agencies in choosing between these options.

The choice has significant implications, however, for the card platform. If an attribute certificate is to be used, the amount of chip memory required will be greater to accommodate the certificate on the card. More importantly, the agency must procure attribute authority services and/or the hardware and software to create certificate requests, route the transactions, and generate, verify, and maintain the certificates.

[31] Ibid. p.C-2-7.

Only after these key decisions have been made, will agencies be able to formulate their comprehensive biometric strategy. Once that strategy is in place, agencies will be in a better position to develop their card platform requirements to support biometrics. The biometric requirements must be completed before your agency's task order can be issued. Additionally, agencies must be aware that there could be a number of potential privacy, personal, religious, cultural, and legal issues associated with the use of a biometric. These types of issues should be fully investigated prior to implementation of a biometric.

4.2.2 SAMPLE APPLICATIONS

The range of potential applications, in addition to physical and logical access control, available to agencies using smart ID cards is substantial. Included within the Smart Access Common ID contract vehicle are the following options:

- **Property Management.** A substantial amount of time is currently spent on obtaining and presenting property passes when an employee takes a laptop computer or other agency assets out of a building. Assets that must be managed include computer equipment, telephones and telecommunication equipment, credentials, arms, automobiles and other agency-specific equipment. A chip-based application provides the capability to enter, update, and delete asset information from the employee's card. This asset information can then be manually read and verified by a guard when the employee enters or exits a building. Alternatively, an agency can place RF tags in assets to be read automatically when the employee passes through a portal.

- **Exchange of Clearance Information.** Much time is spent exchanging clearance information between agencies for employees who must attend meetings or visit other agency facilities. In this situation, the use of the Smart Identification Card as a portable carrier of clearance information may prove to be the most secure and least expensive option. The designated security officer of the home agency can load, date, and digitally sign clearance information on the employee's card. At the receiving agency, the guard can verify the security officer's digital signature, read the clearance information, and match the information with a visitor request generated by the receiving agency employee. If all of these validations are successful, the visiting employee is granted access. At the agency's option, the data on the chip can either be used to create a temporary visitor's card or be uploaded to the physical access control database so that the visiting employee's card is activated to work in the receiving agency's system. This same functionality can be adapted for use of non-employees (i.e., contractors) who must visit government facilities on a routine basis.

- **Rostering.** The rostering application allows data residing on the Smart Identification Card to be retrieved, date and/or time stamped, and transferred to a database that is then used to generate a variety of specialized reports. The rostering application is used not only to retrieve and format data, but also to provide positive proof of attendance. It can be used to track meeting attendance and generate a meeting roster, track usage of meal plans for food services, or verify building occupancy in emergency evacuations.

- **Medical.** The medical application allows basic medical and insurance data to be stored on the card and read, when appropriate, by authorized providers. Additionally, the medical application can be used to populate claim forms.

- **Training/Certification.** The training/certification application allows data about training experiences and job-specific certifications to be entered on the card. Managers can read the card and obtain a view of the employee's training history and licenses or certifications.

- **Electronic Forms Submission.** By combining the use of data maintained on the card with the ability to digitally sign an electronic form, the Smart Identification Card provides the foundation to populate and submit a wide range of standard administrative forms used by virtually all Federal agencies. The electronic forms submission application can be used by employees in multiple agencies to complete, sign, and submit personnel transactions (e.g., SF52, Thrift Savings Plan Elections, Bond Elections); requests for personnel earnings and benefit statements; travel requests and vouchers; training requests; medical claims forms; and other administrative forms.

- **Electronic Purse.** Electronic purse functionality may be required to support a number of applications. It is anticipated that agencies could use the electronic purse to make low value payments to their employees for imprest fund replacement, local travel reimbursements, and transportation subsidies. Employees may use the electronic purse for automated fare collection, vending machine purchases, retail purchases, and parking payments.

- **Credit/Debit.** Some agencies may choose to add existing government credit card applications (including purchase, travel, and fleet) to the Smart Identification Card. A magnetic stripe would be used to access information through an online system for these commercial credit applications. Optionally, a commercial debit capability can potentially be added to the card.

Additional applications (including transportation, library, and agency-specific applications) can also be requested by agencies to customize their platform.

Conclusion

A number of factors will affect which applications an agency chooses to implement. A key determinant is the agency's line of business. Certain applications are more relevant to one agency's line of business than another. For example, an emergency medical application is more useful to an international agency with employees who travel extensively than it might be for a smaller, domestic agency. The importance of security is yet another factor. Agencies with higher security will be more likely to need property management, exchange of clearance applications, and encryption and less likely to adopt financial applications on the card. The required degree of interaction across agencies will determine the practicality of several interagency applications such as property management, exchange of clearance information, and electronic forms. Finally, available resources will constrain the selection process.

4.3 Key Agency Profile-Driven Decisions

In summary, the results from the agency profile are meant to provide a baseline from which the implementing agency can make decisions about their smart card implementation. This profile is intended to help agencies make the key decisions that will drive the card platform and the services that are required under the Smart Access Common ID contract vehicle. The profile helps to highlight the priorities of the agency, and how these often time-conflicting characteristics can be combined to determine where the agency lies within the following spectra:

- **Office vs. Agency-Level Implementation.** One of the first, and most crucial, decisions in planning the card platform is the scope or level (office, facility, campus, metropolitan area, bureau, division, or department) at which the card is to be issued. The answers to many questions in the agency profile depend upon this implementation perspective. It is critical that the administrative level and scope be determined prior to any other planning activities, as it may affect many other decisions. Once the level and scope are decided, the card platform should be coordinated with any agency-wide requirements and/or standards.

- **Low Security vs. High Security.** A second critical characteristic of an agency affecting its card platform is its level of security. Generally, agencies with lower security requirements will be able to implement less-complex card platforms. These lower-level security agencies are unlikely to need biometrics or PKI and can implement a less complex and less costly card platform.

- **Single Location vs. Multiple Locations.** The complexity of the implementation will vary substantially depending on the number of locations. This factor will also affect whether localized or centralized card issuance is desirable for an agency. For single location implementations, interoperability may not be a factor unless the agency wants interoperability across other agency locations and/or external government agencies. Local card issuance is clearly the most convenient approach with a single location, but becomes increasingly resource-intensive as the number of locations increase.

- **Decentralized vs. Centralized Card Management.** Agencies with few facilities or facilities that are within close proximity of each other generally will find decentralized card management more convenient than centralized. As the size, level of geographic dispersion, and complexity grows, agencies may find that central card management becomes more manageable and less expensive. However, other factors may intervene to swing the agency from one end of this spectrum to another.

- **Outsourced vs. In-House Card Management.** Small agencies implementing card projects with limited levels of complexity or very large agencies with extremely high security needs are most likely to opt for in-house card management. Once again the level of security may impact this decision, as agencies requiring the highest levels of security may be reluctant to relinquish control of their card platform. Agencies with limited staff, equipment, and facilities are far more likely to outsource their card implementations.

- **Stand-Alone vs. Interoperable*.** Agencies that are self-contained have far less concern with backward compatibility and standards than agencies that require a high degree of interoperability. In the context of the Smart Identification Card platform, interoperability is interpreted to mean the ability to read from and write to cards and conduct card-based transactions across multiple products and agency implementations. The degree of interoperability, as well as whether interoperability needs to occur across multiple agencies, a limited number of partner agencies, or with the private sector, influences an agency's interest in and approach to PKI, legacy system integration, and open versus closed financial applications.

- **PKI vs. No PKI.** Agencies that are self-contained, have low security needs, and are not actively moving toward electronic commerce and/or electronic service delivery are less likely to have a need for PKI. Those agencies, however, that have a high security level, are interested in interoperability, and are looking toward implementing Internet-based applications for their business partners or the general public will be more likely to be interested in PKI.

- **Biometric vs. No Biometric**. Agencies that have lower level security needs, limited Internet transactions, and are at low risk for sabotage are less likely to want to invest in biometric devices. However, those agencies that have a high security risk, have substantial need to verify their workers identity, or must protect confidential data are more likely to spend the resources required to move to biometrics.

- **Standardization vs. Customization*.** Each agency confronts unique circumstances and supports diverse technical and organizational environments. Because of this diversity, mandating a standard platform is unrealistic. The Smart Access Common ID contract vehicle purposely provides a menu of products and services from which agencies can assemble a Smart Identification Card platform that, at once, can operate across agencies, yet meet the unique needs of each agency. The trade-offs that may need to be made between flexibility and interoperability are likely to affect the ultimate configuration of an agency's card platform. To some agencies, interoperability may be critical, so they will seek to adhere as closely as possible to a "standard" platform. Other agencies may view interoperability as less important, and assemble a highly customized platform that is less likely to function seamlessly with other card platforms. Thus, some agencies may elect to build their platform from standard components based primarily on mandatory bid requirements, while other agencies may concentrate on assembling a variety of optional requirements.

- **Privacy.** For any agency that is considering a smart identification card implementation, data privacy should be a major concern and focus. Implementation of a smart card platform has inherent privacy issues associated with it. These issues include defining exactly what data will be stored on the card, determining by what means data is placed on the card, and defining how that data is secured. Every effort must be made to maintain the integrity of the user's data on the card. Many agencies will find it helpful to conduct privacy and risk assessments in order to identify any risks that may arise during a smart card implementation. The depth and breadth of these assessments should be determined by the implementing agency. At a minimum, the three concerns reference above should be addressed and the agency should also conduct a Privacy Impact Assessment according to the E-Government Act of 2002.

*** It is important to note that there is momentum in the Federal government toward a common credential that would be accepted throughout. This momentum is not expected to subside, thus agencies considering implementation of a smart card platform should give primary consideration to an interoperable, standards-based system.**

To assist those agencies for which interoperability across the government is a high priority, GSA recommends a set of "standardized" card configurations that use prescribed components based on the level of security required. There is a continuum from lowest security card to highest security card. The capabilities, storage, and cost of the card and infrastructure are likely to increase proportionally to increasing security requirements. While agencies may select from a range of products that best meet their individual needs, they must do so with the thought of its impact on interoperability and available resources. Those agencies with lower security requirements, or to whom interoperability is not as important, may be satisfied with lower-end cards. However, a card with the capability to store digital and/or biometric certificates (and the requisite infrastructure to validate these certificates) may be needed to take advantage of the emerging Federal public key infrastructure (FPKI) to achieve government-wide interoperability. Thus, the configuration of the Smart Identification Card system will vary substantially from agency to agency depending upon the card management approach, card personalization and issuance procedures, card capabilities and applications, and technical environment selected by the agency.

Conclusion

Prior to initiating the task order, it is highly recommended that agencies complete the agency questionnaire, analyze the agency's profile based on questionnaire responses, and make decisions on the key issues described above. The results of these analysis activities will provide a framework for achieving consensus on the specifications for the agency's customized card platform. Once this framework is in place, the agency can begin writing the task order.

5. PLANNING & IMPLEMENTATION ISSUES

Goal: Make practical decisions, plan the card platform, and develop procedures for implementing the smart card at your agency.

Even before the task order is in place, planning must begin for the implementation of the card platform. A range of issues must be considered in this planning process. Technical issues will arise when planning how the card platform will be integrated with the existing technical environment. The existing technical architecture could constrain the design of the card platform and potentially impact the requirements included in the task order.

Funding arrangements must also be considered in the planning process. A preliminary budget is needed prior to the writing of the task order. Arrangements or Memorandum of Understanding must be put in place if the cost of the card platform is to be shared across agency departments, programs, or external agencies. If multiple programs or offices are to fund the card platform, the funding allocation formulas should be specified in interagency agreements.

Similarly, organizational roles must be defined to ensure that the multi-application platform can be properly managed and that interagency agreements are in place to define roles and responsibilities of all of the participants, both government and contractor. Many of the initial multi-application smart card pilots suffered because inadequate attention was paid to the management and organizational structure. The smart card platform may bring with it totally new ways of doing business. Organizations that heretofore had no interaction may have to work closely together to maximize the efficiencies introduced by the smart card platform.

The following sections introduce a range of issues that may arise in a multi-application card environment. For the implementation to be effective, these concerns must be addressed by all participants, to ensure that the potential solutions meet the needs of the wide range of stakeholders in this diverse card platform. It is the intent of this section to provide practical advice on some of the challenges that an agency may encounter as it goes through the implementation planning process for the Smart Identification Card platform.

GSA's Center for Smart Card Solutions is available to assist Federal agencies with smart card projects. The Center has technical experts with extensive knowledge of smart card applications and experience in implementing and evaluating smart card projects. The Center can assist Federal agencies in using GSA's Smart Access Common ID contract which is the only government vehicle offering interoperable smart card products and services. The Center can work with other Federal agencies in tailoring smart card solutions for their specific organizational needs. The Center also helps agencies to design solutions using smart cards for physical access and logical access, as well as for other applications, and can assist agencies in gaining the best value from their uses of the Smart Access Common ID contract vehicle.

5.1 Technical Issues

Prior to the issuance of the task order, the scope of the project must be determined. Although a Requirements Document exists for the Smart Access Common ID base contract, the specific requirements of each agency must be documented prior to the issuance of the task order. Agencies are encouraged to contact the GSA Center for Smart Card Solutions for development of their agency specific needs. A general conceptual design of the system is needed prior to the issuance of the task order. Once the task order is awarded, the system design must be finalized based upon the winning contractor's proposed design solution and the components of the card platform actually procured.

The existing technical platform for the participating entities must be studied to determine the constraints that will exist for integration of the card platform with the legacy environment. For example, if an agency is going to integrate its new employee smart card with its legacy physical access control, logical access control, and property applications, the agency must determine the characteristics of these legacy systems, consider what technologies must be supported to create backward compatibility, and design the interfaces with these systems.

Before the card platform can be implemented, it is critical that the agency have a system design. The system design should present the basic components of the card platform and how these components interact with each other. The system design should include:

- **System Overview.** This topic provides a general overview of the major components and interfaces of the system.

- **Functional Description.** This topic describes each system function.

- **System Components.** This topic provides a description of the hardware and software components of the system. It describes both the hardware and software for the workstations, host systems, terminals/controllers, card personalization and issuance components, customer service components, kiosk components, data center, and other aspects of the overall system**.**

- **System Architecture**. This topic describes both the overall system architecture, as well as architecture for each individual site. It should include diagrams to depict the configuration of the hardware components and the telecommunications infrastructure to be used to connect these various components.

- **System Interfaces.** This topic includes a description of the components and functionality of each of the system's interfaces. The specific data transmitted between systems will be specified, as well as the communications protocols to be used to accomplish the transmission of data.

- **User Interface.** This topic describes the way the user interacts with the system. This section will contain general descriptions of screens and menus, and other aspects of how the user accesses the system.

- **Databases/Data Structures.** This topic includes a description of all databases used in the various components of the system and characterizes the structure of these databases.

- **Hardware/Software.** This topic describes all necessary system hardware and software.

- **Security.** This topic describes the system characteristics and procedures to ensure adequate overall system and transaction security. It also will describe how privacy concerns will be addressed.

A sample conceptual architecture is provided in Figure 15 below. This diagram is meant only as an example, to illustrate the components of a typical configuration. While the example architecture assumes in-person registration and issuance, bulk personalization, and separate PKI service providers (i.e., certificate authority and/or attribute authority, many other approaches will be used by the agencies. Different approaches will affect the overall arrangement of the card platform architecture. In this diagram, an integrator assembles photo, biometric, and digitized signature data from the enrollment workstation, access privileges from the physical and logical access control systems, and demographic data from a legacy personnel database. The integrator aggregates data from these separate systems into a single account setup file that is sent to the central card management system. This aggregated file is then sent to the bulk card personalization equipment. The card personalization system is able to extract public keys from the card (i.e., key pairs are generated on-board the card prior to distribution), route the keys to the certificate authority, and receive certificates to load onto the card. Once the card has been personalized, the completed cards can be sent back to a local office for distribution (or mailing) to employees. A diagram that incorporates the options selected by the particular agency in question, such as the one pictured below, should be constructed as part of the card platform design to illustrate the selected card issuance process, as well as the required hardware and software.

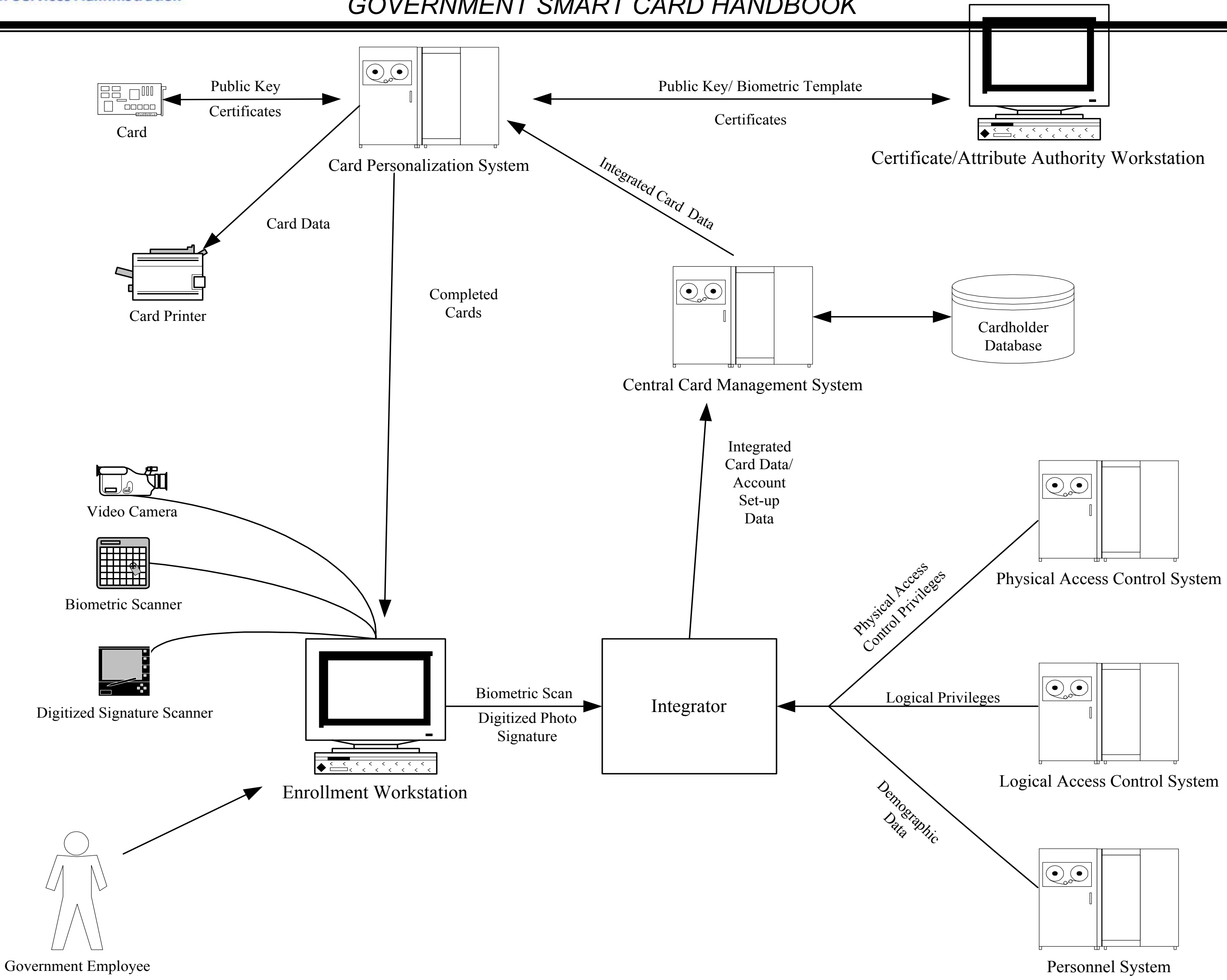


Figure 15: Sample Conceptual Architecture

Once the configuration of the system has been determined, a key part of the system design includes the development of specifications for required hardware and software. The specific hardware and software required depends upon how the agency plans to perform card issuance and personalization, provide customer service, and manage the PKI or biometric infrastructure. The required solutions will determine the necessary functionality of the smart card and, in turn, the card will determine the specifications needed to support the requirements of the design, as well as to address interoperability concerns both across agency divisions and with other partner agencies with which the card-issuing agency requires interoperability. It is the intent of the Smart Access Common ID contract vehicle to ensure that all components of the card platform support an open architecture.

The card design is yet another technical aspect of the project that must be planned prior to the implementation. Both the physical design of the card — the arrangement of the card face including placement of the agency seal, employee photo, and digitized signature (or other characteristics selected for the card surface) — and the allocation of chip "real estate" must be individually specified for each agency's implementation. The card design should consider the selective and economical addition of future applications while minimizing the need to re-issue the card base.

The procuring government agency should select the applicable card specifications to which the vendor must conform. While there is some room for agency discretion, these card specifications generally should be in conformance with the guidelines contained in the Government Smart Card Interoperability Specification – Version 2.1.[32]

Physical card security features are designed to deter counterfeiting and/or lifting of data from the magnetic stripe, employee picture, bar code or chip. The card should be made of tamper-resistant materials such that any attempt to alter or reuse the card should be apparent to the naked eye. The card design should incorporate security features, including full color printing, a hologram, ultraviolet ink, fine-line printing, shadow photo and/or other features that protect against counterfeiting.

A number of additional security issues that affect the Smart Identification Card platform should be addressed in the planning process. Both the characteristics of the card itself and the infrastructure that issues, supports, and uses the card must be considered. According to Section 7.1 of the Government Smart Card Interoperability Specification: "The Government Smart Card infrastructures may include, but are not limited to, those involved with Government Smart Card design; analysis; fabrication; testing; initialization; distribution; encryption key and digital signature key material generation, distribution, and loading; issuance to cardholder; cardholder data uploading to operational systems and to repositories; cardholder data downloading from repositories to replace damaged or lost cards, audit collection and analysis; commercial system interactions such as point of sale terminals, vending machines, and automatic teller machines; and eventual card replacement, retirement, and disposal."[33]

For each component of the Smart Identification Card infrastructure and each card application, an Information System Security Policy (ISSP) should be generated by the implementing agency's information technology security office. The ISSP is used in the development of the Smart Identification Card security requirements, evaluation of alternative system design architectures, and assessment of the security effectiveness of the system design, and implementation of the Smart Identification Card applications.

The security required for the card may vary, depending on the sensitivity of the data and applications on the card chosen by a particular agency. Based on the necessary security levels for a particular agency

[32] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

[33] *Government Smart Card Interoperability Guidelines*, Op. Cit., p. 34.

implementation, the smart card design should include a graded set of access control security mechanisms and enforce access privileges to card files as specified by these mechanisms. At the discretion of the agency, access control mechanisms may involve a PIN, a password, biometric protection, public key-based cryptographic protection, or other approved mechanisms.

- **Privacy.** While not subject to the regulations protecting classified data, each agency's smart card system must be subject to privacy protection. Because the smart card system will contain individual identifying information, its implementation may require that agencies obtain a Privacy Act clearance. As a part of the issuance process, the agency should be vigilant through campaigning and posted information, state clearly that Privacy Act information is being collected, and describe how it will be used for the process. Agencies should be aware that all applicable Federal privacy laws and regulations will apply to protecting the data maintained in the smart card and system components and should plan accordingly. Additionally, agency-specific regulations that protect the confidentiality of data maintained on the smart card and system components must be considered when planning agency specific security measures, as these regulations may vary widely. As the functionality of the smart card may vary from agency to agency, there may be corresponding variation in the levels of sensitivity of data and applications on the smart card. In their card platform design, agencies should put in place a mechanism to address this variation in sensitivity levels. Such a mechanism should be capable of supporting varying levels of protection for public and confidential data.

A final technical issue critical to the planning process for the smart card platform is the integration of the card system with existing legacy systems. Initially, agencies must perform exhaustive analysis to determine which systems to interface to the card system. This may include systems for a variety of functions within the card platform such as obtaining card personalization data (e.g., from personnel or physical access control systems), providing customer service (e.g., from existing Automated Response Units), or acting as a component of a card application (e.g., interfacing the card platform with a legacy physical or logical access control system). Once the applicable legacy systems have been identified, the agency must perform a detailed analysis, resulting in an interface planning document that determines how the interface is to occur (e.g., through file transfer, real-time), what data must be included in the interface, and who should be responsible for creating the interface. If the vendor or integrator is to be responsible, the interface tasks must be specified in the task order. On the other hand, if individual programs or offices within the agency are to build the interfaces, the schedule must be carefully stipulated in the task order and the project work plan so as not to impact the schedule of the system implementation.

Careful and considered planning can mitigate the myriad of technical problems that may arise in the implementation process. "Lessons learned" from early pilots can provide useful assistance, but agencies must remember that each implementation is somewhat unique. What has worked successfully in one implementation may not necessarily be a viable solution in another environment. Consequently, GSA's Center for Smart Card Solutions, composed of seasoned experts in the smart card field, has been assembled to provide consultation and assistance to agencies using the Smart Access Common ID contract vehicle as well as other contract vehicles. The Center can provide advice on many of these issues. Another source for "lessons learned" is the GSA sponsored Smart Card Managers Forum, which meets every two months to share information on government deployments and for presentations on developments in the industry.

5.2 Management and Organizational Issues

For many agencies, moving to a multi-application card platform will be an entirely new experience, which will require a fresh approach to planning many aspects of the card implementation. While agencies have had experience with card management before in a variety of areas, their old procedures may need to change in the multi-application environment. New policies and procedures will be required, as will new management structures for a multi-application card platform.

5.2.1 CARD MANAGEMENT

Before the task order can be written, it will be important to determine the organizational arrangements associated with the card platform. When more than one organizational unit shares the card (e.g., badging, facilities, information technology, training), arrangements must be in place to determine which entity is to take responsibility as the prime issuer. When different entities have separate applications, a number of additional issues arise. Additionally, if an entity shares a card platform across bureaus or with another agency entirely, the organizational issues become even more complex.

Card Platform Ownership

A critical debate centers on who owns and controls the card in a multi-application environment. A basic conflict exists between the card issuer and the application owner or administrator as to who should have primary responsibility for the applications on the card. Who determines how limited card "real estate" is to be distributed and what applications can be put on the card? Should the card issuer, the application owner, or the card user have ultimate control over what is on the card and how the card is to be used? Related is the question of who "owns" the cardholder and what rules should be exercised in multi-jurisdictional applications. Card ownership is even more complex when cards are to be shared between the public and private sectors.

Related to the card ownership issue is the question of who should set up new accounts when there are several application owners sharing a card. Associated with the creation of these new accounts is the related issue of how to maintain account information. Should the card issuer maintain this information centrally in the card management database, or should it be decentralized to the various application owners? If it is decentralized, will security and backup procedures be jeopardized?

Ownership, access, and usage rights to card information must also be considered. Who "owns" the information associated with a given application and how is access to this information controlled? Who is responsible for updating the information on the card and for the accuracy of this information?

Card ownership and liability are areas in which there are both management and legal perspectives that must be considered. From a management perspective, there must be a mechanism put in place that assigns responsibility for card reconciliation to identify and manage duplicate and fraudulent cards. The same "ownership" issue relates to liabilities: is it the card issuer or the application owner that bears the liability and administrative responsibility for lost and stolen cards? These issues become particularly challenging when financial applications reside on the card platform.

Designation of "ownership" affects customer service and security. Who bears the responsibility for arranging and funding customer service facilities, as well as system and card security? Who determines what is adequate security and how best to implement this security?

Many decisions fundamental to the management and organization of a multi-application card platform rely on the designation of card owner and the roles to which the card owner delegate responsibilities for card operation. Both the designation of card owner and the subsidiary roles needed vary depending on the characteristics of the card implementation. No matter who is named as card owner, the card owner is generally designated as the entity that has control over the following decisions:

- Which applications can reside on the card;
- How chip space (i.e., card "real estate") will be allocated;

- What rules will be exercised to govern the usage of the card;
- How costs will be allocated among platform participants;
- How card security will be implemented and who will be responsible for ensuring it;
- How the card will be issued; and
- How liabilities for lost and stolen cards will be assigned.

Because of the complexity inherent to a multi-application environment, the conceivable options for designating a card owner are many. While the conceivable options are substantial, the practical options for the smart card environment are far more limited. The following subset of options can be considered for this particular environment:

- **Government-Owned.** In this option, the government would "own" the card and potentially "rent" space to other governmental entities or commercial vendors for applications that would be of use to the employee population. This scenario would allow the government to exercise substantial control over the decision-making process for the card. However, unless the government were to assume a substantial degree of liability for the card, it is unlikely that commercial entities would have enough incentive to participate without charging fees for service. Otherwise, industry participants would have little control over their applications, yet shoulder substantial financial liability for the card platform. Thus, in this scenario, the government would have to shoulder the complete burden of the cost for the card platform. Industry participants would be paid a fee for their services (e.g., integration, card issuance, card management, application provision). Without the participation of the commercial sector in cost sharing, there would be little opportunity to generate revenue to offset government costs; the government would be predominantly responsible for the cost of the card. Because of the lack of incentive, there would be fewer commercial applications to offer to the employee population**.**

- **Private-Sector-Owned.** In this option, a financial institution would "own" the card and "rent" space to the government for its employee applications. The financial institution would assume the liability risk and control over the card specification. While the financial institution would have control over the card specification and operating environment, it would also have to shoulder a substantial portion of the liability. From the government's perspective, this approach would increase competition and potentially result in a less costly card implementation. Though involving less expense for the government, this approach would result in the government having little control over the card specification and operation, which could be problematic for participating programs. The financial institution would experience greater control, but it would still have substantial liability, necessitating a means to offset the liability costs with potential revenue from card recipients. While this approach might be attractive for a government employee card, it would move the control to the private rather than government sector.

- **Partnership of Stakeholders.** In this option, the government and the private sector would form a partnership to share "ownership" of the card platform. In this scenario, a Management Council, made up of participating stakeholders, could act as the vehicle for carrying out this public/private partnership. The Management Council would be the focal point of the arrangement, taking on many of the tradition functions of the card owner and acting as the managing agent for the consortium of participants. Through the broad-based sharing of control, costs, and liability, this option would limit the risks of the various players, thereby increasing the incentives sufficiently to attract increased participation from both the public and private sectors.

In the smart card environment, it is most likely that agencies will opt for the government-owned model, particularly in the short term. Those agencies with high-level security needs and available resources for their card platform are unlikely to find anything but the government-owned model viable. However, the other two options are introduced to provide models for those agencies wishing an employee identification platform, but whose resources are limited. These other two models provide a potential for funding such card platforms, particularly for agencies with lower security needs. Agencies willing to consider sharing the platform with other agencies or with commercial applications may find unique opportunities to reduce the cost of their card platforms. For smaller agencies or agencies with a commercial mission, the government could adopt the "partnership of stakeholders" option for card ownership. This option can result in more equitable distribution of benefit and risk, thereby encouraging a broader range of participation and increasing the applications available to employees. As a model for the migration to expanded government applications of emerging technology (such as the introduction of a citizen's card or electronic service delivery via the Internet), the platform could encourage the fundamental concepts of public/private partnership and revenue generation to offset government investment.

Management Structure

Critical to the successful implementation of a multi-application platform is a viable management structure to define, coordinate, and control the activities of the platform participants. With the potential for a substantial number of participants in this environment, there must be a mechanism to ensure adequate representation of all stakeholder viewpoints, resolve disputes, and coordinate the myriad roles and responsibilities. The agency initiating the card platform should establish a Management Council, composed of representatives of all participating government programs, private sector companies (including such stakeholders as application owners, service providers, retailers, and medical providers), and employee advocacy groups. Established at the initiation of the project, the Management Council is the focal point of a public-public or public-private sector partnership for a multi-application card.

It is worth noting here how the term "agency" is applied. Since a key objective of smart cards is interoperability, it makes sense for departments and their bureaus to work together. Each initiative should investigate whether or not related activities are under construction. While these partnerships may take some time to establish, the outcome of a single effort will be worth the preparation time. Depending on the size of independent agencies, they may also want to consider partnering as a way to develop their card and systems. The Management Council can be formed from representatives from the different offices and bureaus.

The Management Council can perform a number of critical functions in the organization and management of a multi-application platform. In the technical arena, the Management Council can provide technical direction, encourage adherence to standards, and coordinate data standardization. Responsible for embracing standards to contribute to interoperability, the Management Council can contract with a trusted third party (potentially a technically qualified government office, quasi-governmental agency, trade association, or commercial entity) to certify applications prior to loading. The trusted third party would be responsible for ensuring that every potential application for the card meets the technical and security specifications suggested by the Management Council. As the employee card platform expands in the future and migrates to dynamic allocation of storage and on-the-fly loading of applications, the trusted third party could be designated to load applications, as well as to provide quality control. Under the auspices of the Management Council, a Data Administration Working Group can be designated to define common data structures, encourage adherence to data standards, and provide ongoing oversight of data standardization as new applications are added to the platform.

In the organizational and management arena, the Management Council can perform important services as well. Through consensus of its membership, it can define the roles and responsibilities of the participants including the card owner, program office, prime issuer, application owner, and cardholder. The Management Council is a viable entity to consider key decisions about card ownership, including who owns card applications and data. Its membership is collectively empowered to consider which applications can be placed on the card and how the card "real estate" is to be allocated among participants. Along with its other management responsibilities, the Management Council makes other important decisions about the implementation of the card platform such as required training materials, and marketing approach.

Acting as a forum to bring together the stakeholders for the exchange of ideas, the Management Council can facilitate the resolution of issues that may arise in the building and operation of the Smart Identification Card platform. When necessary, the Management Council, through the empowerment of an ombudsman for the applications, can play a key role in dispute resolution.

If an agency chooses to partner with other agencies, the Management Council can play a substantial role in the legal arena as well. Contractual agreements must be established to provide a basis for business relationships among the participants. Contractual agreements, for example, are needed between the vendors and participating agencies, among participating agencies themselves, and between vendors and retailers if the card platform has an electronic purse, credit or debit applications. However, because of regulations requiring that contractual relationships be established only with legal entities, it may become necessary for a lead agency to be designated to contract with the prime issuer and vendors providing application services on behalf of the other participants. The Management Council can be given the responsibility for selecting a lead agency to act as contract administrator. Through bilateral and multilateral agreements among participants administered by the Management Council, the rules governing the relationships among the interested parties can be formalized. With the necessary stakeholders already participating, the Management Council is a logical forum for developing, and eventually overseeing, the needed application operating rules. Working with its membership to define equitable liability allocations, the Management Council can develop liability guidelines to form the basis of these application operating rules.

From the costing perspective, the Management Council can also provide significant support. This body can help define cost allocation arrangements. It can consider the impact of adding revenue-generating applications to the card platform. The membership can work together to vet revenue-generating proposals that would offset government-incurred costs, yet remain in concert with government policy and objectives. To promote card adoption and use (and potentially increase the revenue offset), the Management Council can coordinate the efforts of the prime issuer, application owners, government programs, and retailers/providers to develop and conduct an extensive marketing and training program. The Management Council is also the logical choice to conduct customer acceptance and card evaluation assessments. Because of the representative makeup of the Management Council, this body offers a potential structure for overseeing many aspects of the card platform operation.

Whether or not the Management Council model is adopted, agencies should consider how the card platform is to be managed prior to issuing their task orders. They must determine a viable mechanism to coordinate the changes that an integrated multi-application card platform will bring to the agency's business processes.

5.2.2 SHIFTING ROLES AND RESPONSIBILITIES

In addition to a Management Council tasked with carrying out the partnership card ownership arrangement, a number of additional roles will be needed in the implementing a multi-application card platform. In both the government-owned and non-government owned management model described above, there could be a tiered approach to delegating roles and responsibilities among multiple program or agency participants. This approach allocates responsibility for card management and application functionality to different tiers of participants. While the government or Management Council should have complete flexibility to adjust roles and responsibilities, it is recommended that the following roles be initially designated for the smart card platform:

- **Agency/Program Office.** An agency sub-division or program office, which are government entities that participate in the smart card platform to increase its efficiency through the electronic delivery of services, has certain defined roles and responsibilities that may vary depending on the circumstances of the platform implementation. The program office always has the following responsibilities:

- Defining application-specific data and participating in the definition of shared data;
- Activating applications when employee eligibility is determined and deactivating applications when eligibility is terminated;
- Sending account setup records (including employee data and user PIN selection, digital certificates, or biometric template) for eligible employees to the application owners;
- Notifying the application owners or service providers of application activation and deactivation status changes;
- Specifying access rights for its applications and data and ensuring that these access rules are enforced by application owners; and
- Certifying applications.

In certain situations, the program office may also be responsible for the following:

- Performing a common intake process to collect and verify common demographic and eligibility data, and
- Performing card personalization and card distribution in a distributed implementation.

- **Prime Issuer.** The prime issuer can be a vendor or government entity responsible for card issuance and card management functions. It may also function as an application owner, especially for commercial applications (such as an electronic purse or travel application). The prime issuer is responsible for card origination, which entails arranging for, and obtaining, card stock from the manufacturer. The prime issuer is also responsible for chip initialization. This process loads the application template and data structures determined either by the government agency or by the Management Council. While the government agency or Management Council determines *which* applications are to be placed on card, the prime issuer determines *how* these specified applications are to be put on chip. While an electronic purse is the only commercial application being contemplated at this time, additional commercial applications could be added to defray the costs of card operations

  When card personalization is conducted centrally, the prime issuer is responsible for card personalization functions such as adding common data to the chip, inscribing the user-selected PIN (or loading a digital certificate or biometric template) on the chip, and mailing the card to the employee or sending the cards to a local office for distribution. All applications are placed on the card at the time of personalization. When individual programs determine a client's eligibility, the program office activates the application already residing on the card. Maintaining the client registry of basic client data and pointers to applications that are active on the cardholder's card is another responsibility of the prime issuer. When the status of an application changes, the application owner or service provider notifies the prime issuer to change the status of the client registry.

  Card replacement is an important function of the prime issuer. When a card is lost or stolen, the prime issuer performs the following functions:

  - Receives notice from the cardholder;
  - Checks the client registry for active applications;
  - Obtains the data backup files for each active application from the application owner or service provider;
  - Loads the replacement card with basic cardholder data and backup data files;
  - Loads the new security device (e.g., PIN, digital certificate, or biometric template) on the chip; and
  - Mails the replacement card to the cardholder or appropriate program office for pickup.

In addition to replacing cards, the prime issuer is responsible for card security, including maintaining the card “hot list.” The hot list files are downloaded to all participating applications on a regular basis. As part of the customer service responsibility, the prime issuer maintains a customer service hot line for cardholders to call for card problems, questions, and lost cards. The prime issuer acts as the initial point of contact for the customer. When necessary, the prime issuer refers the client with application- or program-related questions to the appropriate application owner or program office. Finally, the prime issuer accepts the liability assignments agreed to in the operating rules adopted by the government or Management Council.

- **Application Owner.** The application owner may be a vendor or government program (depending on the nature of the application) that sponsors (perhaps through a “lead” agency acting on behalf of a consortium of agencies) and is responsible for the operation of the application. The application owner may develop, operate, and maintain the application on its own or contract with a service provider to provide the application on its behalf. The application owner may be the same or different agency or vendor for different applications.

  In the smart card environment, application owners will vary. It is anticipated that the government would own the ID authentication and physical and logical access control applications, as well as some shared data storage and retrieval applications. However, the open electronic purse, credit or debit applications are more likely to be owned by a financial institution or another commercial vendor, who would set up and maintain the separate accounts. The medical applications could be owned either by one or a consortium of the agencies participating in the platform or by a commercial health care provider such as a health maintenance organization or a private health insurance company. While possible in the longer term, it is unlikely that the employee cardholder will have a choice of many additional applications in the short term. However, in the future, the government employee platform could have a choice of commercial applications that could be added to the employee identification card at the employee’s option (e.g., travel application, loyalty application).

  The application owner performs application management and contracts with the using government entities to develop, maintain, and/or operate the application. While the application owner is often responsible for maintaining the data associated with the application, it is important to understand that the application owner is not necessarily identical to the data owner. The application owners perform the following functions:

  - Maintaining and updating the client account information in a centralized database;
  - Maintaining the account status through ongoing transaction processing;
  - Safeguarding the security, privacy, and confidentiality of cardholder personal information;
  - Maintaining the shadow database of transactions sent daily (or more frequently, if desired by the program) for backup purposes and ensuring the currency and integrity of this data;
  - Providing information for card replacement when requested by the prime issuer;
  - Appraising the prime issuer of changes in application status when the government office or program has activated or deactivated a client's application;
  - Providing application-specific customer assistance to clients; and
  - Accepting the liabilities for applications assigned by the government or Management Council through the operating rules for the individual applications.

- **Cardholder.** The cardholder, in this case a government employee or government contractor, is an individual who has been issued a card. While the cardholder has the ultimate control over the accuracy of data provided to data collection agents, it is the agency tasked with entering and updating the data that is responsible for the accuracy of the data resident on the card. The definition of data structures is the responsibility of either the government agency or the Management Council (for shared data) or the application owner (for application-unique data). Decentralized applications perform all transactions, but have shadow files maintained in the centralized database of the application owners. The currency of the information, therefore, depends on both the frequency of the data updates and the maintenance of shadow files.

The cardholder ensures the accuracy of personal data; application owners are responsible for protecting personal data provided by the cardholder and maintaining the accuracy of that data. Although unlikely to be available in the immediate future, it is possible that the cardholder in the future will be able to determine which applications, in addition to the government-mandated applications, are to be loaded to the card.

The sponsoring government agency must determine the management structure desired for its card platform. It should determine what roles the agency itself will perform, what roles (if any) it will share with other agencies sharing the card platform, and what roles for which it will need to procure services under the Smart Access Common ID contract vehicle.

5.2.3 TRAINING

Training provides a good example of this paradigm shift in the multi-application world. In the old environment, training for card usage was conducted by the individual entities issuing the card, and there was no question about the card's intended functionality. In a multi-application environment, it is less certain which organizational entity should be responsible for the card training. Furthermore, employees may be uncertain about what applications reside on their cards and how these applications can be used. Studies of card pilot projects have shown that wide-scale acceptance of multi-application cards depends upon adequate education and marketing programs to enable cardholders to understand and accept the concept of a multi-functional card. In an environment with multiple card issuers and application owners, a key management question is how responsibility for training and marketing can be equitably shared among all of the parties.

For employees to feel confident using their cards, they must be aware of which applications are currently active on the card. Further, if financial or commercial applications are included on the platform, cardholders must also understand how to recognize the merchants or service providers that will accept their cards, as well as who is responsible when they have customer service problems such as lost, stolen, or malfunctioning cards. This is particularly an issue if the card platform is not "owned and operated" by a government entity.

Perhaps the most significant issue affecting employee acceptance is the cardholder's degree of confidence in card security and information privacy. Training and marketing programs must focus on educating cardholders about the technical and legal safeguards in place to ensure card security and information privacy.

According to studies conducted by smart card industry groups (e.g., Smart Card Alliance), as well as "lessons learned" from pilot projects, customer acceptance is based on coordinated education and marketing efforts which in turn are based on clearly stated terms and conditions. Based on this feedback, agencies should consider the following recommendations. First, the prime issuer, application owners, government programs, and external retailers or providers, should coordinate marketing efforts to maximize employee understanding. In addition, if the government card is to be used for open commercial or medical applications, acceptance marks should be prominently displayed by appropriate vendors and service providers. It is recommended that the prime issuer be responsible for preparing employee training materials and distributing them at the point of card issuance, program offices, and other highly visible areas. Employees, program personnel, providers and retailers need adequate instruction on applications residing on the card, as well as accepted marks. Finally, continuous employee and provider or retailer feedback, through customer satisfaction surveys or other means, should be used to measure marketing effectiveness and to uncover areas that need improvement.

5.2.4 CUSTOMER SERVICE

Similar questions arise about the provision of customer service. As with training, responsibility for customer service is less straightforward in the multi-application arena. Distinctions among the required types of customer service differentiate among those responsibilities belonging to the card issuer and those best handled by the individual application owner. Inquiries related to the physical card (including card loss or malfunctions) are typically directed to the card issuer, while questions related to the individual applications are routed to the application owners. Generally, the agency issuing the card should have responsibility for establishing the card management or program applications that are required for the employee. Should an agency opt to allow commercial applications on the card platform, the application owners would be responsible for providing customer service and assistance for commercial application customers. Agencies must choose whether or not to provide such customer service in-house or through contracting arrangements procured through the task order.

Clearly defined roles and responsibilities for customer service are important in a multi-application environment because customers require a seamless, single source of information and service. The prime issuer should provide this single point of customer service, including handling lost and damaged card replacements and referrals to application owners (whether the application owners are other programs within the agency, another agency, or commercial entities) for application questions. The prime issuer would also be responsible for providing referrals to individual programs for program-related questions that customer service cannot handle.

5.2.5 PRIVACY ISSUES

As government has moved increasingly to electronic commerce and electronic service delivery, concern has heightened over the adequate protection of an individual’s privacy. Multi-application smart cards have the potential to turn many currently anonymous transactions into traceable and auditable ones. Multi-application cards present many privacy questions. Who owns the personal data stored on the card? Who is responsible for its security and accuracy? Who will have access to a person's transaction diary and under what circumstances (e.g., government agencies, law enforcement personnel, direct marketers, family members, employers, private detectives)? Should the consumer be made aware that transaction records exist and how they may be accessed or used? Individuals are becoming more sensitive about privacy concerns and more determined to assert control of their information. While privacy is a significant concern for government employees participating in the Smart Identification Card platform, it becomes even more challenging if the agency chooses to share its platform with commercial entities.

The following laws and regulations address some of these concerns by providing privacy protection:

- The Constitution. (The First Amendment guarantees the freedom of speech and association, the Fourth Amendment guarantees the freedom from unreasonable searches, and the Fifth Amendment guarantees the right against self-incrimination.)

- Federal statutes and their implementing regulations including Regulation E, Fair Credit Reporting Act, and the Federal Privacy Act.

- Individual agency regulations.

- State constitutions, statutes, and regulations including State Privacy Acts.

- The common law and the codes of various industries and professions (which may or may not have statutory force).

In addition to these laws and regulations, government agencies acting as card issuers must also put rules and procedures in place to safeguard employee privacy and thus establish employee confidence. Feedback from early multi-application smart card pilot participants confirms that the protection of cardholder privacy is a key regulatory issue affecting the success of these multi-application platform pilots. Voluntary employee card adoption will only take place if cardholders are assured that the data stored on the card are not going to be compromised under any circumstances. The following safeguards are particularly important if the government platform is going to include commercial applications:

- Make the employee the "owner" of personal information, thus making the employee responsible for keeping personal information on the card up-to-date;

- Include information about privacy protection procedures in training materials;

- Develop a card acceptance agreement that outlines terms and conditions, including privacy safeguards, and require that this agreement be signed prior to card issuance;

- Make full disclosure of the purposes for which the personal information will be used and under what circumstances it will be disclosed to third parties and ensure that the resale or reuse of data will occur only with cardholder consent;

- State the privacy protection measures that will be followed by the prime issuer, providers, and other parties;

- Use cardholder and provider PINs, biometrics, and other security features to secure sensitive information;

- Provide the employee with the right of access to the information and a process for correcting errors;

- Provide procedures to safeguard the privacy of “shadow” databases, and document these procedures in the card issuer/cardholder agreement (in addition, specify how long the information will be retained); and

- Indicate applications that require compliance with State or Federal laws (e.g., Regulation E, Fair Credit Reporting Act, State Privacy Acts, among others).

Agencies should spend sufficient time and capital to adequately address employees’ privacy concerns. Card security experts point out that cards are only as secure as the card system’s weakest link. Therefore, it is critical that the designers of card systems consider the end-to-end security of the entire system to ensure that privacy is not breached. A comprehensive risk analysis and vulnerability assessment must be performed to assure that the total card system provides adequate security measures and complies with recognized security standards. Additionally, the security of “shadow databases” that hold back-ups of personal information must also be considered when privacy protection mechanisms are being implemented. Agencies will not only have to build privacy safeguards into technical and managerial processes but also address employee fears and educate cardholders about their rights and responsibilities.

5.2.6 OPERATING RULES AND PROCEDURES

Electronic commerce and its accompanying card technology have profoundly affected the way that many entities conduct business. New laws and regulations, as well as evolving interpretations of existing legislation, have emerged to understand and control shifting business paradigms. With these changes in business arrangements have come uncertainties surrounding responsibilities and liabilities in the financial and business communities.

To support a national system for debit and credit cards, the financial services industry has established rules, regulations, and standards that govern the procedures, roles, and responsibilities of various interested parties (e.g., network operating rules, American National Standards Institute standards, and Automated Clearing House operating rules).

Regulation E is one example of a tool used to protect consumers in electronic financial transactions (such as debit transactions) by defining the rights and obligations with respect to electronic transactions affecting consumer accounts. In particular, Regulation E requires documentation in the form of receipts and account statements and sets forth limitations on consumer liability and procedures for resolving errors.

Smart card participants now face a similar need to develop standard procedures to ensure the ability to perform interagency transactions and to enable multiple programs to be delivered through a single card. Government-wide interoperability is a key objective of the Smart Access Common ID contract. Rules will need to describe the roles and responsibilities of agencies, application owners, card issuers/processors, and, if financial applications are included on the platform, the additional financial entities including networks, ATM/POS acquirers, and retailers. Deploying a nonstandard system will most likely result in a need to retrofit the system at a later date at a substantial cost.

Operating rules need to be established for each government program and for potential commercial applications. The operating rules should specify each participant's roles and responsibilities, the distribution of liabilities, and the structure and flow of fees paid by various participants. These rules should also include procedures to be followed if errors occur or disputes arise. For financial applications, operating rules must address consumer protections, including customer liability due to lost, stolen, and damaged cards. Financial liability, however, is only one of many concerns in the government multi-application environment. Operating rules, for example, must also establish liability allocation for the misuse of stored medical or clearance information. In the government environment the consequences of misuse of the card for logical or physical access could be substantial.

5.3 Re-engineering the Business Processes

It expected is that the smart card will have a substantial impact on how agencies conduct their business. Unless the agencies adopting this platform realign their business procedures to take advantage of the economies and opportunities that the platform offers, it is unlikely that anticipated cost reductions from streamlining operations will be realized. Consequently, it is critical that agencies consider from the very start of their platform planning effort what effects a multi-application card will have on their organizational structure.

At a minimum, agencies should review the degree to which the multi-application card and card management platform enable integration of different functions. For agencies contemplating the use of the platform as an employee identification card as well as a physical and logical access control mechanism, it is clear that there are opportunities to combine what were three card issuance functions into a single operation. In this situation, agencies should also consider the integration of multiple databases so that the contents of the badging system, physical access control privilege database, and logical access control privilege database can be combined into a single integrated database maintained as part of the card management system. Procedures for issuing cards and access privileges to new employees can be streamlined, allowing the employee to visit one rather than three offices. In the planning process, agencies should consider the work flow to be used for card personalization, issuance, and application loading to evaluate whether there are opportunities for short-cutting these separate processes in the new, integrated environment enabled by the card platform.

As noted earlier, offices (e.g., security, human resources, facilities, and information technology) that in the past may not have had significant interaction may now need close communication. Operational roles and responsibilities may shift or entirely new jobs may be created. Further, agencies that may not have worked together before may now need to negotiate interagency agreements to enable interoperability across multiple Smart Identification Card platforms.

While significant re-engineering of processes may bring significant efficiencies, it may also bring unexpected resistance to change on the part of agency employees. A key “learning” from the early smart card pilots has pointed out the importance of adequate change management procedures. Pilots that have used change agents and put in place well-thought-out change management strategies have had far fewer hurdles to overcome with their employees than those in which such considerations were ignored. Pilots have also underlined how vital a communications strategy, as well as training program, can be to ensuring card adoption. To encourage card usage, it is critical that the employees understand and feel comfortable with their new multi-application cards. Nothing can take the place of adequate marketing of the card platform or sufficient training of the employees to ensure that the anticipated benefits of the smart card will actually be achieved.

To further support the transition to a multi-application environment, not only must procedures be re-engineered, but also policy and procedure manuals must be updated to reflect the new approaches being put in place in the organization. Agencies sharing the card platform may need to work together to develop operational procedures that work in each unique agency environment. In the planning and budgeting process, it is critical that sufficient staff and/or financial resources be set-aside for updating these manuals. Yet another approach for agencies to consider is use of web-based applications through the Internet and/or agency intranets to provide updated instructions associated with the new business processes.

5.4 Financial Issues

In planning for the smart card platform, the budgeting process is a critical activity. The agency profile and subsequent analysis is meant to assist the agencies in collecting necessary information for this budgeting process. Many of the decisions made as a result of the agency profile will have a profound impact on budget requirements. The cost of the cards, card management, and hardware/software/communications will depend upon the scope of the project. The sections that follow present some considerations for agencies to contemplate when planning their smart card platform budgets.

5.4.1 COST FACTORS

The availability of resources will have a significant impact on the applications and technology selected by an agency. In turn, the selected applications will influence cost. In developing multi-application card systems, participating parties must strike a balance between system cost and desired functionality. The cost of the chip card may vary substantially, depending on the size and capabilities of the chip.

The use of transportation applications on an employee card provides an example of cost/functionality tradeoffs. While it may make sense to add public transit applications (either tokens or an electronic purse for fare payment) to a multi-application employee card because many employees in the Washington Metropolitan area use public transportation, it may not be desirable from a cost perspective. The addition of a transportation application has significant cost implications for an employee card. Transit authorities generally prefer contactless cards for their applications while other agencies may not need this additional functionality.

The use of a contactless physical access control application provides yet another example of the cost/functionality tradeoff. While it may make sense to use contactless chips for physical access control because it substantially increases throughput for perimeter control at busy building entrances, it may not be desirable from a cost perspective. In accordance with this approach, for the purposes of budgeting and planning, each agency will issue a Federal Identity Card credential and develop the required infrastructure for both physical and logical networks as current systems come up for replacement. Multiple interface cards with both contact and contactless capability are more expensive than single interface cards. Participating parties will have to consider whether to use the contactless card, and if so, which party will bear the additional costs associated with contactless card technology. As more and more applications are added in a multi-application environment, the need for chip memory and the corresponding card cost grow. Consequently, the choice of applications to put on a multi-application card may be constrained by cost considerations. Thus a costing methodology is critical prior to issuing the task order.

The budget available for implementation is but one factor in considering cost issues. The card volume required, as well as cost-sharing opportunities may impact the total available resources for the card project. As many vendors provide sliding scales of card prices, agencies that coordinate procurements may realize economies of scale together that allow them to have greater card capabilities at lower prices. Agencies must determine their card volume prior to developing their task orders and may choose to team with partner agencies to improve the cost structure.

Cost savings are also part of the total financial picture. One of the most compelling arguments for the movement to multi-application cards is the cost savings to each program that participates in a multi-application platform, even though single application cards may be less expensive to implement than multi-application cards. Economies of scale resulting in reduced costs will be realized in several areas, especially card issuance and administration. Additionally, card issuers and application owners are expected to benefit from total cost reduction due to sharing:

- **Core Services.** Processing which supports the core services is shared among the programs using card applications resulting in cost sharing and consolidation.

- **Data Collection.** Gathering and storing the common data is shared among the application owners.

- **Personalization.** The card is personalized and issued once, rather than one card per application.

- **Infrastructure.** For many applications, the infrastructure deployment or upgrade can be shared among application owners.

However, while multi-application cards may be cost-effective, they are also more complicated to administer. The complexities of formulating equitable cost distributions across multiple participants in the multi-application environment further complicate the process.

Furthermore, the transition to multi-application chip cards will require modifications to the existing agency infrastructure. In assessing the cost impact of this infrastructure enhancement, it is necessary to determine what parts of the infrastructure will have to be upgraded to support an interoperable employee ID card, what are the costs of such efforts, and who should pay these costs. The applications included on the Smart Identification Card will impact the scope of the effort to upgrade the infrastructure. If, for example, only physical access control is implemented, the infrastructure costs will be significantly less than if both physical and logical access control applications are included (because of the cost of adding smart card readers onto each workstation to implement logical access control). Similarly, the use of biometrics will be more expensive because biometric readers will be necessary in addition to smart card readers.

Investment in upgrading the infrastructure and transitioning to a smart card platform is composed of design and development costs and implementation costs. Design and development costs are commonly associated with the following factors:

- Detailed system design and review;
- Hardware and software development;
- System demonstration and acceptance testing;
- Preparation of operators and users' manuals and training materials;
- Development of implementation plans;
- Project administration; and
- Independent validation and verification.

Implementation costs are commonly associated with the following factors:

- Cost of hardware;
- Switching agreements;
- Licenses;
- Software;
- Telecommunication lines; and
- Terminal deployment.

In addition to the infrastructure costs associated with multi-application cards, there are many start-up and ongoing costs for establishing the smart card program. Start-up costs include development costs, hardware and telecommunication line installations, card issuance and distribution, customer service, and cardholder and employee training. Ongoing costs include fees for operating the card platform. One approach to making the Smart Identification Card more affordable is to team with other agencies to share costs of the platform, infrastructure, and application development.

5.5 Lines of Communication and Agency Support

One finding from the initial smart card pilots was the importance but difficulty of achieving adequate stakeholder communication and participation throughout the planning and implementation processes. These pilots recognized that inadequate stakeholder participation early in the project resulted in “requirements creep,” integration problems, and project management issues later in the project.

Consequently, it is important for agencies to identify the key stakeholders in this procurement from the very beginning. The stakeholders will vary substantially from project to project depending on such things as the applications to be implemented, degree to which card applications are to be developed in-house or outsourced, whether the agency is sharing the platform with any external agencies, and whether the card platform has any commercial partners. Once the stakeholders have been identified, it is equally important to determine how these stakeholders interact with each other. The relationships among the various stakeholders both before and during the project need to be analyzed to understand how these ongoing relationships may affect the operation of the card platform. If there are particular communication problems or misunderstandings, these should be identified and addressed as soon as possible.

Part of the implementation planning should address mechanisms for establishing buy-in by the stakeholders. These relationships may be established through a variety of mechanisms including the Management Council described above, interagency agreements, contractual relationships, and communication plans. Each situation will be unique, so that different mechanisms may be more or less effective depending upon the particular circumstances of the project. Clearly one mechanism that has been highly effective in some of the pilot projects is to use change management programs. These change management programs include the designation of change agents; development of a strategic communications plan; and implementation of a web site or other communications vehicle to keep all stakeholders informed about project issues and progress. Ongoing meetings to apprise employees of the impact of the changes have also been effective in other pilots, as has the willingness of top management to address employee concerns about the changes.

Properly phasing the roll-out can help immeasurably in achieving stakeholder commitment and involvement in the project. The implementation should not occur during periods of high activity or stress for particular stakeholders. During the budgeting process, adequate resources should be allocated to the roll-out, especially to train and provide assistance and consultation to offices during the roll-out period. It is critical that employees understand the full functionality to be offered by the card platform. If necessary, roll-out should be delayed if the applications to be used with the card platform are not yet available.

5.6 Quality Assurance and Contractor Management

Whether the Smart Identification Card platform is to be implemented totally in-house, outsourced, or a combination of the two, it is critical that adequate provision be made for quality assurance (QA) and project management (PM). If the project is to be performed in-house, either a quality assurance and project management office within the agency or an outside consultant must be hired to provide project oversight. Multi-application projects, especially those spanning more than one agency or an agency and commercial partner, are complex enough to require independent verification and validation (IV&V). Conversely, if the project is outsourced, either the agency must designate sufficient staff resources to provide project oversight and deliverable review, or an IV&V contractor should be obtained.

As part of the planning process, the quality assurance and contractor management function should be incorporated into the project plan and the project budget. The agency may choose to obtain such QA/PM services through the initial task order or from a separate contracting arrangement. While either agency staff or an outside contractor may provide quality assurance/project management, for the sake of simplicity, the QA agent will hereafter be referred to as the QA contractor.

The QA contractor (or in-house staff) should assist the agency through quality assurance reviews of the contractor's work plan, design documents, pilot plans, and other documents and deliverables. Additionally, the contractor should assist the agency in planning, conducting, and evaluating system testing of the Smart Card platform. Acceptance criteria should be established for each deliverable review and an acceptance procedure should be stipulated in the contractual agreements between the agency and the contractor. The acceptance procedures, used to ensure quality control of the technology and implementation process, should be stipulated in the task order.

An example of the use of acceptance criteria is provided below. Thus, for example, the review of the work plan should ensure the following:

- Scope of tasks is detailed enough to allow for project management monitoring, tracking and reporting;

- Levels of resources indicated are sufficient;

- Sufficient steps are included to reduce risks and to promote effective risk management, including timely problem identification and intervention;

- Task progression is logical (both sequential and concurrent tasks) and have an accurate depiction of dependencies (internal and external);

- Sufficient time is allocated to plan, perform and to modify/correct (as necessary) with on-time completion; and

- Use of the project work plan as the primary project management tool is clearly understood by the contractor and agreements are made related to timeliness of updates and method of distribution.

The QA contractor should review all smart card contractor plans and conduct all aspects of systems testing. This should include the evaluation of the Smart Identification Card contractor testing proposals, scripts and scenarios. The test phase is a critical milestone in the project. The QA contractor should be involved in all aspects of systems testing. The tests to be performed by the Smart Identification Card contractor should include functional demonstrations, acceptance testing, network performance test, system stress test, interface test, and automated response unit (ARU) test.

There are proven test tools available that can be used by the QA staff, including test data and volume testing tools. Text data formulates processing using transactions that are representative of the conditions. The design of the test data is implemented using certain tools, such as the test deck. The test deck should use valid and invalid data. Invalid data are used to test the effectiveness of the controls within the program, such as the ability to flag rejections, and also test the ability of the system to edit routines.

The QA contractor should determine the correct results of all tests before running the data, in the correct entry form, through the computer. Test data can be derived from actual or simulated records. By studying a master file, the QA contractor can select suitable actual records for testing. Simulated records can be prepared through source documents and processed through the system program. Either way, the test is run in a separate test file to avoid complications or confusion. A step-by-step testing process involves:

- Establish resources. What are the allocated resources including test time frame?

- Establish conditions. Under what conditions should the tests be conducted?

- Rank and select conditions. Which conditions have the highest priority? Based on resources, what are the most important conditions to be tested?

- Establish correct results. What are the results that the program should provide?

- Prepare test transactions. What is the method used for establishing readable transactions?

- Documentation. All situations and results have to be documented.

- Run test. Tests should be run under a test condition or using simulated data.

- Verify test, make corrections. Are problems due to systems error or data error?

Factors involved during the installation test phase, such as methodology, integration, accuracy and completeness, and integrity can be determined through a variety of test techniques and tools, as shown in the following matrix.[34] This matrix (shown in Figure 16) is not intended to be exhaustive, but rather provide a sample of the types of factors that should be considered in system testing.

[34] Based on information from:
Perry, William E. *Structured Approach to Systems Testing*. Wellesley, MA: QED Information Sciences, Inc., 1983.

Figure 16

Test Process		
Test Category	**Test**	**Tool**
Methodology Compliance	Are the procedures for data processing installation complete? Are the most current versions of the programs being used? Are there sufficient materials on hand for the test? Are the new files labeled correctly? Can data processing groups support the new application? Are the most current versions of the operating procedures being used? Has the installation been done according to procedures?	Review/inspect for compliance
Insure Correctness of Program	Does the program contact have sufficient authority and knowledge to oversee installation? Are there reasonable criteria for installation acceptance? Are there reasonable procedures for reporting errors? Have errors been addressed before operating the new system? Have all anticipated problems been identified? Has assignment of knowledgeable personnel been made for error spotting? Does the new system produce the same results as the old system?	Confirm for compliance; perform examinations through check-lists and walkthroughs and use of suppositions
Monitor Integration	Has the installation criteria been met? Is the budget and security adequate for installation? Is there a method/trail for reviewing the installation and verifying file integrity? Can the installation be verified for accuracy and completeness? Have only installation funds been used for installation? Have all items in the installation schedule been identified and completed?	Confirm for compliance; examine execution; perform inspections
Verify Reliability	Are all files for conversion identified and complete? Are the data validation routines complete? Are the test plan and test results complete? Has one knowledgeable person been appointed as accountable? Are the procedures adequate and does the converted file contain all necessary data? Have the detected errors been corrected prior to completing the installation phase?	Confirm and examine for compliance; examine test data samples
Confirmation of Authorization	Does the installation comply with authorized procedures? Can new data entry be traced to an authorized individual? Does the system prohibit new entities during installation? Has financial data been altered or deleted during installation? If there are data changes, have they been authorized by management? Have all changes in field length or field structure been authorized? Have other changes (e.g., in coding) been authorized? Have changes in customer records or financial data been authorized?	Confirm through check list, examination of test data, and inspection
Integrity/Continuity	Have the previous system's programs been retained? Have the previous system's operating instructions been retained? Have the previous system's master files been retained? Have the recirculating transaction files been retained? Have the manual procedures been retained? Have the independent control totals been retained? Has the system user been notified of all specifications, which were not implemented? Are project personnel assigned to maintenance experienced?	Confirm with operations

Test Process

Test Category	Test	Tool
Installation Audits	Have arrangements been made to save old files and programs for an adequate period of time? Have arrangements been made for a review of production file changes? Will program changes be kept for an adequate time frame? Will a record of changes to manual systems be maintained? Has a qualified person been charged with maintaining record of changes? Will operations maintain a record for review of operator actions? Does an individual have the authority to maintain the review record for a period of time adequate to cover the proof of integrity of the new system?	Confirm
Installation Planning	Is the installation plan adequate? Does each step have an estimated time frame assigned? Can reversion to the old system be accomplished (in case of new system failure)? How long would it take? What is the fail-safe point? Has an adequate period of time been allotted for returning to the old system? Who is the authority responsible for returning to the old system? How will personnel be notified of the system type in place on the next business day?	Examine; confirm
Security Planning	Has an adequate security access been put into place? What are the security procedures? Are they adequate and has enough time been allowed for implementation? Can important data be removed from interim media? Has a record of operations been produced and reviewed? What are the procedures for security breaches?	Examine records; confirm procedures
Portability of Documentation	Is the system hardware, software, and coding documentation complete and current? Is data file documentation complete? Does documentation include current portability restrictions, special features and jargon?	Confirm through inspections
Maintenance of Documentation	Is all documentation - operating, user, data, security, program, system, audit and recover - current and complete?	Confirm through inspections
Clarity of Instructions	Have all users been advised of the date and plan for implementation? Are there adequate personnel to assist with possible problems? Do the instructions explain objectives and clearly delineate user and problem procedures? Does the system monitor transactions for completeness?	Confirm through examination and inspections
Operating Procedures	Are procedures produced in appropriate manuals and distributed? Are forms and storage materials available? Has the appropriate computer media been identified and have assignments for operations been made?	Confirm through examinations and inspections
Coordination of Interface	Have system users - input providers and output receivers - been notified of the date of implementation? Do control clerks, records, operations, data librarians and security personnel know the implementation date? Do programmers know the system is going operational?	Confirmation through examination

As with the its other quality assurance activities that it conducts under this engagement, the QA contractor should provide the agency with a written evaluation of the system testing activities for each system test. In these reports, the QA contractor should evaluate the results of the specific test and recommend any actions to be taken by the state or the smart card contractor to remedy errors or inconsistencies in the system operations.

The QA contractor should follow a defect-severity rating system in evaluating the tests that includes logical "categories" or "priority levels" that defects can be assigned. Following, in Figure 17, is an example of a defect-severity ranking scheme that has been used at other acceptance tests.

PRIORITY	DESCRIPTION	ACTION
1	Major system defect/malfunction	Testing is halted until problem is resolved. Once resolved, testing starts over.
2	Defect/major malfunction of processing component	Testing is halted in particular processing component, but continues in other components. Scripts will be adjusted if necessary and problem resolution will be performed. Testing will restart in this component once defect is corrected. Defect will be included as a part of regression testing.
3	Minor function problem	Testing will continue on all aspects of the system. Defect will be included as a part of regression testing.
4	Edit/cosmetic error	No effect on testing. To be corrected prior to system being placed in production environment.
5	All others including design clarifications	No effect on testing. To be addressed as a future system enhancement or design update.

Figure 17

The quality assurance methodology should be based upon an iterative process that helps ensure that the final smart card system meets or exceeds the original requirements. For example, the implementation task order should set forth the requirements for the smart card system. The winning proposal should describe the bidder's technical and management approach to implement these requirements. Each successive design document should therefore provide additional detail and tie back to these "core" documents and to each preceding version. The system functional demonstration should be sufficient to provide confidence that the ultimate system performs as designed. Similarly, tests such as system and acceptance tests should be designed to ensure that the functionality described within the design document is available and performs as expected. It is important to note that requirements and designs evolve through this process. The QA contractor should work in partnership with the agency and the Smart Identification Card contractor to ensure that changes are appropriate, documented, and tested.

5.7 Card System Interoperability

A key requirement for many of the agencies implementing the smart card platform is their ability to achieve interoperability. While agencies may vary as to the degree to which interoperability is necessary to their own business processes, virtually all agencies agree that interoperability on the physical level, at least, is critical to widespread adoption of smart cards across the government. Consequently, GSA considered the achievement of interoperability across card systems as one of its main priorities in developing the Smart Access Common ID contract.

5.7.1 INTEROPERABILITY SPECIFICATION DEVELOPMENT PROCESS

The process for achieving interoperability was initiated by the Smart Access Common ID contract solicitation, which required all awardees to work together to develop an interoperability specification to which all Smart Identification Card contractors would have to adhere. After the May 26, 2000 contract award, GSA convened a meeting of the five selected prime contractors to begin the development of the interoperability specification. The Interoperability Committee, comprised of GSA staff, contractors, and government agency representatives, was formed to develop the interoperability specifications. Over one hundred people participated in the meetings of the five Interoperability Committee work groups that were formed to work on specific areas of concern. Technical representatives from the prime contractors and their subcontractors participated in the following work groups:

- Architecture;
- Physical Access;
- Logical Access/Cryptography/PKI;
- Biometrics; and
- Conformance Testing.

Each subgroup wrestled with the interoperability issues confronting its respective area of concern. These subgroups developed the policy and technical specifications that were needed to achieve interoperability across vendors. After working for approximately six weeks, an initial draft of the architecture was released at the end of July, 2000. The prime contractors reviewed the draft architecture. The final architecture document incorporated their comments and was released in September 2000. The Government Smart Card Interoperability Specification focuses on the use of common data across applications, encryption/decryption services using both public key infrastructure and symmetrical key infrastructure, and authentication including cardholder verification and external verification.

The initial document produced by the architecture subgroup provided the basis for the interoperability specification. This document sought to achieve interoperability in the following critical areas:

- **Interoperability between Cards and Readers.** The Interoperability Committee has specified a common mechanism for card type recognition and communications parameter negotiation at the interface between cards and readers such that any card will work with any reader at the physical and data link layers.
- **Interoperability between Cards and Applications**. Card related services would be provided to applications through a standard interface.
- **Card Interoperability**. Different types of smart cards (e.g., file system cards, and interpretive cards such as Java cards and Windows smart cards) that operate within the Government Smart Card Interoperability Specification must have a card edge interface that allows these cards to interoperate with applications through a standard interface.

5.7.2 SMART CARD INTEROPERABILITY ARCHITECTURE

The post-award Interoperability Committee has defined a comprehensive architecture to achieve interoperability. Figure 18 provides a graphical overview of this architectural model. This architecture provides the fundamental structure for the *Interoperability Specifications*. Appendix F provides access information to the current version of the *Interoperability Specifications*.

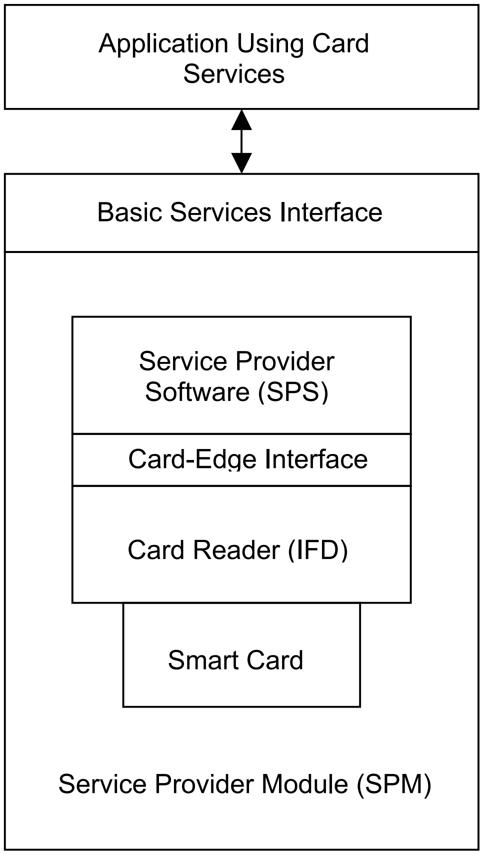

Application Using Card Services
Basic Services Interface
Service Provider Software (SPS)
Card-Edge Interface
Card Reader (IFD)
Smart Card
Service Provider Module (SPM)

Figure 18

The following components comprise this architecture:

- **Government Smart Card Service Provider Modules (GSC SPM).** The GSC Service Provider Module consists of cards, card readers, and driver software. The purpose of a GSC SPM is to provide card related services and functions to client applications through a set of standard interfaces. The SPM addresses data management, security, and access to the common data model.
- **Service Provider Software (SPS).** The host-side software component of an SPM is referred to as the Service Provider Software.
- **Basic Services Interface (BSI).** The BSI is a set of basic services and a corresponding interface that allows the card to interact with the application using card services. The BSI provides the following:
    - A single common interface between each contractor’s SPM and client applications;

  - Card-related services that support logical access control, physical access control, cryptography, and biometric applications that are interoperable;
  - Methods for digital signature services and access to biometric templates stored on the card for use by external biometric and identification authentication applications;
  - File-oriented access methods (Common Data Model objects and biometric templates); PIN submission for cardholder authentication; and cryptographic services (challenge-response authentication, digital signature generation/verification); and
  - The first level of interoperability, protecting the application using smart cards from needing to know about any specific smart card.

- **Extended Services Interfaces (XSI).** For the agencies that required additional card-related services beyond those available through the BSI, there are the Extended Services Interfaces (XSIs). The XSIs provide card-related services to a wide range of applications. Various services, defined at the task order level, will be implemented within an SPM and provided to client applications through an XSI. These extended services are designed to meet the application-specific requirements of a given organization.
- **Card Edge Interface.** The second level of interoperability is provided by the card edge interface that allows any SPS provider to interoperate with any smart card that supports the defined card edge interface. The card edge interface includes:
  - A basic data model for the common shared data (currently known as the “J.8” data);
  - A basic set of cryptographic services that includes the public key infrastructure and symmetric key infrastructure cryptographic capabilities required for the BSI; and
  - A functional interface.

A key characteristic is the concept of a Card Capability Container. Each card has its own Card Capability Container that contains the identifying information of the card system and a set of basic commands. Thus, once the Card Capability Container is processed, the SPM can configure itself to interface with the card and execute the most important commands to achieve a minimum level of interoperability. In a file system card, the Card Capability Container is implemented as a file structure, while on an interpretive card (e.g., Java, Windows or MULTOS card), it is implemented as a Generic Container Applet. The Card Capability Container enables interoperability between a broad range of cards without the problems and costs associated with configuration management techniques used in the past.

In order to achieve true interoperability across the government, agencies and their commercial partners must commit to adherence to these specifications. By conformance to this specification, agencies can achieve interagency sharing of data, convenient exchange of employee identification information, unrestricted movement of employees across government facilities, and the flexibility to modify their systems in the future to adopt new technology or take advantage of hardware cost reductions. Although substantial benefits can be accrued from realizing this interoperability, such conformity is not without cost, both from a financial and an organizational perspective. Agencies must be willing to invest in the time and effort needed to ensure adherence to the agreed upon standards.

6. WRITING THE TASK ORDER

Goal: Determine specifics of your agency's task order.

6.1 Technical Issues

Selecting Applications

During the planning stages, the agency must make some preliminary decisions about the applications and technologies needed for the card platform. These decisions must be refined before the task order can be issued. GSA can assist agencies in the decision-making process for specific requirements of their Smart Card Programs. To size the chip (e.g., approved processor and memory size) and determine the types of technologies needed for the card, the agency must finalize what applications it plans to implement both in the short-term and eventually in the future. Each agency must consider its own work flow and the efficiency of its current methods of doing business when selecting the applications for its platform. The specific applications will depend upon a number of factors, which will be different for every agency. These factors may include, but are not limited to:

- Agency mission and business lines;
- Agency priorities;
- Degree of staff mobility;
- Extent of business travel;
- Condition of existing legacy systems;
- Existing technical environment;
- Degree of information sharing desired with other agencies;
- Extent to which agency wishes to re-engineer processes;
- Extent to which agency wishes to migrate to electronic commerce and/or electronic service delivery;
- Agency's target audience and approach to interacting with the public and business partners;
- Agency's required level of security;
- Agency's vulnerability to risk/consequences of compromise;
- Agency's geographic dispersion; and
- Efficiency of administrative operations.

Once the agency has selected its applications, the agency must ask the following questions about each application:

- What technology is needed to support each application (e.g., contact chip, contactless chip, magnetic stripe, proximity, bar code)?
- Will the application make use of digital certificates?
- Will the application make use of biometrics
- Will the application require attribute certificates if it uses biometrics?
- Does the application have limited or extensive data needs?
- Is the application memory intensive or does it use limited memory?
- Is the application unique to the agency or will it be shared by other agencies/programs?
- Will the application need an interface with a legacy system?
- Will the application be replacing an existing application or will it be new?
- Must the application interoperate or share data with other applications?

Sizing the Chip

The selection of applications has significant implications for the card platform. Both the number and complexity of applications will drive the size of the chip and type of chip. For example, some applications operate with the contact chip while others work more efficiently with the contactless interface. Applications that use a digital signature capability will require that the chip have a co-processor. Furthermore, if both digital certificates and attribute certificates (for biometrics) reside on a card with other applications, more memory will be required to accommodate these dual certificates. Biometrics will have a tremendous impact on the size of the chip. Moreover, the capacity of the chip itself limits the number and type of applications that can be placed on the card. Thus, the mix of applications can affect the memory required and the cost of the card, because certain types of applications require substantially more memory than others.

In a multi-application environment, it is necessary to plan ahead for all future applications that ultimately may be needed on the card to ensure that there is sufficient memory. However, the balance between functionality and cost may affect the planning of the card's memory. There can be a substantial cost tradeoff between two differing approaches: (1) carefully planning applications ahead of time to gauge the minimum memory needed to support the required applications and (2) obtaining more than enough memory to support any future application that potentially could be added to the card.

FIPS Certification

All government cards must follow the requirements established in the NIST Federal Information Processing Standards 140-2 if the card is to manage any cryptographic functions. The certification process assures the government the chip has been tested and fulfills the requirements. Not all chips are certified and this must be specified in the task order.

Interfaces

The required interfaces with legacy systems may influence the technology on the card as well. If backward compatibility is required for an existing proximity physical access control system, for example, the agency might purchase a proximity card with an embedded chip, making the eventual transition to contactless chip somewhat more complicated because the contactless RF technology and the proximity RF technology may not operate efficiently on the same card. Backward compatibility with legacy systems may also influence the card readers procured for an agency's card platform. However, in recommending the technologies to be included on a card, the concern to maximize functionality and ensure client ease of use must be balanced against the added complexity and cost of including additional technologies to the card.

As more technologies are added to the card, the complexity of training will increase, as will the difficulty of assigning card real estate and developing applications. Added technologies will also affect the cost of the card. While the desire to reduce complexity may argue for limited technologies, the overriding need to establish a migration path from existing to emerging technologies must be adequately addressed.

Memory Allocation

In a multi-application environment, a number of technical issues arise that are not prevalent in other environments. For example, there is a need to develop procedures for allocating the user memory on the card among the various applications. As more and more applications (as applications are increasingly maintained on the card in the future) and associated data structures are added to the card, the partitioning of memory becomes increasingly complex. If new applications are added to the card, there may be a need to arbitrate which transactions will be removed, and in what order, to accommodate the new applications. The fact that different cards use different memory allocation schemes should be considered in writing the task order.

Security

Furthermore, in a multi-application environment, procedures to control access to various areas of the card become particularly important. The degree of security changes with the degree of sensitivity of the data associated with the application. The issue of data security becomes more complex in a multi-application environment because different applications on a single card may require different levels of security. Some applications may require no security; others may be adequately protected by a PIN; others may demand the use of biometrics to protect access to particularly sensitive applications. Additional related issues revolve around the question of data ownership on a multi-application card. In the multi-application arena, protection of privacy becomes especially relevant when medical or financial data reside on a card with less sensitive applications. Access to certain applications may need to be restricted to ensure privacy. Liability for the accuracy of data also becomes an issue when medical providers are relying on data placed on the card to provide treatment information. The types of applications on the card and the sensitivity of these applications may impact the technical characteristics of the card, as well as which operating system is chosen.

Yet another issue in a multi-application environment, particularly when there is more than one card issuer, is the increasing complexity of physical security and control. The physical security of card stock may be more vulnerable if inventory must be maintained in multiple locations. As the card distribution function is diversified, the level of security risk increases. In addition, secure inventory control and protection during transport may become more difficult to achieve. To achieve a viable implementation of physical security for the Smart Identification Card, implementers must balance employee and program convenience with the increased complexity of physical security resulting from a distributed approach to card issuance. In the different agency environments, it may be necessary to combine multiple approaches to implementing physical security to better address the specific needs of the agencies in different environments. The decisions about card management will influence the content of the agency's task order.

Data Backup and Recovery

Also influencing the task order are decisions about how best to provide data backup in a multi-application environment. Because of the possibility of card destruction, loss, or theft, there must be a system in place to provide a backup of the data maintained on the card. Typically, an online backup database, known as a “shadow file,” is maintained for data required to be re-created in the event of card loss or destruction.

In a multi-application environment, the question of data backup responsibility becomes more difficult, as there are many potential ways to delegate responsibility for data protection and recovery. If the issuer maintains backup data in a central location, it is easier to repopulate the replacement card when the original card is lost. However, when medical and other sensitive data are maintained on the card, a centralized database may cause privacy concerns for application owners and cardholders. In addition, from a technical perspective, as the central database grows in size, it becomes increasingly difficult to manage the potentially large size of a single database for all cardholders. Another approach is to decentralize responsibility for backups to each application owner’s remote system. With this approach, consideration must be given as to whether or not reissuance uses a card management system that allows application owners to repopulate application information from a secured application database. While this approach resolves the privacy issue, it is highly inconvenient for the cardholder. When the card is lost, the cardholder must go to numerous locations to repopulate the card. Yet another approach is to shift responsibility for backup to employees, who would back up their own information, as desired, in a central location. Before completing the task order, an agency must decide which approach is most viable for that agency to ensure responsibility is appropriately attributed in the task order.

6.2 Financial Issues

In the planning stage, key financial decisions were made that are likely to affect the costing of the task order. Once a “ball park” budget is in place and the agencies have made any arrangements they are considering with other agencies and/or commercial entities for sharing the card platform costs, they are in a far better position to determine the resources available for the task order. At this point, decisions about the products and services to be requested in the task order may be adjusted to meet any necessary budget constraints.

The following are some typical questions to help agencies identify relevant cost factors that will impact vendor responses to the task order. This list is not meant to be exhaustive, but rather to suggest the types of considerations that should go into developing a task order. The answers to these questions are meant to assist agencies in calculating “ball park” costing estimates, to verify that the likely vendor responses will be within the allocated budget.

- How many employees currently receive cards?
- How many replacement cards are issued each month?
- What is your current lost rate for cards?
- What is the projected growth or decline in the number of cards issued in the next year? In the next three years? In the next five years?
- How many employees currently receive cards for physical access control?
- What is the current rate of physical access control card loss?
- How many replacement physical access control cards are issued each month?

- What is the projected growth or decline in the number of physical access control cards issued in the next year? In the next three years? In the next five years?
- How many employees currently receive cards for logical access control?
- What is the current rate of logical access control card loss?
- How many replacement logical access control cards are issued each month?
- What is the projected growth or decline in the number of logical access control cards issued in the next year? In the next three years? In the next five years?
- What other cards are issued to employees? For what purposes are these cards issued? Are these cards issued to all employees or a select group? How many cards are issued of each card type?
- What applications are you planning to put on the card? How many applications are you planning for the card within the next year? Within the next five years?
- What technologies do you require on the card?
- What type of card do you need (i.e., chip technology, multiple technology, multiple interface)?
- What size chip do you need?
- Do you require a cryptoprocessor on the card?
- How do you currently personalize and issue cards? How do you plan to personalize and issue cards? What hardware and software will you require for card personalization and issuance?
- What data is currently maintained on your card face? What data do you plan on the face of your Smart Identification Card (e.g., agency seal, digital photograph, digitized signature, other)?
- How do you currently handle lost, stolen and damaged cards? How do you plan to handle lost, stolen and damaged cards?
- Do you currently provide customer service for any of your badging or card programs? How do you plan to provide customer service?
- In what systems do you currently maintain card data for each of your current card programs? How do you plan to maintain and backup card data?
- Do you currently have a physical access control system? What technology does that system use? What technology do you plan to use for your physical access control system? Do you plan to install a new system, replace the legacy physical access control system, or swap out readers and integrate the card with the legacy system?
- If you plan to replace your system, how many card readers will be needed? If you plan to swap out readers, how many readers must be swapped out?

- Do you currently have a logical access control system? What technology does that system use? What technology do you plan to use for your logical access control system? Do you plan to install a new system, replace the legacy system, or swap out readers and integrate the card with the legacy logical access control system?

- If you plan to replace your system, how many card readers will be needed for logical access control? If you plan to swap out readers, how many readers must be swapped out?

- With what other legacy systems does your card system need to integrate? How do you plan to implement system interfaces?

- Are you planning to implement PKI? If so, how are you planning to implement PKI? Do you plan to issue and/or verify certificates in-house? Do you plan to provide registration authority functionality in-house?

- Are you planning to implement biometrics on the card platform? If so, how are you planning to implement biometrics? Will you use an attribute certificate to bind the biometric to the card? If so, how do you plan to issue, verify and renew attribute certificates? What biometric are you planning? Where will biometric readers be required?

- Are you planning any financial applications on the card? What financial applications are you planning? Will they be commercial magnetic stripe credit or debit applications or chip-based applications? Will they be open or closed applications? What type of readers will be required for the financial applications? How many card readers will be required for the financial applications?

- What other readers will be required for the additional applications on your card? Will these readers be needed within the agency? Will readers be needed external to the agency (such as at private health care providers)? Will the agency provide these external readers?

Section 5.4.1 provides additional information on factors that need to be considered in developing preliminary budgets for the task order. Depending upon the individual characteristics of each agency's implementation, additional costing factors may have to be considered. Once again, the Smart Card Initiative Team can assist agencies with preparing budget estimates and translating those budgets into viable task orders for their card programs.

A very significant aspect of the budgeting process is to determine how the costs of the card platform are to be allocated across divisions within an agency or among multiple agencies or programs, if the card platform is to be multi-agency. Section 5.4.2 provides information to assist with developing a strategy for cost allocation. From the perspective of writing a task order, it is important to decide whether the card platform will be for the agency itself or shared among agencies, as well as whether or not the card platform can be shared with commercial entities. If so, the agency should determine whether the platform will be government-owned, private sector-owned, or a partnership of stakeholders (see Section 5.4.2 for further information about this issue). Further, the budget should take into account any effort to generate revenues from the card platform to offset government costs (see Section 5.4.3 for further information about this issue). Depending on the policies of individual agencies, revenue generation may be a viable solution for agencies with few available resources for the card platform, or it may be totally unacceptable to the agency. However, this is an avenue for funding the card platform that agencies should at least explore in the early planning stages.

6.3 Policy and Programmatic Issues

Build versus Buy

A number of policy questions must be decided before the task order can be written, because these issues will determine what services are actually being procured by the task order. A key issue is whether to build or buy a system. Because of the potential complexity of the smart card platform, the "build/buy" decision may have to be made for various components of the card platform. The "build/buy" issue must be determined first for the card management process. An agency must decide among the following options:

- Build its own card management system and operate it in-house;
- Acquire a commercially available card management system and operate it in-house; or
- Contract for card management services.

Building the card management system in-house will be labor-intensive and take a substantial amount of staff resources. Clearly purchasing a system and customizing it will take far less time. Most agencies, unless they have very unique card management needs or a substantial development capability, should first consider either adapting commercially available card management systems or outsourcing this functionality to a card issuer. The decision as to whether card management is provided in-house or outsourced affects many other decisions about the platform including what hardware and software must be purchased, what telecommunications services are needed, and whether or not integration services are required.

Similar issues will arise with other platform components including the physical and logical access control, PKI, and biometric systems. Depending upon the individual needs, an agency may opt to build and/or procure different parts of the platform and, consequently, will need integration services. These decisions will directly impact how the task order is written.

Training

A closely related question is how to handle training requirements. Agency personnel issuing and servicing the card, as well as providing support to the card applications, will need training. Additionally, employee cardholders will need training about card usage and individual applications.

Once the scope of the training is identified, agencies must decide what types of training they prefer (e.g., contracted trainers, train-the-trainers, computer based training, web-based training). Agencies may opt for a combination of training approaches.

Further, in a multi-application environment, designating responsibility for training may be less clear-cut. Training responsibility may split between the card issuer and the individual application administrators. The task order will reflect the types of training assistance needed from the card platform contractor. The task order must include adequate requirements for training.

6.4 Environmental Concerns

Level of Implementation

A key decision is the level at which the implementation is planned. The implementation level will not only affect the size and cost of the procurement, it will also impact technical architecture, legacy system involvement, and numerous organizational issues. If implementation is planned at a level below agency-wide, the design and planning must be coordinated at the agency level to ensure interoperability of systems in the future. Department-wide standards must be supported. Once card platform standards are agreed upon, responsibility must be assigned for enforcing these standards as other entities within the Department begin to move toward the concept of a common card platform.

Stakeholder Relations

One of the first steps should be to identify the main stakeholders in this procurement. The stakeholders will typically include the organizational entities responsible for personnel, card issuance, badging, facilities and systems security, procurement, property, and other administrative functions. A crucial stakeholder, top management, must also be thoroughly committed to the card implementation, because it may well require re-engineering of the agency's business processes and establishing new roles and responsibilities. A representative to convey cardholder concerns is also highly recommended. If commercial applications reside on the card, private retailers may also become part of the equation. The stakeholders must meet early on and determine the objectives, scope, and requirements of the card platform. These stakeholders must address how to govern the interactions with each other. This will be especially challenging if the card platform is to be shared across agencies or with the private sector. Thus, it will be critical to develop an organizational structure to manage the implementation of this card platform, as well as to put in place the interorganizational agreements that will be needed to specify the operating environment of the project prior to the issuance of the task order.

Application providers, who may come from a variety of stakeholder groups, must agree to procedures in a variety of areas, including card issuance, card distribution, card recovery, data sharing, and costing. In a multi-application environment, the application providers may come from either the public or private sectors. In the public sector, agreements initially may be needed among various Federal agencies, but cooperation between government and the private sector may become increasingly common. At issue are how the management structure will be defined and how this structure will function to determine the roles and responsibilities of each of the application providers.

A closely related issue is the impact of contractual agreements among stakeholders. There is a need to take into account the existing contractual relationships between card issuers and system integrators, merchants, service providers or other stakeholders to understand how these relationships may constrain or facilitate cooperation. Where contractual relationships do not yet exist, there may be a need to establish bilateral or multilateral stakeholder contractual agreements.

Currently, in the absence of formal operating agreements, the rules governing the relationships among providers are being worked out through negotiations among interested parties. There is, however, a need for a more formal structure to define stakeholder interactions. Further, there is a need for agencies to plan how they will solicit concerns and establish buy-in with their partnering stakeholders. Whether an agency is coordinating the card platform across multiple organizational entities within the agency, across multiple external agencies, or with private sector entities, the Management Council (described in greater detail in Section 5.2.1) provides a strong model for mutual control of the platform. If the Management Council has been put in place during the planning process, it can be used as an effective forum to address conflicting needs across stakeholders and to resolve issues needed to finalize the task order.

6.5 Publicizing the Awarded Task Order

As part of the task order planning process, agencies should determine strategies for publicizing the availability of the products and services procured under the task order. If the Smart Card task order is at the agency-wide level, lower level sub-divisions need to be made aware of the availability of the task order for their use. A comprehensive communications plan needs to be put in place to enable the lower level subdivisions to understand for what services and products the task order provides, as well as the agency-wide approaches to outsourcing, selected technologies, available standard applications, and proposed integration with agency legacy systems. A guiding document should accompany the task order that describes to the sub-divisions how the task order can be used to accommodate customized needs within the different divisions.

If the task order is awarded at a level below agency-wide, a mechanism is needed to coordinate and ensure interoperability across multiple sub-divisions. In this environment, multiple task orders may be in place that will have to be reconciled to achieve standardization. One approach is to use the Management Council concept, in this case with representatives from different agency sub-divisions that have their own task orders in place.

6.6 Task Order Process

Once all the policy issues have been resolved, the task order can be written. The specific content of the task order will depend upon the circumstances of the agency issuing the task order. Although the *Smart Identification Card: Final Requirements Document* provides a range of requirements for the task order, the agency must customize these requirements for the specific card platform it has decided upon.

In preparing the task orders, agencies must adhere to their agency-specific procurement regulations. Should agencies have technical issues or questions that may affect the task order, the Center for Smart Card Solutions can provide technical assistance with drafting the task order.

6.6.1 OVERVIEW OF THE TASK ORDER

The task order should include the following components:

- **Introduction and Background.** This section should discuss the purpose, goals, and objectives of the procurement and provide any necessary background information on the Smart Access Common ID contract, the participating programs, and related projects or initiatives in other agencies that may impact this project.

- **Terms and Conditions**. This section should include the contractual terms and conditions appropriate to the task order.

- **Current Environment.** This section should give an overview of the current environment of the participating agencies and programs, including any technical specifications that will be of assistance to potential respondents.

- **Statement of Work and Deliverables.** The Statement of Work (SOW) should describe, in general terms, all of the work to be performed by the Smart Access Common ID implementation contractor. This SOW should clearly define the technical systems requirements and any parameters and limitations that may restrict the major tasks and subtasks to be performed by the vendor. This section should identify all documentation, reports and delivery dates for deliverables that are to be furnished by the Smart Access Common ID implementation contractor during the contract period. It presents the agency's functional and technical requirements. Detailed requirements for the Smart Identification Card platform must be included in the task order and a Requirements Traceability Matrix (RTM) can be used to present these requirements. The RTM can organize and track all the agency's requirements collected during the planning stages of this effort. An RTM is a simple, but highly effective tool that can be built using virtually any commercially available spreadsheet package. Once the requirements are included in the RTM, any number of columns can be added to track information pertaining to the specific phase of the implementation lifecycle. While typically developed in the requirements gathering phase, the RTM can be used in a variety of ways throughout the systems development life cycle. For example, the RTM can be used by agencies to:

    - Compare within the feasibility study how different system and technology alternatives would address the requirements and thereby validate the feasibility documents;

    - Identify the similarities and differences in the requirements across different participating agencies and/or programs;

    - Provide a succinct means to communicate requirements to vendors in the implementation task order;

    - Compare how various vendors propose to implement the requirements in the acquisition phase;

    - Track whether and how all requirements have been met by the system design;

    - Assist in the development of test scripts for the functional demonstration phase of the system testing; and

    - Help in the development of acceptance criteria and support the documentation that all system requirements have been met in the acceptance testing phase of the project.

Once the RTM has been developed for the Functional Requirements Document, it can be adapted for inclusion in the task order to help vendors verify that they have responded adequately to all RFP requirements.

- **Response Requirements.** This section should include all proposal, technical, pricing, and formatting requirements for the proposals. It should also include any necessary administrative information, such as designation of contact, submission of questions, and key dates. The Technical Response Requirements generally include:
  - **Overview of the System Design.** This section requires a description of the system configuration including all processing components, databases, interfaces and participating entities.
  - **Preliminary Project Work Plan.** This section requires a project plan with a detailed project schedule, project staffing plan, and project tasks and deliverables.
  - **Design and Functional Specifications.** This section requires the vendor's response to the general system design and functional requirements presented in the Statement of Work;
  - **Pilot and Implementation Plan.** This section requires the vendor's approach for meeting the pilot and implementation requirements specified in the SOW.
  - **Management Plan.** This sections requires the vendor to describe the relevant qualifications, capabilities and resources of any proposed team members for furnishing the services requested in the SOW.
  - **Corporate Qualifications.** This section requires vendors to provide evidence of their corporate qualifications for performing the work specified in the SOW.
  - **Staff Capabilities.** This section requires vendors to describe the capabilities of proposed project staff.
  - **Background Investigations and Clearances** – Articulate the type of security clearances the project will require, when they will be required and who will pay for investigations, which will be conducted. Also indicate if there will be other special building access requirements. If this information is too sensitive for the task order, provide information when requested and when appropriate.
  - **Security Plan.** This section requires respondents to present a comprehensive plan for meeting the requirements of the security policy included within the SOW.
- **Evaluation of Responses**. This section typically discusses how proposals will be evaluated and the scoring methodology to be used.

Section C. of the Task Order is the key section on which agencies must focus their effort. Many of the decisions made in other sections of this Handbook will be the precursor to preparation of Section C. However, the agencies will need to provide input into the following additional sections in order to ensure their Task Order adequately reflects their needs:

- **Section B: Supplies or Services and Price.** Agencies should determine whether the task order requires a turn-key system or system components. Agencies may also use the task order to procure integration services.

- **Section F: Deliveries or Performance.** Agencies should provide information about their required time frame. This section presents the government's delivery schedule.

- **Section H: Special Contract Requirements.** Agencies should work with procurement to develop any unique contractual clauses that need to be included in their task order, including any service level agreements and performance based terms and conditions.

- **Section L: Instructions, Conditions, and Notices to Offerors.** Agencies should determine how they wish the offers to be presented. This section should describe the format of proposal to be provided and indicate whether a written proposal or oral presentation is needed.

- **Section M: Evaluation Factors for Award.** Agencies should decide about their priorities in evaluating the proposals and work in concert with procurement to ensure that the evaluation criteria support the Agency's priorities. The evaluation criteria should be tailored to the specific task order.

6.6.2 THE EVALUATION PROCESS SUMMARIZED

Once the proposals are received the procuring agency must begin the evaluation process immediately. In a well-planned procurement, the total evaluation will be completed within 20-60 days.

Evaluation is an ongoing process, which starts upon the receipt of proposals, continues during written or oral discussions and concludes with the evaluation of final proposal submissions. The purpose of the evaluation process is to determine how well each proposal can meet the contract requirements. Evaluation is accomplished by rating or scoring each offeror against the stated requirements.

Personnel participating in the evaluation process must not discuss or reveal information concerning the evaluations except to an individual participating in the same evaluation proceedings, and then only to the extent that the information is required in connection with the negotiation phases of the acquisition to offerors or to personnel having a need to know.

The Contracting Officer must instruct personnel participating in the evaluation of the requirements of the GSA Standards of Conduct, and ask each evaluator to sign a statement that he/she understands the GSA Standards of Conduct and does not have an actual or apparent conflict of interest relating to the proposed acquisition.

There are three essentials of the evaluation process:

(1) Determine which proposals are acceptable.
(2) Determine from among the acceptable proposals received which one is most advantageous to the Government considering cost or price and other factors outlined in the solicitation.
(3) Provide a sound basis for the Source Selection Authority (SSA) to make an informed and objective selection by:
  (a) Presenting a sharp definition of the issues considered during evaluation.
  (b) Identifying areas of uncertainty as well as those in which there is substantial assurance of a successful outcome.
  (c) Listing the pros and cons of available approaches to the solution of operational, cost, or managerial problems.

The methods used for evaluating proposals should focus on realizing the highest attainable measure of objectivity. Evaluation should frame the issues of the selection decision with such clarity and visibility that the SSA will have little difficulty in arriving at a sound choice.

Proposal evaluation requires a mixture of fact finding, reporting, and the application of professional judgment to provide a well-rounded and comprehensive picture of the adequacy of each offer. This calls for:

(1) Validation of the representations, estimates, and projections presented in each proposal, particularly by comparison with independent Government estimates of performance, schedule, cost, and established requirements.
(2) Examination and judgment of the merits of each proposal submitted as compared to the standards for each factor selected for evaluation.
(3) Examination and judgment of the merits of each firm with respect to other factors bearing on its performance potential (e.g., experience, past performance).

The component tasks of the evaluation vary in number, content, and sequence with each source selection. The following paragraphs describe some of the more typical tasks arranged in their order of their probable occurrence in a source selection, from the receipt of the proposals to the announcement of a decision by the SSA.

Prior to the receipt of proposals each evaluator should be required to read the statement of work and other requirements of the RFP. This review should preferably begin well in advance of the date the proposals are to be received. Furthermore, the Source Selection Evaluation Board (SSEB) should be convened before the proposals are received to discuss the selection plan and scoring methods. In this way, the evaluators can begin work immediately upon receipt of the proposals.

Sometimes language in a proposal is ambiguous. In other instances, proposal language may simply be unclear, and the evaluator cannot understand it well enough to evaluate it without guessing at its meaning. Each instance in which an evaluator finds he cannot make a sound evaluation because proposal language is ambiguous or, if for other reasons, the meaning of the proposal cannot be fully understood, should be identified in writing by the evaluator and provided to the contracting officer. Evaluators must not contact offerors to obtain clarification. The contracting officer must handle any contact with offerors concerning proposals. This will be handled during negotiations.

An offeror will sometimes describe, in general terms, a particular approach proposed for use in performing some part of the contract work but will not provide enough detailed information about its approach and how it will actually apply to permit an evaluation of its feasibility and merit. Each instance in which this occurs must be identified in writing by the evaluator so that the contracting officer can advise each offeror what additional information is needed in order to permit sound evaluation.

Evaluators must identify strengths and weaknesses of the technical aspects of proposals. The documentation of strengths and weaknesses is an essential element of the evaluation report submitted to the SSA. In order to appreciate the technical merits of a given proposal and to compare it intelligently with others, the SSA needs to understand the ways in which a given proposal is considered technically strong, as well as the ways in which it is weak or deficient. As evaluators review each proposal, they should document the strengths, weaknesses, and deficiencies.

Evaluators must identify each respect in which an offeror or the approach being offered is inadequate to meet the Government’s minimum requirements. A determination of unacceptability must be based on minimum requirements that are clearly and definitely stated in the RFP. These requirements may concern either the technical qualifications of the offeror or the adequacy of what is being proposed. For each deficiency identified the evaluator must provide:

(1) An explanation as to why it is felt that one or more minimum requirements outlined in the solicitation will not be met.
(2) An opinion with supporting rationale, as to whether the deficiency can be remedied by the offeror.
(3) An opinion with supporting rationale, as to whether correcting the deficiency, if it is technically feasible to do so, would entail so substantial a revision of the proposal as to amount to allowing the submission of second proposal.

Generally, the fact that a proposal for a negotiated task order is deficient as submitted does not mean that it is excluded from further consideration. It should be discussed, and in order to make discussion meaningful, the offeror should be advised of the nature of the deficiency so that he may have an opportunity to remedy it.

It is to the Government's advantage to maintain a healthy competitive atmosphere throughout the process that leads to final selection. Therefore, any doubts about the propriety of excluding an offeror on the basis that a deficiency is not technically capable of being corrected or that the necessary revisions would result in a virtually new proposal should be resolved in favor of the offeror. Do not forget that GSA must be in a position to defend and support any exclusion with a sound and reasonable rationale.

Examine each proposal in detail to measure its contents against the established standards for evaluation factors, and assign a score (numerical or otherwise) to each factor. This constitutes the core of the evaluation process. The effectiveness of prior planning and preparation becomes apparent at this critical stage of the proposal evaluation process.

Because numerical scores or other types of grading may not convey fully the individual evaluator's judgment of some aspects of the proposal, each evaluator must supplement the rating with a concise narrative evaluation, which includes discussion and interpretation of the limitations of the rating. The narrative records what the contractor offered and how it met the established requirements and summarizes the strong and weak points of what the contractor has proposed. In instances where the contractor has failed to meet a critical requirement, the evaluator assesses what should be done to remedy the deficiency and what the impact of the deficiency (corrected or uncorrected) is on the overall proposal.

All errors, omissions, and deficiencies must be considered by evaluators in determining the initial score to be given the offeror for each factor. Regardless of how they are scored, they must be identified, described, and reported to the contracting officer for discussions with the responsible offeror unless the evidence of technical unacceptability is so strong that further negotiation would not be warranted. Before reaching such a decision, the chairperson of the SSEB should review the matter with the contracting officer, his legal adviser and SSEB members as applicable.

The initial score assigned to each technical proposal is determined by a consensus of the SSEB. Each evaluator should first independently evaluate all the technical aspects of the proposals. By so doing, GSA gains the benefit of having several opinions on the relative technical merits of each proposal. Different evaluators, however, may arrive at differing conclusions on a given point. The true value of the SSEB system emerges when the SSEB as a whole arrives at a balanced conclusion that reflects the different viewpoints and contributions of the SSEB members. Hence, after the individual members have separately evaluated the proposals, including preparation of their narrative explanations, the SSEB should meet and formulate its collective conclusions.

GSA policy requires the relative importance of cost or price be stated in the RFP in terms of its relationship to the combined weight of the other award factors.

In evaluating the offers, the technical evaluation results and price are considered. When the lowest priced acceptable proposal approach is used, the award is made to the offeror submitting the lowest priced technically acceptable proposal.

When the “greatest value concept” is used, the first step is to array the proposals’ technical ratings and prices. Cost or price must be used by the SSEB to judge the value of the work to be done and quality of services to be furnished, and not as an addition to the cumulative score or rating resulting from the technical evaluation.

The technical elements as well as the price proposal must be examined by the contracting officer before a decision is made as to whether or not the proposal is in the competitive range. Cost and technical tradeoffs are performed to determine the best value.

An award can be made based on the initial offer. In order to make an award based on initial offer, the solicitation must include a notice alerting offerors of the possibility of an award based upon initial offers. The Federal Property and Administrative Services Act, as amended by the Competition Act, provides that an award may be made without discussions when it can be clearly demonstrated from the existence of full and open competition or accurate prior cost experience with the product or service that acceptance of an initial proposal without discussions would result in the lowest overall cost to the Government.

Where there is uncertainty as to the pricing or technical aspects of any proposals, the award should not be made without further exploration and discussion prior to award. Also when the proposal most advantageous to the Government involves a material departure from the stated requirements, consideration should be given to offering the other offerors who submitted proposals an opportunity to submit a new proposal. When the contracting officer has evaluated the proposals and made a determination that it is not in the Government’s best interest to award on the basis of initial proposals, the decision must be made as to which offerors will be selected for competitive negotiation. This is accomplished by determining which offerors are in the competitive range.

Negotiations must be conducted with all offerors within the competitive range. At the end of discussions and negotiations, all offerors remaining in the competitive range are provided one final opportunity to submit revisions, which must be received by a common cutoff date.

The SSEB performs a final evaluation. When the final proposal submissions or revisions are returned, those portions of the original submission affected require reevaluation and rescoring. New scores are then computed and the relative standing of the offerors determined again.

When the greatest value concept is applied to a source selection, the SSA has the flexibility to make cost and technical trade-off judgments. The SSA has broad discretion in determining the manner and extent to which the technical and cost or price evaluation results are used.

After the proposals have been evaluated, an initial evaluation report should be prepared and furnished to the contracting officer by the SSEB chairperson and maintained as a permanent record in the contract file. The final evaluation report should rank each offeror’s proposal from the most advantageous to the least advantageous.

The final report should include a recommendation to the SSA regarding the source(s) to be selected. A recommendation to award a higher-priced, higher-scored offeror must be supported by specific recommendation that the technical superiority of the higher-priced offer relative to other offers in the competitive range warrants the additional cost. The rationale for the finding of technical superiority must be documented in detail.

When the SSA has made the choice, the chairperson of the SSEB prepares a document setting forth the rationale of the decision for the SSA's signature. The selection statement should stand-alone and cover the following basic points.

(1) A description of the acquisition;
(2) The names of the offerors;
(3) A summation of the strengths and weaknesses of each proposal and offeror; and
(4) Reasons why the firm selected provides the greatest probability of satisfying the Government's requirements.

After the SSA signs the source selection decision document, the contracting officer executes and distributes the contract.

6.6.3 NOTIFICATION AND DEBRIEFING OF UNSUCCESSFUL OFFERORS

The contracting officer will provide notification to each offeror whose proposal was in the competitive range but was not selected for award. The offerors will be told the number of proposals received, the name of the offeror receiving an award, the total award price, and the reasons that the proposal was not accepted.

If an offeror requests, it can receive a debriefing. The contracting officer chairs this debriefing, and the individuals who conducted the evaluations provide support. The debriefing includes the Government's evaluation of the significant weaknesses or deficiencies in the offeror's proposal, if applicable; the overall evaluated cost or price and technical rating, of the successful offeror and the debriefed offeror; past performance information on the debriefed offeror; the overall ranking of all offerors, when any ranking was developed by the agency during the source selection; a summary of the rationale for award; for acquisitions of commercial items, the make and model of the item to be delivered by the successful offeror; and responses to questions about whether source selection procedures contained in the solicitation and applicable regulations were followed. The debriefing does not include point-by-point comparisons of the debriefed offeror's proposal with those of other offerors. Moreover, the debriefing does not reveal any information prohibited from disclosure by FAR 24.202 or exempt from release under the Freedom of Information Act.

7. SUMMARY RECOMMENDATIONS

From the analysis of existing smart card pilots and review of requirements from a number of agencies a number of key recommendations have emerged that form the foundation for the implementation of a Smart Identification Card platform. These fundamental requirements, presented below, are inherent to the successful implementation of a card platform that can be used by multiple programs. Public programs can use this platform to re-engineer their current processes to take advantage of electronic service delivery mechanisms, capitalize on efficiencies already commonplace in the commercial world, and reduce overhead by spreading their costs across an ever-widening range of potential participants. While agencies initially may be reluctant to share a government card platform with the private sector, the trend to cooperative projects will increase in the future. By working hand-in-hand with the private sector, government programs can offset their costs, increase the efficiency of their operations, and provide the impetus for card-based applications that can be easily adapted for commercial markets.

While a few of the requirements are unique to a platform developed for the government employee audience, many others can be transferred to card platforms targeted at citizens, corporations, or consumers. The basic conceptual foundation for a multi-application card must be flexible enough to adapt to changing target audiences and customer needs. Consequently, many of the central technical and organizational precepts underpinning a Smart Identification Card multi-application platform are meant to be scalable to increasingly open environments as the movement to electronic commerce affects the delivery of government and commercial services to ever-growing populations.

In migrating toward these open, chip card-based environments, program developers can also benefit by recognizing some of the primary levers for driving program participant satisfaction, acceptance, and participation at all levels:

- **Assignment of Liability Can Be Negotiated.** Banks and industry indicate that this may be their greatest perceived risk in a multi-application program. If government or individual programs were willing to help bear this risk, commercial providers might find participation in these programs more appealing.

- **Cost Allocation and Revenue Offset.** Equitable distribution of cost is often the driving pressure point in a program implementation. Costs must be allocated according to the level of benefit achieved by participants, with costs being shared by both government and commercial sectors. Revenues that are generated from commercial card usage should be used to reduce the government's overall costs.

The above points, along with the "lessons learned" in Section 2.6, should be considered as applicable to not only the government employee card platform but to almost any card program.[35]

7.1 Technical Recommendations

Throughout a Smart Identification Card project, the technologies and technical issues that define the fundamental form and function of a card-based program serve as a launching point into other areas of discussion. Clearly, establishing the technical basis of a card platform is an essential early step in a program development. However, identifying the technical foundation cannot be done in isolation from the

[35] Much of the information in this section is based upon pilot evaluations , interviews, and ideas about an Enhanced EBT Smart Card Platform contained in the following report:
Guidelines For Implementing An Enhanced EBT Multi-Application Smart Card Platform – Draft, Phoenix Planning & Evaluaion and Coopers & Lybrand, June 5, 1998.

organizational, management, legal, regulatory, and cost issues. Over the course of a project, it is clear that there are a variety of existing, technical design solutions available to support many stakeholder requirements. Consequently, the technologies that define the card platform must be viewed as enablers to achieving the program goals.

The discussion below highlights some technical recommendations that agencies should consider in designing their individual card platforms:

- **Multiple Technology Card.** A multiple technology card (e.g., using magnetic stripe and chip) can be the foundation of the program. The industry unanimously supports a mix of these technologies providing a step-by-step migration toward a purely chip-based environment. In developing a smart card program, agencies should also consider other card capabilities such as contactless chips that may better match the needs of particular applications (e.g., physical access control and transportation). While multiple technology cards may play a critical role in the migration to smart cards, it must be pointed out that each technology and the printing on the card are single points of failure and, as such, add complexity to achieving life expectancy of the card.

- **Fixed versus Dynamic Allocation of Card Memory.** In the not too distant past, industry consensus supported the selection of a fixed allocation of memory because a fixed allocation model was more manageable, easier to implement, and less costly than the dynamic model. However, as the technologies associated with dynamic allocation have matured, they have become more stable and are likely to become the preferred model because of the flexibility they allow for changing applications.

- **Non-Dynamic versus Dynamic Loading of Applications.** The fixed allocation structure (previously discussed) supports the ability to install predefined applications and data structures at the time of card initialization, rather than deal with the complexities of adding these applications downstream. In a dynamic allocation model, the applications are loaded on an as-needed basis, typically followed immediately by additional card personalization steps. Because of an agency's need to be able to add additional applications to the card platform in the future, it is recommended that agencies strongly consider chip operating systems that support dynamic loading of applications.

- **Optimal Use of a Common Data Field.** Because of the existence of substantial shared data across programs and applications, the card design should maximize utilization of a common data field. During the design phase, a detailed data requirements analysis for each application will result in a clear indication of candidate items for a shared data field. These common data should be available to multiple applications, with access being granted by the specific application being used. Ultimately, the various application providers will need to negotiate the final content of the common data field.

- **Security and Access to Card Applications.** The driving objective of logical security and control decisions should be to match protection mechanisms with the level of security and sensitivity required by each application in a multi-application platform. However, these decisions cannot omit consideration of the cardholder. Consequently, it is suggested that protection mechanisms should vary by application, to the extent that the mechanisms do not become so complicated as to confuse or overwhelm the cardholder and discourage card usage. For example, some medical applications might require that both user and provider PINs are verified prior to accessing or updating data, while other applications may not require any PIN entry after the initial card authentication process. Agencies with the highest level of security requirements should strongly consider biometrics or digital certificates to be used to authenticate identity prior to access to applications.

- **Digital Signature Capability.** As the government moves to an employee identification smart card platform or citizen cards, a digital certificate becomes increasingly important, if not indispensable. In these environments, the digital signature used in signing documents and in non-repudiation meets a widely anticipated need. A caveat that must be kept in mind, however, is that the latest legal opinion suggests that unless the private ID key is generated on the card and never leaves the card, it will be difficult to prove non-repudiation. Even those agencies without an immediate need for digital signature capability should consider including it within its platform requirements. Building digital signature capability into the original card design makes good business sense. In this way, it can be cost-effectively available for use once it is needed to provide secure Internet access for government service delivery.

- **Data Intake and Card Issuance.** Centralized and decentralized data intake and card issuance should both be considered, depending on the individual characteristics of each agency and/or program office. No single approach will be viable for all circumstances. Even within a given program, no one solution will suffice because the method of service delivery may vary depending upon whether the program office delivering in a particular part of the government is rural or urban, high or low traffic, or easy or difficult to secure. Agencies should study the individual characteristics of the program offices to be included in a card program. Once this assessment has been completed, a physical security strategy can be developed that takes into account the unique characteristics of the various agencies sharing the platform.

- **Mix of Open and Closed Applications.** If agencies opt to have financial applications (e.g., credit/debit and stored-value) on the card platform, these applications should be open, allowing use of the card nationwide, and even internationally. The credit/debit and stored-value applications should take advantage of the existing commercial networks, perhaps supporting the concept of the card issuer as a player in this network. For the short term, the Smart Identification Card platform may benefit from the relative simplicity of defining other card applications (especially those that are health care-related) as closed applications. However, it is quite realistic to design a Smart Identification Card platform to accommodate a migration to open health care and other interoperable applications. To facilitate this migration, the initial design agents should make extensive use of G8 and other widely accepted standards that would encourage additional agency participation as the program evolves.

- **Backup Procedures and Card Replacement.** Balancing recipient convenience with the importance of adequate security, agencies should create shadow files of all transactions and route these at least daily to the application owner's remote database. To ensure prompt and convenient customer service in the case of a card loss, the prime issuer maintains a client registry that provides pointers to all application owner databases for all applications active on the card. The prime issuer uses the client registry to determine which applications are active and queries the application owner for the client backup database in the case of card replacement. This solution achieves one-stop card replacement to ensure customer convenience, while decentralizing maintenance of data to allay privacy and storage capacity concerns.

Agencies may want to consider using GSA's Center for Smart Card Solutions or consultants to assist in planning their smart card program. A review of the request for proposals (RFP) prior to full release is also useful to ensure that the RFP is asking for items that are practical and realistic.

7.2 Organizational and Management Recommendations

To be successful, the Smart Identification Card platform must be built upon a solid organizational and management structure that clearly defines roles and responsibilities within the context of meaningful, enforceable agreements and realistic business relationships among the diverse participants. Any useful management structure must be able to provide an unambiguous roadmap to coordinating and controlling the myriad of interests that will converge when stakeholders with diverse needs come together to implement a multi-application card. Public and private sector resources must be skillfully directed in a common effort that maximizes the capabilities of each to meet the needs of all. Through a public-/private-sector partnership, a “win-win” approach can result in greater functionality for the card user, cost containment for the government, and new marketing opportunities for industry.

If it is to successfully manage a multi-application card program, the government must develop and administer a formalized rules structure that codifies the business arrangements among the parties. Based on operating rules and working agreements to which all participants subscribe, these business relationships define the key roles and the interrelationships among these roles in a card implementation. Which entities actually fill these key roles may well shift depending on the business relationships that are ultimately implemented. These contractual relationships must be built among card issuers, application owners, programs, card recipients, providers, retailers and other stakeholders and they must define how all of the players allocate costs, responsibilities, and control. The commercial card associations in the credit and debit industries today provide such a standard operating environment.

To successfully achieve a multi-application platform, the government must rethink its current program-based orientation and put in place a viable structure to coordinate the card platform while supporting public/private cooperation. The government should capitalize on the significant “lessons learned” in Electronic Benefits Transfer (EBT) card implementations and the Quest Operating Rules. In these prior EBT efforts, the National Automated Clearing House Association (NACHA) EBT Council provided a successful model of public-private partnership upon which to build operating rules and contractual relationships. Over forty states have voluntarily agreed to participate in the Council because they directly benefited from such participation. By joining the EBT Council and endorsing the QUEST operating rules, these states achieved surety in terms of their roles, expectations, liabilities, and risk. Emulating the EBT Council model, a Management Council could be implemented as a formal structure for the guidance of a Smart Identification Card multi-application platform.

Such a Management Council, composed of representatives of all participating government agencies/programs, private sector companies (including application owners, service providers, third-party processors, retailers, and medical providers) and employee advocacy groups, can be key to the success of a program. The Management Council can function as both the symbolic and practical focal point for the critical public/private sector partnership, benefiting all stakeholders of a multi-application Smart Identification Card.

Along with the Management Council, a tiered approach to delegating roles and responsibilities among participants is needed to ensure consistency and ongoing cooperation. As was presented earlier in section 5.2.2, these key responsibilities include: card owner; program/agency office; prime issuer; application owner; and cardholder. In addition to an effective management structure, clearly defined roles and responsibilities, and operating rules that reduce risk through liability assignment, the government platform must include incentives for commercial participation if it is to be successful. The government must adjust its perspective to find ways to support the concept of private/public partnership, revising policies to allow resale of software, usage fees, branding, and other marketing mechanisms to encourage commercial participation.

7.3 Legal Recommendations

Feedback from a number of pilot participants confirms that the protection of client privacy is a key legal issue that will affect the success of a government or citizen multi-application Smart Identification Card platform. Employee card usage will only take place if cardholders are assured that the data stored on the card are not going to be compromised under any circumstances.

As the Federal government becomes involved in a multi-organizational, multi-application smart card program, the importance of compliance with Federal privacy protection guidelines will grow. In such a multi-dimensional environment, the challenge of implementing privacy protections will increase exponentially, as will the potential degree of liability faced by the government. Consequently, the implementation of a multi-application Smart Identification Card platform will demand the accompanying definition of a comprehensive privacy program, based on requirements set by privacy experts, with input from privacy advocacy groups and ongoing involvement of a full range of stakeholders. Partners will have to not only build privacy safeguards into technical and managerial processes but also address employee fears and educate cardholders about their rights and responsibilities.

7.4 Cost Recommendations

Several types of costs must be considered to implement a multi-application Smart Identification Card platform, including infrastructure, start-up, and ongoing costs. The investment required to migrate to the chip infrastructure needed to support this platform will be substantial. For cards used across programs or agencies, these costs can be shared by all agency or program participants.

Start-up and operations costs also must be taken into account. Evenhanded cost distribution across programs and incentives to entice the commercial sector participation are needed to implement programs on a large scale. Government programs, commercial application vendors, retailers, medical providers, and employees can all contribute in some way to the financial viability of a multi-application card. Cost-sharing arrangements are needed that encourage commercial participation and adhere to the following guiding principles:

- Distribution of application development costs across the programs that share the application, based on usage statistics;
- Provider contributions recouped from cost savings achieved through reduced paperwork processing time, consolidation of processes, automation of existing processes, and reductions in personnel achieved through automation;
- Contribution of program funds recovered through savings in paperwork processing, reductions in staff time, consolidated processes, and reduction in fraud (e.g., reduced staff time through a common intake process);
- Retailer or provider investment for interfaces to their legacy systems;
- Vendor contributions recouped through fees for use of commercial applications such as an electronic purse on the chip;
- Employee contributions for voluntary personal use of electronic purse, credit or debit applications; and
- Charging cardholders for other commercially-provided, value-added services that are outside the closed government applications.

Despite contributions from other stakeholders, the primary responsibility for funding the Smart Identification Card platform for the foreseeable future will rest with the government programs using the card. Although there are many cost allocation methodologies, one recommended approach earmarks costs according to program usage by each application, thereby assigning costs based on the degree of benefit realized by the participating programs. Costs that can be directly attributed to a specific agency or program should be paid for by that program. These costs may include the client account management fee, transactions, and other assets used by the particular program in the implementation of its application (described in greater detail in section 5.4.2). All other costs (e.g., core card-related services fee, capital investment for infrastructure for shared applications, and non-transaction-based application services) must be distributed based on a negotiated cost allocation methodology.

Depending on government policy, there are various potential sources of revenue that can offset government costs. Government should partner with the commercial sector to take advantage of these revenue-producing opportunities and provide a "win-win" scenario for the government and commercial stakeholders.

7.5 Standards and Interoperability Recommendations

The success of the Smart Identification Card platform will ultimately depend upon whether the system is viable in an open, interoperable government and commercial environment. Interoperability is more than just a technical obstacle—it is also a management and administrative issue. In order to achieve interoperability across other agencies and eventually with retailers and medical providers, partners will not only have to develop technical specifications, terminal interface protocols, and application specifications, but also operating specifications and business agreements.

The Management Council should be given the responsibility of taking steps to ensure that the system continually migrates toward interoperability. The Management Council should manage standards adherence and work with other industry groups to foster the development of applicable standards and to monitor standards development. To facilitate this migration, the Management Council should consider the following recommendations:

- **Adopt the GSC-IS v2.1[36] and other related government/industry efforts.** A major goal of GSC-IS 2.1 was to lay the foundation for interoperability for contact and contactless cards. Agencies should use the GSC-IS v2.1 to the extent practical, as a framework for promoting interoperability throughout the government. Additionally, the agencies should ensure that all vendors awarded contracts under the Smart Access Common ID contract adhere to the GSC-IS v2.1. Other groups such as the Federal PKI Steering Committee and the Biometrics Consortium are developing standards and APIs that will also help achieve interoperability.

- **Monitor standards development within the smart card industry groups.** This will allow the partners to benefit from lessons learned in other pilots.

- **Adopt G-8 Health Record Format.** This will allow an employee medical application to transition from a closed, to an open, health care system. By adopting the G-8 format, private insurers can read or write to the data on the card using their own applications, thereby allowing greater flexibility for the cardholder. Government agencies participating in medical care provision will be able to exchange medical data if they all adhere to the G-8 health record format. In addition, the adoption

[36] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

of the G-8 health record format may facilitate the resale of government medical applications to the private sector, resulting in cost savings to the implementing agencies.

- **Develop operating rules to cover shared government applications.** Expand the concept of operating rules for financial applications to apply to other shared applications. By setting the operating environment in place, it will be far easier to achieve interoperability across non-financial applications.

Until an interoperable infrastructure is achieved, it will be difficult for multi-application cards to achieve widespread acceptance. Multiple technology cards will provide the bridge from the existing infrastructure to the evolving interoperable infrastructure. As interoperability evolves, it will increasingly provide the foundation for multi-application smart cards to be used by an increasing number of service providers. Just as the multiple technology card provides a technical “bridge” from the existing magnetic stripe infrastructure to the emerging chip environment, so too must there be a slow migration to the new management and cost sharing arrangements required in a multi-application environment.

7.6 Lessons Learned

To prepare this Handbook, participants from a number of smart card projects were interviewed and asked to offer any lessons learned from their experience. The lessons resulting from these interviews represent important concepts for agencies to consider when establishing their own multi-application smart card program. While there are certainly many lessons to consider, the following are considered as critical success factors for ongoing multi-application card based programs:

- Private sector partnerships are an integral part of any card program. The private sector can, in many instances, deliver services more efficiently and more cost effectively than independent government initiatives.

- Government cannot afford to reinvent capabilities that are available in the private sector. Government needs to “piggy-back” multi-application card capabilities on existing commercial infrastructures, not reinvent them for proprietary applications.

- Early stakeholder involvement and commitment is critical to program success.

- A viable management structure that includes representation from all stakeholder groups participating in the platform must be established from the earliest stages of a project. A coordinated effort between an agency’s management in both the physical access and logical access sides is essential.

- Contractual and implementation personnel should be in constant communication with one another working together towards a common goal. An agency’s budget is often the driver for the smart card implementation. Business case development is a key element of gaining approval to proceed with a project and obtaining the necessary budget. An agency’s business case needs to show varying applications of its smart card program beyond increased security to include areas such as digital signature, financial purse, parking, and metro.

- Increasing the number of features on a card stimulates adoption and decreases the number of lost cards.

- Interoperability is, perhaps, the most critical success factor in promoting adoption and diffusion of sustainable card-based technologies. It is fundamental that an agency understands its interoperability goals as they relate to its card and system requirements including physical access, logical access, PKI and biometrics.

- Privacy concerns remain one of the most formidable barriers to widespread adoption of card technology. A thorough marketing and education plan is essential to educate an agency's user population on the use of smart card technology as well as to address privacy concerns.

Perhaps the overriding theme across these lessons can be found in the adage that "the whole is greater than the sum of its parts." Card-based programs must look to build teams that institutionalize this philosophy and foster an environment where value is created, rather than simply transferred.

7.7 Looking Forward – Implications of an Employee Multi-Application Smart Card Identification Platform

Applying the lessons learned from the multi-application pilots is an important step in establishing an interoperable smart card-based government-wide employee identification card. However, the nature of the smart card itself – particularly, as a foundation for the government-wide interoperable employee identification card – creates an expectation that there are many new lessons to be learned and capabilities to be leveraged.

Looking forward, the government envisions that multi-application smart card technology will set new precedents not only in how technology is used, but also in how these technologies enable a new relationships between government, industry, and citizens. Smart cards can revolutionize how the government does business because they provide:

- **A Bridge between Unique, Proprietary Systems and Applications.** Smart card technology provides a vehicle for interacting with various independent systems that could otherwise never communicate without substantial investment in connectivity and interface programs. Consequently, the smart card represents a low-cost, time-saving solution to achieve interoperability between systems. Even in the relatively simple model of a closed government card sharing applications across agencies, the opportunity for time and cost efficiencies is staggering.

- **A Basis for Dramatically Enhancing Identification and Authentication Capability.** Smart card-based technologies offer a variety of enablers for reliably identifying participants and authenticating exchanges in the digital world. Biometrics, for example, provide added levels of real and, perhaps more importantly, perceived security through identification and authentication. On another level, digital signature and PKI technologies provide the ability to authenticate an individual's identity online—thereby allowing secure transactions over the Internet. Today, reliable means of identification and authentication loom as the greatest barrier to widespread electronic communication and commerce.

- **A New Model for Communication between the Government, Industry, and Citizens.** As card-based technologies spread across the government sector, their impact will be reflected in the operations of commercial industry as well as in the day-to-day events of private citizens. Traditionally, government-industry and government-citizen interaction is driven by the "communicate down" model. In this model, industry and citizens mainly respond or react to a government action. Through enabling card-based capabilities, industry, for example, will recognize a new model of doing business with the government that is founded on real-time communication, timely transactions, cost efficiencies, and processes that are mutually beneficial. This new model has the potential to erode barriers to effective communication and other impediments that have traditionally discouraged partnerships between government and industry, particularly at the small business level. At the citizen level, the impact of the new model may become evident in the willingness of the public to readily *initiate* communication and interaction with the government, rather than simply respond to government requests. Moreover, the public perception of the benefits of these card-based capabilities will bring better access to government services. Similar to the evolution of automated teller machines, card-based capabilities will move from a "convenience" to a "need." In the private sector, as citizens increasingly have access to personal computers, businesses will enhance communication with their customers. Increased usage of PCs will expand citizen access to electronic banking and Internet purchasing, as well as to electronic delivery of government services.

Paralleling this migration are numerous benefits such as reduced transaction costs through technology and economies of scale, increased customer convenience, and improved speed and quality in service delivery. From today's predominantly face-to-face, common intake/output model (that is typically very costly and time consuming), communication will naturally evolve to an electronically based "many to one" or "one to many" interface (that leverages the power on the Internet to rapidly disseminate or gather information to/from a wide or targeted audience.) By shifting to electronically-based intake for participant data collection supporting service delivery processes, government will realize a dramatic reduction in required personnel and corresponding costs while consumers will realize significant increases in convenience and speed of service delivery. Additionally, the private sector will be connected to an untapped market, providing a variety of economic incentives and profit opportunities. More importantly, however, are the opportunities to redefine communication paths between stakeholders that will arise through this migration. This migration should force us to rethink how citizens, retailers, providers, and government programs are interacting on a daily basis. Holistically, card-based technologies allow for total change in how services are delivered.

The path from an employee card that shares functionality and data across multiple agencies to a citizen's card that shares transactions between the government and its constituents is logical and can yield benefits for all stakeholders. It is anticipated that the Smart Access Common ID contract will proliferate smart card technology across the government, causing agencies first to consider how this technology can be used to achieve internal operational efficiencies, but soon to examine how it can be used to better serve its customers. Card-based technologies, at a minimum, provide public electronic access to the Federal government's services and information. More likely, card-based technologies will do more than simply replace manual processes with electronic processes – they will dramatically redefine the way we communicate.

7.8 Maintaining On-Going Progress

Through GSA's second version of its 'Government Smart Card Handbook', GSA has responded to the recommendations defined by GAO in its January 2003 report on electronic government[37]. The items below detail GSA's response to GAO's recommendations of: updating the 'Government Smart Card Handbook', referencing the GSC-IS in the standards section, providing guidance on using the interoperability specification, and referencing critical technologies such as contactless cards and biometrics.

- Successfully updated the original version of the 'GSA Smart Card Policy and Administrative Guidelines.'
- Section 2.1.9 Synopsis of Standards includes a detailed reference to the Government Smart Card Interoperability Specification version 2.1[38] (GSC-IS v2.1, also known as the NIST Interagency Report 6887 – 2003 edition).

[37] ELECTRONIC GOVERNMENT - Progress in Promoting Adoption of Smart Card Technology, GAO, January 2003.

[38] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification,* Version 2.1, July 16, 2003.

- Section 2.1.6 provides explicit guidance on using the GSC-IS v2.1[39] for contact and contactless smart card interoperability.
- Section 2.1.5 Smart Card Interfaces Contact and Contactless Card describes the technology and capabilities of contactless cards.
- Section 2.4.5 Biometrics and Smart Cards describes the current status of biometric technology, as well as the technologies strengths and weaknesses.
- Section 4.2.1 Technology Capability describes in detail the current uses for smart card technology including PKI and biometric applications.

[39] Ibid.

8. APPENDIX A – GLOSSARY OF TERMS

Algorithm – A computational procedure used for performing a set of tasks such as encryption process, digital signature process, or cardholder verification.

American Association of Motor Vehicle Administrators (AAMVA) – An association of administrators representing motor vehicle agencies in the United States and Canada.

Anti-tamper – Refers to the technology available to prevent unauthorized alteration or modification of cards.

Anti-tearing – The process or processes that prevent data loss when a smart card is withdrawn from the contracts during a data operation.

Application Program Interface (API) – A formal specification of a collection of procedures and functions available to a client application programmer. These specifications describe the available commands, the arguments (or parameters) that must be provided when calling the command, and the types of return values when the command execution is completed.

Attribute Authority (AA) – An entity responsible for issuing and verifying the validity of an attribute certificate.

Attribute Certificate – A message, similar to a digital certificate, which is intended to convey information about the subject. The attribute certificate is linked to a specific public key certificate. Thus, the attribute certificate conveys a set of attributes along with a public key certificate identifier or entity name.

Authorization – The process of determining what types of activities or access are permitted for a given physical or logical resource. Once the identity of the user has been authenticated, they may be authorized to have access to a specific location, system, or service. In the context of logical access control, the process whereby a user’s privileges to access and manipulate data objects are assigned.

Automated Response Unit (ARU) – A designated system for answering telephone calls and providing information to callers via recorded messages, or transferring calls to a customer service center (CSC).

Bar Code – The set of vertical bars of irregular widths representing coded information placed on consumer products and other items (such as identification cards) that may require this type of identification.

Binding – An affirmation by a Certificate Authority/Attribute Authority (or its acting Registration Authority) of the relationship between a named entity and its public key or biometric template.

Biometric Template – Refers to a stored record of an individual’s biometric features. Typically, a “livescan” of an individual’s biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template.

Biometrics – An automatic identification process for identity verification of individuals based on unique behavioral or physiological characteristics. These are unique things that we do or unique physical characteristics that we have. Behavioral biometrics include voice, signature, and keyboard typing technique. Physical biometrics include fingerprint, hand geometry, facial recognition, and iris and retinal scan.

Bridge Certificate Authority – An entity that links two or more Certification Authorities who do not have a cross-certification agreement in place. The Bridge Certificate Authority allows CAs to validate each other's certificates.

Card Accepting Device – A device that is used to communicate with the Integrated Circuit Card (ICC) during a transaction. It may also provide power and timing to the ICC.

Card Hot List – A list of cards that have been reported as lost, stolen or damaged.

Card Initialization – Refers to the process of preparing a card for use by performing the following tasks: searching for initialization files, locating definite values to use in place of variable values, and loading these values.

Card Personalization – Refers to the modification of a card such that it contains data specific to the cardholder. Methods of personalization may include encoding the magnetic stripe or bar code, loading data on the ICC, or printing photo or signature data on the card.

Card Printer – Equipment capable of printing information on the physical surface of the card.

Card Reader – Equipment capable of reading the information on a card such as that in the magnetic stripe or chip.

Certificate Authority (CA) – The Certificate Authority is a component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates. Digital certificates may contain the public key or information pertinent to the public key.

Certificate Arbitrator Module – (CAM) – A system that interfaces with agency applications that receives a request for the status of a certificate, passes the certificate validation request to the appropriate CA, receives the certificate validation request response, returned from the CA, and reports the response to the requesting agency application.

Certificate Policy – A document that sets forth the rules established by the policy issuing entity governing the issuance, maintenance, use, reliance upon, and revocation of digital certificates.

Certificate Repository – A database of certificates and other PKI-relevant information available on-line.

Certificate Revocation List (CRL) – A periodically issued list, digitally signed by a CA, of identified certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates' serial numbers, and the specific times and reasons for suspension and revocation.

Certification Practice Statement (CPS) – A document that states the practices that a Certificate Authority employs in issuing certificates.

Chip (Card) Operating System (COS) – The operating system within a card's integrated circuit that interprets commands sent by the workstation and performs the functions requested.

Compromise – A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.

Contact Interface – A chip card that allows interface through a contact. A contact is an electrical connecting surface on an ICC and/or interfacing device that permits a flow of energy current, thereby transmission of data.

Contactless Interface – An ICC that enables energy to flow between the card and the interfacing device without the use of contact. Instead, induction of high-frequency transmission techniques is used through a radio frequency (RF) interface.

Cryptographic Co-Processor – An integrated circuit chip processor that performs cryptographic functions.

Cryptography – The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

Data Integrity – A condition in which data has not been altered or destroyed in an unauthorized manner.

Digital Certificate – A portable block of data, in a standardized format, which at least identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certificate authority issuing it.

Digital Signature – A unique electronic signature that accompanies documents and messages. The digital signature serves two primary functions: verifies the authenticity of the party sending the message, and verifies that the content of the message has not been altered.

Digitized Signature – A written signature that has been read by a computer scanner and converted into digital data.

Distinguished Name – A set of data that identifies a real-world entity, such as a person in a computer-based context.

Electronic Purse – A mechanism that allows end users to pay electronically for goods and services. The function of the electronic purse is to maintain a pool of value that is decremented as transactions are performed.

Encryption – Refers to the process of translating data into a cipher, a more secure form of data. Encrypted data is less likely to be intercepted and accessed by unauthorized persons. This mechanism is particularly important in executing sensitive transactions.

Enrollment Station – A designated workstation that collects data to enroll individuals for the Smart Access Common ID Card.

Extensions – Extension fields in X.509 Version 3 certificates.

False Acceptance Rate (FAR) – Refers to the rate at which an unauthorized individual is accepted by the system as a valid user.

False Rejection Rate (FRR) – Refers to the rate at which an individual authorized to use the system is rejected as an invalid user.

Graphical User Interface (GUI) – A user interface to a computer that is graphics-based, rather than textual or command-based.

Hashing – A software process which computes a value (hashword) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

Identification Authentication – The process of determining the identity of a user that is attempting to access a physical location or computer resource. Authentication can occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, or other techniques.

Integrated Circuit Chip Card – A card containing a microcontroller and memory capable of making decisions and processing data.

International Standards Organization (ISO) – A worldwide organization dedicated to fostering the development of systems standards. National standards organizations from 100 different countries are members of the ISO, including the United States (American National Standards Institute – ANSI). Member organizations participate in the development of ISO standards.

Interoperability – Refers to a system or a product that is capable of operating with another system or product directly, (i.e., without any additional effort from the user). Interoperability can be achieved through mutual conformance to a set of common standards and specifications. Interoperability may also be achieved through the use of a "service broker" able to convert one interface into another interface directly.

Key – A value that particularizes the use of a cryptographic system.

Key Management – The process and means by which keys are generated, stored, protected, transferred, loaded, used, revoked, published, and destroyed.

Key Pair – The key pair consists of a private key and its matching public key.

Lightweight Directory Access Protocol (LDAP)– LDAP is an emerging software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

Logical Access Control – An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

Local Access Panel/Controller (LAP/C) – Refers to a device used to monitor and control access to a site by utilizing an intelligent local processing capability in combination with downloaded database processing.

Mean Time Between Failures (MTBF) – The estimated length of time that a system is available and operational between failures.

Mean Time To Repair (MTTR) – The estimated length of time needed to bring a system back up and make it fully operational following a system failure.

Nonrepudiation – Refers to the determination that data was sent by one party and received by another party, and can be verified by the inclusion of information about the origin or delivery of the data. Nonrepudiation protects both the sender and the recipient of data from false claims that the data was either not sent, or not received.

Open Database Connectivity (ODBC) – Refers to an open or standard application programming interface (API) used to access a database. A database that is ODBC-compliant facilitates the importing, exporting and converting of files from external databases.

Open Systems Environment – A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. An open platform is composed of hardware and software components that adhere to common standards and are non-proprietary such that multiple vendors can supply these components interchangeably. In an open platform, components from multiple vendors using different technological approaches may be assembled and interoperability across products can be ensured. The objective of an open platform is to achieve vendor independence and allow easy transition to emerging technologies.

Personal Identification Number (PIN) – A private series of numbers that a user knows that are used to increase confidence in a user's professed identity.

Physical Access Control – Refers to an automated system that controls an individual's ability to access to a physical location such as a building, parking lot, office, or other designated physical space. A physical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token prior to providing access. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

Point of Sale (POS) – Generally refers to a site where purchases are made. For the purposes of this document, POS refers to a site where purchases may be made electronically through an electronic cash register or card acceptance device.

Primary Account Number (PAN) – A unique identifying number used to reference a financial account.

Private Key – A mathematical key (kept secret by the holder) used to create digital signatures, and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Proximity – Refers to a technology used to provide physical access control. This technology uses a contactless interface with a card reader. An antenna is embedded in the card, which emits a unique radio frequency when in close proximity to the electronic field of the card reader.

Public (Asymmetric) Key Cryptography – A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who is to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Infrastructure (PKI) – The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Further, a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Included also in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

Public Key – A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

Radio Frequency Identification (RFID) – Refers to an access control system that features a tag embedded with both a circuit and an antenna. As the antenna enters the electronic field of the reader, it generates energy for the circuit, and transmits the identification number in the tag to the reader.

Registration Authority (RA) – The Registration Authority is a component of the Public Key Infrastructure. The RA acts as a gatekeeper by providing verification to the Certificate Authority before granting a request for a digital certificate.

Relying Party – A recipient who acts in reliance on a certificate and digital signature.

Renewal – The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.

Revocation – The process of permanently ending the operational period of a certificate from a specified time forward. Generally, revocation is performed when a private key has been compromised.

Root – The CA that issues the first certificate in a certification chain. The root's public key must be known in advance by a certificate user in order to validate a certificate chain.

Secret (Symmetric) Key Cryptography – A cryptographic system that uses the same key, known as a "secret key algorithm" to encipher and decipher messages. This is contrasted with asymmetric key cryptography, which uses a secure public/private key pair.

Secure Access Module (SAM) – A software module contained in a card access device that allows the card and terminal to mutually authenticate each other.

Sensitive Compartmentalized Information Facility (SCIF) – A designated physical location that requires high-level security clearance for entry. An area that is generally used to maintain top secret documents and systems.

Source Selection Evaluation Board (SSEB) – A group of government employees charged with evaluating offerors' responses to a task order and determining to which vendor the task order is to be awarded.

Speaker Identity Verification (SIV) – The key feature of voice recognition software that extracts and compares unique features of a speech sample with a known sample, and accepts or rejects access based on this comparison.

Storage – An electronic and/or mechanical-magnetic device that holds information for subsequent use or retrieval.

Subscriber – A person who is the subject of, has been issued a certificate, and is capable of using, and authorized to use, the private key that corresponds to the public key listed in the certificate.

Tampering – Refers to any unauthorized alteration or modification of a card.

Token – A hardware security token that contains a user's private key(s), public key certificate, and optionally other certificates.

Wiegand – Refers to a technology that provides physical access control capability by way of a contact interface that is "swiped" similar to a magnetic stripe card. A Weigand card is more secure and durable than a magnetic stripe card because it is embedded with a magnetic coating during production.

9. APPENDIX B – SURVEY OF FEDERAL SMART CARD PROJECTS

The following matrix provides general information on key Federal smart card projects. A variety of examples from both military and non-military Federal agencies are presented. Each project entry provides a description of the project, the project technology and the current status of the project. This information may assist an agency in learning how smart cards and their applications can be useful tools for the Federal Government. The information in the survey is current as of February 2004. To view the most current survey, please visit http://www.smart.gov/smartgov/smart_carddata.cfm.

Agency	Project Name	Status	Technology	Project Description
DOD-Air Force	Deployment Personnel Accountability Readiness Tool (DPART), Commando Card	Completed	8K Chip, Bar code	The purpose of the Deployment Personnel Accountability and Readiness Tool (DPART) is to integrate disparate, stove-piped personal deployment readiness information for Air Expedientiary Force (AEF) deployments via a distributed, web-based environment. Personal information will be placed on a smart card and interface with a central readiness database. DPART is being tested in an eighteen month pilot program with cooperation from the Air Expeditionary Force Battelelab at Mountain Home Air Force Base, Idaho and the Department of Defense Smartcard Technology Office. The cards, called Commando cards, have been issued to the 16th Special Operations Wing and tenant units involved in the mobility process at Hulbert Field, Florida. The Commando Card is used to make a large number of programs paperless. The combination of a bar code and chip streamlines the mobility process, easing the creation of manifests, verifying training requirements and medical records and reducing the manual processing associated with the frequent mobilizations at Hulbert. The card can also store information for use in logistics, security forces and for work center managers.
DOD-Air Force	U.S. Air Force Identification Card	Completed	Chip, Magnetic stripe, Bar code	The U.S. Air Force plans to issue approximately 700,000 new identification cards using smart card technology in December 2000. It has not yet been determined what applications, other than identification, the card will be used for. However the Air Force is studying the use of smart cards for physical and logical access, stored value and record keeping. It is predicted that by mid-2002 all active duty members will have smart cards. As of June 2001 the CAC card is no longer being issued. The currently issued cards are still however, being used. Continuing card issuance is currently pending.
DOD-Air Force	Lackland Air Force Base (AFB) Recruit Card	Completed	Gemplus 271 card	This pilot, launched July 2, 1998, issued Visa Cash cards to recruits arriving for training at Lackland Air Force Base. Recruits are issued a smart card as they arrive that confirms their arrival, completes their registration and disburses $250 as an initial pay advance. The stored value can be used to pay for goods and services at the barber, post exchange, dry cleaners, phone center, on-post banks and credit unions and to make donations to the post chaplain. Nations Bank expects to issue approximately 40,000 cards per year to recruits at Lackland Air Force Base. The program changed in 2002 from Visa Cash to Gemplus 271 card using FRB SmartCity platform and was consolidated into the Ezpay Card.
DOD-Army	Bosnia/Fort Polk Army Multiple Application Smart Card	Completed	Chip	The Second Armored Calvary Regiment tested the Multiple Application Smart Card during its 1998 redeployment from Bosnia to its home base at Fort Polk, Louisiana. The unit was issued 2500 cards as part of a deployment exercise during the Summer of 1998. Five applications were embedded and tested on the card, including Personnel Tracking, Access Control, Manifesting, Joint Reception, and an In-Theater Database for the Joint Task Force Commander. The primary purpose of the Bosnia demonstration was to have In-Transit Visibility of soldiers moving from port of debarkation to port of embarkation. This demonstration supported the operational and administrative objectives of the mission and, most importantly, showed firm support for warfighter capability. Overall, the card increased efficiency and significantly reduced processing time. This project was absorbed into the CAC.
DOD-Army	Army Saudi Arabia Smart Card	Completed	8K chip card,	On March 17, 2000 the 320th Air Expedentiary Group Personnel Support for Contingency Operations unit and the

			Bar code, Photo	Army Central Command-Saudi Arabia personnel office issued more than 1,300 smart cards to U.S. forces deployed at Eskan Village, Saudi Arabia. The card was used to improve head-count accuracy at the Mirage Dining Facility, which previously used a paper sign-in system. The Air Force and Army issued smart cards to their own personnel and planned to integrate with the DoD CAC once implemented. Other capabilities of the card included: access control, manifesting and medical and personnel record keeping meant that the card could potentially be used for more than food service. The card was proposed to be issued at Prince Sultan Air Base, Saudi Arabia but was not implemented. As of January 2001, the card is no longer in use.
DOD-Army	Fort Knox Stored Value Card	Completed	Gemplus 271 card	In June 1997, Ft. Knox launched a smart card pilot for new recruits. The cards are personalized with the soldier's demographic information and a PIN. An initial pay advance is loaded onto the card at the time of issuance. Soldiers then use the card to make purchases on post. Mellon Bank expects to issue 11,000 cards to recruits per year. In 2000 the program changed to a Visa Cash card with Bank of America. The program no longer uses a PIN. Then in 2002 the program changed to a Gemplus 271 card using FRB SmartCity platform. This project was consolidated into the Ezpay Card.
DOD-Army	Fort Leonard Wood Campus Card	Completed	Gemplus 271 card	This pilot program was launched in May 1997 when smart cards were issued to approximately 28,000 Army recruits. The card is used as an electronic purse to issue cash advances to recruits. In the past the recruits were given cash. By eliminating the need for currency the Department of Defense hopes to reduce its cash handling costs. The recruits use the card to make purchase on base at locations equipped with card reader terminals. In 2002 the program changed from a Visa Cash card to Gemplus 271 card using FRB SmartCity platform. This project was consolidated into the Ezpay card.
DOD-Army	Fort Sill Enhanced Stored Value Card	Completed	icc, signature, Gemplus 271 card	This one year pilot, launched on March 2, 1998, used smart card technology to pay soldiers at Fort Sill. The pilot also aimed to provide more secure and convenient access to funds and streamline the accounting process. Approximately 18,500 Army recruits in a seven-week basic training course at the base were issued cards used for $4 million in salary payments. The soldiers used the stored value card to make purchases from Army merchants. Recruits inserted their card into the point-of-sale terminal and place their index finger on the biometric sensor to verify identification and authorize the purchase. The Ft. Sill card was the first large-scale use of fingerprint biometrics for financial applications. In 2000 the program changed to a Visa Cash card with Bank of America. The program no longer uses biometrics. Then in 2002 the program changed to a Gemplus 271 card using FRB SmartCity platform. The pilot at Ft. Sill was consolidated into the Ezpay Card project.
DOD	Multi-Technology Automated Reader Card (MARC)	Completed	icc, bcd, mgs, photo	The 25th Infantry Division in Hawaii was chosen for the field test of the MARC card. An initial test was conducted in August of 1994. Then in October, 30,000 cards were issued to military personnel. Today the program has expanded to nearly 200,000 U.S. Navy, Marine and Army users. The card's applications include field medical documentation, mobility processing, manifesting, personnel accountability, health care and food service. The benefits of using the MARC card are demonstrated most clearly in the ease with which units in Hawaii are processed for deployment readiness. A process which normally took a day or more is now reduced to a matter of hours and military personnel no longer waste time waiting in line. Integrated into the CAC.
DOD	Cobra Gold '98 Smart Card	Completed	8K chip, Magnetic stripe	The Cobra Gold exercises in the Spring of 1998 represent the first time the Department of Defense has sent smart cards into the field. Approximately 8,000 cards were issued to U.S. Army, Navy and Air Force personnel and Thai military personnel during the exercises. The card was used primarily for the automation of transportation manifests. This application reduced the load time for a 350-passenger plane from four hours to 35 minutes. Card readers attached to notebook computers were also used to track cardholder's field locations. The Cobra Gold Project has been integrated into DoD CAC Project.
DOD-Marines	Marine Corps Smart Technologies Pilot	Completed	8K Contact chip, Magnetic stripe	1,000 cards were issued to Marines at New River at the start of this pilot in September 1997. The pilot then expanded to include 1,000 additional Marines at Camp LeJeune. This project was implemented to improve the travel process, reduce administrative errors and costs, enhance readiness, improve food service, armory check-in/check-out, and property accountability. The card also has several commercial applications including a stored value application for personal funds, travel allowance storage and credit card capabilities. This project has been absorbed into the CAC.
DOD-Navy	Navy Smart Card Pilot	Completed	PKI	Approximately 70 employees at the Navy Chief Information Officer (CIO) office were provided with smart cards that

				had been loaded with personalized PKI certificates. Through the use of a commercial-off-the-shelf (COTS) application, the personnel were able to use their digital certificates to send signed email and visit secure Department of Defense web sites. The cards were also used for logical access, which enables a secure method for logging on to the LAN and for users to lock their workstations (these tasks do not require PKI). The second phase of this project will include approximately 20 users that will utilize PKI (MS Active Server with smart card) for logical access.
DOD-Navy	Smart Card Program National Training Center (NTC) Great Lakes	Completed		Upon reporting for recruit training, each recruit receives a smart card that contains basic demographic information issued by the local Defense Automated Printing Office. The recruits are also issued $200 written to the smart card electronic purse which is accessed with a PIN number and can be used for purchases at the Navy Exchange. The card is used for automated food service check-in, immunization records, drug screening, dental information and the physical exam process as well.
DOD-Navy	Atlantic Ships Smart Card Program	Completed	Chip	Each ship in the battle group has implemented different smart card applications. The USS George Washington currently uses smart cards for morale, welfare, and recreation (MWR) issue and ATM-at-sea III. Additional applications including physical and logical access and tool control. The USS Normandy uses smart cards for service records check out and ATM-at-sea. Issue control capability is planned for the following: electrical tools, organizational gear, MWR equipment, computer video games and video equipment, classified material, IVCS headsets, library materials, weapons and berthing assignments. The USS Hawes has implemented smart cards for accountability for tool control, combat systems electronic gear, gas masks, classified publications, special clothing seabag stowage and weapons. Future accountability applications include service, medical and dental records. USS Briscoe uses smart cards for service records, test equipment and safety harness accountability. Future implementation will include tool and foul weather gear accountability, USS Simpson plans to implement cards for physical and logical access and service records control. USS Ashland uses smart cards for safety equipment and tools accountability and plans to expand to classified material, small arms, gear, personnel records and medical and dental information.
DOD-Navy	Pacific Multi-application Smart Card Project	Completed	chip, photo	The Pacific Multi-application Smart Card Project has been deployed at over thirty land and ship-based locations including: Pearl Harbor, Hawaii, Okinawa, Japan and the USS Kittyhawk. The card is comprised of over fifteen software applications, including physical and logical access control, medical rostering, electronic forms and electronic purse. The card is also used as a visual ID.
DOD-Navy	Strong Angel Relief Exercise	Completed		The Strong Angel exercise centered around humanitarian relief efforts at a mock refugee camp. The smart cards and related applications were utilized to support identification, management, and support of refugees and support staff. 100% personnel accountability was attained and demonstrated remotely to senior staff members from the United Nations High Commissioner for Refugees (UNHCR), United nations Children's Fund (UNICEF), and the World Food Programme (WFP), as well as 3rd fleet personnel.
DOD-Navy	Naval Consolidated Brig Miramar Smart Card Program	Completed	Chip	The smart card program at the Miramar Brig has two applications. The primary application is the centralized monitoring of staff, prisoners and visitor movement within the brig. This system is presently undergoing a three phase upgrade. The upgrade will provide an Application Program Interface (API) between the Correction Management Information System (CORMIS) and the Security Access System. Phase I was funded in FY99. Phases II, and III will add an additional 24 card readers and four more control nodes. The card is also used to control the issue of tools for jobs in the brig as well as recreation gear or any other materials requiring issue control.
DOD-Navy	Naval Academy Campus Pilot	Completed	Not yet determned	The US Naval Academy in Annapolis, Maryland is planning to implement a pilot smart card project for building security on their campus. Academy officials expressed an interest in smart cards after visiting GSA's Smart Card Technology Center in Washington, DC. Meetings were held between Academy officials and GSA personnel from Washington, DC and Philadelphia, PA. The Academy has entered into an Interagency Agreement with GSA through Region 3 in Philadelphia to launch the project. Approximately 100 cards will be issued initially and the Academy intends to eventually expand the use of smart cards throughout the Academy after first piloting them at several key buildings on campus. The card will provide both identification and physical access security.
DOD-Navy	Naval Reserve Readiness	Completed	8K Contact	Naval Reserve Readiness is a smart ID card to integrate the Reserve and Active components. This initiative is a

			chip, Bar code, Magnetic stripe, Photo	"Smart Business Practice" that will support the mobilization, deployment, and employment of both Active Component (AC) and Reserve Component (RC) personnel. It will reduce the administrative burden of paperwork and enhance the quality of life of the sailor as Commanders in Chief (CINCs) continue to track large numbers of personnel through their area of responsibility (AOR). The card's chip technology allows the removal of the visual "RESERVE" status discriminator printed in the upper right hand corner of the ID card and eases the tracking the frequent status changes of the Reservists from RC to AC.
FED-COM	Smart Card Access Control System (SACS)	Completed		This application is comprised of two subsystems, TBACS and SACS. This initiative replaced traditional password-based computer and network access with smart-token based access. The smart token's onboard processor and memory are exploited to provide sophisticated security mechanisms in a portable device. In addition to access control, the systems may be used for random number generation, cryptographic key generation, data encryption, data authentication, and secure data storage.
FED-EDU	SFA Multi-Tech ID	Completed	Contact and contactless hybrid smart card	Student Financial Assistance (SFA) will be moving to a new location, Union Plaza 3, and plans to utilize a smart card for physical access, transit benefits, and asset management. Other applications may be added later.
FED-IND	2001Transition of the Presidency	Completed		Smart card applications were installed but never utilized due to election delay in Florida.
FED-IND	1997 Presidential Inauguration Card	Completed	2K & 3K contact chip, Magnetic stripe, Bar code	This project provided access control, housing, and telephone support to 3,000+ staff and visitors who were allowed access to the event. The applications included physical access for Federal employees and inaugural visitors to the Inauguration Committee Headquarters and inventory control of over one million dollars worth of communications equipment for portable communications during the 1997 presidential inauguration. The system was networked to allow security personnel to monitor movements within the facility and maintain ingress/egress rosters for secured areas.
FED-IND	FTS Multi-Application Smart Card	Completed	16K Java card, Magnetic stripe, Biometrics, Photo, Signature	GSA's Federal Technology Service is conducting a pilot at the Willow Wood facility of various telecommunications technologies, office automation technologies and architectural strategies. The multi-application smart card platform is one of the three main components of the FTS pilot. To study the impact of moving from multiple single application cards to a single multi-application card, FTS employees at the Willow Wood Facility were issued smart cards during the Summer of 1999. As of December 1999, approximately 450 cards had been issued. The card applications include identification with picture and signature, physical access, logical access, property management, American Airlines electronic boarding pass, purchase card, travel card and Sprint calling card. Ongoing evaluation is being conducted to determine if the multi-application card and other innovative technologies can achieve the FTS goals of enhanced and cost effective service.
FED-IND	Smart Card System Electronic Payment System Implementation	Completed		The purpose of this project is to create a smart card based national electronic payment system in Armenia. The activity is directed toward achieving USAID's goal of supporting the growth of the Armenian private sector and is aimed at strengthening the banking sector. This project is expected to increase the quality and sophistication of financial services in the Republic of Armenia. Creation of a payment system based on smart cards, as well as a processing system within it, will allow Armenian banks to issue, acquire, and process local and international cards. USAID and the Central Bank of Armenia have assisted in the formation of ARCA (Armenian Card), a Unified Processing Center that will provide the Republic of Armenia with the technical infrastructure for the electronic payment system for debit and credit cards with the use of smart card technology. In the early part of 2001 the payment system application is expected to be installed and equipment is expected to be procured and delivered. While the smart card project was originally welcomed the card met with a negative reaction and the project has since been discontinued.
FED-VA	Bronx Stored Value/ID Card	Completed	Visa Cash	The VA projects put an estimated 30,000 cards in the hands of patients, physicians, visitors, volunteers and employees of the VA facility in Bronx, to test the combined applications of ID card and electronic purchases from vending machines, cash registers and terminals and cashless ATMs using Visa Cash. The stored value cards were

				accepted by the onsite Veterans Canteen Service which supplies food, clothing, other goods and vending services to all 172 VA hospitals. The pilot was terminated approximately a year after it began in 1999 due to low volumes of activity as well as operational and technical challenges. The pilot locations were the Veterans Affairs Medical Center, New York City and the James A. Haley Veteran's Medical Center, Tampa, Florida
FED-VA	Tampa Stored Value/ID Card	Completed	Visa Cash	The second phase of this project was launched on November 24, 1997. The projects puts Visa Cash in the hands of patients, physicians, visitors, volunteers and employees of the VA facility in Tampa, FL to test the combined applications of ID card and electronic purchases from vending machines, cash registers and terminals and cashless ATMs.
Other-USPS	Government Express Store	Completed		The Government Express Store program is intended to provide citizens with easy access to government and postal services via the Internet using existing web portals and applications. Smart card functionality will be added to these applications and a Personal Private Portal will be accessed via a smart card. The Government Express Store will be implemented in North Dakota and offer information about Federal, State and local programs, Postal Service products and services, and University of North Dakota student information.
Other-USPS	Net Post.Certified	Completed	32K chip	This pilot smart card project has been in place for approximately two years. The project facilitates the sharing of information between the Health Care Finance Administration (HCFA), Social Security Administration and Internal Revenue Service. The use of smart cards allows for the secure transfer of information and the confirmation of identity. The cards are issued to these agencies and to the participants of programs, such as Medicaid and Medicare, at U.S. Post offices.
State-CA	Smartcard Passport	Completed		The Ventura County Transportation Commission in California is currently implementing a countywide contactless smart card system across six independent transit operators. Ventura County's Passport is a prepaid monthly bus pass that lets riders get around all of Ventura County. With the Passport, riders can use any bus system in the county without having to carry cash, tokens, tickets or other passes. A monthly sticker allows riders to get unlimited rides on all bus systems during that calendar month. The Passport is accepted on the following public transit systems in the county: Camarillo Area Transit (AT); Moorpark City Transit; Simi Valley Transit (SVT); South Coast Area Transit (SCAT); Thousand Oaks Transit (TOT); Ventura Intercity System Transit Authority (VISTA). This card is no longer in use as a smartcard due to Y2K concerns. Riders currently use the card as a flashpass (monthly ride stickers are affixed to the card).
DOD-Air Force	Falcon Card	Operational	4K contact chip card, Bar code, Photo	In May of 1998 the Air Force Academy issued to all cadets the first multiple application card to carry independently loaded applications. The cards allow cadets to use the electronic purse to pay for laundry, snack purchases in the laundry areas, and copiers in the library. Additional point of sale locations are being added. Disposable cards in $10 and $20 values can be purchased by USAFA faculty, employees, and family members. The following additional applications have been planned and will be added to the card: student visibility, manifesting, physical access, network access, medical and dental, inventory control, physical and aerobic fitness test results, training qualification, test results and food services. The system was designed to allow the Air Force Academy to continue to add these non-financial applications as well as to be independent yet interoperable with the U.S. Department of Defense Smart Card program.
DOD-Air Force	Standard Asset Tracking System (SATS)	Operational	8K chip	SATS (Standard Asset Tracking System) began as a paperless initiative to track assets into and out of Air Force Base Supply using bar code and radio frequency technology. Before SATS, a base only used the Standard Base Supply System (SBSS). SBSS uses paper documents and signatures, which creates endless handling and filing of the documents and makes it difficult to track assets. SATS now uses a portable, hand-held terminal (HHT) with a bar-code scanner and a smart card reader to process the customer receipt of assets instead of the previous method of using paper documents and signatures. All customers have their own smart card, much like an ATM card, and a Personal Identification Number (PIN) to confirm the use of the information on the smart card and their acceptance of the receipt of the asset. When Supply delivers an asset to a customer, the customer enters their smart card into the HHT smart card reader, the bar code on the asset is scanned, the information on the smart card is read, and the

				privilege of the customer to receive the asset is verified. The customer then enters their PIN into the HHT, to confirm their acceptance of the asset. The HHT uses radio frequency data collection (RFDC) technology to instantly send the transaction back to SATS. If for some reason the RF is lost, the HHT stores the transaction for later downloading. Besides making assets easier to track, the Proof of Concept test at Shaw Air Force Base, South Carolina showed SATS reduced the processing time required for the warehouse pull of an asset to the customer delivery of that asset by 81 percent. SATS also cut manpower by 60 percent in the Receiving element and by 75 percent in Document Control. Additionally, SATS reduced the use of paper documents by 96 percent. SATS already has been implemented at 39 Air Force installations worldwide, and is currently being installed at each Air Force Reserve and Air National Guard installations throughout the US. The rest of the active-duty bases are scheduled to follow suit by the end of 2002. The Air Reserve Component also wants to implement SATS and is expected to do so in 2002.
DOD-Army	Eagle Cash	Operational	Gemplus EMV card	On December 8, 1999 all soldiers and Department of Defense civilians were issued stored value smart cards, called Eagle Cash, at Camp McGovern, Bosnia. As of March 2000, there were approximately 1,250 cardholders. The Eagle Cash system's main function is to eliminate the use of U.S. currency at the Camp. Users load credits on to the Eagle Cash card from payroll payments, bank account withdrawals and cashed checks. All merchants at the Camp accept the card as payment for goods and services. The card can also be used to purchase foreign currency. Due to the success of the project and the multiple benefits it provides, FMS and the Army have recently deployed similar stored value programs at Camp Dobol, Camp Comanche and Eagle Base in Bosnia and the U.S. base in Taszar, Hungary. Approximately 4,000 for Bosnia, 6,000 for Kosovo and about 700 for Honduras now use smart cards for their financial transactions while deployed in the deployed Army. The program expects to issue approximately 27 thousand cards in FY 2004. There have been approximately 44,350 cards issued to date as of June 30, 2003 and a total of over $59 million loaded onto the cards.
DOD	Common Access Card	Operational	bcd, mgs, 32K icc, pki, web-enabled functionality	The Common Access Card (CAC) has been designed to allow physical access to secure areas, permit logical access to the DoD's computer networks, and serve as an authentication token for the DoD's public key infrastructure (PKI). Initially the cards contained identification and security information, however, later versions shall include other data, such as inoculations, medical and dental records, and finance allotments. Approximately 7K of the chip's 32K usable data space shall be reserved for the services to program with any application they choose. This card is intended to consolidate card systems (where applicable) to merge identification and access card systems. In November 2000, three Air Force bases and an Air National Guard unit began testing the software used to produce the new identification card. Langley Air Force Base, Virginia, Osan Air Base, Korea, Ramstein Air Base, Germany and the 203rd Red Horse Unit, Virginia were selected to begin the initial phase in of the card. The second phase, beginning in January, added Hulbert Field, Florida. The third phase in February 2001 involved issuing new cards to about one-third of the Air Force target population, with the remaining two-thirds receiving cards by September 2002. As of January 2004, DoD had issued 3.4 million smart cards on the way to a population of 4 Million, a goal that they expect to achieve by Spring 2004. Organizational focus is moving towards a web-centric environment with the development of applications that support or work in conjunction with the CAC.
DOD-Marines	MarineCash/ Recruit Smart Card Project	Operational	8K Gemplus EMV Contact chip	The U.S. Marine Corps recruit smart card project became operational at Parris Island on March 6, 2000. Marine personnel issue cards to recruits when they arrive at Charleston Airport. Phase I of the project, allows the personal information stored on the cards issued to create the manifest for the trip to Parris Island. At Parris Island, the card is also used to populate forms, document recruit training, assist with issuing weapons at the armory and includes an electronic purse. Phase 2 of the project was rolled out on March 19, 2001. This phase has added additional card applications including add/drop, visibility and separation capabilities for drill instructors. In 2001 San Diego joined the same process with the SVC. Together both sites issue approximately 50,000 a year. There have been approximately 105,000 cards issued to date as of June 30, 2003.
DOD-Navy	Navy Marine Corps Intranet Project	Operational	CAC card	This initiative is to transition all unclassified networked computers in the continental US to the DoD smart card and public key technology. These tools will be used for: Cryptographic log-on to the network, Digitally signing electronic mail, Client-side authentication to all provate web services, and digitally signing forms and other e-transactions.
DOD-Navy	Pensacola Smart Card Program	Operational	Chip	There are five (5) applications designed for use with the Common Access Card (CAC). These applications include:

				Card Maintenance Utility, Food Service, Manifest Tracking, Warrior Readiness and Weapons Issuance. A variety of these applications are currently active at Army, Navy and Marine Corps sites: Great Lakes, IL; Dam Neck, VA; NAS Oceana, VA; NAS Pensacola, FL; Hawaii and Japan. The Program Management Office also provides support to Non-CAC applications to include Morale Welfare and Recreation (MWR) Participation Tracking and Smart Dental Information (SDI).
FED-AGR	Automated Buying Point System	Operational	24K EEPROM card, TPL-0720 I/O box at buying points, AS400 System computers in Data Collection Center	Smart cards are being used to automate the collection of peanut marketing data, a task that used to be cumbersome and paper-intensive. USDA county offices issue smart cards to each farmer eligible to market peanuts under the government's peanut quota system. The card contains the farmer's (or farm operator's) name, the farm number, the farm's peanut quota in pounds, the crop loan eligibility information, and transaction records. When a farmer takes peanuts to a buying point, the smart card is inserted into a terminal to determine whether peanuts can be purchased under the quota or an alternative marketing category. Each marketing transaction is recorded on the system where the previous balances are maintained. At the end of the harvest, farmers return the smart card to the county office so the information can be electronically reconciled to marketing information that was telecommunicated from the buying point computers to the USDA central computers.
FED-IND	Common Access Card Smartcard Upgrade	Operational	HID Corporate 1000 Proximity Cards Datakey 330 smartcard chips	Employees and select contractors are adjudicated by the physical security badging office. A National Agency Check is performed prior to issuing new cards. The combined cards are administered using the established policies for issuing and replacing cards. All card related activities are managed by Physical Security. Employees with new or replacement cards must be enabled by the Information Security Staff before Public Key Infrastructure (PKI) services are available. The same processes used for administering new accounts and restoring passwords apply.FDIC laptops and desktop computers have smartcard readers affixed. The deployment of a common card followed a completive procurement and was coordinated with the corporate upgrade to Windows XP.
FED-DOS	Smart Card Access Control Project	Operational	8K, Hand geometry biometrics	The U.S. Department of State (DOS) is in the process of implementing an automated access control system using a Smart ID Card for its employees and visitors in an effort to provide the safest and most secure environment during a time of heightened awareness against domestic terrorist threats. Implementation of a Smart ID Card will partially aid DOS in accomplishing this goal. The access control project will include the Harry S. Truman Building, the United States Mission to the United Nations, the Blair House (the President's guest house) and approximately 35 facilities located within the United States. These facilities [DOS] process an estimated one-half million visitors annually. A select group of employees have been issued Smart ID Cards to finalize testing of the new access control system. In April 2002, 20,000 employees working in the National Capital Region will be issued Smart ID Cards. DOS employees located outside the U.S.[overseas] will be issued a Smart ID Card as they rotate back into the U.S. Migration of the DOS Smart ID Cards at all overseas U.S. Embassies is anticipated in the future. The DOS Smart ID Card will initially be used for physical and logical access and will also serve as the hardware token for DOS public key infrastructure (PKI) certificates. It is also anticipated that the DOS Smart ID Card may be used for many other applications in the future.
FED-TRS	EZpay Card	Operational	Gemplus 271 card	The first Army/Air Force pilot began at Fort Leonard Wood in May 1997 using a Visa Cash card. Fort Knox was added June 1997 utilizing a PIN and a SmartCity card. Fort Sill began their pilot March 1998 using a Biometric SmartCity card. Lackland was added June 1998 as a Visa Cash pilot. In 1999, Fort Benning and Fort Jackson began using the Visa Cash card. Since the pilots began, the programs were consolidated into the best practices and in 2002 all six became the EZpay program using a SmartCity card without PIN or Biometrics. Recruits are issued a smart card as they arrive that confirms their arrival, completes their registration and disburses $250 ($300 for female) as an initial pay advance. The stored value can be used to pay for goods and services at the barber, post exchange, dry cleaners, phone center, on-post banks and credit unions and to make donations to the post chaplain. The programs expect to issue approximately 165,000 cards per year to the recruits. There have been approximately 800,000 cards issued to date as of June 30, 2003. The locations participating in the Ezpay Card program are

				Lackland Air Force Base (Texas); Fort Knox (Kentucky); Fort Leonard Wood (Missouri); Fort Sill (Oklahoma); Fort Benning (Georgia); and Fort Jackson (South Carolina)
DOD-Navy	NavyCash/MarineCash ; ATM at Sea	Pilot	32K chip, Branded Magnetic Strip	The NavyCash/MarineCash application went live with its first implementation in April 2001. NavyCash/MarineCash has since been implemented on a total of 8 prototype ships. NavyCash/MarineCash is a financial management application that employs chip technology to replace bills and coins on board Navy ships. NavyCash/MarineCash significantly improves quality of life on board ship. When at sea, Navy Cash/Marine Cash provides off-line access to the users' bank and credit union accounts using the shipboard communications. When in port anywhere in the world, Navy Cash/Marine Cash provides on-line access to a Navy Cash/Marine Cash account at ATMs worldwide and merchant retailers using the existing global banking infrastructure. The Navy Cash/Marine Cash program evolved from the Navy's thirteen-year-old Automated Teller Machines-at-Sea (ATM-at-Sea) program. The program expects to add additional ships in FY 2004 and issue approximately 10,000 cards totaling over $14 million. There have been approximately 20,000 cards issued with over $19 million to date as of June 30, 2003.
FED-COM	Patent Work at Home (PWAH) program	Pilot		On September 6, 2001, the US Patent and Trade Office (USPTO), in the Arlington, VA area purchased smart cards, readers and applications utilizing PKI to establish a secure remote entry system for its Patent Work at Home (PWAH) program employees. The PTONet Remote Access System currently utilized by the PWAH program utilizes a two-factor authentication process. In an effort to increase existing system security, the migration to a Smartcard will bolster the PTONet PKI system while providing securely stored digital certificates for strong authentication, digital signatures, and local encryption and ensure interoperability. The new smart card will be a multi-application card with the combined functions of Metro subsidy and property pass functionality while maintaining GSA's interoperability standards. The smart chip card provides each cardholder logical remote access to their facilities. The card is used in conjunction with a chip card reader as a means of controlling access to the USPTO workstation and data networks. The card controls access to local and remote workstations as well as access to the USPTO network. Cardholders insert their card into the card reader and provide a password to gain workstation and network access.
FED-VA	Veterans Administration (VA) Express Card	Pilot	Chip	A formal pilot is being conducted to determine functional utility of the VA Express Card and the return on investment. The initial implementation is currently taking place at VA medical, benefits and cemetery facilities in Milwaukee and Iron Mountain. Cards were issued to approximately 40,000 veterans in this area during the week of February 19, 2001. The initial pilot, which would have deployed nearly 200,000 VA Express Cards in VISN 12, was determined to be larger than necessary. The card will contain demographic, emergency, and eligibility data that can be available at VA and non-VA facilities, as well as Public Key Infrastructure (PKI) keys for security. The project is aimed at implementing health card technology, evaluating the benefits of the functionality included on the card, evaluating the interfaces to existing systems, and evaluating the use of PKI keys to digitally sign electronic service delivery transactions. The card was designed to accommodate G8 medical data elements in an effort to be interoperable across federal agencies.
State-DE	DART Transit Card Delaware	Pilot	Stored value card	DART First State announced that on Monday, May 21, 2001 it will unveil its new, leading-edge, and simple to use "DARTCard." The DARTCard is a stored-value fare card that can be used on any DART First State fixed route bus service anywhere in the State, including the Wilmington - Dover Intercounty Route 301, and seasonal resort services. Seven (7) multi-valued DARTCards will replace the eighteen (18) different multi-ride fare cards and passes presently used by riders. The DARCard can be used to purchase a cost saving daily pass on the bus, or to pay on a per ride basis. A rider's best value with the DARTCard is a daily pass when transferring and/or taking 3 or more bus trips during the day. The new color-coded DARTCards will be available in seven different amounts offering riders several options and the freedom to choose the DARTCard that works best for their traveling budget and needs. The stored-value DARTCards can be used just like cash. When the rider inserts the DARTCard into the bus's fare box, the appropriate fare for that service will be deducted from the card each time it is used. Each time the

				DARTCard is used, the value remaining on the card will be printed on the back of the DARTCard so that the rider can better manage their traveling budget. The card can be used as long as there is sufficient value left on the card. When the value on a rider's DARTCard is less than the fare, the rider can use its remaining value and pay the difference required by the fare with either another DARTCard or with cash. Riders are encouraged to pay for all fares with a DARTCard minimizing carrying and handling cash. Cash fares are exact change using coinage and only one dollar bills. DARTCards will be available for purchase from DART First State Transportation Stores, statewide fare card outlets, and by mail or phone on May 21, 2001. For more information, call 1-800-652-DART, or visit our web site at www.DartFirstState.com.
State-IL	Smart Transit Card Chicago	Pilot		Quite simply, it's a permanent, rechargeable farecard. It's plastic -- like a credit card -- and is embedded with a special computer chip that keeps track of the value of the card. It can be used to pay fares on all CTA buses, at all CTA train stations and on PACE (suburban) buses. Instead of inserting a farecard into the farebox or turnstile, you simply touch your Smartcard to the Smartcard Touchpad -- located on the front of the bus farebox and rail turnstile -- and go. Your fare or transfer will automatically be deducted.
State-New England	New England PARTNERS Project	Pilot	hybrid chip/magnetic stripe card	The New England PARTNERS Project is a joint initiative of the States of Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont in cooperation with the U.S. Department of Agriculture's Food and Nutrition Service to develop and implement a hybrid card–based (i.e., magstripe and smart card chip) delivery system to meet the service and benefit needs of participants from a variety of public health and human service programs. The New England PARTNERS Project will conduct pilot programs in each of the six contiguous states, linking multiple programs via a common participant card—in effect testing the efficacy of public health and human services delivery via electronic card technology. Building on the Food Stamp Program's electronic benefit transfer (EBT) experience, the system will expand the EBT concept and use an electronic service delivery (ESD) model. In addition to the financial benefits, ESD supports multiple functions in the delivery of health-related services including eligibility determination, health assessment, case management, and referrals. The PARTNERS multi-state, multi-function information and services delivery system will improve the quality and convenience of government payment processes, increasing access and streamlining such processes for citizens, participants, patients, and professionals alike. From health care providers to retail grocers, PARTNERS will reduce paperwork and improve the efficiency of reporting and reimbursement systems. PARTNERS will achieve its objective by using new technologies to bridge and build upon a number of government and private systems, including program data processing, retail point-of-sale, provider point-of-interaction, health care providers and fiscal agent and financial reporting. Using hybrid participant card (magnetic stripe and integrated chip), intelligent point-of-service terminals, online and offline technologies, web-based communication, and other telecommunications methods, PARTNERS will establish a "virtual network" of recipients, providers, vendors, and administrators across the six-state region. Pilots will be undertaken in each of the six States, with each testing a different combination of programs and services. All efforts are organized under a Memorandum of Understanding executed by the six State health agency commissioners. Administrative activities are being managed by New Hampshire. Funding has been provided by the US Department of Agriculture, Food & Nutrition Service, the US Department of Health & Human Services, Centers for Disease Control, an private sector food industry supporters. In September 2000, PARTNERS initiated its implementation phases by competitively procuring a Project Management and Quality Assurance (PMQA) contractor. The PMQA contract was awarded to Burger, Carroll & Associates (BCA). PARTNERS has initiated a competitive procurement to obtain a system implementation contractor (IC) and an evaluation contractor (EC). The IC will assist PARTNERS in establishing pilot programs in each of the six states by 2003; bids are due February 15, 2002. The EC will conduct a formal evaluation of those

				pilots to advise the states as to whether the PARTNERS system should be implemented regionwide.
State-ND-NV-WY	Health Passport Project (HPP) GSA WGA ND NV WY	Operational	8K chip, Magnetic stripe	HPP is a federally funded state project sponsored by the Western Governor's Association (WGA), to integrate multi-applications of client demographics, immunization status, client medical providers, medical program participations, and medical results and status. The first phase of the pilot was launched in June 1999 and is scheduled to run until December 2001. It is estimated that Health Passport cards will initially be issued to 25,000 pregnant women, mothers and children eligible for programs such as WIC, Head Start, Food Stamps and other public health programs. The main application of the Health Passport card is the sharing of information between several different healthcare programs. Demographic, health, appointment and WIC benefit information from clinics, doctors and grocery stores is stored on the cards. The user controls who may view the information with a personal identification number. Health care providers are able to read and write information on the card with card readers connected to their computers. The HPP card can also be used for the electronic transfer of WIC benefits. Phase Two of the Health Passport system will test the concept of a Web-based patient account as well as the use of the card to bridge multiple systems.
DOD-Navy	Fleet Combat Training Center (FCTC)\Naval Air Station (NAS) Oceana Smart Card Program	Planning	Chip	This smart card program is similar to the Pensacola card program. Defense Automated Printing Service issues the card to all students and staff members. The card's applications include access control at the FCTCLANT (Fleet Combat Training Center Atlantic) Headquarters, automated food-service check-in and immunization recording and tracking.
FED-DHS	DHS US Secret Service	Planning		IRMD recently decided to begin planning an initiative to provide smart cards to a few hundred employees to use as a building pass (physical access), as well as for logical access. No project manager has been assigned and technology decisions have not been finalized. Other decisions have not yet been made, but the Secret Service (working through the Treasury) will be going through the GSA.
FED-INT	Firefighters Training Card	Planning	Not Applicable	The National Parks Service is considering a smart card application that would include qualification and certification information (this would replace the "Red Card" they currently use). 250,000 firefighters, pilots and other personnel that provide support during forest fire operations would receive the card.
FED-SSA	Property Accountability & Pass	Planning		The Social Security Administration plans to use smart card technology to track government property. Information regarding property eligible for removal from Government Facility will be stored on the card.

10. APPENDIX C – INDEX OF SMART CARD WEB SITES

The following is a listing of key web sites that are a good source of information on smart card technology and policy. These sites provide further guidance to agencies to learn more about smart cards and their applications. These sites cover a wide range of topics including:

- Smart Card Applications;
- Federal Smart Card Programs;
- Public Key Infrastructure;
- Biometrics; and
- Electronic Payments.

Name	Web Address	Description
Access Certificates for Electronic Services (ACES)	http://www.gsa.gov/aces	The ACES website provides information on the Government-wide public key infrastructure.
Avanti	http://www.biometric.freeserve.co.uk/avanti.htm	This site provides background information about biometrics, their use in everyday business situations and how they are deployed.
Biometrics Consortium	http://www.biometrics.org	The Biometric Consortium serves as the US government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology.
Card Europe	http://www.cardeurope.demon.co.uk/index.htm	Although primarily focused on Europe, Card Europe has expanded to encompass the whole world. The site provides access to a database of information as a starting point for information concerning smart card related products, services and activities.
CardTech/ SecurTech	http://www.ctst.com	CardTech/ SecurTech promotes the advancement of card, biometric and transaction security technologies through educational resources for professionals at every level of expertise.
CommerceNet of Massachusetts, Information Technology Division Legal Department, The PKI Page	http://www.magnet.state.ma.us/itd/legal/backers.htm	This site provides background papers on PKI, cryptography, digital signatures and electronic commerce.
E-Authentication	http://www.cio.gov/eauthentication/	The E-Authentication site promotes public trust in meeting the authentication business needs in E-Gov transactions.
Electronic Frontiers Georgia (EFGA)	http://www.efga.org	The EFGA web page provides information about emerging technology, with links to information about digital signatures and cryptography.
Federal Bridge Certificate Authority	http://www.cio.gov/fbca/	The FBCA site provides information relevant to an entity accepting certificates issued by another entity for a transaction.
Federal Identity and Credentialing Committee	http://www.cio.gov/ficc	The FICC site describes policy recommendations for the use of identity credentials in the federal sector.
Federal PKI Policy Authority	http://www.cio.gov/fpkipa/	The FPKIPA site describes the group's supervision of FBCA and its promotion of agency-to-agency PKI interoperability.

Name	Web Address	Description
Federal PKI Steering Committee	http://www.cio.gov/fpkisc/	The FPKISC site provides information regarding the government's initiatives in implementing PKI.
Georgia Digital Signature Task Force	http://www.emory.edu/BUSINESS/gds.html	The Georgia Digital Signatures Task Force has links to digital signature and cryptography references.
International Card Manufacturers' Association	http://www.icma.com/index-flash.htm	ICMA provides information and resources in support of the plastic card industry in general, including their use as smart cards.
Internet Engineering Task Force, PKI Working Group	http://www.ietf.org/html.charters/pkix-charter.html	This site provides several resources on public key infrastructure.
National Automated Clearing House Association	http://www.nacha.org	This site provides the latest information on the world of electronic payments.
NIST's Computer Security Resource Clearinghouse	http://csrc.nist.gov/pki/	This site provides information on NIST's PKI Program. NIST is taking the lead in developing a Federal Public Key Infrastructure that supports digital signatures and other PKI security services.
Silicon Valley Software Industry Coalition: Digital Signatures Working Group	http://www.softwareindustry.org/coalition/dswgopen.html	This site has links to working group documents on digital signatures and digital signature legislation.
Smart Card Alliance	http://www.smartcardalliance.org	The Smart Card Alliance provides information on Smart Card Technology, Industry News, Research, and seeks to promote the understanding and adoption of smart card technology.
Smart Card Central	http://www.electronics-ee.com/Computer/Electronic_Commerce/Smartcards.htm	Smart Card Central is a resource for research, news and technical information about smart card technology.
SmartGov	http://smart.gov	The SmartGov site offers information on smart card technology government, business, education and citizens. Highlights include a smart card tutorial, the SmartData database of Federal smart card projects and information on the Smart Access ID Program.

11. APPENDIX D – REFERENCES

Allen, Catherine, "Smart Cards Part of U.S. Effort in Move to Electronic Banking*", Smart Card Technology International: The Global Journal of Advanced Card Technology,* ed. Robin Townsend, London: Global Projects Group, 1995

American Association of Motor Vehicle Administrators, *Best Practices Imaging Standard for Photographs and Signatures*, Prepared by the Digital Imaging Standards Subcommittee, November 1994

American Association of Motor Vehicle Administrators, *Best Practices Recommendations for the Use of Bar Codes, Version 2.0,* Prepared by the Motor Vehicle Imaging Standards Bar Code Working Group, April 1996.

American National Standards Institute (ANSI), ANSI X3. 182-1990, *Bar Code Print Quality – Guideline*, 1990.

American National Standards Institute (ANSI), ANSI X9.69, *Cryptographic Key Management Extensions*.

Andersen Consulting, LLP, *Evaluation of Automatic Identification Technologies*, January 10, 1997.

Automatic Identification Manufacturers (AIM) USA, *PDF-417*, July 1994.

Barkley, John, *Comparing Simple Role Based Access Control Models and Access Control Lists*, National Institute of Standards and Technology, August 11, 1997.

Barkley, John, Cincotta, Anthony V., Ferraiolo, David F., Gavrilla, Serban, Kuhn, D. Richard, *Role Based Access Control for the World Wide Web*. National Institute of Standards and Technology, April 8, 1997.

Burr, William E., Nazario, Noel A., and Polk, W. Timothy. *A Proposed Federal PKI Using X.509 V3 Certificates*, Gaithersburg: National Institute of Standards and Technology.

Clinger-Cohen Act (P.L. 104-106) Section 5113

Dillaway, Blair, "PC/SC Workgroup Specification for PC-ICC Interoperability", Presentation at CardTech/SecurTech '96 West, December 1996

E-Government Act (P.L. 104-347) Section 203

Electronic Industries Association (EIA) *232-D, Interface between Data Terminal Equipment and Data Circuit-Termination Equipment Employing Serial Binary Data Interchange*.

Europay International, MasterCard International Incorporated, and Visa International Service Association, *EMV 1996 Integrated Circuit Card Specification for Payment Systems, Version 3.0*, June, 1996.

Federal Information Security Management Act (P.L. 107-347) Section 3544(a)

Ferraiolo, David F., Barkley, John F. and Kuhn, D. Richard, *A Role Based Access Control Model and Reference Implementation within a Corporate Intranet*, National Institute of Standards and Technology.

Ferraiolo, David, and Barkley, John, *Specifying and Managing Role-Based Access Control within a Corporate Intranet*, National Institute of Standards and Technology,

Federal Identity Credentialing Committee, *Policy Issuance Regarding Smart Cards Systems For Identification and Credentialing of Employees*, February 2004, http://www.smart.gov/smartgov/whats_new.cfm

FIPS Publication 112, *Password Usage,* National Institute of Standards and Technology (NIST), May 30, 1995.

FIPS Publication 140-1, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology (NIST), January 11, 1994.

FIPS Pub 180-1, *Secure Hash Standard (SHS),* National Institute of Standards and Technology (NIST), April 1995.

FIPS Publication 186-1, *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, (NIST), May 1994. (revision December 15, 1998).

FIPS Publication 190*, Guideline for the Use of Advanced Authentication Technology Alternatives*, National Institute of Standards and Technology, (NIST), September, 1994.

FIPS Publication 196, *Entity Authentication Using Public Key Cryptography*, National Institute of Standards and Technology (NIST), February 18, 1997.

Gips, Michael A., "Assessing Trends in Access Control," *Security Management*, September 1998.

IAW RFC 1321, *the MD5 Message-Digest Algorithm*, Internet Activities Board, April 1992.

IETF PKIX Working Group, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC2459)*, January, 1999

ISO/IEC 7810: 1995, *Identification Cards – Physical Characteristics*.

ISO/IEC 7811-1: 1995, *Identification Cards – Recording Techniques – Part1: Embossing*.

ISO/IEC 7811-1: 1995, *Identification Cards – Recording Techniques – Part 2: Magnetic Stripe*.

ISO/IEC 7811-1: 1995, *Identification Cards – Recording Techniques – Part 3: Location of Embossed Characters on ID-1 Cards*.

ISO/IEC 7811-1: 1995, *Identification Cards – Recording Techniques – Part 4: Location of Read-Only Magnetic Tracks – Tracks 1 and 2*.

ISO/IEC 7811-1: 1995, *Identification Cards – Recording Techniques – Part 5: Location of Read-Only Magnetic Tracks – Track 3*.

ISO/IEC 7811-1: 1996, *Identification Cards – Recording Techniques – Part 6: Magnetic Stripe – High Coercivity*.

ISO/IEC 7812-1: 1993, *Identification Cards – Identification of Issuers – Part 1: Numbering System*, December 1, 1993.

ISO/IEC 7812-2: 1993, *Identification Cards – Identification of Issuers – Part 2:Allocation and Registration Procedures*, December 1, 1993.

ISO/IEC 7813: 1995, *Identification Cards – Financial Transaction Cards*, August 15, 1995.

ISO/IEC 7816-1: 1987, *Identification Cards-Integrated Circuit(s) with Contacts – Part 1: Physical characteristics, July 1, 1987.*

ISO/IEC 7816-2: *Identification Cards-Integrated Circuit(s) with Contacts – Part 2: Dimensions and location of the Contacts*.

ISO/IEC 7816-3: 1997, *Identification Cards-Integrated Circuit(s) with Contacts – Part 3: Electronic Signals and Transmission Protocols*.

ISO/IEC 7816-4: 1995, *Identification Cards-Integrated Circuit(s) with Contacts – Part 4: Interindustry Commands for Interchange,* September 1, 1995.

ISO/IEC 7816-5: 1994, *Identification Cards-Integrated Circuit(s) with Contacts – Part 5: Number System and Registration Procedure for Application Identifiers,* June 15, 1994.

ISO/IEC 7816-6: 1996, *Identification Cards-Integrated Circuit(s) with Contacts – Part 6: Inter-industry Data Elements*.

ISO/IEC 7816-7: *Identification Cards-Integrated Circuit(s) with Contacts – Part 7: Interindustry Commands for Structured Card Query Language (SCQL).*

ISO/IEC 7816-8: *Identification Cards-Integrated Circuit(s) with Contacts – Part 8: Security Related Interindustry Commands*.

ISO/IEC 7816-10: *Identification Cards-Integrated Circuit(s) with Contacts Part 10: Electronic Signals and Answers to Reset for Synchronous Cards*.

ISO/IEC 8824-1: 1996/Amd. 1: 1996, *Information Technology – Open Systems Interconnection – Abstract Syntax Notation One (ASN.1) – Part 1: Specification of Basic Notation First Edition, Amendment 1*, 1996.

ISO/IEC9075: 1992, *Information Technology – Database Languages – SQL2.*

ISO/IEC 9992-1: 1990, *Messages between ICC and CAD – Part 1: Concepts and Structure.*

ISO/IEC 9992-1: 1990, *Messages between ICC and CAD – Part 2: Functions, Messages, Data Elements, and Structures.*

ISO/IEC 9594-1:1997, *Information Technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models, and Services*, 1997.

ISO/IEC 9594-2:1997, *Information Technology – Open Systems Interconnection – The Directory: Models,* 1997.

ISO/IEC 9594-6:1994, *Information technology – Open Systems Interconnection –The Directory: Selected Object Classes*, 1994.

ISO/IEC 9594-6: *Information Technology – Open systems Interconnection – The Directory: Selected Attribute Types*, September 15, 1995.

ISO/IEC 14443: *Contactless integrated circuit card – remote coupling cards*.

ISO/IEC 10536: Identification *Cards Close Coupling Cards communication (Parts 1-3),* September 15, 1992.

ITU/ISO. Recommendation X.500 – Information technology – Open Systems Interconnection –The directory: Overview of concepts, models, and services. November 1993.

ITU/ISO. Recommendation X.509 – Information technology – Open Systems Interconnection –*The directory: Authentication framework*. November 1993.

Kaplan, Jack M., *Smart Card: The Global Information Passport*, New York: International Thomson Computer Press, 1996

Lee, Stephen, “The Case for Multifunctional Smart Cards”, *Smart Card Technology International: The Global Journal of Advanced Card Technology,* ed. Robin Townsend, London: Global Projects Group, 1996

Maritime Transportation Security Act (MTSA) 2002

Mitre Technical Report, *Department of Defense (DOD) Medium Assurance Public Key Infrastructure (PKI) Functional Specification (DRAFT) Version:* October.

Moore, Bill, *Presentation: Access Control Technology*, Systech Group, October 5, 1998.

Multi-Technology Automated Reader Card (MARC) Project Final Draft, Prepared for: Joint Staff and the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence, October 1, 1996.

National Automated Clearing House Association, The Internet Council, Authentication and Network of Trust Pilot Program. *Certificate Policy (Draft),* January 1998.

National Automated Clearing House Association, The Internet Council, Authentication and Network of Trust Pilot Program, *Proposed NACHA X.509 Certificate and CRL Profile*, December 5, 1997.

National Security Agency, Central Security Service. *Guidelines for Placing Biometrics in Smart Cards*, Version 1.0, September 11, 1998.

National Strategy for Homeland Security, OHS 2002.

National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, *Government Smart Card Interoperability Specification*, Version 2.1, July 16, 2003.

OMB A-130: Management of Federal Information Resources, 1996.

OpenCard□Framework Website, http:/www.nc.com/opencard/

OpenCard Consortium. *OpenCard Framework (Version 1.0)*, General Information Web Document, October, 1998.

PC/SC Workgroup, *Interoperability Specifications for ICCs and PC Systems – Part 1 through 8, (Version 1.0: Final).*

Perry, William E., *Structured Approach to Systems Testing,* Wellesley, Massachusetts: QED Information Sciences, Inc., 1983

Phoenix Planning & Evaluation and Coopers & Lybrand, *Guidelines for Implementing an Enhanced EBT Multi-Application Smart Card Platform – Draft*, June 5, 1998

Public Key Infrastructure (PKI) Version 1 Technical Specifications:

Polk, W. (Ed.). Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1)

Part A: Requirements. (NIST PKI Technical Working Group) January 1996.

Nazareno, N. (Ed.). Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) Part B: Technical Security Policy . (NIST PKI Technical Working Group) January 1996.

Burr, W. (Ed.). Federal Public Key Infrastructure (PKI) Technical Specifications

(Version 1) Part C: Concept of Operations. (NIST PKI Technical Working Group) November 1995.

Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) Part D:

Interoperability Profiles. (CygnaCom Solutions, Inc. for the NIST PKI Technical

Working Group) September 1995.

Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) Part E: Certificate and CRL Extensions Profile. (NIST PKI Technical Working Group)

Reed, Richard B., *Standard Badge for Government White Paper with Memorandum of Agreement,* Facilities Access Working Group, Facilities Protection Committee, U.S. Security Policy Board, February, 1998.

RSA Laboratories, *PKCS #1: RSA Encryption Standards" Version 1.5*, RSADSI, November 1992

RSA Laboratories*, PKCS #6: Extended-Certificate Syntax Standard*, RSADSI, November 1993.

RSA Laboratories*, PKCS #9: Selected Attribute Types*, RSADSI, November 1993.

RSA Laboratories*, PKCS #10: Certification Request Standard*, RSADSI, November 1993.

RSA Laboratories, *PKCS #11: Cryptographic Token Interface Standard, Version 1*, RSADSI, April, 1997.

RSA Laboratories *PKCS #15 V.1.0: Cryptographic Token Information Format Standard*. RSADSI, February 1999.

Russell, James, *Comparison of Dynamic versus Static Technology with Relation to Memory and Security*, MasterCard International, September 2003.

Smart Card Alliance white papers including those on secure physical access, privacy and smart cards, contactless technology, smart cards and biometrics, smart cards and retail payments, contactless payments, digital security case studies, available at www.smartcardalliance.org.

Smedinghoff, Thomas J., *Model Certificate Policy: Preliminary Discussion Draft*, Government Information Technology Services. Federal PKI Task Force. Business and Legal Work Group, November 25, 1997.

Sparkman, Randy P., *Digital Certificates Within a Public Agency: Utilization and Preparation in the National Aeronautics and Space Administration: A Case Study,* Gaithersburg: Public Forum on Certificate Authorities and Digital Signatures: Enhancing Global Electronic Commerce, July 24, 1997.

Tarbox, Andrew and John Tunstall, “EMV Specifications Update”, *Smart Card Technology International: The Global Journal of Advanced Card Technology*, ed. Robin Townsend, London: Global Projects Group, 1996.

Technical definitions, WhatIs.com, http://whatis.techtarget.com/

Technology Committee – Standards Subgroup, *Smart Card Forum Standards ad Specifications of Smart Cards – An Overview,* March 1996.

The Aviation and Transportation Security Act, 2001.

The Electronic Signatures Act, 2002.

The Enhanced Border Security and Visa Entry Reform Act, 2002.

The Government Information Security Reform Act (GISRA), 1999.

The Government Paperwork Elimination Act (P.L. 105-277).

The Government Paperwork Reduction Act (PRA), 1995.

The Information Technology Management Reform Act, 1996.

The Port and Maritime Security Act, 2001.

The Privacy Act, 1974.

The Homeland Security Act. 2002.

Three G International. *Smart Card Access Control*.

USA Patriot Act, 2001.

U.S. Chief Financial Officers’ Council, *Systems Interface and Functional Requirements for Card Management Systems, Draft*, August 28, 1998.

U.S. Department of Defense, *Certification Practices Statement for the Certificate Management Infrastructure of the Defense Information Infrastructure, Version 0.2,* April 10, 1998.

U.S. Department of Defense, *Public Key Infrastructure Roadmap for the Department of Defense, Version 2.0,* April 19, 1999.

U.S. Department of Defense, Security Enterprise Integration Working Group (SEIWG), SEIWG-012, *Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC)*, February 28, 1994.

U.S. Department of Defense, Smart Card Technology Office, Functional Working Group For Security, *Recommendations for the Secure Implementation of Multiple Applications on Smart Card Devices, First Draft,* May 3, 1999.

U.S. Department of Energy, Office of Safeguards & Security, *DOE Badge Program, Vol. I,II, & III*, November 18, 1998.

U.S. General Services Administration, Office of Federal Protective Services*, Document #PBS P 5390.17B*.

U.S. General Services Administration, Federal Telecommunications Service, Office of Information Security. *Access Certificates for Electronic Services (ACES) Request For Proposals (RFP) Multiple Award Schedule (MAS) TIBA98003A*, January 4, 1999.

Vulnerability Assessment of Federal Facilities. U.S. Department of Justice, June 28, 1995.

Walder, Bob, *Smart Cards: The Use of Intelligent Plastic for Access Control, White Paper,* Bedford, England: Network House, September 1997.

Zoreda, Jose Luis and Jose Manuel Oton, *Smart Cards,* Boston: Artech House Inc., 1994.

12. APPENDIX E – INTEROPERABILITY STANDARDS

* Go to http://www.smart.gov for the current version of the Smart Card Interoperability Specifications *

13. APPENDIX F – AGENCY PROFILE QUESTIONNAIRE

The Agency Profile helps an agency develop a profile that will impact whether or how a smart card will be implemented. Prior to initiating a task order for smart cards, it is critical that each agency understands its own specific requirements and goals for the smart card platform. Toward that end, we have provided the following questionnaire that will guide you to the most suitable smart card for your agency. The Agency Profile questionnaire develops an agency profile by focusing on the following key areas:

- Security requirements
- Current architecture
- Interoperability
- Size and geographic distribution
- Card management
- Applications
- Resources

Name & Title:

Name of Specific Department or Agency:

Business Line

How would you characterize the business line of your agency?

(a) Military/Security
(b) Financial
(c) Customer Service
(d) Law Enforcement
(e) Grant Administration
(f) Other: Please Specify

How will this impact your decision making related to the Smart Access Common ID Card?

Security

Physical Access
Which of the following most closely describes how employees enter your agency premises?

(a) Employees may enter/exit the premises without restriction.
(b) Employees must show a government-issued picture ID to enter the premises.
- How many employees enter the premises with a government-issued picture ID on a daily basis?
(c) Employees must use a card or biometric to enter the premises.
- How many employees enter the premises with a card or biometric on a daily basis?
(d) Employees must use an RF/proxy card to enter the premises.
- How many employees enter the premises with an RF/proxy card on a daily basis?
(e) Other: Please specify.

On a scale of 1 to 4, one being “low risk” and 4 being “high risk”, what is the level of risk associated with a breach of entry to the premises? 1 2 3 4

Which of the following most closely describes how employees move about your agency/office once inside?

(a) Employees have unrestricted access to any part of the agency once inside.
(b) Employees have access to only certain areas of the agency and require additional levels of clearance to enter specified higher-security areas.
- How many employees access restricted areas of the agency which require additional clearance level on a daily basis?
(c) Other: Please specify.

On a scale of 1 to 4, one being “low risk” and 4 being “high risk”, what is the level of risk associated with a breach of access to restricted areas? 1 2 3 4

Which of the following most closely describes how agency employees move among different agency buildings within their Department?

(a) Employees have unrestricted access to any agency buildings within their Department.
(b) Employees must present a single Department level ID card to enter all agency buildings with their Department.
How many employees present a single Department level ID card enter the premises with a card or biometric on a daily basis?
(c) Employees must present a single Department level ID card to enter only certain agency buildings within their Department, but are unrestricted in entering others.
(d) Employees must have separate IDs to enter other agency buildings.

On a scale of 1 to 4, one being "low risk" and 4 being "high risk", what is the level of risk associated with a breach of entry to restricted buildings? 1 2 3 4

Does your agency have Sensitive Compartmentalized Information Facilities (SCIFs) that require secure access?

Do you have a need to protect top secret files or documents?

Does your agency have a lot of expensive resources/equipment on its premises?

Does your agency have any other special physical security requirements?

Does your agency presently have a physical access system in place? If so, what technology is used?

Do you need to secure entrance to agency parking facilities?

Logical Access
Does your agency presently use any kind of logical access system for its computers or networks? If so, what technology is used?

How many employees have restricted access to the agency's computers and networks?

Are there varying levels of access? Please describe.

On a scale of 1 to 4, one being "low risk" and 4 being "high risk", what is the level of risk associated with a breach of access to restricted information? 1 2 3 4

If you use the DOD assurance levels of restricted usage, how many employees are classified on each level?
__ 2
__ 3
__ 4
__ 5

Please indicate each of the following that applies to your agency:

(a) Agency employees often travel or telecommute, requiring remote access to your computer system.
(b) Agency employees are granted different levels of access to the computer system.
(c) Agency employees transmit and/or receive data across open networks.
(d) Agency employees transmit confidential or high security data or information.
(e) Agency employees transfer and/or receive electronic forms.
(f) Agency provides or is planning to provide services or information to citizens via the Internet.

(g) Agency provides or is planning to provide services or information to businesses or other government agencies via the Internet.
(h) Agency has a need to encrypt transactions sent over open networks or via the Internet.
(i) Agency exchanges clearance information with other agencies.
(j) Agency exchanges other confidential information (i.e. Visa information, immigration information, passport information) with other agencies.
(k) Agency employees are assigned separate passwords for each different system they access.

What procedures do you currently use to verify an employee's identity and authorization?

Current Architecture

Please describe the current hardware, software, and databases used for physical access and the number of years each group of components has been used or in operation.

Please describe the current hardware, software, and databases used for logical access and the number of years each group of components has been used or in operation.

Interoperability

Please indicate each of the following that applies to your agency:

a. Agency employees regularly visit other offices/buildings within the agency.
b. Agency employees access numerous computer systems within the agency.
c. Agency employees regularly visit a range of other government offices/departments.
d. Agency employees regularly access other government agency computer systems and/or data.
e. Agency employees regularly visit multiple agencies within the United States or internationally.
f. Agency employees regularly visit specific other government offices/departments.
g. Agency transmits data and/or confidential documents to government agencies overseas.

Do your geographically disperse offices have network connectivity?

Do you have network connectivity with other government agencies?

Size and Geographic Distribution

How large is your agency?

(a) Fewer than 1000 employees
(b) 1000 – 2,500 employees
(c) 2,500 – 5,000 employees
(d) More than 5,000 employees

How many offices/sites does you agency have?

(a) Only 1 office/site
(b) 2 – 5 offices/sites
(c) 6- 10 offices/sites
(d) More than 10 offices/sites

Which of the following best describes your agency?

(a) Office in 1 location only (i.e. Washington, DC)
(b) Offices in multiple locations within a limited geographic area (i.e. campus setting)
(c) Offices in multiple locations throughout the United States
(d) Offices in one or more locations within the United States and at 1 location overseas
(e) Multiple offices within the United States and overseas
(f) Other: Please specify

Do your agency have facilities in privately-owned buildings?

Card Management

How does an employee at your agency enroll to receive an ID card?

How and where are ID cards personalized with employee information?

How and where are the ID cards issued to employees? Over-the-counter? Mail issuance?

Would your agency prefer to issue the Smart Access Common ID Card from one central location for the entire agency or from multiple local sites?

Where do employees go, if they have a problem with their card (i.e. lost, stolen, inoperable)?

Does agency ID database contain demographic data only or is it integrated with logical or physical access control information?

Would your agency prefer to handle card customer service issues in-house or outsource that functionality? Why?

Applications

PKI

Does your agency have a need to authenticate the identity of its employees?

Do agency employees to transmit/receive digitally signed documents over networks?

Does your agency have the need to conduct secure electronic transactions (i.e. procurement documentation)?

Would you like your system to be interoperable across agencies?

Do your employees frequently access high security systems?

Do your have employees that routinely make procurements of more than $100 thousand?

Biometrics

Does your agency have a need for high security physical access?

Do agency employees need access to many secure areas within your agency?

Do you have a need for highly secure network and computer access within your agency?

Does your agency have the need to conduct high value financial transactions?

Do you have any need to verify identification for access to high security documents/meetings?

Property Management

Do you currently issue any type of property pass? What is the process? Is it time-consuming?

What is your agency's current property loss rate?

What type of property/equipment do you need to manage (i.e. computers, firearms, chemicals)?

Do your employees often need to take valuable agency equipment (i.e. laptop computers) from the building?

Is equipment shared or transferred between offices or with another agency?

Who is responsible for property management in your agency? Is it a centralized or distributed responsibility?

Is your current asset management system integrated with your card issuance system?

Rostering

Do employees in your agency conduct frequent large meetings at which there is a need to track attendance?

Do you need to keep track of who has entered/exited a certain area of a building or ship?

Do you need to track attendance for education/training or for any other purpose?

Does your agency have in-house food services?

Electronic Purse

Does your agency have vending machines or a cafeteria?

Are your agency facilities localized or in a campus setting?

Do your employees often need cash advances (i.e. travel advances, petty cash) to conduct agency business?

Does your agency provide transportation subsidies to its employees?

Debit/Credit Applications

Do your employees frequently make high volume, low-dollar purchases?

Do you have employees that frequently travel for business purposes?

Does your agency operate and/or maintain a fleet of vehicles?

Does your agency have or plan to implement an electronic procurement system?

Medical Information

Does your agency have a need for quick access to employee vital medical information?

Do your employees need quick access to insurance benefit information?

Do your employees need quick access to immunization records?

Do your employees often travel for business throughout the U.S. and overseas?

Resources

What level of resources does your agency have to commit to implementing a Smart Access Common ID Card?

(a.) Less than $500 thousand
(b.) $500 thousand to $1 million
(c.) $1 million to $5 million
(d.) $5 million to $10 million
(e.) More than $10 million

How much money does your agency have available to commit to implementing a card system?

Does your agency have sufficient human resources to dedicate to implementing, operating, and maintaining a card system?

Does your agency have sufficient facilities available for housing and maintaining a card system database, and card access terminals?

Does your agency have access to a high security computing environment?

14. APPENDIX G – AGENCY PROFILE

General Information

The business line and size of an agency card implementation is likely to have a fundamental impact on the solution required. These key characteristics will impact both the technology and the applications needed for the card platform. They may also dictate whether an agency needs an outsourced or in-house approach to card management. Further, the level of the implementation (i.e., agency-wide, bureau-wide, campus facility, single facility, etc.) will change the response to many aspects of the questionnaire. The following sections detail these key questions.

Business Line

The business line of the agency may well impact the characteristics and applications necessary for the card platform. For example, military/security organizations are more likely than civilian agencies to have more stringent security needs. Similarly, agencies involved in law enforcement or financial business lines are also more likely to need higher levels of security and require secure transactions across open networks. Financial and grant administration agencies typically handle electronic transfer of large sums of money more frequently than other types of agencies, and will therefore, require mechanisms for secure identity authentication and the ability to sign electronic documents to ensure non-repudiation. The questions below are meant to help characterize the nature of the agency's business and how that might affect the choice of a card platform.

1. *How would you characterize the business line of your agency?*

(g) Military/Security
(h) Financial
(i) Customer Service
(j) Law Enforcement
(k) Grant Administration
(l) Health Care
(m) Other: Please Specify

2. *How will this impact your decision making related to the Smart Identification Card?*

Agencies whose mission promotes the need for high security levels or high-value procurements are more likely to need digital signature and/or biometric technology. Those agencies with the highest levels of security needs are more likely to prefer in-house approaches to PKI services and card management so that they are better able to control the issuance of cards and digital certificates. Agencies that handle confidential information (e.g., medical or financial information) are also more prone to use PKI or biometrics. On the other hand, agencies whose business requires substantial customer service are predisposed to easy access to facilities and agency databases. At the same time, these agencies will eventually require the means to authenticate the identity of their customers, if they are to move to electronic delivery of services in the future.

Size and Geographic Distribution

Questions about size of agency and scope of card implementation will affect all other decisions. The answers to many of the subsequent questions on the questionnaire will be significantly impacted by the level at which the card implementation is to take place. Agencies may consider various approaches to implementation. The smallest agencies may want to procure cards for the entire agency all at once because the logistics are not as complex as they would be for a larger agency. Most agencies, however, are likely to take a piecemeal approach, procuring cards for various parts of the agency. Consequently, the questions below should determine the level at which the agency want to procure cards. Once that decision has been made, the questions should be answered again within the context of the specific procurement level being considered.

3. How large is your agency?

(e) Fewer than 1000 employees
(f) 1000 – 2,500 employees
(g) 2,500 – 5,000 employees
(h) More than 5,000 employees

4. How many offices/sites does your agency have?

(e) Only 1 office/site
(f) 2 – 5 offices/sites
(g) 6- 10 offices/sites
(h) 10 - 50 offices/sites
(i) More than 50 offices/sites

5. Which of the following best describes your agency?

(g) Office in 1 location only (i.e., Washington, DC)
(h) Offices in multiple locations within a limited geographic area (i.e., campus setting)
(i) Offices in multiple locations throughout the United States
(j) Offices in one or more locations within the United States and at 1 location overseas
(k) Multiple offices within the United States and overseas
(l) Other: Please specify

6. Does your agency have facilities in privately-owned buildings?

Please complete the following table with your answers from Questions 3 through 6. In the row marked "Identification of each site", please provide the official name of the agency site. Provide the required information for each of the sites identified.

SIZE AND GEOGRAPHIC DISTRIBUTION OF AGENCY				
Number of Sites	4			
Identification of each site	Site A	Site B	Site C	Site D
Number of employees at each Site	1,500	20	1,000	200
Location of each site	Portland	Washington	Denver	Paris
Building ownership	Public	Public	Public	Private

Large scale, agency-wide card projects will require the most significant level of effort. If the card implementation is to be agency-wide, there may be significant interoperability and standards issues. The card will have to support multiple physical and logical access control systems across divergent divisions/bureaus. Agencies with widely disbursed geographic sites will require substantial networking and distribution capabilities that may add to the complexity of the implementation. International agencies that operate with sites overseas will face additional levels of complexity dealing with issues related to communications, encryption, card management and distribution, and varying standards and regulations in foreign countries. Procedures may need to be standardized across divergent divisions to achieve any efficiencies of operation. Although more complicated to achieve successfully, agencies implementing a wide-scale card platform are more likely to experience significant economies of scale and cost reductions.

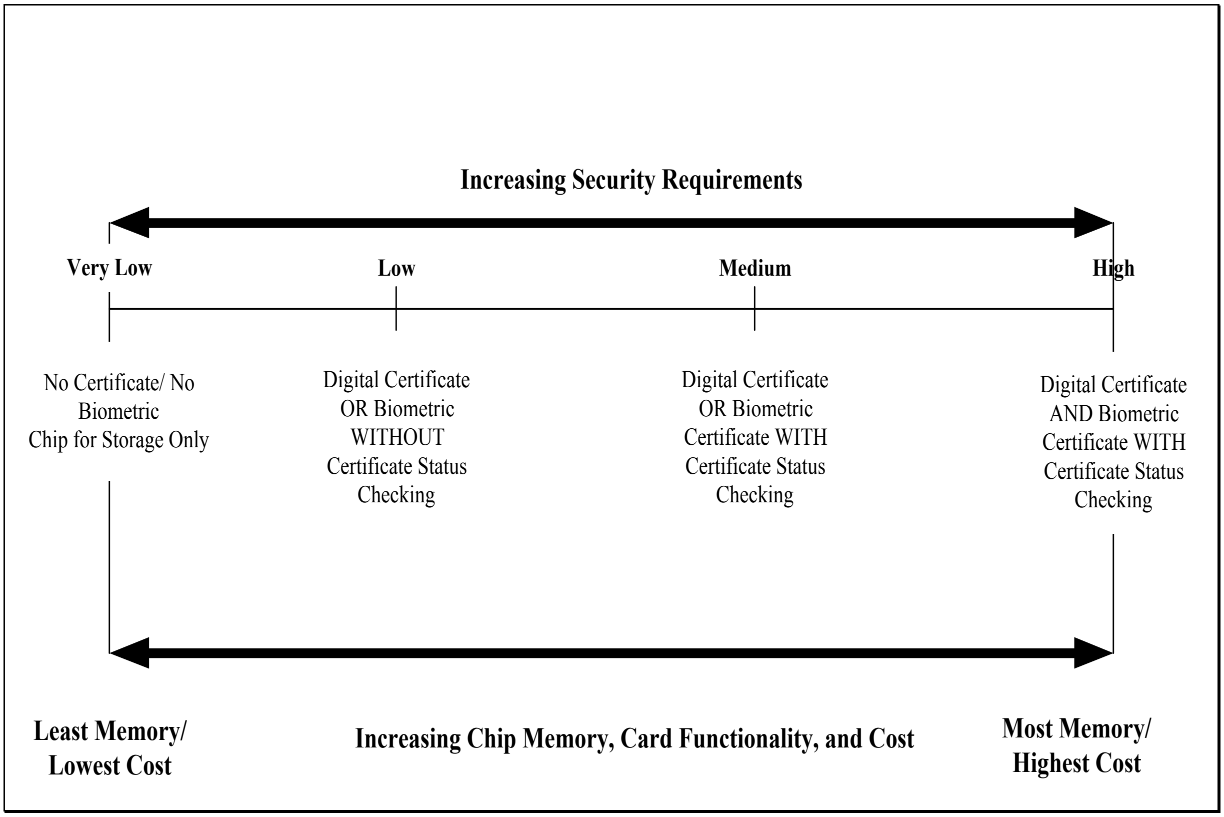
Medium size implementations across a division/bureau (e.g., Bureau of Land Management), single geographic location (e.g. Metropolitan Washington), or campus environment (e.g., National Institute of Health) will present fewer complexities. The logistics of card issuance will be easier and achieving interoperability is likely to be less challenging. Interfaces to fewer legacy systems will be required. Selection and enforcement of standards will be easier as well. Such an environment may particularly lend itself to outsourcing card management and PKI services. Achieving re-engineered processes may also be more manageable on this smaller scale. Although less complicated to achieve in the short-term, this may result in more costly implementations and integration issues in the longer term.

Small implementations for a single facility or several non-dispersed facilities will be the least complex. Although interoperability within the facilities will be easier to achieve, interoperability with other divisions or external agencies may remain a problem. Generally, agencies with this type of implementation will have somewhat lower security needs. If this is the case, lower end cards may well suffice for this type of environment.

Security

Because agencies may require different levels of assurance, they will correspondingly vary in the capabilities they need for their card platforms. Figure 7 shows an example of a possible continuum of characteristics from lowest security card platform to highest security card platform. As this diagram indicates, the capabilities, storage, and cost of the card/infrastructure are likely to increase in proportion to increasing security requirements. Additionally, interoperability requirements (e.g., to store multiple certificates) will impact the capability, size, and cost of the card. Agencies are free to select from a range of products and implementation approaches to best meet their individual needs. Those agencies with lower security requirements or to whom interoperability is not as important may be satisfied with lower end card platforms. However, agencies with the need for higher levels of assurance or more pressing interoperability requirements, may need a more comprehensive card platform with the capability to store digital and/or biometric certificates (and the requisite infrastructure to validate these certificates).

Agencies may “mix and match” different approaches using PKI or biometrics or both to achieve more secure identification authentication. Therefore, agencies will utilize different card platforms depending on how they implement identification authentication and what applications they want to use the card to access. Those agencies, for example, which are going to employ the emerging Federal Public Key Infrastructure (FPKI) to achieve government-wide interoperability may need a far more sophisticated card platform with increased chip memory and a cryptoprocessor.


Increasing Security Requirements
Very Low
Low
Medium
High
No Certificate/ No Biometric Chip for Storage Only
Digital Certificate OR Biometric WITHOUT Certificate Status Checking
Digital Certificate OR Biometric Certificate WITH Certificate Status Checking
Digital Certificate AND Biometric Certificate WITH Certificate Status Checking
Least Memory/ Lowest Cost
Increasing Chip Memory, Card Functionality, and Cost
Most Memory/ Highest Cost

The Department of Defense has defined a set of assurance levels (levels 1 through 5) that are differentiated by specific characteristics and provide requirements for the types of security required. It is anticipated that many agencies will adopt this security framework when developing their requirements for the Smart Identification Card task orders.

Governments and businesses alike must ensure the security of their properties (physical access) as well as their networks and computer systems (logical access). For the most part, these entities use a photo identification for building access and passcodes for system security. The following sections will address physical and logical access and describe methods for using the Smart Identification Card to enhance and combine security methods for both.

Physical Access

The need to ensure secure physical access to government buildings can vary greatly across government agencies and departments. These differences can be on several levels. Some agencies have largely low-level security needs but have highly restricted areas for access by only a few employees. Others may require a mid-level of security for anyone who enters the building. It is not just the levels of security needed, but also the number of people who will need the different levels of access. Thus, if only a handful of people require complex security needs on the card, the agency would not design its entire card or platform based on the needs of this group of people. Whatever the security needs and configuration, this will impact the types of cards and equipment required.

The questions in this section are designed to evaluate and determine these needs. The tricky part here is that the questions are designed to evaluate current practices but also to evaluate needs that could potentially be fulfilled with a smart card platform. So, for example, an agency may currently have only a proxy card for general building entry, but utilize a separate means to allow access to restricted areas, e.g., a separate card or passcode. In this case, the chip on the card could be used to accommodate both requirements. Do not include pilots in questionnaire responses.

The section that follows addresses general building access, restricted area access, other building access, and systems access.

General Building Access

Government agencies typically issue identification cards to its employees, which are used for entry onto the general premises. Entry is granted in a variety of ways. In some agencies, a security guard visually compares the photo on the card to the card presenter. In others, the card presenter passes his/her proxy card across a sensor, which results in a comparison between card data and a database. Still others perform a similar comparison by means of magnetic stripe technology.

An important part of determining potential needs is to evaluate the traffic and security needs of the agency. This section will go through the first few questions on the questionnaire. The questions that follow are to determine the number of buildings; the amount of traffic; and the number of access points associated with an agency's properties. This will provide potential vendors with basic information.

7. *How many buildings does your agency have? ____*

8. *How many entrances are there to the premises of each building? ____*

9. *How many employees/people enter and exit the premises on a daily basis at each building? ____*

Please complete the following table with your answers from Questions 7 through 9. In the row marked "Identification of each building", please provide the official name of the agency building or premises. Provide the required information for each of the buildings identified.

GENERAL BUILDING ACCESS POINTS				
Number of buildings	4			
Identification of each building	Building A	Building B	Building C	Building D
Number of entrances to each building	3	2	1	2
Number of people entering/exiting premises daily	300	200	500	300
Number of people entering/exiting each access point (entrances) daily (Row	100	100	500	150

4 ÷ 3)				

Questions 10 and 11 are designed to determine the current method of controlling access to the premises.

10. Which of the following most closely describes how employees enter your agency premises?

(a.) Employees may enter/exit the premises without restriction.
(b.) Employees must show a government-issued picture ID to enter the premises.
(c.) Employees must use a card (via insertion/mag stripe) or biometric to enter the premises.
(d.) Employees must use an RF/proxy card to enter the premises.
(e.) *Other. Please specify:*

11. Is the same type of card/technology used at all buildings? If not, please describe the method(s) used at the other buildings and state how many employees/individuals enter/exit these buildings on a daily basis.

Questions 12, 13 and 14 are designed to determine access/card requirements for the future.

12. *On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a breach of entry to the premises?*

    ___1 ___2 ___3 ___4

13. *Is the current method used for general building entry adequate? If not, describe the inadequacies of the method.*

14. *Considering the answer to Questions 12 and 13 (or other agency issues), which of the following describes how your agency expects to control entry to agency premises by its employees in the future?*

    (a.) Employees will be able to enter/exit the premises without restriction.
    (b.) Employees will show a government-issued picture ID to enter the premises.
    (c.) Employees will use a card (via insertion/mag stripe) or biometric to enter the premises.
    (d.) Employees will use an RF/proxy card to enter the premises.
    (e.) Other. Please specify:

The charts below are designed to determine general equipment requirements. Any vendor will do a site survey, but this is for initial development of the task order.

Please describe the agency's equipment for its existing building access function.

EXISTING EQUIPMENT for GENERAL BUILDING AREA ACCESS			
	Vendor	Number of Pieces of Equipment	Age of Equipment
Card Readers			
Controllers (or LAP/C)			
Access Control Software			
Host/File Servers			

Please check the boxes that apply. (If your "existing" method is the same as your "required" method, do not place an X in required method rows.)

REQUIRED EQUIPMENT FOR GENERAL BUILDING ACCESS					
EXISTING METHOD	Have No Access Equipment	Have Mag Stripe Readers	Have Biometric Readers	Have RF/Proxy Readers	
Entry without restriction					
Entry with photo ID					
Entry with mag stripe card					
Entry with biometric					
Entry with RF/proxy card					
REQUIRED METHOD	Require No Access Equipment	Require Mag Stripe Readers	Require Biometric Readers	Require RF/Proxy Readers	Require Chip Card Readers
Entry without restriction					
Entry with photo ID					
Entry with mag stripe card					
Entry with biometric					
Entry with RF/proxy card					
Entry with chip card					

Develop your equipment needs statement based on where you have placed the X's. For example, "Have no access equipment; require biometric readers for general building access."

A critical consideration in choosing technology for a physical access control system is compatibility with existing legacy systems. Agencies should determine if they have legacy physical access control systems and the prevalence of these legacy systems. If such a system exists, in one or more buildings, the agency must determine if it is to replace the system now or in the immediate future. If so, the card technology will not be influenced by the legacy system architecture and technical environment. If not, the agency must choose from one of the following options:

- **Adapt the existing card readers.** Some systems can use hardware and/or software modifications to enable the old readers to read new types of cards.

- **Swap the out the existing readers.** Some agencies may to leave the legacy physical access control system in place, but install new smart card readers and adapt the older system to work with the new cards and readers.

- **Select a multi-technology card.** Agencies with an extensive installation of a legacy system (e.g., proximity or magnetic stripe) may select a card with additional technologies to accommodate backward compatibility with the technology of the legacy physical access control system.

Restricted Area Access

Some agencies have physical areas for which access is restricted to a subgroup of employees. To gain entry to these areas, a variety of methods may be used: passcode/combination lock; guard who checks photo ID against list of employees with authorized entry; biometric; or a card-based technology such as magnetic stripe or chip cards. In many cases, an employee may have a separate card from his/her general identification card for the purpose of gaining entry to restricted areas.

Questions 15 and 16 are to determine the current method for controlling access to restricted areas; the number of buildings; the amount of traffic; and the number of access points associated with an agency's restricted areas. This will provide potential vendors with basic information.

15. *Which of the following most closely describes how employees move about your agency/office once inside?*

    (a.) Employees have unrestricted access to any part of the agency once inside.
    (b.) Employees have unrestricted access to any part of the agency once inside, however, the agency will restrict one or more areas in the future.
    (c.) Employees have access to only certain areas of the agency and require additional levels of clearance to enter specified higher-security areas.
    (d.) Other: Please specify.

If the answer to Question 15 is b, c, or d, please answer Questions 16 through18.

16. *How many restricted areas do or will your agency have?*

17. *How many entry points are there to each current or proposed restricted area?*

18. *How many employees/people enter and exit on a daily basis at each current or proposed restricted area, which requires (or will require) an additional clearance level or authorization?*

Please complete the following table with your answers from Questions 16 through 18. In the row marked "Identification of each restricted areas", please provide the official name of the agency area, particularly Sensitive Compartmentalized Information Facilities (SCIFs). Provide the required information for each of the restricted areas identified.

RESTRICTED AREA ACCESS POINTS				
Number of restricted areas	4			
Identification of each restricted area	Area A	Area B	Area C	Area D
Number of access points to each restricted area	1	2	1	2
Number of people entering/exiting restricted area daily	30	40	20	50
Number of people entering/exiting each access point daily (Row 4 ÷ 3)	30	20	20	25

19. *Is the same type of card/technology used at all restricted areas? If not, please describe the method(s) used at the other areas and state how many employees/individuals enter/exit these areas on a daily basis.*

Questions 20 and 21 are designed to determine access/card requirements for the future.

20. *On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a breach of access to restricted areas?*

    ___1 ___2 ___3 ___4

21. *Is the current method used for restricted area access adequate? If not, describe the inadequacies of the method(s).*

22. *Considering the answer to Questions 20 and 21 (or other agency issues), which of the following describes how your agency expects to control entry to restricted areas by its employees in the future?*

    (a.) Employees will be able to enter/exit areas without restriction.
    (b.) Employees will show a government-issued picture ID to enter the restricted areas.
    (c.) Employees will use a card (via insertion/mag stripe) or biometric to enter the restricted areas.
    (d.) Employees will use an RF/proxy card to enter the restricted areas.
    (e.) Other: Please specify.

The following charts are designed to determine general equipment requirements. Any vendor will do a site survey, but this is for initial development of the task order.

Please describe the agency's equipment for its existing building access function.

EXISTING EQUIPMENT FOR RESTRICTED AREA ACCESS			
	Vendor	Number of Pieces of Equipment	Age of Equipment
Card Readers			
Controllers (or LAP/C)			
Access Control Software			
Host/File Servers			

Please check the boxes that apply. (If your "existing" method is the same as your "required" method, do not place an X in required method row.)

REQUIRED EQUIPMENT FOR RESTRICTED AREA ACCESS						
EXISTING METHOD	Have No Access Equipment	Have Mag Stripe Readers	Have Biometric Readers	Have Passcode Readers	Have RF/Proxy Readers	Have Chip Card Readers
Entry without restriction						
Entry with photo ID						
Entry with mag stripe card						
Entry with biometric						
Entry with passcode						
Entry with RF/proxy card						
Entry with chip card						
REQUIRED METHOD	Require No Access Equipment	Require Mag Stripe Readers	Require Biometric Readers	Require Passcode Readers	Require RF/Proxy Readers	Require Chip Card Readers
Entry without restriction						
Entry with photo ID						
Entry with mag stripe card						
Entry with biometric						
Entry with passcode						
Entry with RF/proxy card						
Entry with chip card						

Develop your equipment needs statement based on where you have placed the X's. For example, "Have no access equipment; require biometric readers for general building access."

In considering the issue of secured access to general parts of the building, it is important to determine whether a small number of employees have this special need, or whether it is typical for many employees to have specialized access requirements. Agencies may need to choose among the following options:

- **Issue Multiple Cards.** If only a few employees need access to specialized parts of the building, it may be more economical to issue separate cards to those particular individuals.

- **Issue Limited Multiple Technology Cards.** Some agencies may to issue less complex types of cards to the majority of employees, but issue multiple technology cards to those employees with special access control needs (e.g., mag stripe for general entry into the building with added chip capability for a biometric or digital certificate for employees who need access to a SCIF).

- **Issue High End Cards to Majority of Employees.** If many employees will have need for multiple levels of access, it may be more practical to buy "high end" cards for the majority of employees in bulk quantities.

Agencies should use the statistics gathered from the charts above to help them determine the most economical approach to use in the task order procurement.

Other Building Access

In some implementations, employees issued cards must have access to buildings other than the building for which the particular card was issued. There are various levels of "other building access" that must be considered. Internal agency access includes those instances in which an employee must regularly go to other buildings belonging to the same or other divisions of the employee's agency. This situation is most likely to occur when the card implementation is at the division/bureau or office level within a larger agency. External agency access includes those instances in which an employee must go to a building owned by an agency other than the employee's agency. The questions below are designed to explore these two types of access.

23. *Which of the following most closely describes how agency employees move among different agency internal buildings (e.g., another division's buildings) and among external agency (e.g., a different agency's buildings) buildings?*

    (a.) Employees have unrestricted access to any agency buildings with which they have regular interaction.
    (b.) Employees have unrestricted access to any agency buildings with which they have regular interaction, however, the agency will restrict access to one or more buildings in the future.
    (c.) Employees must present their existing ID card to enter all agency buildings with which they have regular interaction.
    (d.) Employees must present their existing ID card to enter only certain agency buildings, but are unrestricted in entering others.
    (e.) *Employees must have separate IDs to enter other agency buildings.*

If the answer to Question 23 is b, c, d, or e, please answer Questions 24 through 28.

24. *How many other restricted buildings do or will your agency have?*

25. *How many entry points are there to each current or proposed restricted building?*

26. *How many employees/people enter and exit on a daily basis at each current or proposed restricted building which requires (or will require) an additional clearance level or authorization?*

Please complete the following table with your answers from Questions 24 through 26. In the row marked "Identification of each other building", please provide the official name of the agency area. Provide the required information for each of the restricted areas identified.

OTHER BUILDING ACCESS POINTS				
Number of buildings	4			
Identification of each building	Building A	Building B	Building C	Building D
Number of entrances to each building	3	2	1	2
Number of people with separate ID cards	120	80	60	120
Number of people entering/exiting each access point (entrances) daily (Row 4 ÷ 3)	40	40	60	60

27. *Is the same type of card/technology used at all other buildings? If not, please describe the method(s) used at the other areas and state how many employees/individuals enter/exit these areas on a daily basis.*

Questions 28 through 33 are designed to determine access/card requirements for the future.

28. *On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a breach of access to other buildings?*

    ___1 ___2 ___3 ___4

29. *Is the current method used for access to other buildings adequate? If not, describe the inadequacies of the method(s).*

30. *Considering the answer to Questions 31 and 32 (or other agency issues), which of the following describes how your agency expects to control entry to restricted areas by its employees in the future?*

    (a.) Employees will be able to enter/exit other buildings without restriction.
    (b.) Employees will show a government-issued picture ID to enter the other buildings.
    (c.) Employees will use a card (via insertion/mag stripe) or biometric to enter the other buildings.
    (d.) Employees will use an RF/proxy card to enter the restricted areas.
    (e.) Other: Please specify.

To what degree do the number of employees with access to restricted areas and other buildings overlap?

DEGREE OF OVERLAP			
	Restricted Area Access	Other Building Access	Access to Both
Number of Individuals with Access			

The degree of overlap required across buildings is critical to developing an approach to interoperability. There are several levels of interoperability: across different buildings for employees of the same agency, across agencies with whom the home agency does frequent business, and across multiple agencies. Both general and restricted access may be needed in each of these situations:

- **Internal Agency Interoperability.** In some instances, agencies have little need for employees to move from one agency facility to another. If, however, the employees need to move freely between different buildings, the issue of legacy systems becomes increasingly important. Agencies that have a high level of employees moving from building to building and that are issuing cards on an agency-wide basis may need to consider multiple technologies on the card to address compatibility with existing legacy systems or full scale replacement of physical access control systems. For those agencies with little interbuilding traffic, it may be more practical to issue multiple cards or guest building passes on the rare occasions when an employee needs to go from building to building. If a significant number of employees need both access to other buildings and access to restricted areas, the use of a multi-technology card becomes more practical.

- **External Agency Interoperability.** Employees from a given agency may have a need to go to a limited set of other agencies on a regular basis. In this situation, interoperability agreements should be put in place to ensure that the partner agencies will procure compatible cards. Another approach is for each agency to issue regular visitors guest cards as mentioned above. When more global interoperability is required, legacy system compatibility issues have a far more significant impact. In a global environment, compatibility across multiple legacy physical access control systems must be addressed.

Parking Access

Requirements for parking access will impact the choice of technologies required on the card. Typically, parking access requires that a card can be read from a distance. Physical access control systems typically do not require that the card be readable from a distance. Thus, the card technology needed for the physical access control system may be different from that needed for parking access. The questions that follow assess the impact of parking access on an agency's card technology requirements.

31. Does the agency have restricted parking facilities?

32. Is the parking facility operated by the agency or an outside entity?

33. Is the agency interested in having parking access privileges incorporated onto the card?

34. *How many employees access the restricted parking facilities?*

Please complete the following table with your answers from Questions 31 through 34. In the row marked "Identification of each other building", please provide the official name of the agency area. Provide the required information for each of the restricted areas identified.

RESTRICTED PARKING ACCESS				
Number of buildings	4			
Identification of each building	Building A	Building B	Building C	Building D
Building has restricted parking access	Yes/Privately Owned	Yes/Agency Owned	No	No
Number of employees accessing restricted parking facilities	40	40	60	60

Typically parking access requires a proximity or contactless chip card technology to allow for extended distance access. This card may require different technology from the card used for the physical access control system, especially if the card is being adapted to a legacy system. Because of this potential incompatibility, cards being used both for parking access and building access may need multiple technologies. Alternatively, readers could be swapped into the existing physical access control system that would accommodate both the legacy physical access control system and the parking access. The magnitude of the overlap of employees needing both parking access and building access will determine the most practical solution. If the overlap is high, it will be practical to issue multi-technology cards. On the other hand, if the overlap is low, or confined to a particular building, it may be more viable to use a separate card for parking access than to incur the expense for a multi-technology card to accommodate a small number of employees.

Summary of Key Decisions in Physical Access Control

In selecting a card platform, the physical access control application may impact a number of decisions ranging from type of technology to size of chip. The agency in developing its card platform must make the following decisions based on its emerging agency profile:

- Is physical access control to be one of the included applications?
- If it is, what technology is desired for physical access control (e.g., magnetic stripe, proximity, contact and/or contactless chip using an access code, biometric, or digital certificate) to support the needed level of security within the constraints of resource availability?
- Is an existing legacy system in place? If so, does the agency to maintain that system?
- Does the agency need the new card platform to be compatible with the legacy physical access control system, or will the system itself be adapted?
- Does the agency need different levels of access to different parts of the building?
- Do many employees need different access levels or just a few? Can more than one card be used to accommodate the exceptions?
- What level of interoperability is needed across facilities within the agency? Is it needed by many employees or only by a special few?
- What level of interoperability is needed across agencies? Is interoperability needed with just a few partner agencies or is more global interoperability across multiple agencies needed?
- Is access to parking facilities needed? If so, is it needed by many employees or a few?

- Are physical access control privileges currently maintained in a separate physical access control system, badging system, or an integrated card management system?

- How does the agency intend to handle this in the future?

- Do the logical access control and physical access control personnel in the agency work closely together?

Logical Access
Agencies can vary greatly in their requirements for network and system access. Some agencies do not require a passcode to access agency systems while others do. Currently, the most widely used method is still the passcode. But in an era of computer hacking and the concern over confidentiality, government agencies are taking a closer look at stronger means to secure access to systems and data.

In addition to protecting system and database access, some agencies have the need to ensure that information created and received by its employees is safeguarded through means of encryption and authentication.

General System Access
Government agencies typically have not used employee identification cards to date to control system access. System access is currently granted in a variety of ways. By far, the most prevalent mechanism is a passcode. However, some higher security agencies are beginning to adopt some type of token mechanisms.

An important part of determining potential needs is to evaluate the traffic and security needs of the agency. The questions that follow are to determine the general approach to system security; the number of systems; the amount of traffic; and the type of access control preferred by an agency. This will provide potential vendors with basic information.

Questions 35 through 38 are designed to determine the current method of controlling access to the systems, networks, and databases. Hereafter, when the term system is used, it is meant to refer to the complete system including any hardware, software, telecommunications, and databases.

35. *Does your agency presently use any kind of general access system for its computers or networks? If so, what technology is used?*

36. *How many PCs/access points are there to the general system?*

37. *How many employees require access to the system on a daily basis?*

38. *Which of the following most closely describes how employees gain access to the general system?*

    (a.) Employees may gain access without restriction.
    (b.) Employees must enter a passcode to gain access.
    (c.) Employees must use a biometric to gain access.
    (d.) Employees must use a smart card to gain access.
    (e.) Employees must use a PCMCIA card to gain access.
    (f.) *Other: Please specify.*

Questions 39, 40, and 41 are designed to determine access/card requirements for the future.

39. *On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a breach of entry into the general system?*
___1 ___2 ___3 ___4

40. *Is the current method used for general system access adequate? If not, describe the inadequacies of the method.*

41. *Considering the answer to Questions 39 and 40 (or other agency issues), which of the following describes how your agency expects to control entry to agency systems by its employees in the future?*

(a.) Employees will be able to gain access without restriction.
(b.) Employees will enter a passcode to gain access.
(c.) Employees will use a biometric to gain access.
(d.) Employees will use a smart card to gain access.
(e.) Employees will use a PCMCIA card to gain access.
(f.) Other: Please specify.

The following charts are designed to determine general equipment requirements. Any vendor will do a site survey, but this is for initial development of the task order.

Please describe the agency's equipment for its existing system access function.

EXISTING EQUIPMENT SYSTEM ACCESS			
	Vendor	Number of Pieces of Equipment	Age of Equipment
Card Readers			
Controllers			
Access Control Software			
Host/File Servers			

Please check the boxes that apply. (If your "existing" method is the same as your "required" method, do not place an X in required method rows.)

REQUIRED EQUIPMENT FOR GENERAL SYSTEM ACCESS					
EXISTING METHOD	Have No Access Software	Have Passcode Software	Have Biometric Readers	Have Smart Card Readers	Have PCMCIA Readers
Access without restriction					
Access with passcode					
Access with biometric					
Access with smart card					
Access with PCMCIA card					
REQUIRED METHOD	Require No Access Software	Require Passcode Software	Require Biometric Readers	Require Smart Card Readers	Require PCMCIA Readers
Access without restriction					
Access with passcode					
Access with biometric					
Access with smart card					
Access with PCMCIA card					

Develop your equipment needs statement based on where you have placed the X's. For example, "Have passcode application; require biometric readers and software for general system access."

Agencies that have low level security needs for their systems may determine that passcode security is sufficient. However, those agencies that have higher level security needs across the board for their systems should consider a chip card to enable the use of a biometric, digital certificate, or card-based passcode for system access. Few agencies will require token secured access for every employee. Most agencies will have employees with a variety of access levels and may choose either to purchase cards with multiple technologies or to purchase different cards for different employee levels.

Restricted System Access

Some agencies, particularly agencies with high level security needs, may have systems requiring additional clearance levels for access. Questions 42 and 43 are to determine the current method for restricting access to these "high risk" systems. This will provide potential vendors with basic information.

42. Which of the following most closely describes how employees access restricted systems?

(a.) Employees have unrestricted access to all "high risk" agency systems.
(b.) Employees currently have unrestricted access to any agency system, however, the agency will restrict one or more "high risk" systems in the future.
(c.) Employees have access to only certain agency systems and require additional levels of clearance to access other agency "high risk" systems.
(d.) Other: Please specify.

If the answer to Question 42 is b, c, or d, please answer Questions 43 through 45.

43. How many restricted systems does or will your agency have?

44. How many PC/access points are there to each current or proposed restricted system?

45. How many employees/people access current or proposed restricted systems on a daily basis, which requires (or will require) an additional clearance level or authorization?

Please complete the following table with your answers from Questions 42 through 45. In the row marked "Identification of each restricted system", please provide the official name of the system. Provide the required information for each of the restricted systems identified.

RESTRICTED SYSTEM ACCESS POINTS				
Number of restricted systems	4			
Identification of each restricted system	System A	System B	System C	System D
Number of access points/PCs to each restricted system	20	35	20	50
Number of people with restricted access to system	30	40	20	50

46. Are there varying levels of access for each system? Please describe.

If employees are granted different levels of access to one or more systems, please indicate below. Complete the following table for each restricted system:

LEVELS OF ACCESS FOR RESTRICTED SYSTEMS				
Identification restricted system	System A			
	Level 2: (Identify)	Level 3: (Identify)	Level 4: (Identify)	Level 5: (Identify)
Number of people with privileges at this level and below				
Identification Method				

Questions 47, 48, and 49 are designed to determine access/card requirements for the future.

47. On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a breach of access to restricted systems?

___1 ___2 ___3 ___4

48. If you use the DOD assurance levels of restricted usage, how many employees are classified on each level?

___ 2 ___ 3 ___ 4 ___ 5

49. Is the current method used for restricted system access adequate? If not, describe the inadequacies of the method(s).

50. Considering the answer to Questions 47 through 49 (or other agency issues), which of the following describes how your agency expects to control entry to restricted systems by its employees in the future?

(a.) Employees will have unrestricted access to all agency systems.
(b.) Employees currently have unrestricted access to any agency system, however, the agency will restrict one or more systems in the future.
(c.) Employees will have access to only certain agency systems and require additional levels of clearance to access other agency systems.
(d.) *Other: Please specify.*

Please check the boxes that apply. (If your "existing" method is the same as your "required" method, do not place an X in required method rows.)

REQUIRED EQUIPMENT FOR RESTRICTED SYSTEM ACCESS					
EXISTING METHOD	Have No Access Software	Have Passcode Software	Have Biometric Readers	Have Smart Card Readers	Have PCMCIA Readers
Access without restriction					
Access with passcode					
Access with biometric					
Access with smart card					
Access with PCMCIA card					
REQUIRED METHOD	Require No Access Software	Require Passcode Software	Require Biometric Readers	Require Smart Card Readers	Require PCMCIA Readers
Access without restriction					
Access with passcode					
Access with biometric					
Access with smart card					
Access with PCMCIA card					

Develop your equipment needs statement based on where you have placed the X's. For example, "Have passcode application; require biometric readers and software for restricted system access."

While passcode access is probably sufficient for general systems access in many agencies, many agencies will have certain "high risk" systems that require a higher level of access control. Generally, access to these systems is restricted to a relatively small number of individuals. Agencies with even a few systems that require this enhanced security should consider a chip card to enable the use of a biometric, digital certificate, or card-based passcode for restricted system access. Because agencies usually will have employees with a variety of access levels, it may not be practical to purchase "high end" cards for all employees. Agencies may opt to purchase cards with multiple technologies or to purchase different cards for different employee levels.

Secure Transactions

In addition to the need to protect systems, networks and databases, many agencies have the need to not only secure the transmission of information, but also to verify and authenticate the identity of employees participating in such transactions. If this is the case, there are several technologies available that can accomplish these objectives. These technologies could be supported by the Smart Identification Card. To assess the importance of these technologies to your agency, please answer the following questions.

51. Please indicate each of the following that applies to your agency:

(l) Agency employees often travel or telecommute, requiring remote access to your computer system.
(m) Agency employees transmit and/or receive data across open networks.
(n) Agency employees transmit confidential or high security data or information.
(o) Agency employees transfer and/or receive electronic forms.
(p) Agency provides or is planning to provide services or information to citizens via the Internet.
(q) Agency provides or is planning to provide services or information to businesses or other government agencies via the Internet.
(r) Agency has a need to encrypt transactions sent over open networks or via the Internet.
(s) Agency exchanges clearance information with other agencies.
(t) *Agency exchanges other confidential information (i.e., Visa information, immigration information, passport information) with other agencies.*

If any of the conditions (a through i) in Question 51 apply to your agency, please answer Questions 52 through 59. Questions 52 through 59 are designed to determine the extent to which your agency must support secure transactions in the future.

52. Does your agency routinely have the need to conduct secure electronic transactions (i.e., procurement documentation)?

53. If yes, approximately how many employees routinely have the need to conduct secure electronic transactions?

54. Does your agency routinely have the need to verify/authenticate the identity of an employee/individual sending and/or receiving a transaction (e.g., financial and sensitive information)?

55. If yes, approximately how many employees routinely have the need to conduct transactions in which the identity of the employee must be verified and authenticated?

56. Do agency employees have any need to transmit/receive digitally signed documents over networks?

57. Does your agency have employees that routinely make procurements of more than $100 thousand?

58. Does your agency routinely have the need to perform secure and/or authenticated transactions with other agencies?

59. Does your agency routinely have the need to perform secure and/or authenticated transactions with the public?

If employees have a need to perform secure transactions, please indicate below the number of employees and the frequency of the activity. Complete the following table for each function based on your responses to Questions 52 through 59:

REQUIRED SECURE TRANSACTIONS					
	Have Need for Secure Transactions with Other Agencies/ Businesses/ Public	Have Need To Authenticate Employee/ Individual's Identity	Exchange Confidential Information with Other Agencies/ Businesses/ Public	Have Need for Electronic Forms	Make High Value Purchases
Number of Employees					
Frequency of Transactions					

60. *To what degree do the number of employees with access to restricted systems and need for secure transactions overlap?*

DEGREE OF OVERLAP			
	Restricted System Access	Secure Transactions	Access to Both
Number of Individuals			

The degree of overlap between employees with the need to access restricted systems, as well as to ensure secure transactions will impact the technology required for the agency's card platform. If there is a high number of employees who need both capabilities, as well as secure physical access control, it is probably necessary to purchase a higher end card with enough memory and/or a cryptoprocessor to support a digital signature or biometric capability. On the other hand, if this overlap is relatively small, a lower end card may be sufficient for most employees.

Develop your digital signature and/or biometric needs statement based on the frequency and number of needed secure transactions, as well as the overlap between restricted access systems and secure transactions. For example, "Have routine requirements for electronic forms, secure transactions, and high value purchases so that the agency needs a digital signature application." Another example might be, "Have substantial need only to authenticate employee identity, so agency needs biometric."

Summary of Key Decisions in Logical Access Control

In selecting a card platform, the logical access control application may impact a number of decisions ranging from type of technology to size of chip. In developing its card platform, the agency must make the following decisions based on its emerging profile:

- Is logical access control to be one of the included applications?
- If it is, what technology is desired for logical access control (e.g., contact and/or contactless chip, fortessa (a specific type of high-security card) card, biometric, or digital certificate) to support the needed level of security within the constraints of resource availability?
- Is an existing legacy logical access control application in place? If so, does the agency to maintain that system?
- Does the agency need the new card platform to be compatible with the legacy logical access control system, or will the system itself be adapted?
- Does the agency have a large number of restricted systems?
- Does the agency need different levels of access to different systems?
- Do many employees need different access levels or just a few? Can more than one card be used to accommodate the exceptions?
- What level of interoperability is needed across systems within the agency (e.g., across divisions or bureaus)? Is it needed by many employees or only by a special few?
- Do many employees need remote access to the agency's system?
- What level of interoperability is needed across external agency systems? Is interoperability needed with just a few partner agencies or is more global interoperability across multiple agencies needed?
- Does the public need to access any agency systems?
- Are secure transactions required? If so, for what purpose?
- Are electronic forms contemplated for use in the agency?
- Are logical access control privileges currently maintained in multiple separate applications or in an integrated card management system?
- How does the agency to handle this in the future?
- Do the logical access control and physical access control personnel in the agency work closely together?

Interoperability

Interoperability refers to the cooperative processing of an application by distinct software, hardware/firmware, various generations of cards and terminals, operating procedures, or administrative procedures. Interoperability can exist at the following levels in smart cards:

- Physical attributes;
- Electrical attributes;
- Communications protocols;
- Application protocols;
- Application programming interfaces;
- Command and response mechanisms; and
- Secure application modules.

Common standards and specifications are imperative to achieving interoperability. Interoperability, in turn, will contribute substantially to the wide-scale acceptance of a multi-application employee identification card across the government. Consequently, it is crucial that the issues surrounding standards be resolved if an interoperable multi-application environment is to become the norm in the government.

The Government Smart Card Framework will encompass a broad range of applications. Within this framework, no single card can necessarily be expected to provide all the services and capabilities required by all envisioned applications. A range of card implementations will be needed with different capability set and cost/performance characteristics tailored to meet the needs of particular applications. However, all vendors supplying government card solutions under the Smart Access Common ID contract vehicle must provide a common, interoperable set of services that supports physical and logical access control, biometrics, and cryptographic services.

Although interoperability at the card level is mandated, use of an interoperable employee card to gain universal access across agencies is a good example of how achieving higher levels interoperability may continue to be challenging in the near future. A key barrier to the implementation of a common identification card across multiple agencies is the presence of incompatible legacy physical and logical access control systems. These legacy systems use a range of technologies and proprietary protocols for interacting with the databases that maintain employee privileges and control access to facilities and systems. Until existing proprietary physical access control systems can be modified or replaced, for example, interoperability within the context of a physical access control application may mean little more than the ability to read employee data carried on the card and the use of such data to populate a visitor log. While the long-term objective of this project is to achieve multiple levels of interoperability, a more limited approach to interoperability may be needed in the short term. Although the vendors participating in the Smart Identification Card procurement are bound to achieve interoperability at the card levels, “true” interoperability may be harder to attain because of the issues surrounding legacy systems, divergent agency policies and procedures, and lack of operating agreements.

In the longer term, it will become increasingly possible to achieve more extensive interoperability. While attaining interoperability at the card level is currently being addressed, accomplishing interoperability at the application level continues to be challenging when legacy systems remain prevalent in many agencies. However, the emerging PKI may provide a potential mechanism for achieving government-wide interoperability at the higher application level.

Currently, the existing logical and physical access control systems have responsibility for reading the access card, ensuring the identity of the cardholder, validating the status of the card, checking for access privileges, and providing or barring access depending on the results of this validation process. While this approach is successful for validating employees in their home agencies, it cannot accommodate employees seeking entrance to another agency’s facilities or systems because different agencies’ systems employ different technologies and protocols for conducting this validation process. Consequently, agencies have adopted various incompatible approaches to authenticating identity, managing access privileges, and granting access to visiting government employees.

To address the complexities of achieving interoperability across incompatible physical and logical access control systems, theoretically one could use the emerging PKI as a mechanism for verifying the identity of the cardholder and the validity of the card. This approach assumes: 1) a government-wide access card that can be read interoperably by card readers at different agencies; and 2) the infrastructure to validate the status of digital certificates carried on the card.

The Federal PKI Steering Committee is currently working on putting this infrastructure in place and has begun the effort to establish a Bridge Certificate Authority (for definition of this and other related terms, see the Glossary in Appendix B) to enable agencies using different Certificate Authorities (CA) to interoperably exchange certificates. The viability of this approach will depend upon the mix of applications selected by individual agencies and their unique security requirements. For agencies requiring high security, a digital certificate (or an attribute certificate carrying a biometric template) could be used as the basis for employee identification and authentication.

A reader at Agency B's facility could read a card carrying a digital or attribute certificate for an employee from Agency A. A standardized application could be used to retrieve the certificate and pass the certificate to the Certificate Authority (CA) for Agency B. Agency B's CA, in turn, could pass the certificate on to Agency A's CA through a Bridge Certificate Authority. Agency A's issuing CA would be responsible for validating the certificate and sending an approval/denial message to the initiating access control application through an appropriate Application Programming Interface (API). The access control application can then securely grant or deny access based on the results of the validation process. Thus, employees visiting agencies could be validated and granted secure access without having to be included in the visited agency's access control database.

An alternative for agencies with lower level security needs is to check only for the presence of a certificate signed by a trusted CA, without validating the certificate status through the Bridge Certificate Authority. This approach is less complex and less costly. It would not depend upon a Bridge Certificate Authority being in place. Thus, the level of security required by an agency, as well as available resources, will dictate the corresponding solution and degree of interoperability acceptable to the agency.

Agencies will vary substantially in the degree to which they need interoperability with other agencies. Some agencies will have partner agencies with which they conduct ongoing business. At least initially, few agencies will require global interoperability across the government. Agencies will need to assess the level of interoperability they can accept both in the short- and long-term. While the potential of using the FPKI to surmount the issues surrounding incompatible legacy systems may be appealing, it is likely to be expensive and relatively complex to implement. Consequently, it is imperative that agencies realistically assess their interoperability needs, so as to procure systems that achieve an "acceptable" degree interoperability for the agency in question.

Questions 61 through 63 are designed to elicit information about your agency with regards to the need for interoperable applications.

61. Please indicate each of the following that applies to your agency:

(a.) Agency employees regularly visit other offices/buildings within the agency.
(b.) Agency employees access numerous computer systems within the agency.
(c.) Agency employees regularly visit a range of other government offices/departments.

(d.) Agency employees regularly access other government agency computer systems and/or data.
(e.) Agency employees regularly visit multiple agencies within the United States or internationally.
(f.) Agency employees regularly visit specific other government offices/departments.
(g.) Agency transmits data and/or confidential documents to government agencies overseas.

62. Do your geographically dispersed offices have network connectivity?

63. Do you have network connectivity with other government agencies?

The degree of interoperability required by an agency will impact the choice of a card platform. For agencies requiring limited interoperability, adherence to the standards agreed to by the Smart Identification Card vendors, as well as adoption of vendor supplied, common, interoperable services may well achieve necessary interoperability. However, if global interoperability across multiple agencies, legacy systems, and procedural environments is required, higher end cards providing PKI and/or biometric capabilities, as well as an extensive set of interagency agreements may be required.

Card Management

There are a number of decisions that agencies must make in the card management area before an agency can write a task order under the Smart Access Common ID contract. First, agencies must develop their approach to card issuance, deciding whether to procure the services of a card issuer (i.e., outsource) or perform the issuance function in-house. Depending on the outcome of this decision, the agency must determine who will be responsible for card initialization and personalization. This decision, in turn, is dependent upon an agency's approach to card distribution. Agencies must agree on whether local or central card distribution best meets their needs. Program needs may dictate the card distribution method. For example, when cards are used in the Supplemental Food Program for Women, Infants, and Children (WIC), they must be issued locally because regulations dictate that benefits must be available immediately. Card distribution could not be centralized and comply with these regulations. If program regulations do not stipulate a particular approach, other considerations such as logistics, degree of geographic dispersion, customer convenience, viability of integration of the physical and logical access control functions, and availability of issuance facilities will impact the card personalization and distribution approach.

A second major concern is how to maintain card management and account data. Depending on the approach to card issuance (i.e., outsource versus in-house), either the contractor will have to provide account maintenance functions, or the agency will have to determine department responsibility for this function. If performed in-house, agencies may have to rethink their badging procedures to determine the appropriate jurisdiction (e.g., facilities, security, or information technology offices) for the card issuance and account maintenance functions. Responsibility for data update, back up, and recovery must be assigned.

Related to account maintenance is the issue of card replacement. Agencies must determine how they will handle lost, stolen, and damaged cards. These lost/stolen/damaged cards must be reported and "hot listed" to avoid unauthorized usage. In a multi-application environment, it is particularly difficult to assign responsibility for accepting lost card reports, maintaining the hot list, and informing all program users of the "hot listed" cards.

Responsibility for customer service is yet another issue. Once again, if card issuance is outsourced, the contractor typically provides customer service. However, if card issuance is performed in-house, the agency must decide how it will provide necessary customer service to its employees.

The methods for all aspects of card management, in turn, will dictate characteristics of the card platform and the equipment and/or services that must be procured. If card management is to be outsourced, agencies will have to decide which aspects are to be contractor provided (e.g., initialization, personalization, issuance, account maintenance, customer service, etc.) and which must remain agency functions. Alternatively, if card issuance is to be performed by the agency, then card management procedures must be decided upon in advance, so as to be able to determine the necessary equipment and software to procure. For example, if card issuance is to be centralized, less equipment will be needed than if it is performed locally over-the-counter. Furthermore, if digital certificates or biometrics are to be part of the platform, agencies must decide if they will outsource PKI and/or biometric services for identity proofing and biometric template registration. Thus, the following questions are targeted at agencies to help them establish their card management requirements.

Questions 64 through 68 are designed to help your agency develop an optimal card management strategy.

64. How does an employee at your agency enroll to receive an ID card?

To start, agencies should scrutinize current procedures to provide information about the enrollment process within the agency. While the current processes may change in a multi-application card environment, certain existing characteristics could constrain an agency's choices. While reflecting on the current processes, agencies should be looking for opportunities to streamline the enrollment process. Agencies should consider the following factors:

- Is there currently an employee identification card/badging facility?
- What organization is currently responsible for issuing employee identification cards?
- Are employees enrolled locally or centrally?
- What organization currently performs enrollment?
- What is the source of enrollment data?
- Is enrollment data maintained centrally or locally?
- What organization is responsible for updating enrollment data?
- How is enrollment data updated if it changes?
- What levels of resources are currently devoted to the enrollment process?
- Is the current employee ID used for any purpose other than identification? If so, what purpose?
- Does the organization currently providing enrollment services work with any other organization within the agency to consolidate employee identification and authorization procedures? If so, what other organizations?

65. How and where are ID cards personalized with employee information?

Again, agencies should start with their current ID card personalization process and consider how it could be streamlined in a multi-application card environment. Before finalizing the approach for card personalization, agencies should determine what technologies and applications they to have on the card. The specific technologies and applications could have an impact on the viability of a particular card personalization approach. For example, if the agency plans to use digital certificates or biometrics, it will have to accommodate the processes for obtaining digital certificates and/or “live” biometric scans during the personalization process. If both logical and physical access control applications are to be part of the card platform, the agency should determine where access privileges are to be maintained and how they are to be obtained for the personalization process (i.e., is the card management system going to maintain physical access and logical access authorizations or are they to be maintained in separate database entirely). Some agencies may choose to outsource the entire card issuance process, while others may elect to use a contractor only to personalize cards and either mail them out or send them to the agency for distribution. Agencies will have to make a number of choices when designing their card personalization processes. Agencies should consider the following factors:

- Is there currently a facility for personalizing employee identification cards?
- Is there currently equipment available for card personalization?
- What organization is currently responsible for personalizing employee identification cards?

- What data needs to be printed on the face of the card (e.g., picture, agency logo, digitized signature, etc.)? What data would need to be carried on the chip?

- Are cards personalized locally or centrally?

- What is the source of personalization data?

- Are personalization data maintained centrally or locally?

- Do card personalization data come from multiple databases?

- What level of resources is currently devoted to the personalization process?

- What level of resources would be available in the future for card personalization?

- Is the agency interested in outsourcing card personalization? If so, what delay is acceptable between enrollment and receipt of card?

- What technologies are planned for the card?

- Could the current card personalization equipment handle these technologies? If not, is there an adequate facility/space for card personalization equipment to be housed?

- Is the card personalization environment secure enough to support issuance of digital certificates?

66. How and where are the ID cards issued to employees? Over-the-counter? Mail issuance? Would your agency prefer to issue the Smart Identification Card from one central location for the entire agency or from multiple local sites?

As in the other card management areas, the agency should start with current procedures and then modify for the future. A key issue in selecting issuance procedures revolves around central versus decentralized card distribution. The level of geographic dispersion may well affect that choice. Agencies with a high degree of geographic dispersion can enhance customer convenience by providing over-the-counter enrollment and distribution, but that will require significantly higher investment in card personalization/issuance equipment. The scale of the implementation will also strongly influence this choice. Issuing centrally for an entire agency may result in substantial economies of scale and corresponding reduction in costs, but it may entail problematic customer logistics for agencies that are widely dispersed, particularly when international sites are involved. When issuing to an entire agency, local issuance may be difficult to manage across multiple organizations, yet it may be far more manageable when issuing to a campus or non-dispersed division,

A second key decision involves whether to outsource or perform card issuance in-house. This decision may be impacted by the same factors as the centralization/decentralization issue, but will have the added complexity of determining whether sufficient resources (e.g., facilities, staff, security, equipment, etc.) are available to perform the function in-house or whether outsourcing would be more economical. Outsourcing to an entire agency could streamline the issuance logistics, but significantly impact customer convenience. Further, an entire agency is more likely to be able to afford the substantial investment in card issuance equipment. In a small-scale implementation, in-house issuance may be logistically easier to accomplish but could require too substantial an up-front investment.

Agencies should consider various alternative card management strategies including but not limited to: (1) partially outsourced initialization/personalization with in-house distribution; (2) totally outsourced initialization, personalization, and issuance; (3) in-house enrollment with outsourced personalization and issuance; (4) in-house central enrollment, personalization, and issuance; (5) in-house local enrollment, personalization, and issuance; and (6) in-house centralized enrollment, personalization, and issuance. In assessing these options, agencies should weigh their goals and priorities (as defined in the card platform framework); the benefits and problems associated with their current process; the technology and applications required for their card platform; their available resources including dollars, staff, facilities, and equipment; their level of geographic dispersion; and their existing database environment to determine optimal card management strategies. Agencies should consider the following questions:

- Are employees in multiple locations and are these locations widely dispersed geographically?
- Can employees conveniently access a central location for card distribution?
- Are there program requirements or time constraints that could impact the viability of centralized mail-out of cards?
- Does the agency have the staff and/or facilities to perform local over-the-counter distribution of cards?
- From where are ID cards currently distributed to employees?
- What organization is currently responsible for distributing employee IDs?
- Are cards currently distributed locally or centrally?
- What organization currently performs card distribution?
- What level of resources is currently devoted to the card distribution process?
- Does the organization currently providing card issuance work with any other organization within the agency to consolidate employee identification and authorization procedures? If so, what other organizations?

67. Where do employees go, if they have a problem with their card (i.e., lost, stolen, inoperable)? Would your agency prefer to handle card customer service issues in-house or outsource that functionality? Why?

Card replacement for lost, stolen, or inoperable cards is generally handled by a customer service function. Responsibility for customer service is a significant issue in a multi-application card environment, particularly when there is contractor-based card issuance and multiple programs sharing applications. Responsibility for this service is less straightforward in the multi-application arena. Distinctions among the types of customer service demanded differentiate between those responsibilities belonging to the card issuer and those best handled by the individual application owners. Generally, inquiries related to the physical card (including card loss or malfunctions) are directed to the card issuer, while questions related to the individual applications are routed to the application owners.

Agencies must decide whether to provide their own or outsource customer service. If card issuance is performed in-house, agencies can either perform their own customer service or outsource just the customer service support function. Agencies choosing the in-house approach must have sufficient resources to maintain the customer service support required for a successful card implementation. This service would include providing assistance to employees, replacing lost/stolen cards, notifying all application "owners" of lost/stolen cards, and providing assistance with use of the applications on the card platform. If card issuance is outsourced, customer service usually is part of the services contract with the card issuer, but the contractor organization would have to carefully coordinate with agency programs that maintain separate applications on the card. The agency should consider the following questions when deciding on how to provide customer service:

- How are lost/stolen/damaged cards currently handled?
- What organization is responsible for providing customer service currently?
- Are there sufficient resources (i.e., facilities, staff, equipment, software, communications, etc.) to provide in-house customer service?
- Are there any regulatory or program requirements that would preclude outsourcing customer service?
- Does the agency anticipate any usage of the card to authenticate transactions with the public?
- Does the agency contemplate having financial applications on the card? If so, how would liability issues be addressed if card issuance were outsourced?

68. Does agency ID database contain demographic data only or is it integrated with logical or physical access control information?

Maintenance of card data provides yet another contentious issue. Currently, most employee identification cards are single function. Separate cards are issued for employee identification, physical access control, logical access control, travel, purchase, fleet and other purposes. Typically, the data associated with each card type are maintained in separate databases. Data are often input and updated by different organizational units. In a multi-application environment, it may be more efficient to maintain a single, integrated card management system that maintains demographic data, physical access privileges, logical access privileges, and other data depending upon the applications residing on the card platform. Such an arrangement may require a re-engineering of agency processes so that card issuance is streamlined. This re-engineering may require that departments that were once separate be integrated (e.g., badging office, security office, ADP office, etc.) and that separate legacy systems incorporate interfaces to the newly built card management system. When migrating to a multi-application employee identification card, individual agencies will have to customize their own unique process flow for card issuance, taking into account their existing organizational structure, potential opportunities for process improvement, legacy systems, existing and planned technical environment, and other factors. In deciding upon the optimal level of integration and the card management process, agencies should consider the following questions:

- What separate card databases currently exist?
- Where does card management data currently reside?
- What organization is responsible for maintaining card management data?
- How is card management data updated if it changes?

- When new applications are added to the card, where is the data for the applications managed?
- What level of resources is currently devoted to managing card management data?
- Is the current employee ID used for any purpose other than identification? If so, what purpose?
- Does the organization currently providing card management services work with any other organization within the agency to consolidate employee identification and authorization procedures? If so, what other organizations?
- How should data on the card be backed-up?
- How should data on the card be restored if the card is lost/stolen/damaged?

Resources

While other sections of the agency profile questionnaire are targeted at gathering requirements for a multi-application employee identification card, this section focuses on pinpointing constraints that could have impact on an agency's decision to implement the card, choices affecting the specific line of attack for card implementation, and the characteristics of the card platform. Resource availability will also help determine whether an agency uses an in-house, outsourced, or combination of both approaches to implement the Smart Identification Card.

Questions 69 through 73 are designed to determine the full range of resources available to support or constrain a card implementation.

69. What level of resources does your agency have to commit to implementing a Smart Identification Card?

(f.) Less than $500 thousand
(g.) $500 thousand to $1 million
(h.) $1 million to $5 million
(i.) $5 million to $10 million
(j.) More than $10 million

The level of resource availability, in and of itself, provides limited information for project planning. To gain any significant understanding of the impact of the budget on the characteristics of the card implementation, the funds available must be considered within the broader context of the project—the scope of the implementation (i.e., level of card implementation and number of cards to be issued), the technologies and applications required, project goals and priorities, and approach preferences. The point of this question is to help agencies settle on a "ball-park" figure to determine project feasibility, guide platform choices, and help refine project expectations.

70. How much money does your agency have available to commit to implementing a card system?

As in the question above, the level of resource availability for the full card "system" must be considered within the context of the project. While the number of cards is less important to this measure, the scope of the implementation is still important because it helps determine the magnitude of system components that will be required. In developing a budget for the full system implementation, the technologies and applications required, project goals and priorities, and approach remain critical to the total system cost calculation. For this figure, a decision must be made as to whether the required platform services (such as card issuance, PKI, biometrics, etc.) will be delivered in-house (so that appropriate equipment, software, and telecommunications can be sized) or outsourced (so that service costs can be assessed). Once again, the point of this question is to help agencies settle on a "ball-park" figure to help refine project scope and approach.

71. *Does your agency have sufficient human resources to dedicate to implementing, operating, and maintaining a card system?*

The availability staff resources will have a significant impact on the decision to manage the card platform in-house or to use contracted services for card issuance and management, PKI, and/or biometrics. To manage the card platform in-house the following types of staff will be required:

- Technical staff to implement and operate day-to-day the card management system, install and maintain card issuance equipment, and maintain card readers, other equipment and software associated with the different applications that comprise the card platform;

- Program staff to personalize and issue cards, manage card inventory, and update employee accounts;

- Customer service staff to replace cards, maintain the card hot list, and provide other customer service;

- Registration Authority staff to perform identity proofing and registration services (if PKI or biometrics are included within the platform); and

- Certification Authority staff to issue, publish, revoke/suspend, and validate digital or attribute certificates (if PKI or biometrics are included within the platform).

The number of staff required will vary substantially, depending on such factors as the scope of the implementation, the approach to card issuance and management (i.e., centralized versus decentralized), and the degree of integration among the participating functions. Very small, simple card implementation projects may prefer to use an outsourced approach rather than make the substantial investment to build the required infrastructure and to amass the necessary staff to support in-house card management. Although larger agencies and/or agency-level implementations are more likely to have the available personnel resources to invest in an in-house operation, the added complexity of implementing cards in multiple locations may cause even some larger agencies to consider outsourcing at least some parts of their card operations.

72. *Does your agency have sufficient facilities available for housing and maintaining a card system database, and card access terminals?*

The availability of facilities will also have an impact on the decision to manage the card platform in-house or to use contracted services for card issuance and management, PKI, and/or biometrics. To manage the card platform in-house the following types of facilities will be required:

- Data center to house the central card management system host;

- Centralized facility to house card personalization and issuance equipment if cards are issued centrally;

- Space in multiple local facilities to house card personalization and card issuance stations if cards are issued locally;

- Space for card readers/writers, computers, and printers at each program site using the card platform for applications;

- Facility for performing identity proofing or capturing “live” biometric scans if digital signatures and/or biometrics are included in the card platform; and

- Facility for housing key generation workstations and certificate issuing workstations if a digital certificate is included on the card platform.

The amount of space required will vary substantially, depending on such factors as the scope of the implementation, the approach to card issuance and management (i.e., centralized versus decentralized), and the degree of integration among the participating functions. Once again, the smaller card implementation projects may prefer to use an outsourced approach rather than make the substantial investment to build the required facilities or find the additional space to support in-house card management. Larger agencies and/or agency-level implementations are more likely to have the available space resources to invest in an in-house operation. However, the added complexity of a large scale implementation, particularly one including many locations or locations overseas, may make even those agencies with substantial resources consider an outsourced approach.

73. Does your agency have access to a high security-computing environment?

Although the availability of a high security computing environment will have little impact on whether or not card management is outsourced or performed in-house, it will have a significant impact on the decision to use contracted services for PKI and/or biometrics. The sensitive nature of the services performed by the Certificate Authority or the Attribute Authority demands a high security-computing environment. Because of the potential liability associated with performing Certificate/Attribute Authority services in-house, it would be critical to outsource these services if a trusted workstation was not available to issue digital/attribute certificates and load them onto the employees’ cards.

Applications

The applications to be included as part of the card platform will dictate both the technologies and the chip size needed for an agency's Smart Identification Card, as well as the peripheral equipment needed to support the card systems. The selected applications, in turn, will depend upon a number of factors including the business line of the agency, the administrative needs of the agency, the existing technical environment and legacy systems, the resources available to the card project, and the needs of various program offices. Agencies should be able to select applications based upon their unique needs. While the following sections describe some standard administrative applications that are likely to be shared across multiple agencies, once the card platform is in place, it is likely that mission specific applications will be added to the agency customized platform. Therefore, agencies should consider these potential applications in sizing their system requirements. The common administrative applications include:

- Property Management;
- Rostering;
- Financial Management including Electronic Purse and Credit/Debit;
- Medical Information; and
- Training Information.

Property Management

A labor intensive and time consuming administrative area that many agencies must deal with is property management. A substantial amount of time is currently expended on obtaining and presenting property passes when an employee is to take a laptop computer or other agency assets out of the building. Assets that must be managed include:

- Computer equipment;
- Telephones/telecommunication equipment;
- Credentials;
- Arms;
- Automobiles; and
- Other agency specific equipment.

Currently, the employee must obtain a paper property pass that specifies the characteristics of the equipment in his/her possession. Completing the paper property passes is often a time consuming task. Guards must verify the property passes each time the employee enters or exits the building. The passes are generally issued for short periods of time and must be frequently renewed, requiring substantial paperwork. When surveyed, agency personnel indicated that a substantial amount of time can be spent on issuing, updating, and checking property passes. Furthermore, employees may need to bring equipment in and out of guest agency buildings.

Questions 74 through 80 are designed to help your agency assess whether a property management application is needed for its card platform.

74. Do you currently issue any type of property pass? How many property passes per day do you issue? What is the process? Is it time-consuming? How many property passes per day do you verify?

The most critical issue in determining whether a property management application is needed in your agency is the volume of property passes being issued and the time used to issue and verify these passes. If few passes are issued, it probably is not cost effective to implement this application. On the other hand, if your agency's property pass issuance rate is relatively high, this application could save substantial staff time. Further, the property pass application, working in concert with an automated physical access control system, could reduce the guard coverage needed at non-public building access points.

75. *What is your agency's current property loss rate?*

The amount of time devoted to property pass issuance and validation is only part of the decision process. Your agency must also determine the effectiveness of your property pass process, by reviewing your agency's current property loss rate. If your issuance rate is high and your loss rate is relatively low, it may be worth investing in an automated system to reduce the cost of effective deterrence. On the other hand, if your agency's loss rate is low and your agency is currently using little or no property control, this application may be of little use for your agency.

76. *What type of property/equipment do you need to manage (i.e., computers, firearms, chemicals)? On a scale of 1 to 4, one being "low risk" and four being "high risk", what is the level of risk associated with a loss of property that your agency manages?*

___1 ___2 ___3 ___4

Another aspect of the determination process revolves around the magnitude of the risk of property lost. It your agency manages expensive or dangerous equipment, your need to protect the equipment is substantially greater than if your agency is handling less critical property. Those agencies with relatively inexpensive property and/or a low risk of loss should not consider this application.

77. *Do your employees often need to take valuable agency equipment (i.e., laptop computers) from the building?*

Agencies whose employees often need to take agency property from the building are more likely to find the property management application cost effective.

78. *Is equipment shared or transferred between offices or with another agency?*

Agencies whose employees often need to share or transfer agency property between offices or with another agency are more likely to find the property management application cost effective, particularly in an interoperable environment. The ability to easily transport equipment across multiple agencies would provide substantial convenience to agencies whose employees work frequently in each other's facilities.

79. *Who is responsible for property management in your agency? Is it a centralized or distributed responsibility?*

Agencies that have centralized asset management and physical access control systems could load property passes along with access control privileges to the card as part of the personalization process prior to card distribution. This approach would make the issuance of property passes relatively simple. Distributed property management would require relatively more time to load property passes, thus making the property management application less cost effective. The greater the level of integration between the property management, badging, facility access control, and logical access control application owners, the easier the implementation of a multi-application card platform and the greater cost reductions could be achieved.

80. *Is your current asset management system integrated with your card issuance and/or physical access control system(s)?*

Agencies that have integrated asset management and card issuance/physical access control systems could most easily load property passes along with access control privileges to the card as part of the personalization process prior to card distribution. This approach would make the issuance of property passes relatively simple. The greater the level of integration between the property management, badging, facility access control, and logical access control application owners, the easier the implementation of a multi-application card platform and the greater cost reductions that could be achieved. Agencies who use RF property tags in their equipment and portals at entrances and exits could substantially increase the throughput at their access points, as well as reduce the necessary guard force.

Please complete the following table with your answers from Questions 74 through 80. In the row marked "Identification of each building", please provide the official name of the agency building or premises. Provide the required information for each of the buildings identified.

BUILDING PROPERTY PASS EVALUATION				
Number of buildings	4			
Identification of each building	Building A	Building B	Building C	Building D
Number of entrances to each building	3	2	1	2
Number of people entering/exiting premises daily	300	200	500	300
Number of people entering/exiting each access point (entrances) daily (Row 4 ÷ 3)	100	100	500	150
Number of property passes issued per day	10	20		
Time to issue property pass	15 minutes	10 minutes		
Time to issue passes per day (Row 5 X 6)	150 minutes	200 minutes		
Number of property passes verified per day/per access point	25			
Time per person to validate property pass	2 minutes			
Time to verify passes per day (Row 8 X 9)	50 minutes			
Current Property Loss Rate/Risk Level				
Frequency Of Property Transfer across Buildings/Agencies				
Degree of Asset Management/Physical Access Control Integration				

Rostering

The Rostering application allows data residing on the Smart Identification Card to be retrieved, date/time stamped, and transferred to a database that is then used to generate a variety of specialized reports. The Rostering application can be used not only to retrieve and format data, but also to provide positive proof of attendance. For example, it could be used in the following ways:

- **Meeting Attendance.** Meeting participants are required to insert their cards into a reader as they enter a meeting. Demographic data, such as name, office address, agency, office telephone number, office fax number, and email address are retrieved from the card and uploaded to a database. From this database an attendance listing can be generated.

- **Food Services.** Some agencies provide subsidized food facilities for their employees. Employees are required to insert their card into the reader upon entry into the dining facility. The card is read, providing positive proof of attendance at a meal session. The attendant can view the employee’s meal plan privileges, determining from this information whether the employee has a meal plan and has already eaten on the plan, or whether money for the meal should be collected.

- **Emergency Evacuation.** In fire drills or emergency evacuations, employees are required to insert their cards in readers as they exit a building. Demographic data are retrieved from the card and date/time stamped. Reports can be generated to list which employees have been evacuated from the building. From these reports, missing employees can be identified.

Questions 81 through 84 are designed to help your agency assess whether a rostering application could be useful on its card platform.

81. *Do employees in your agency frequently conduct large meetings at which there is a need to track attendance?*

82. *Do you need to keep track of who has entered/exited a certain area of a building or ship?*

83. *Do you need to track attendance for education/training or for any other purpose?*

84. *Does your agency have in-house food services?*

The rostering application is a generic administrative application that could be adapted for different agencies to address specific attendance tracking needs. Agencies should consider the various ways in which this administrative application could be customized to meet specific agency needs when they are planning their card platform.

Electronic Purse

A chip card with an electronic purse can be loaded with “electronic” value that can be decremented as purchases are made. The electronic purse application includes the capability to revalue the electronic purse, track account balances, and settle electronic purse transactions. The electronic purse functionality could be used by agencies to support a number of different applications. For example, agencies could use the electronic purse to make low value payments to their employees for the following reasons:

- Payments to replace imprest funds;
- Payments for local travel reimbursements; and
- Payments for transportation subsidies.

Electronic purses may include PIN based and non-PIN transactions. Further, depending on the uses needed by an agency for the electronic purse, this application could be implemented using either a contact or contactless interface. The differences in security and transaction processing requirements may result in the need to support multiple purses on a single chip. Potential applications for agencies to explore for its employees include:

- **Automated Fare Collection.** This application, used by agencies to provide public transportation subsidies to its employees, is likely to require a contactless interface and non-PIN based transaction processing.

- **Vending Machine/Cafeteria Purchases.** Agencies could install vending machines or use the card in employee-subsidized cafeterias for low value transactions that use a contact interface and are non-PIN based.

- **Retail Purchases.** Employees should be able to make commercial purchases, if the electronic purse is to be used by agencies for travel advances or in place of imprest funds. When used for commercial purchases, the e-purse is likely to require a contact interface and PIN based transactions.

- **Parking Payments.** Agencies may choose to allow employees to use their employee cards for making parking payments. This application may be contact or contactless and use a non-PIN based transaction.

The agencies that opt to implement an electronic purse capability on the card must comply with any relevant escheat laws, as well as Regulation E requirements regarding stored value purses.

Questions 85 through 88 are designed to help your agency assess whether an electronic purse application could be used on its card platform.

85. Does your agency have vending machines or a cafeteria?

Agencies that have vending machines or a cafeteria for their employees can save money in cash handling expenses by moving to electronic purse applications. Additionally, the electronic purse can provide convenience to employees making small purchases in the agency building.

86. Are your agency facilities localized or in a campus setting?

Agencies whose buildings are in close proximity or in a campus setting can conveniently and relatively inexpensively set up a closed electronic purse that can be used within the buildings of the campus for small purchases.

87. Do your employees often need cash advances (i.e., travel advances, petty cash) to conduct agency business?

Agencies that have a need to provide employees with small amounts of cash to spend on business purposes could save administrative costs by moving to electronic payment systems. Electronic value can be loaded to a card, which could then be used to pay for items that used to require cash subsidies. The far less labor-intensive electronic transfer of value could be used to replace the imprest funds operations.

88. Does your agency provide transportation subsidies to its employees?

Chip cards are particularly well suited to providing payments for transportation. An electronic purse could be used to purchase transportation subsidies that could be decremented as the public transportation rides were used up. Transportation authorities may adopt either contact or contactless interfaces. As more and more public transit systems adopt electronic payment mechanisms, agencies may find that the employee card platform is a convenient and viable mechanism for cost effectively providing public transportation subsidies for employees.

The electronic purse application is a generic administrative application that could be adapted by different agencies for various uses in conducting agency business. Any type of purchase in which low value electronic payments could be used is a candidate for the e-purse application. Agencies could use the e-purse as a way of replacing cash, thereby simplifying various types of employee reimbursements and/or cash advances. Agencies should consider the various ways in which this administrative application could be customized to meet their specific agency needs when they are planning their card platform.

Debit/Credit Applications

Some agencies may add to the Smart Identification Card their existing government credit card applications including the following card programs:

- Purchase;
- Travel; and
- Fleet.

Card platforms including these credit/debit applications would need magnetic stripe technology. The magnetic stripe would be used to access information through an on-line system for these commercial credit applications. Optionally, a commercial debit capability could potentially be added to the card. Both the functionality and data set of the existing magnetic stripe-based capability could be added to the Smart Identification Card.

Those agencies considering commercial financial applications must be concerned with interoperability for financial applications in an open environment. To promote an open system environment and achieve such interoperability, the Smart Identification Card should comply with the EMV ’96: Integrated Circuit Chip (ICC) Specifications for Payment Systems (Version 3.0).

Questions 89 through 92 are designed to help your agency assess whether credit or debit applications would be desirable on its card platform.

89. Do your employees frequently make high volume, low-dollar purchases?

Agencies whose employees frequently make low dollar purchases would clearly benefit from a credit card application. The purchase cards allow low dollar purchases to be made with a substantial reduction of paper work in the procurement and invoicing processes.

90. Do you have employees that frequently travel for business purposes?

Agencies whose employees frequently travel for business purposes would clearly benefit from a credit card application for travel. The travel card allows business expenses to be charged so as to reduce the paper work associated with travel advances and employee reimbursement for travel expenses. Additionally, the chip on the Smart Identification Card could be used to maintain an employee travel profile, electronic ticketing, and other travel related services.

91. Does your agency operate and/or maintain a fleet of vehicles?

Agencies whose employees frequently use agency vehicles for business purposes would clearly benefit from a credit card application for fleet services. The fleet card allows gasoline and vehicle maintenance expenses to be charged so as to reduce the paper work associated with travel advances and employee reimbursement for vehicle operation expenses.

92. Does your agency have or plan to implement an electronic procurement system?

Agencies planning electronic procurement systems will need a viable and secure mechanism for electronic payments to be used with their procurement systems. Either credit/debit magnetic stripe or electronic purse chip-based applications could be used for payments across the Internet. Even those agencies considering electronic commerce applications in the long-term should ensure they have the capability to activate credit, debit, or electronic purse applications when selecting their card platforms so that they are ready for electronic payments when they migrate to electronic purchasing.

A key issue for agencies to focus on with financial applications is whether or not they should co-reside on the same card platform. While some agencies may to combine both security and financial applications on the Smart Identification Card, other agencies may be opposed to placing financial and security applications on the same card platform. The combination of financial and security applications raises potential security risks and interoperability issues that must be addressed in such a multi-application environment. For those agencies reluctant to mix security and financial applications on the same card, GSA has existing contractual relationships with financial institutions for credit and debit applications (as well as for provision of smart cards) through the GSA Smart Pay Contract. GSA recommends that agencies consider the use of that vehicle for cards requiring commercial financial applications, if they do not combine financial and security applications.

Medical Information

The Medical application allows basic medical and insurance data to be stored on the card and read, when appropriate, by providers. Additionally, the Medical application can be used to populate claim forms. Agencies could use this application in the following ways:

- **Emergency Medical Information.** In emergency situations, basic medical and emergency contact information can be obtained from the card. Such information may include blood type, allergies, next of kin, next of kin phone number, and special medical needs.

- **Insurance Status.** The card provides information about the cardholder’s insurance coverage including both primary and secondary health insurers. This data may be used at public or private providers, as well as during the claims submission process.

- **Claims Submission.** Demographic and insurance data on the card can be retrieved to populate electronic claims submission forms.

Questions 93 through 96 are designed to help your agency assess whether medical applications would be practical on its card platform.

93. Does your agency have a need for quick access to employee vital medical information?

The employees of some agencies may have a greater risk of exposure to hazardous conditions than those of other agencies. For example, high risk employees of military, intelligence, and international agencies may have a more pressing need for an emergency medical application on the card than employees of civilian or commercial agencies. The nature of the work force and specific job responsibilities will dictate the practicality of a medical application for agencies. Agencies whose work force is particularly mobile, such as military or international aid organizations, are most likely to benefit from a card-based medical record.

94. Do your employees need quick access to insurance benefit information?

Many agencies, both civilian and military, could benefit from quick access to insurance benefit information. In addition to providing a convenience for employees, such records could help reduce claims processing costs.

For example, the card could provide information on both primary and secondary insurers, as well as deductibles and co-payments. This information would ensure that claims are submitted correctly and for the right amount, thereby helping to speed up claims processing. Demographic data residing on the card could also be used to populate electronic claims forms, reducing the claims cycle time.

95. Do your employees need quick access to immunization records?

Those agencies with employees who may have a risk of exposure to environments in which infectious diseases are prevalent may have a particular interest in tracking immunizations. For example, Department of State, various international aid agencies, and the military may need a portable immunization record. Once again, the nature of the work force and specific job responsibilities will dictate the practicality of an immunization application for the card platform. Agencies whose work force is likely to travel to undeveloped countries, such as military or international aid organizations, are most likely to benefit from a card-based immunization record.

96. Do your employees often travel for business throughout the U.S. and overseas?

Those agencies with employees who travel a good deal for business, both in the United States and abroad, may have a particular interest in the various medical applications. For example, employees of the Department of State, Department of Commerce, agencies promoting international trade and business, and the military and/or intelligence agencies may need to carry portable medical and insurance information on their employee identification cards.

Training/Certification Functionality

The Training/Certification application allows data about training experiences and job-specific certifications to be entered on the card. Managers can read the card and obtain a view of the employee's training history and licenses/certifications. This application can also be used to track when employee certifications expire and to document attendance at required training.

Questions 97 through 99 are designed to help your agency assess whether a training and/or certifications applications would be useful on its card platform.

97. Does your agency need to track employee training?

Some agencies have mandatory requirements for certain types of training that may be related to safety, security, or particular job categories. For example, NASA requires that all its employees have annual safety training. The Food and Drug Administration requires that certain classifications of employees be trained in handling hazardous materials. A generic training application can be adapted to meet individual agency needs.

98. Does your agency need to track employee certifications and/or licenses?

Similarly, agencies need to track issuances and expirations of licenses and certifications. Numerous law enforcement agencies, for example, require licenses for weapons and/or tracking of credentials. Particular job categories may also require certain certifications such as registered nurses or specially trained laboratory technicians. These certifications can be carried on the card, along with either a digital certificate or a biometric to ensure that the person carrying the card is in fact the authorized cardholder.

99. Does your agency need to have quick access to employee skills?

Agencies with mobile workers may need an application that allows managers to quickly view assigned skills or attended classes to assist with assignments. Such an application would be useful in agencies that assist with disaster assistance or other projects that require quick assignment and reassignment of mobile workers.

Exchange of Clearances

A substantial amount of time is expended exchanging clearance information between agencies for employees who must attend meetings or visit other agency facilities. While the intelligence community and military agencies are most likely to pass clearance information among themselves, a small percentage of employees from the civilian agencies must also occasionally exchange clearance information when visiting other facilities. Members of the intelligence and military communities who routinely pass clearance information among themselves are already linked through an on-line system that allows clearance information to be distributed through networked servers. Such a solution works very well in this closed environment in which agencies have established both interagency agreements and the technical capabilities to exchange clearance information with known partners. However, when clearance information needs to be exchanged in a more open and less routine environment, the transfer of such information becomes more problematic. In this scenario, an employee may be from an agency that does not have pre-established agreements or technology enabled links with the receiving agency. Because clearance transactions need not be exchanged routinely, the cost of creating on-line links between a multitude of agencies would be prohibitive. Agencies whose employees must provide clearance information to partner agencies on a regular basis may have an interest in using the Smart Identification Card as a portable carrier of clearance information. This approach may prove to be the least expensive option to allow such information to be exchanged securely.

In such an application, the designated Security Officer of the home agency could load, date, and digitally sign clearance information on the employee's card. At the receiving agency, the guard could verify the Security Officer's digital signature, read the clearance information, and match the information with a visitor request generated by the receiving agency employee. If all of these validations were successful, the visiting employee would be granted access. At the agency's option, the data on the chip could either be used to create a temporary visitor's card or be uploaded to the physical access control database so that the visiting employee's card could be activated to work in the receiving agency's system. This same functionality could be adapted for use of non-employees (i.e., contractors) who must visit government facilities on a routine basis.

Questions 100 through 101 are designed to help your agency assess whether a clearance exchange application would be useful on its card platform.

100. *Does your agency have many employees or contractors with top secret or higher clearances?*

Agencies with a high percentage of employees and/or contractors with security clearances are likely to have instances in which its employees must exchange clearances with another agency or in which employees from another agency must present clearances to the agency. For such agencies, a convenient and portable means to securely exchange clearances with other agencies could save substantial time. Thus, such agencies could be interested in a generic application for this purpose.

101. Does your agency have many employees who must attend top-secret meetings or obtain access to top-secret documents and/or systems in other agencies?

Similarly, agencies with a high percentage of employees and/or contractors who must attend meetings or share secure information with a variety of other agencies may also find it convenient to have a portable means to securely exchange clearances with other agencies. Again, such agencies are likely to be interested in a generic application for this purpose.

Sample Models

The intent of this section is to assist agencies in making the key decisions that will inform their approach to implementing a card platform. It presents an analysis of several generic agency models that are meant to guide agencies in developing their own customized profiles. Based on the salient characteristics attributed to these "sample" agency types, a case study demonstrates the logic used to make specific platform choices. ***The agency models are not meant to reflect actual conditions in any particular agency; rather, these models are a composite of the characteristics of various different agencies, selected to illustrate the analysis process that an agency should go through to define its card platform.*** Each scenario demonstrates the considerations weighed to translate individual agency needs into a particular approach to card management and to formulate the ultimate composition of the card platform.

This section is not meant to encourage agencies to retrofit their requirements into one of the models provided. Rather, these models are intended as examples for the agencies to follow in defining their own unique profiles. Agencies may find it helpful to select one generic model that is closest to their individual circumstances and then determine the ways in which they are similar to and different from the selected model. While the agency may emulate certain selections from their "model" agency, it is likely that the unique situation of each agency will dictate a number of deviations from the models presented.

The table on the next page summarizes the characteristics of the sample models. The following sections present for each "sample" model the salient characteristics and an analysis describing the selected card platform. For these generic scenarios, certain assumptions are made that in turn impact the selection of the card platform. These assumptions are presented in the description of the agency characteristics. ***It should be understood that the descriptions of the agencies herein presented are not meant to reflect the "real life" situation in any specific existing agency, but rather to depict fictitious agencies created to help the reader understand the dynamics of the decision making process.*** The following generic models are merely used to illustrate some of the judgments that must be made in selecting a card platform:

Category	Small Agency Model	Campus/ Metro Area Model	Civilian Agency Model	Commercial Agency Model	International Agency Model	Intelligence Agency Model
SECURITY						
Physical	Perimeter Control	Perimeter Control	Perimeter control and some internal control	Perimeter control and some internal control	Significant perimeter control and some internal control	Significant perimeter controls and internal controls/ protection of high security documents
Logical	Password	Secure access to DB	Secure access to DB	Secure access to DB	Secure access to DB.	Secure access to DB.
DOD Assurance Level	2	3	4	4	4	5
Communications	N/A	N/A	Authenticated messaging.	Authenticated messaging	Authenticated and encrypted messaging.	Authenticated and encrypted messaging.
INTEROPERABILITY						
Physical & Logical	Stand-Alone	Interoperable within agency at multiple locations.	Interoperable with most agencies within the United States.	Interoperable within agency at multiple locations nationwide and with several other agencies.	Interoperable with several specified agencies in the U.S and overseas.	Interoperable across specified agencies in the U.S. and overseas.
SIZE/ GEOGRAPHIC DISTRIBUTION						
Size	Small	Medium	Large	Large	Large	Large
Geographic Distribution	One location	Multiple locations within a limited geographic area.	Multiple locations in multiple areas.	Multiple locations in the U.S.	Multiple agencies in multiple locations in the U.S. and overseas.	Multiple locations in the U.S. and overseas.
CARD MANAGEMENT						
In-house/ Outsourced	In-house	In-house	Outsourced	Outsourced	Outsourced	In-house
Enrollment	Local	Local	Local & Centralized	Local	Local	Local
Personalization	Local	Local	Local & Centralized	Centralized	Centralized	Centralized
Distribution	Over-the-Counter	Over-the-Counter	Over-the-Counter	Mail Issuance	Over-the-Counter	Over-the-Counter
Database Integration	Separate	Separate	Integrated	Integrated	Integrated	Integrated
PKI STRATEGY						
In-house/ Outsourced	N/A	Outsourced	Outsourced	Outsourced	Outsourced	In-house
Enrollment	N/A	Centralized	Centralized	Centralized	Centralized	Centralized
Open/ Closed	N/A	Closed	Open	Open	Open	Open
BIOMETRIC STRATEGY						
In-house/ Outsourced	N/A	N/A	Outsourced	Outsourced	Outsourced	In-house
Enrollment	N/A	N/A	Local	Local	Local	Local
Authentication	N/A	N/A	w/o Attribute Authority	w/o Attribute Authority	w/o Attribute Authority	w/ Attribute Authority
APPLICATIONS						
Logical	Password on Card	PKI	PKI or Biometric	PKI	PKI	PKI/Biometric
Physical	Number on Card	Prox/ Number on Card	PKI or Biometric	PKI or Biometric	Biometric	Biometric with AA
Other	N/A	Property Management Closed Purse	Property Management, Financial, Rostering, Training	Financial,/Open Purse, Encryption, Medical	Clearance, Property Management, E-forms, Encryption, Medical, Rostering, Financial/E-	Clearance, Property Management, E-forms, Encryption, Medical, Rostering

Category	Small Agency Model	Campus/ Metro Area Model	Civilian Agency Model	Commercial Agency Model	International Agency Model	Intelligence Agency Model
					Purse	
TECHNOLOGY						
Card	Contact; 2K	Contact; RF; 8K with co-processor	Combi-card; 16K with co-processor, Bar Code, Mag Stripe	Contact; 16K with co-processor, Mag Stripe	Contact card; 16K to 32K with co-processor	Combi-card; 16K to 64K with co-processor
Hardware						
Contact Readers	T	T	T	T	T	T
Contactless Readers			T	(Future)		T
Proximity Readers		T				
Biometric Readers			T	T	T	T
Card Issuance Workstations	T	T	T	T		T
Host Computer	T	T				T

- **Small Agency Model.** This model is intended to characterize either small agencies or implementations that are limited to a bureau, division, or office within a larger agency that have a single building location.
- **Campus/Metropolitan Area Model.** This model is intended to characterize a small to medium sized agency, bureau, division, office or other organizational entity with multiple facilities within close geographic proximity. These multiple facilities may be within a campus environment or a single metropolitan area.
- **Civilian Agency Model.** This model is intended to characterize a medium to large agency that includes multiple locations in diverse geographic areas. This model has relatively low security requirements, but high interoperability requirements as its employees may do business and exchange information with a large number of other agencies.
- **Commercial Agency Model.** This model is intended to characterize a larger agency with multiple locations in diverse geographic areas and a somewhat higher level of security and interoperability requirements, as its employees may do business and exchange information with other civilian agencies as well as financial institutions and external commercial entities.
- **International Agency Model.** This model is intended to characterize a larger agency with geographic dispersion around the United States and abroad. It is likely to have certain partner agencies with which it must communicate on a regular basis.
- **Intelligence Agency Model.** This model is intended to characterize a large, high security agency with operations all over the world.

Small Agency Model

AGENCY PROFILE CHARACTERISTICS

The Small Agency Model (referred to hereafter as Agency A) requires a card platform appropriate to a small agency, a small division or bureau of a larger agency, or a particular facility within a larger organizational entity. This model has the lowest level security needs (DOD Assurance Level 2) of all the models described. Employee cards are to be used in a single geographic location. This sample agency has no existing physical access control system, but rather relies on guard services to visually inspect the card at a central entrance. It currently uses only passcodes to protect its computer systems.

The physical access control and logical access control functions are totally un-integrated. This agency has a badging office that currently issues employee identification cards. There is no separate physical access control system. However, there is a system under the auspices of the information technology office that manages user passcodes. Users are issued passcodes through the mail. This agency has limited resources to devote to procuring the card platform and has few plans to move into electronic commerce or electronic service delivery in the near future.

CARD PLATFORM ANALYSIS:

Security

The Small Agency Model has limited security requirements. Because it has a relatively low DOD assurance level, its security needs are the most limited of all example models. While this agency is interested in perimeter control, it does not have any specialized areas that need more extensive physical access control. It does not have an existing physical access control system but rather uses a single guard station based on visual inspection of the card. This agency has few locations and each location currently has a separate badging office. New employees go directly to the badging office for their plastic identification cards that are produced on location at the badging office.

Currently this agency uses passcodes for all of its computer systems. The Information Technology Office issues passcodes to employees for each separate system for which an employee needs access. Very few agency employees need remote access to its computer systems nor does the public need access to information in the agency's computer systems. The agency has worked with passwords in the past and is satisfied that passcodes provide adequate security for its needs. However, Agency A's employees often lose or forget their various passcodes and that is a burden on the limited IT staff. Agency A would like a mechanism to assist with the management of multiple passcodes for its employees.

Interoperability

Agency A has limited need for interoperability with other divisions within its larger agency and with other government agencies, as its work is self-contained. Agency A is using its card for a single location, and few of its employees need to go to other locations within the agency or to other external agencies. Because the agency's mission requires little interaction with other agencies and has a low security profile, its physical and logical access control systems can be stand-alone. Agency A is not concerned about communications systems supporting transactions across internal divisions and/or other agencies. Further, this agency has little need to put in place interoperability agreements with partner agencies.

Card Management

Because of its small size and lack of geographic dispersion, Agency A thinks it would be practical to maintain its past practice of locally issuing employee identification cards. It has experience with local enrollment and card personalization and wants to continue the over-the-counter card distribution to which its employees have become accustomed. Agency A has limited resources to spend for card issuance services and already has in place sufficient staff and an organizational structure to distribute cards. Consequently, Agency A opts for in-house card management. However, since it has a separate badging system, no physical access control system, and a legacy logical access control system, it decides it will not integrate its card management and access control databases at this point in time. In the future, as the legacy systems are replaced and more applications are added to the card platform, Agency A will re-consider an integrated database for card management and access control applications.

PKI/Biometric Strategy

Agency A has considered both public key and biometrics to enhance its security. When it considered these options in detail, however, Agency A decided that it does not currently need secure remote access, high value Internet-based transactions, electronic forms, or controlled access to specialized areas of the building. Since it is not yet ready to implement electronic commerce and its mission includes limited interaction with the public, Agency A has little need to authenticate its employees to outside agencies and/or to the public, nor does it need to secure electronic transactions across multiple agencies. Consequently, because Agency A's resources to fund the card platform are limited and its security needs are relatively low, it has determined that neither PKI nor biometrics are worth the expense in the near future.

Applications

While Agency A is aware that there are some applications that would be useful in the future, it currently is only to integrate its employee identification card with physical and logical access control capabilities. Agency A prefers to move slowly, piloting a limited multi-application card platform until all the pitfalls have been identified and solutions worked out. In the future, Agency A believes there are several applications that could be considered, but not until the agency feels comfortable with its card management role.

Technology

Based on the key decisions described above, Agency A has selected a relatively simple card platform. Because Agency A is not supporting many applications, nor is it implementing PKI or biometrics, it will need less memory than other implementations. It is considering a contact chip based physical access control system that will require the installation of only a few readers. The chip will carry only an identification number to use to query physical access privileges housed in a local controller, as well as multiple system access levels and passcodes for each system to which the cardholder has access authority for logical access control. Since the card will carry only limited data and several identification numbers, it will require limited memory. Since a 2K chip will likely be sufficient, Agency A can purchase a less expensive card. In the future, Agency A may choose to load additional data and/or applications on the chip.

Agency A has impacted the hardware and software required for its card platform by choosing to perform card management in-house and deciding against biometrics or PKI. By deciding to use contact chip for both physical and logical access control, Agency A's platform was simplified. Agency A can purchase relatively inexpensive contact card readers for use on its central entry as well as on workstations to be able to read the chip when individuals use the card to provide more secure and convenient access control privileges. Additionally, Agency A will need card issuance workstations and card printers to be used to personalize the cards and to print the face of the card at the local card issuance office. To maintain the card management database, as well as a new physical access control system, Agency A will need a host computer. Alternatively, Agency A may investigate the possibility of maintaining physical access control privileges in its card management system. If Agency A determines it will provide in-house customer service, the Agency may also require Automated Response Unit hardware and software to support the customer service function.

Campus/ Metro Area Model

AGENCY PROFILE CHARACTERISTICS:

The Campus/Metro Area Agency Model (hereafter referred to as Agency B) requires a card platform appropriate to a medium sized agency, a division or bureau of a larger agency, or a campus housing multiple facilities within a larger organizational entity. The National Institute of Health or the Food and Drug Administration centers are examples of this type of agency profile. This model has the next higher level of security needs (DOD Assurance Level 3), but it is still relatively low security. Employee cards are to be used in multiple locations within a limited geographic area such as a single geographic campus location with multiple buildings or across multiple buildings within a limited metropolitan area. This sample agency has an existing proximity based physical access control system that provides perimeter control and parking only. Within the campus complex, there is currently a single separate badging office. New employees go directly to the badging office for their plastic identification cards that are produced on location at the badging office and then go to the facilities office to get their separate proximity card to use for building and parking access.

Although Agency B currently uses only passcodes to protect its computer systems, it is concerned that improved authentication is needed to secure access to its various databases. Both the physical access control and logical access control systems must be interoperable across the multiple buildings housed at the single geographic location. However, organizationally, these two functions remain un-integrated. This agency has a badging office that currently issues employee identification cards for all of the buildings on the campus or within the metropolitan area. While the card provides visual authentication for agency facilities outside the campus environment, the physical access control system is different from, and not necessarily compatible with, systems at agency offices outside the campus environment. There is a separate physical access control system database, managed by the facilities organization, which maintains an employee's physical access control privileges and issues the proximity card.

Similarly, there is a system under the auspices of the Information Technology Office that manages user passcodes. Users are issued passcodes through the mail. Although Agency B has limited resources to devote to procuring the card platform, it understands the importance of enhancing its security, especially for employees seeking remote access to its systems. While Agency B is not currently conducting electronic commerce, it understands the importance of electronic transactions to its agency's mission and plans to move into electronic commerce and/or electronic service delivery within the foreseeable future.

CARD PLATFORM ANALYSIS:

<u>Security</u>

The Campus/Metropolitan Area Model has more extensive security requirements than the Small Agency Model. Agency B is mainly interested in perimeter and parking control, but it does have some specialized areas that need more extensive physical access control. It currently has an existing physical access control system that requires backward compatibility with proximity technology. This agency has a single badging office to issue cards for multiple buildings, but because the buildings are in close geographic proximity, it remains convenient for employees to go to the one badging office. New employees can conveniently access the badging office for their plastic identification cards that are produced right on location. However, they must go to a separate office to receive their proximity card to be used for building and parking lot access.

Currently this agency uses passcodes for all of its computer systems. The Information Technology Office issues passcodes to employees for each separate system for which an employee needs access. Employees are increasingly in need of remote access to Agency B's computer systems and several of the buildings on the campus are linked by local area networks. Although no public access program currently exists, the agency envisions the need for both businesses and the public to be able to access information in the agency's computer systems. Although the agency has worked with passwords in the past, it is increasing concerned that passcodes do not provide adequate security for its needs, especially as they evolve toward greater use of the Internet for both internal and external applications.

Interoperability

Agency B has a greater need than Agency A for interoperability, particularly with other divisions within its larger agency. Because Agency B's mission requires greater interaction with other internal organizations and has a higher security profile, its physical and logical access control systems should be compatible such that they can be made capable of interoperating across the larger agency. This need for greater interoperability makes Agency B more concerned about communications systems supporting transactions across internal divisions. However, because Agency B is most concerned about interoperability within the larger organization, rather than across multiple agencies, it still has relatively little need to put in place interoperability agreements with partner agencies.

Card Management

The physical proximity of the existing card issuance office and the convenience it has offered employees in the past has had on impact on Agency B's decision about card issuance. The organizational structure is already in place for local card personalization and distribution, as are the procedures and the staff. The size and geographic distribution of the implementation remain manageable, so that Agency B believes it to be more efficient to perform card management in-house.

PKI/Biometric Strategy

The increased need for security, both now and in the foreseeable future, suggest that some sort of PKI strategy could be effective for this type of agency. By providing PKI, Agency B can begin to migrate away from passcodes to more secure digital certificates for logical access control. Further, a digital certificate system, once implemented could be easily adapted to use for both remote access for internal employees, as well as for authentication of transactions when the agency moves to electronic commerce and service delivery. While PKI may be practical for Agency B, it is unlikely that both PKI and a biometric would be necessary for an agency with relatively low-level security requirements. Furthermore, an agency with this lower level Assurance Level is not likely to have the trusted computing environment needed to maintain the PKI repository and accompanying infrastructure. Therefore, it would be most practical for Agency B to procure Certificate Authority (CA) services through outsourcing. Registration for a digital certificate could easily be handled through the central badging office, which could forward the request for the certificate to a centralized CA that would then download certificates to the badging office to be loaded onto cards prior to card issuance. Since the PKI initially would be used for logical access control and employee identity authentication, a closed PKI (one in which there is only one CA and no cross-certification required) could most easily be put in place.

Applications

In a campus environment, several additional applications may be useful to Agency B. For example, in this environment in which employees may move freely from one building to the next, it is likely that employees will need to transport computers and other equipment from building to building. Therefore, a property pass application would be highly desirable for this platform. Additionally, a campus environment lends itself to a closed electronic purse that could be used for vending machines and cafeterias in various buildings across a complex. By implementing a closed purse rather than an open, commercial purse, Agency B avoids some of the interoperability and liability issues associated with a commercial electronic purse.

Technology

Based on the key decisions described above, Agency B needs a somewhat more complex card platform than Agency A. Because Agency B is supporting several applications, including PKI, it will need more memory (most likely at least 8K) and a co-processor to provide cryptographic functionality. To ensure backward compatibility with its proximity-based physical access control system, Agency B will require a multi-technology card that combines a chip embedded within a proximity card. The proximity capability will be used for physical access control, while the chip will be used to carry demographic data, as well as the digital certificate to be used to verify the cardholder's identity and to provide logical access control. The chip will also be used for the property pass and the electronic purse applications. In the future, Agency B may choose to load additional data and/or applications on the chip's remaining space.

Agency B has impacted the hardware and software required for its card platform by choosing to perform card management in-house and outsourcing PKI. By deciding to retain the legacy proximity physical access control system and acquiring cards with proximity capability, Agency B avoided having to replace the physical access control card readers throughout its facility. However, it will have to purchase inexpensive card readers for use on workstations to be able to read the chip when individuals use the card to provide more secure and convenient access control privileges. Additionally, Agency B will need card issuance workstations and card printers to be used to personalize the cards and to print the face of the card at the local card issuance office.

To accommodate the PKI capability, Agency B will have to acquire a secure workstation to generate digital certificate requests, as well as secure telecommunications to transmit the request for a digital certificate to the Certificate Authority and to receive the signed digital certificate and load it on the card. Additionally, Agency B will need a host computer to maintain the card management database. If Agency B determines it will provide in-house customer service, the Agency may also require Automated Response Unit hardware and software to support the customer service function. However, Agency B may choose to outsource its customer service in addition to its CA functionality.

Civilian Agency Model

AGENCY PROFILE CHARACTERISTICS

The Civilian Agency Model (hereafter referred to as Agency C) requires a card platform appropriate to a relatively large, geographically dispersed agency, or a large division or bureau of a larger organizational entity. This model is generally used to characterize a diverse, large agency that offers multi-dimensional services from offices around the country, but whose mission is geared in some way to assisting the civilian public, businesses, or other governmental agencies. An example of this type of agency is the General Services Administration or the Department of Interior. This model has the next higher level of security needs (DOD Assurance Level 4), but is not yet a high security agency. Because Agency C has diverse installations across multiple locations, the security needs of its various facilities may vary substantially from one office to another. Some of the agency's offices may actually be located in commercial buildings or in malls, store fronts, or other non-governmental facilities. Employee cards may need to be used in multiple locations across widely dispersed and variant geographic areas. This sample agency needs both perimeter control and some internal security for access to special areas within certain buildings. Employees from Agency C may need access to a variety of buildings with many incompatible legacy physical access control systems.

Agency C has a vast number of systems that are likely to use various different access control devices. While many of the systems currently use only passcodes, other systems may be experimenting with more sophisticated security devices. At this security level, Agency C needs both secure access to its databases, as well as authenticated messaging across systems. In this environment, it is likely that many employees will need secure remote access to the agency's systems. Agency C employees are likely to frequently visit a wide range of other agencies and to use information from other internal divisions and external agency systems. Interoperability with a wide range of other civilian agencies is very important to the conduct of Agency C's mission. Both the physical access control and logical access control systems must be interoperable across the multiple buildings housed in diverse locations.

Agency C has centralized badging for its larger locations (e.g., such as within a metropolitan area or within a region of field offices), but may have localized distribution for its geographically outlying offices. Generally, demographic information is maintained in large scale personnel systems and can be downloaded to different geographic card issuance locations. Agency C has a large number of separate physical access control databases for different locations, managed by the local facilities organization, which maintains employee's physical access control privileges and issues a separate card for the individual facility at which the employee works. Similarly, a number of different databases, maintained under the auspices of different information technology offices, manage user passcodes or other security mechanisms (e.g., tokens for remote access to certain high security systems). Currently, there is little communication among the disparate physical and logical access control systems and offices, but Agency C seeks to improve that situation.

Because of the vastness of the implementation, Agency C has significant resources to devote to procuring the card platform. Its highest priorities include enhancing security, both internally across divisions and externally with other agencies, as well as promoting interoperability across multiple agencies. Agency C is currently conducting electronic commerce pilots and is moving actively toward setting up electronic forms for use across disparate agency locations. It is working actively to streamline its business processes and to move as many administrative forms as possible to electronics. Actively seeking administrative applications for its card platform, Agency C is also beginning to experiment in using web-based applications for the public. Agency C understands the importance of electronic transactions to its agency's mission and it is moving aggressively into electronic commerce and/or electronic service delivery as quickly as possible.

CARD PLATFORM ANALYSIS:

Security

The Civilian Agency Model has more extensive security requirements than the Campus/Metro Area Model. In addition to being interested in perimeter and parking control, Agency C has increasing interest in enhancing security in some internal areas. Because of the diversity of buildings that it must address, achieving backward compatibility across a variety of legacy physical access control systems is a particularly thorny issue for Agency C. Agency C plans a variety of approaches to deal with the wide range of legacy physical access control systems. It will slowly upgrade its local legacy systems, swapping out readers across multiple buildings to upgrade to more standard contactless chip readers. In a small number of circumstances, Agency C will opt to use a second card for physical access control in commercially owned buildings. To achieve interoperability with external agencies, Agency C will pilot the PKI process described above in section 3.1.3 to determine if this is a viable approach to physical access control across a relatively open environment.

In the past Agency C has maintained multiple local badging offices, so therefore, has a tradition of local card issuance. While it would like to move to a more centralized scheme in its metropolitan areas, it continues to favor local distribution in its outlying areas. This agency is looking toward a centralized badging office to issue cards for multiple buildings in major metropolitan areas. Because the buildings are in reasonably close geographic proximity, it remains convenient for employees to go to the one badging office in the larger cities for enrollment and to receive their cards through these offices. However, in outlying field offices, where convenient access may be more difficult, a local office that obtains the account information from a centralized personnel system, but personalizes the cards locally may be needed.

While currently this agency uses passcodes for all of its computer systems, keeping track of multiple user IDs is becoming increasingly difficult. Agency C is interested in moving to digital certificates or to biometrics for standardized logical access control. While in the past, multiple Information Technology Offices issued passcodes to employees for each separate system for which an employee needs access, Agency C is trying to centralize and streamline its logical access control processes. Employees who travel, and are spending time in other agencies and on site in field offices, are increasingly in need of remote access to Agency C's computer systems. Many buildings in metropolitan areas are linked by local area networks and wireless communication. Wide area networks and the Internet are increasingly being used to create system linkages from remote field offices. Further, Agency C is beginning to put in place public access programs to enable both businesses and the public to be able to access information in the agency's computer systems. Although the agency has worked with passwords in the past, it is increasing concerned that passcodes do not provide adequate security for its needs, especially as they evolve toward greater use of the Internet for both internal and external communications.

Interoperability

Agency C has a greater need than Agency B for interoperability, particularly with other external agencies. Because Agency C's mission requires greater interaction with other external organizations and has a higher security profile, its physical and logical access control systems require interoperability both within the agency and with a multitude of external government agencies. This need for greater interoperability makes Agency C highly concerned with telecommunication systems, including private virtual networks for internal operations and Internet transactions for external organizations. Because Agency C is highly concerned about interoperability across multiple agencies, it is striving to put in place interoperability agreements with a multitude of government agencies.

Card Management

Agency C seeks an outsourced solution that combines a centralized and decentralized card issuance process to ease the cost and burden of the large-scale card distribution, while maintaining local service in outlying areas. Agency C would forward demographic data from its personnel system, as well as in-person identity proofing or biometric scans to the contractor maintained centralized card issuance office for a metropolitan area. The central office would personalize and distribute cards over-the-counter to employees from buildings all over the area. The unique requirements of outlying field offices will be addressed by designating local offices to collect in-person proofing and/or biometric templates, combine this data with demographic data from the centralized personnel system and digital certificates downloaded from the contract CA, personalize the card and distribute them through the local office.

PKI/Biometric Strategy

Agency C's increased need for security, interoperability across multiple agencies, and a mechanism for secure identity authentication make a PKI strategy important for this agency. Agency C can use secure digital certificates for logical access control, as well as to achieve interoperability across multiple agencies for physical access control. Further, Agency C can use the PKI for both remote access to its systems for internal employees, as well as for authentication of transactions with businesses or the public for its pilot electronic commerce and service delivery projects. A digital signature capability would make it possible for Agency C to transition to electronic approval and submission of administrative forms, a capability that supports the re-engineering initiatives of importance to this agency.

Because of the diversity of locations and the expense of implementing an in-house PKI infrastructure, Agency C finds it most practical to procure CA services through outsourcing. In this instance, registration for a digital certificate could be handled by local registration authorities operating in multiple agency locations. The local registration authorities could perform in-person identity proofing, forwarding the completed request for the certificate to a centralized CA. The CA would issue the certificates and download them to either the centralized or the decentralized card issuance facilities in each location to be loaded onto cards prior to distributing the cards from these offices.

The need for interoperability across multiple government agencies makes it important for Agency C to participate in an open PKI, one that allows certificates from multiple CAs to be cross-validated. It is anticipated that different agencies in the government will use different CAs so that a mechanism, such as a Bridge Certificate Authority (see Glossary in Appendix B), or a Certificate Arbitration Module (see Glossary in Appendix B), is needed to process and route transactions to verify digital certificates from different CAs.

Smaller divisions within Agency C may adopt a biometric to use for certain applications. The biometric provides enhanced identity authentication for the user without *necessarily* requiring the large infrastructure associated with PKI. Depending on the level of security required, biometrics can be implemented with or without using an attribute certificate to bind the biometric template to a smart card (see section 2.2.5 for further information). While using the attribute certificate to bind the biometric template to the smart card provides greater assurance of the cardholder's identity, it requires substantial overhead in setting up the Attribute Authority infrastructure, and is therefore a more costly approach to implementing biometrics. If the biometric is used without the attribute certificate, a "live" scan can be verified against the biometric template on the card without having to send the attribute certificate to the Attribute Authority for verification. This approach to using biometrics is less burdensome and expensive, but not as secure as using the attribute certificate to bind the biometric template to the card. While the biometric without an attribute certificate may not be as secure as it would be with the certificate, it still is more secure than many other approaches to identity verification. Since Agency C has a mid-level security need and limited resources for the card platform, an appropriate compromise for this environment is to provide the biometric without the extra cost of implementing an Attribute Authority infrastructure.

Agency C subdivisions can use the biometric for either logical or physical access control in some locations. The biometric also can be used in combination with the PKI so that certain applications (such as electronic forms) can use the digital signature capability, while others (such as access to high security areas of the building) use biometrics. Agency C may choose to use the biometric for certain cardholders only. For example, if the biometric is used to control access to specialized areas, such as a computer room, only those people who have the need to access these specialized areas will be issued the biometric card.

Applications

In Agency C's diverse environment, a range of additional applications will be needed. For example, in this environment in which employees have business in variety of agencies, it is likely that employees will need to transport computers and other equipment from building to building. Therefore, a property pass application would be highly desirable for this platform. With multiple meetings with internal and external agency participants, a rostering application also would be valuable. With the scale and diversity of Agency C's staffing requirements, training is yet another application that is desirable for Agency C's platform. Additionally, as Agency C is currently expending substantial resources to re-engineer its administrative processes, it is interested in adding travel, purchase, and fleet card financial applications to its card platform.

Technology

Based on the key decisions described above, Agency C needs yet a more complex card platform than Agency B. Because Agency C is supporting a number of applications, including PKI and/or biometrics, it will need more memory (most likely at least 16K) and a co-processor to provide cryptographic functionality. To ensure backward compatibility with a multitude of physical access control systems, as well as to support financial applications, Agency C will require a multi-technology card that combines chip, bar code, proximity (in some locations) and magnetic stripe.

To enable fast throughput at its busier metropolitan offices, Agency C will begin its efforts modernize and standardize its legacy physical access control systems by swapping out old readers and re-equipping major access points with contactless chip readers. However, when agency employees go to other buildings with older physical access control systems that have not yet been upgraded, they should be able to use magnetic stripe or bar code. The contact chip will be used to carry demographic, property pass, and training data as well as the digital certificate to be used to verify the cardholder's identity and to provide logical access control. The chip will also be used for the biometric template for those cardholders who have need to access areas protected by the biometric. To accommodate its need to have both contactless and contact chip interfaces, Agency C will purchase combi-cards with extra memory. This memory can be loaded with additional data and/or applications in the future, as Agency C's platform requirements grow. Because Agency C is planning on open, commercial magnetic stripe credit applications, the cards it purchases must have magnetic stripe formats that conform to commercial standards. To promote an open system environment and ensure interoperability, Agency C's card should comply with the *EMV '96: Integrated Circuit Chip (ICC) Specifications for Payment Systems (Version 3.0).*

Agency C has impacted the hardware and software required for its card platform by choosing to outsource card management and PKI services. This decision means that no hardware or software must be procured for the card management function nor for customer service. Card management and customer service hardware/software will be supplied by the contractor to whom card management has been outsourced. The contractor will be responsible for equipping both the centralized and local card issuance offices.

By deciding to either to swap out readers or replace various legacy physical access control systems across the agency, and acquiring cards with multiple technologies, Agency C has adopted a multi-prong strategy to deal with legacy compatibility. Agency C will have to procure contactless readers for a number of its legacy physical access control systems, as well as the software to adapt these systems to the new readers. For those areas with specialized access control using biometrics, biometric readers must be acquired and adapted to the physical access control systems.

Additionally, Agency C will have to purchase inexpensive card readers for use on workstations to be able to read the chip for its PKI and/or biometric logical access control systems. The offices within Agency C that opt for biometrics rather than PKI for logical access control will need keyboards with built-in or attached biometric readers. To accommodate the PKI capability, local registration authorities will need a secure workstation to generate digital certificate requests, as well as secure telecommunications to transmit the request for a digital certificate to the Certificate Authority. Secure telecommunications will also be needed between the CA and the central card issuer to receive the signed digital certificates and load them on the cards.

Commercial Agency Model

AGENCY PROFILE CHARACTERISTICS:

The Commercial Agency Model (hereafter referred to as Agency D) requires a card platform very similar to that of Agency C, appropriate to a relatively large, geographically dispersed agency, or a large division or bureau of a larger organizational entity. This model is generally used to characterize a homogeneous, large agency whose mission is geared in some way to assisting the business or financial communities. Because of this mission, Agency D typically deals with financial transactions and/or proprietary business information. An example of this type of agency is the Department of Commerce or Department of Treasury. Agency D requires a relatively high level of security (DOD Assurance Level 4), but is not yet at the highest security level. Because Agency D has installations across multiple locations, the security needs of its various facilities may vary substantially from one office to another. Like Agency C, some of this agency's service providing offices may actually be located in commercial buildings or other non-governmental facilities. Employee cards may need to be used in multiple locations across widely dispersed and variant geographic areas. This sample agency needs both perimeter control and an enhanced level of internal security for access to high risk areas within certain buildings. Employees from Agency D may need access to a variety of buildings with many incompatible legacy physical access control systems. Additionally, members of the financial and business communities may need a significant amount of access to Agency D's buildings.

Agency D has a vast number of systems that are likely to use various different access control devices. Because of the sensitivity of the financial and proprietary business data in its systems, Agency D is actively pursuing a more sophisticated security strategy. For Agency D, secure telecommunications transmissions are critical, as electronic funds are being transferred and highly confidential data (such as electronic tax submissions) are being transmitted across open networks. Agency D needs both secure access to its databases, as well as authenticated messaging across networks. In this environment, many employees need secure remote access to the agency's systems. Agency D employees are less likely to frequently visit a wide range of other agencies, but rather have relationships with certain other key agencies with which they do business. These employees do use information from other internal divisions and external agency systems. Additionally, Agency D is likely to be exchanging confidential information with the business and financial communities. Interoperability with a limited number of other government and commercial agencies is very important to the conduct of Agency D's mission. While interoperable physical access control is important, the security and interoperability of Agency D's networks and systems is of the highest priority.

Agency D has a history of centralized badging and prefers this approach even for its geographically dispersed locations. Further, Agency D has a number of centralized information systems that maintain demographic information and other personnel information. For Agency D's environment, these data can be downloaded most conveniently to a central card issuance location. Because of its geographic dispersion, Agency D has a large number of separate physical access control databases for different locations, managed by the local facilities organization, which maintains employee's physical access control privileges and issues a separate card for the individual facility at which the employee works.

Because of the nature of Agency D's mission, its information systems are of particular interest to hackers. Consequently, increasingly aware of the vulnerability of its information systems, Agency D has tried to consolidate its logical access control function and maintain security in a centralized manner. Because its employees more frequently need highly secure remote access to its systems, Agency D has been experimenting with tokens for remote access to its higher security systems.

Agency D's highest priorities include enhancing security, both internally across divisions and externally with other commercial institutions, as well as promoting interoperability with the private sector. Agency D is on the leading edge of electronic commerce and is moving actively toward setting up electronic forms not only for internal use, but also for government-to-business transactions. It is working actively to encourage the adoption of electronic forms for all types of interactions with the business community. Agency D is concentrating its resources in building secure electronic applications for its partner agencies, and for a specific segment of the public (i.e., large, private commercial and financial institutions). Agency D understands the importance of electronic transactions to its agency's mission and is moving aggressively into establishing government-to-government and government-to-business strategies for electronic commerce.

CARD PLATFORM ANALYSIS:

Security
The Commercial Agency Model has more extensive security requirements than the Civilian Agency Model, especially within the area of logical access control. In addition to being interested in perimeter and parking control, Agency D has particular interest in enhancing physical security in some internal areas. Although Agency D must deal with a diversity of buildings, achieving backward compatibility across a variety of legacy physical access control systems is less of a priority for Agency D. Like Agency C, Agency D plans a variety of approaches to deal with the wide range of legacy physical access control systems. Overtime, Agency D will slowly replace its local legacy systems, providing new, standardized physical access control systems using a contactless chip. However, as an interim measure, Agency D is to switch out some readers to use a contact chip for physical access control or to use multiple technologies on the card to achieve backward compatibility. Until that replacement process is completed, Agency D opts to use the PKI process described in section 3.1.3 to provide interoperability both internally and with external agencies.

Interoperability
Agency D has multiple offices located across the country in major cities. It has a need for locations within the agency to be interoperable with each other. Additionally, as Agency D conducts commercial transactions with its business partners, it has the need to interoperate with several external agencies in order to conduct its mission.

Card Management
Although enrollment will need to be performed locally to allow for in-person identity proofing and capture of biometric templates, centralized card issuance makes sense for Agency D. Agency D seeks an outsourced, centralized card issuance process to ease the cost and burden of the large-scale card distribution. It is assumed that the contractor will be able to achieve economies of scale such that Agency D could not afford to purchase the hardware and software needed to provide card issuance in such a diversity of locations. The lack of physical proximity of the existing card issuance office and the inconvenience with which employees in the past have met has had an impact on Agency C's strategy for card issuance. The large number of locations and the accompanying staff that would be required for local personalization and distribution make that approach unmanageable for Agency D. New employees can conveniently access their local registration authority office to provide in-person identity proofing or biometric capture, but the cards will be produced in a central location and mailed to the employee.

A centralized, outsourced card issuance process is most viable for the large-scale implementation needed by Agency D. Using downloads from its centralized personnel system, as well as data captured from localized in-person identity proofing or biometric scans, the centralized card issuance office would act as an integrator, receiving demographic data, digital certificates, and biometric templates to load on the card. The central management database should contain demographic as well as physical and logical access control privileges. To streamline operations, overtime Agency D will disband its duplicative organizations currently devoted to maintaining physical and logical access control databases in separate systems. The transition to the centralized database for card management, physical access control, and logical access control will be gradual, as will be the replacement of legacy physical access control systems with new contactless chip technology.

PKI/Biometric Strategy

Agency D is particularly interested in digital certificates for standardized logical access control. A substantial number of transactions will occur over networks, and these transactions must be encrypted for security. Further, as many of these are high value or confidential transactions, it is critical that the identity of the transaction originator and receiver be verified. This identity authentication is necessary both for internal transactions and for government-to-business transactions. Digital signatures are particularly well suited for this environment.

Agency D has a somewhat different need for interoperability than Agency C. Agency D's mission requires greater interaction with external business and financial organizations and has a higher security profile. Its logical access control systems require interoperability within the agency, with a few closely related external government agencies, and with specific private organizations. Because Agency D's requirements are more specific, it has less of a need for a fully open PKI structure. The need for interoperability across a limited number of government agencies and private financial institutions makes it important for Agency D to participate in an open, but bounded PKI. A "membership" PKI, in which relationships among partners are defined, is more viable for this environment. This PKI strategy enables certificates from multiple CAs to be cross-validated, but interoperability agreements exist among the participating "members" of the PKI. It is anticipated that partner agencies and financial institutions will develop agreements among themselves as to which certificates are acceptable for validation.

Thus, interoperability agreements are as critical for Agency D as Agency C, but they need to be in place with only a limited number of partner agencies and external organizations.

Agency D's increased need for security and interoperability when conducting transactions with non-governmental commercial entities make a mechanism for secure identity authentication particularly important to this agency. Thus, Agency D needs a PKI strategy to support its need to make payments and support financial transactions across the Internet. While Agency D can use secure digital certificates for logical and physical access control, it has an even greater need to use digital certificates for identity authentication for high-value financial transactions. For Agency D, PKI will be an enabler for its commercial interactions with a limited number of partners.

Because of the diversity of locations and the expense of implementing an in-house PKI infrastructure, Agency D, like Agency C, finds it most practical to procure CA services through outsourcing. Again, its level of geographic dispersion makes it most efficient to handle registration for digital certificates by local registration authorities operating in multiple agency locations. The local registration authorities could perform in-person identity proofing, forwarding the completed request for the certificate to a centralized Certificate Authority. The CA would issue the certificates and download them to the centralized card issuance facility to be loaded onto cards prior to the mailing of the cards.

Agency D, like Agency C, may adopt a biometric to use for certain applications. However, because it does not require the highest level of security, it would be less costly for Agency D to use a biometric template without the verification infrastructure required by the attribute certificate. Agency D will use the biometric by verifying a "live" scan against the biometric template on the card, without verifying the authenticity of the attribute certificate with an Attribute Authority. It will trade-off some security in this case for a less costly implementation.

Applications

The nature of Agency D's business will require a number of applications, in addition to physical and logical access control. Agency D is not concerned about mixing security and financial applications and wants a "one card fits all" solution. It will acquire a hybrid card with both chip and magnetic stripe for its travel, fleet, and purchase credit card applications. In this environment, an open electronic purse would also be useful for employees who have numerous dealings with outside financial institutions. Because it often sends and receives high-value transactions, as well as confidential financial data and proprietary company data, Agency D has a need for an application to enable transaction encryption. Finally, because Agency D employees travel extensively, it wants an emergency medical application on its card platform.

Technology

Agency D requires a platform very similar to that of Agency C, with at least 16 K and a co-processor for cryptographic capability. The contact chip will be used to carry demographic data, as well as the digital certificate to be used to verify the cardholder's identity and to provide logical access control. The chip will also be used for the biometric template for those cardholders who have need for the biometric. Agency D does not have the resources right now to expend on wide-scale distribution of combi-cards, but rather will concentrate on its logical access control application with a chip card and purchase multi-technology cards to achieve interoperability with local physical access control systems. In the future, Agency D will shift to combi-cards to adopt to the planned contactless chip-based physical access control systems being implemented down the road. Because Agency D is planning open, commercial magnetic stripe credit applications, the cards it purchases must have magnetic stripe formats that conform to commercial standards. To promote an open system environment and ensure interoperability, Agency D's card should comply with the *EMV '96: Integrated Circuit Chip (ICC) Specifications for Payment Systems (Version 3.0).*

Agency D has impacted the hardware and software required for its card platform by choosing to outsource card management and PKI services. This decision means that no hardware or software must be procured for the card management function nor for customer service that also will be outsourced as part of the card management functions.

By deciding to either to swap out readers or replace various legacy physical access control systems across the agency, and acquiring cards with multiple technologies, Agency D has adopted a multi-prong strategy to deal with legacy compatibility. Initially, Agency D will not have to procure contactless readers, but will add these in the future as it transitions its systems to this standard. However, Agency D will have to procure contact card readers and biometric readers, if it chooses to use this technology. The offices within Agency D that opt for biometrics rather than PKI for logical access control will need keyboards with built-in or attached biometric readers. To accommodate the PKI capability, local Registration Authorities will need a secure workstation to generate digital certificate requests, as well as secure telecommunications to transmit the request for a digital certificate to the Certificate Authority. Secure telecommunications will also be needed between the CA and the central card issuer to receive the signed digital certificates and load them on the cards. However, this equipment will be supplied by the contractor providing Registration Authority services.

International Agency Model

AGENCY PROFILE CHARACTERISTICS:

The International Agency Model (hereafter referred to as Agency E) requires a card platform appropriate to a very large, highly geographically dispersed agency, with locations around the country and overseas. This model is characterized by agencies providing diverse services that run the gamut from routine administrative tasks to highly sensitive diplomatic assignments. An example of this type of agency is the Department of State or the Agency for International Development. Although this model has a relatively high level of security needs (DOD Assurance Level 4), it does not have the highest DOD Assurance Level. Because Agency E has diverse installations across multiple locations, the security needs of its various facilities may vary substantially from one office to another. Physical access control, especially perimeter control, is of particular interest to this agency. Internal control is also important as sensitive documents may be maintained within the Agency E's buildings and systems. Authenticated and encrypted messaging is needed by Agency E to protect its confidential and often sensitive transactions. Employees from Agency E may need access to a variety of buildings both within the agency and with partner agencies. Additionally, employees may need access to facilities of foreign governments and foreign nationals may need access to Agency E's buildings.

Agency E's systems vary tremendously in their level of sensitivity. Many systems have routine information, while other systems contain highly confidential information. The control mechanisms also vary across these systems. While many of the systems currently use only passcodes, other systems may be experimenting with more sophisticated security devices. Telecommunications are particularly sensitive for this agency, which requires encrypted message traffic. An extremely high percentage of employees will use secure remote access to the agency's systems. While employees in Agency E may share information across a few agencies with which they have routine contact, they are unlikely to visit a wide range of agencies nor to use information from other external agency systems. Broad-based interoperability is less pressing a concern for Agency E.

Agency E has localized badging, particularly for its overseas locations. As with many of the other agencies, demographic information is maintained in large scale personnel systems, but currently cards are issued by manually inputting data into the badging system. Agency E has a large number of separate physical access control databases for different locations, managed by the local facilities organization, which maintains employee's physical access control privileges and issues a separate card for the individual facility at which the employee works. Similarly, a number of different databases, maintained under the auspices of different information technology offices, manage user passcodes or other security mechanisms (e.g., tokens for remote access to certain high security systems). Currently, there is little communication among the disparate physical and logical access control systems and offices, but Agency E is to move toward a more integrated solution.

Agency E's highest priorities include enhancing physical security, particularly for its foreign facilities. Another priority is the security of its systems and particularly, its telecommunications. Agency E is first and foremost concerned about ensuring the security of internal agency transactions, and is far less interested than other agencies in external transactions with the public and private companies. Expending most of its available resources on improving security, it has limited resources to devote to re-engineering its processes or to developing electronic service delivery for citizens.

CARD PLATFORM ANALYSIS:

Security

The International Agency Model has more extensive security requirements than the Civilian or Commercial Models. In addition to being particularly focused on perimeter and parking control, Agency E has an increasing interest in enhancing security in some internal areas. Agency E has some unique requirements for physical access control. Because of concern for emitting radio frequency waves using contactless chip technology, Agency E is interested in contact chip technology for its card. Although like other agencies, Agency E faces a diversity of buildings and substantial issues with backward compatibility across a variety of legacy physical access control systems, achieving interoperability across facilities is of less significance to Agency E than ensuring the security of particular buildings. As this is a priority for Agency E, it is planning to replace and/or swap out readers for physical access control systems as quickly as possible with standard chip readers rather than to attempt to achieve interoperability through multiple technologies.

In this environment in which physical security is so key, Agency E is to use a biometric because it believes this to provide the highest level of security. The biometric is secure and available on-board the card if on-line systems are down during an outage or some other emergency. Local biometric readers will be used to capture live scans to use to compare against the template maintained on the card. If the match is acceptable, access is granted, based on access privileges carried on the card.

Agency E is interested in moving to digital certificates for standardized logical access control. Agency E is to centralize and streamline its logical access control processes. Employees from the International Agency travel a great deal and need remote access to the agency's systems from various parts of the country, as well as from abroad. Additionally, Agency E is highly concerned about the security of its transactions being passed between national and international offices. Although the agency has worked with passwords in the past, it is increasing concerned that passcodes do not provide adequate security for its needs, especially as they evolve toward greater use of the Internet for both internal and external communications.

Interoperability

Agency E has a limited need for interoperability, particularly with other external agencies. Although interoperability is important across locations within the agency, it is less critical across multiple agencies, because Agency E has specific agencies with which it works frequently, but its employees rarely need blanket access to multiple government agencies. Thus, Agency E must put in place interoperability agreements with the specific agencies with which it needs to be compatible.

Card Management

Like other geographically dispersed agencies, Agency E has had in the past multiple local badging offices. That geographic dispersion makes it both desirable and undesirable to have central card issuance. From the perspective of customer service, it is far more convenient to have local badging offices. However, from the perspective of management, it is far more complex and costly to personalize cards locally in so many places. To address that tradeoff, Agency E would like to have local enrollment and over the counter distribution. However, the card issuance contractor would perform the card personalization centrally. This enables close geographic proximity for the card issuance functions that actually require the employee to be available face-to-face, while it supports the economies of scale that can be obtained through centralized, outsourced operations. The card issuer acts, in essence, as the card platform integrator, retrieving relevant data from personnel, physical access control, logical access control, medical and other legacy systems to populate the card. Additionally, the contractor oversees the efforts of the PKI and/or biometric services providers. The data are maintained and backed-up centrally to reduce the complexity of card replacement in case of loss or damage.

Agency E has decided to outsource its card issuance process, but it wants a solution that combines a centralized and decentralized card distribution process. By moving to this solution, Agency E can achieve economies of scale, while providing convenience to the employees in widely dispersed offices. Local offices would provide a location to gather biometric scans and perform in-person identity proofing. The local office would forward demographic data from its personnel system and "live" biometric scans to the contractor maintained centralized card issuance office. The local office would also perform in-person identity proofing, sending digital certificate requests to the Certification Authority. The CA in turn would generate digital certificates and download them to the centralized card facility. The contractor supplied central issuance facility would personalize the cards, load them with digital certificates received from the Certificate Authority, and mail them to local offices for over-the-counter distribution to employees.

PKI/Biometric Strategy

Agency E's increased need for security and for a secure, encrypted messaging mechanism make PKI important for this agency. Agency E can use secure digital certificates for logical access control and for remote access to its systems for internal employees. It can use the PKI structure for encryption as well. Additionally, a digital signature capability would make it possible for Agency C to convert to electronic forms.

Agency E's international locations and geographic dispersion, as well as its lack of a trusted computing environment make it impractical for Agency E to provide its own in-house PKI services. Therefore, Agency E will procure CA and Registration Authority (RA) services through outsourcing. As with other agencies outsourcing PKI, registration for a digital certificate could be handled by local registration authorities operating in multiple agency locations. The local registration authorities could perform in-person identity proofing, forwarding the completed request for the certificate to a centralized card issuance location. The keys on the card could be generated and sent within a secure request for a digital certificate to the Certificate Authority. The CA would issue the certificates and download them to the centralized card issuance facility, which in turn would load the certificate on the card and send the cards to local offices. For overseas locations, the cards could be sent via the diplomatic pouch.

While Agency E may need interoperability currently within its agency and with a few partner agencies, it is anticipated that in the near future, Agency E may be moving toward the use of secure email to communicate with other foreign governments. The eventual need for interoperability across multi-national agencies requires Agency E to have access to an open PKI, one that allows certificates from multiple CAs to be cross-validated. Although of limited scale initially (the cross-certification initially will be limited to partner international agencies), it is anticipated that eventually the certificates of agencies outside the U.S. government will have to be verified. Therefore, Agency E will require a fully open approach to PKI.

As Agency E has decided to adopt a biometric to use in lieu of the PKI for physical access control, it will have to determine its biometric strategy. First, Agency E will select the particular biometric that best meets its needs. Section 4.2.1.3 provides a discussion of criteria for Agency E to use in making this selection. Second, Agency E must decide whether or not it wants to outsource for biometric services. As Agency E is currently using a contractor for card issuance and PKI services, it believes that implementing the biometric services outside the agency would simplify the transition process. Agency E currently has little expertise with biometrics, nor does it have the staff resources to run a biometric system. Third, Agency E must determine whether to implement its biometrics with or without using an attribute certificate to bind the biometric template to a smart card. Since Agency E is not at the highest security level and is using the biometric for physical access control, the additional overhead of checking the attribute certificate would be impractical for this physical access application. In Agency E the biometric would be used for both perimeter control and control for access to higher security internal areas. Agency E is considering using a multiple biometrics for its card platform for certain individuals with higher security needs than the rest of the staff.

Applications

Agency E's card platform will include a variety of applications. As conduct of meetings is so important in this agency, it desires a rostering application that can be used to generate listings of meeting attendees. Because of the sometimes sensitive nature of Agency E's meetings, attendance may require clearances. Additionally, Agency E staff may attend meetings in outside agencies that also require exchange of clearances. Consequently, the clearance application is particularly useful for Agency E. The mobility of Agency E's workforce will also dictate additional useful applications. A property management pass would make it more convenient for employees to take laptops and other equipment with them when they travel. Similarly, a medical application with emergency medical and immunization information would be very expedient for employees who frequently travel internationally. An electronic ticketing application or a travel profile application would also be useful in this environment. An added convenience for travelers would be financial applications including both an open purse and credit card applications. Finally, Agency E has an interest in developing electronic forms for use both within the agency and with other governments.

Technology

Agency E needs a card platform that has sufficient memory to support a number of applications, including PKI and biometrics. In addition to at least 16 K (and probably 32K would be more viable), the chip needs a co-processor to provide cryptographic functionality. To support financial applications, Agency C will require a hybrid card that combines chip and magnetic stripe.

Since Agency E's highest priority is physical access control, this agency plans to replace its physical access control systems with a standard biometrics-based system. The contact chip will be used to carry the biometric template to be used to verify the cardholder 'live' scan for physical access control systems, as well as the digital certificate to be used to verify the cardholder's identity in Internet-based transactions, digitally sign electronic forms, and provide logical access control. If the PKI application described in section 3.1.3 is maintained by the other agencies to which Agency E employees must have access, the digital certificate could be used to provide interoperability across different physical access control systems in other agencies. Otherwise, the approach to achieving interoperability across the limited number of agencies with which Agency E must have interaction can be included in the interoperability agreements. Because Agency E is adding open, commercial magnetic stripe credit applications to its platform, the cards it purchases must have magnetic stripe formats that conform to commercial standards. To promote an open system environment and ensure interoperability, Agency C's card should comply with the *EMV '96: Integrated Circuit Chip (ICC) Specifications for Payment Systems (Version 3.0).*

By choosing to outsource card management, PKI, and biometric services, Agency E has influenced the hardware and software required for its card platform. Although no hardware or software must be procured for the card personalization and printing functions, equipment will be needed to generate requests for digital certificates and for capturing and maintaining biometric templates at local RA offices. If the PKI and biometric services are outsourced, the vendor must provide and maintain this equipment at local offices. Customer service and the requisite equipment also will be outsourced as part of the card management functions. The contractor will be responsible for equipping both the centralized and local card issuance offices.

The agency will need to purchase upgraded physical access control systems, or at the very least, biometrics readers to swap out with the existing legacy systems. Agency E will have to purchase inexpensive card readers for use on workstations to be able to read the chip for its digital certificates to be used by the logical access control systems. Additionally, Agency E will need a mechanism for routing digital certificate verification transactions among Certificate Authorities. Software such as a Certificate Arbitration Module (CAM) (see Glossary in Appendix B), must be available in an open PKI.

Intelligence Agency Model

AGENCY PROFILE CHARACTERISTICS:

The Intelligence Agency Model (hereafter referred to as Agency F) requires the most complex card platform. This model is generally used to characterize a homogeneous, large agency whose mission is geared to providing intelligence or defense operations. Because of this mission, Agency F's highest priority is security. An example of this type of agency is the National Security Agency or certain specialized components of the Department of Defense. This model applies primarily to the intelligence community and ***only the small subset*** of the defense community that has the very highest security needs. A number of Agency F employees may require the highest level of security (DOD Assurance Level 5). However, most DOD employees (particularly those slated to receive identification cards under the Common Access Card program) will not require this highest level of security.

Because Agency F has installations across multiple locations both in the United States and abroad, the security needs of its various facilities may vary substantially from one office to another. Employee cards will need to be used in multiple locations across widely dispersed and variant geographic areas. Portability of information is particularly key in this model. Agency F needs both significant perimeter control and an extremely high level of internal security for access to Sensitive Compartmentalized Information Facility (SCIF) areas within certain buildings. Additionally, Agency F must protect high security documents. Employees from Agency F typically require ongoing access to their partner agency buildings that also require very high security.

Agency F has a vast number of systems with different degrees of sensitivity and varying access control devices. Both physical and logical security is of the utmost importance to this agency. For Agency F, secure telecommunications transmissions are critical, as highly sensitive and confidential data are transferred both across secured point-to-point networks and through Virtual Private Networks. Agency F needs both secure access to its databases, as well as encrypted messaging across networks. A majority of employees need secure remote access to the agency's system, depending upon their posts and positions. Agency F employees infrequently visit civilian agencies, but rather have relationships with certain other intelligence agencies with which they do business. Additionally, Agency F is likely exchanging confidential information with other intelligence agencies both within the United States government and with foreign governments. Interoperability with a limited number of other government and foreign agencies is a key part of Agency F's mission. While interoperable physical and logical access control is important in certain cases, the security of Agency F's buildings, networks, and systems is of the highest priority.

Agency F has typically used decentralized badging supported by centralized personnel databases. These data can be downloaded most conveniently to a central card issuance location. Because of its immense geographic dispersion, Agency F has a large number of separate physical access control databases for different locations, managed by the local office or base, which currently maintains employee's physical access control privileges and issues a separate card for the individual facility at which the employee works.

Agency F's mission make its information systems particularly vulnerable to attack. Because its employees very frequently need highly secure remote access to its systems, Agency F has concentrated substantial resources to exploring the best options for adequately protecting these higher security systems. Additionally, Agency F requires encrypted messaging for a significant portion of its message traffic.

Agency F's highest priorities include enhancing security, both internally across different organizational units and externally with other partner agencies. While implementing electronic purchasing is important to Agency F, especially with established regular vendors, Agency F's emphasis for its employee identification card is on security not financial applications. In fact, Agency F is adamantly opposed to combining security and financial applications on the same card.

CARD PLATFORM ANALYSIS:

Security

The Intelligence Agency Model has the most extensive security requirements of all the models (Agency F has a DOD Level 5 designation). Agency F has interest in significant perimeter and internal access control, as well as protection of high security documents. SCIFs are commonplace in Agency F's environment. Agency F, like other agencies, faces a diversity of buildings and substantial issues with backward compatibility across a variety of legacy physical access control systems. However, to Agency F, achieving interoperability across facilities is of less significance than ensuring the highest overall level of security in all of its buildings. Thus, physical access control is a significant priority for Agency F. Consequently, it is planning to replace and/or swap out readers for physical access control systems as quickly as possible with standard biometric readers rather than to attempt to achieve interoperability through multiple technologies.

Interoperability

Because of the nature of Agency F's mission, it does not to have interoperability across a number of agencies. The high security requirements of Agency F preclude open exchange of information across the gamut of

Federal agencies. However, Agency F does work co-operatively with certain partner agencies in both the United States and abroad, so it does need interoperability with a few closely related agencies.

Card Management

Agency F has new employees inducted at a variety of locations across the U.S. Cards may have to be provided under field conditions, both in the Unites States and abroad. Enrollment will need to be performed locally for cardholder and issuer convenience. Because of its size, mission, security environment, and previous experience with card issuance, Agency F has chosen to issue and manage its employee identification cards in-house. Local offices manned by Agency F employees will be set-up to capture biometric templates and perform identity proofing for the initiation of digital certificates. The local offices will also perform card personalization, using data maintained in the centralized personnel system. Card management data will be kept in this distributed environment, but it also will be uploaded to and maintained in a back-up centralized data center. Physical and logical access control privileges will also be maintained at the local card issuance facility, and duplicated at a centralized data center. Demographic and access information will be integrated into a single card management system. The local offices will request digital certificates (and, in the case of Agency F, attribute certificates) from the in-house Certificate Authority and/or Attribute Authority. The local office performing card personalization will act as the integrator, collecting demographic data, access privilege data, digital photographs, digital certificates, and attribute certificates with the biometric template maintained in the attribute certificate and loading the card with this data.

Different organizational units vary over whether Agency F should use PKI or biometrics for logical access control. On the one hand, Agency F's geographic dispersion ensures that a substantial number of its transactions will occur over networks, and these transactions must be encrypted for security. The criticality of many of these transactions make identity authentication for both the transaction originator and receiver essential. Electronic forms are particularly viable for this organization because of the substantial number of forms circulated by Agency F, as well as the dispersion of its personnel. Thus, digital signatures are particularly well suited for this environment. On the other hand, biometrics provides a high level of security and is already selected for the physical access control application.

PKI/Biometrics Strategy

While Agency F employees need to move freely between their home agency and a few other partner agencies, it typically does not have a need for interoperability across multiple agencies. Its physical and logical access control systems require interoperability within the agency, with a few closely related external government agencies, and potentially with some foreign governmental organizations. Like other agencies with limited partners and high security needs, Agency F has a need for an "open but bounded" membership PKI structure. Because of its mission, Agency F has existing secure computer environments, resources to man these environments, and the need to closely control the PKI implementation. Therefore, to be able to fully control the implementation of its PKI environment, Agency F has decided to develop an in-house PKI infrastructure. The in-house CA would be set-up centrally, receiving digital certificate requests from local offices and downloading certificates to these local card personalization systems.

Biometrics is of particular importance to Agency F because of its higher security needs. After evaluating several biometric technologies, Agency F decided upon fingerprints because of its relatively low cost, ease of implementation, cardholder convenience, and ability to exchange information with law enforcement agencies. Because of its high security requirements, Agency F will use an attribute certificate to bind the biometric to the chip card. Additionally, Agency F will use the in-house Certificate Authority to verify both digital and attribute certificates. Thus, Agency F will use the biometric by verifying a "live" scan against the biometric template on the card, as well as verifying the authenticity of the attribute certificate with the in-house CA acting as an Attribute Authority. Agency F has opted to trade-off a more costly implementation for better security.

Applications

Agency F's mission makes a number of applications, in addition to physical and logical access control, viable in this environment. The rostering applications would have a number of applications in this agency. As conduct of meetings is so important, a rostering application can be used to generate listings of meeting attendees. The rostering can be used to account for individuals within a facility during emergency evacuation procedures. The rostering can also be used to track usage of food services, another important application for this Agency. Because of the prevalence of SCIFs, top secret documents, and sensitive meetings, Agency F has a special need to provide portable clearance information that can be securely transported from one facility to another. Additionally, Agency F staff may attend meetings in outside agencies that also require exchange of clearances. Consequently, the clearance application is particularly useful for Agency F. The mobility of Agency F's workforce will also dictate additional useful applications. A property management pass would make it more convenient for employees to take laptops and other equipment with them when they travel. Similarly, a medical application with emergency medical and immunization information would be very expedient for employees who frequently travel internationally or are in field locations where on-line telecommunications may not be available. Because of the significant number of forms used by this agency, Agency F could save substantial time using an electronic forms application.

Technology

Agency F will need the "highest end" card. The number of applications, as well as the need to support both digital and attribute certificates, dictate a chip card with substantial memory requirements. At least a 16 K card and preferably a 32 K or 64 K card, with a co-processor for cryptographic capability, is needed to support the requirements of Agency F. The contact chip will be used to carry demographic data, as well as the digital and attribute certificates (containing the biometric template) to be used to verify the cardholder's identity and to provide physical and logical access control. The chip will also carry the other applications developed for Agency F. For access to the most secure areas, Agency F is considering the use of a multi-layer biometric that is, the use of more than one biometric type to add additional security. Additionally, the card should include a magnetic stripe and bar code capability to allow backward compatibility with Agency F's legacy systems.

The hardware and software required for its card platform is determined by Agency F's decision to provide card management, as well as PKI and biometric services in-house. To perform card management, Agency F will need card issuance workstations (including the peripherals such as card printers, card readers, biometric readers, digital camera, etc.) for each local office performing card issuance, as well as a host computer for maintaining the card management database. It will also need ARU hardware to support the customer service function that will be required if card management is performed in-house. Card management and customer service software will also be needed.

To support the in-house PKI, Agency F must have secure hardware to generate the digital certificates and maintain a repository in which to publish the certificates. It must also provide the hardware to process certificate verification transactions. To accommodate the PKI capability, local registration authorities will need a secure workstation to generate digital certificate requests, as well as secure telecommunications to transmit the request for a digital certificate to the in-house Certificate Authority. Secure telecommunications will also be needed between the in-house CA and the local card issuers to receive the signed digital certificates and load them on the cards. Certification authority software, as well as software to route and process certificate verification transactions is needed. Similarly, hardware and software to support the attribute authority functionality is needed, as are biometric readers to take initial scans for creating templates for the cards.

By moving to biometric based physical access control systems, Agency F will have to decide to either to swap out readers to replace with biometric readers, or replace various legacy physical access control systems. Additionally, Agency F will have to procure contact card readers and biometric readers. The offices within

Agency F that will use biometrics rather than PKI for logical access control will need keyboards with built-in or attached biometric readers.

Conclusion

The intent of this chapter is to enable agencies to document and understand their individual characteristics, and use these characteristics to formulate an optimal platform to support these characteristics. The models presented a brief overview of how agencies with very different characteristics planned their card platform. This chapter analyzes what decisions need to be made in order to select and procure a card platform. The following chapter presents the key decisions that must be made before a task order is written for the procurement of the card platform and auxiliary systems.

15. INDEX