UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Chief Information Officer Human Resources Line of Business

Identity and Authentication Reference Model Version 1

August 2010

a New Day for Federal Service

Executive Summary

In June 2009 a working group of cross-agency subject matter experts was formed to identify and analyze the issues around E-Authentication and formulate recommendations for their resolution. The workgroup agreed that system owners have differing interpretations of E-Authentication, are investigating different solutions, and are often unable to work with agencies on E-Authentication implementations. As a result, some agencies have implemented compensating controls for meeting respective assurance levels. Therefore, a unified approach must be developed for meeting E-Authentication and single sign-on requirements, and consistently enable agencies to implement E-Authentication for Federal systems that are managed outside the agency, i.e. FedTraveler, eOPF, Employee Express, eQIP, CVS. This unified approach will:

- Establish a common understanding among system owners of what E-Authentication is and the value it provides for agencies;
- Explain/clarify OPM/GSA's role in supporting implementation of E-Authentication;
- Provide a standard description/definition of a common process and steps for agencies working with OPM/GSA on implementing E-Authentication;
- Secure OPM commitment to support these implementations for OPM-managed governmentwide systems; and
- Define a standard Information Exchange Package (IEP) for E-Authentication containing "identification data" that agencies and governmentwide systems can use to achieve data integration, data standardization, and work flow integration

The development of the Human Resources Line of Business (HR LOB) Identity and Authentication Reference Model (IARM) is the first step in a unified approach. The purpose of the IARM is to set the context for "Identity" and "Authentication" as applicable to the HR LOB. Further, the IARM will serve as a framework for describing and understanding concepts within this context of discussion by defining significant relationships between the elements of identity and authentication.

Table of Contents

Tables and Figures

1.0 Introduction

The Open Government Initiative promotes transparent, collaborative, and participatory government that fully engages the public – while protecting citizen privacy and ensures the safekeeping of data that is exchanged. Identity and authentication management plays a crucial role in the security of data and applications that impact every line of business within the Federal government. Identity management issues have been well documented by the Government Accountability Office (GAO), National Science and Technology Council (NSTC), and the Office of Management and Budget (OMB). The Human Resources Line of Business (HR LOB) is especially affected by identity and authentication issues because this line of business deals with human resource functions such as hiring and separation.

The HR LOB Identity and Authentication Reference Model (IARM) builds upon the work done by the Identity Credential and Access Management (ICAM) sub-committee of the Chief Information Office (CIO) Council. The IARM describes the fundamental concepts and relationships of "Identity and Authentication" elements in the HR LOB domain. Also, the reference model establishes a common understanding of E-Authentication within the HR LOB context among users, stakeholders, implementers, and service providers, while providing value for agencies.

1.1 HR LOB Background

The Office of Personnel Management (OPM) launched the HR LOB initiative in 2004. The HR LOB Concept of Operations (CONOPS) describes a service delivery model in which designated core HR services relative to human resources information systems (HRIS) and payroll operations move from agencies to shared service centers (SSCs). Over time, as SSCs evolve and expand their capabilities, more transactional and administrative activities may shift from the agency to an SSC.

The overall vision of the HR LOB is governmentwide, modern, cost-effective, standardized, and interoperable HR solutions providing common, core functionality to support the strategic management of human capital and to address duplicative HR systems and processes across the Federal Government.

Under the HR LOB CONOPS, federal agencies must obtain Human Resource Information Technology (HRIT) services for the core functions of Personnel Action Processing, Benefits Management, and Compensation Management (payroll operations) from an SSC. At a minimum, SSCs must provide HRIT services for the core functions of Personnel Action Processing and Benefits Management. Additionally, SSCs may also offer core Compensation Management (payroll operations). Other non-core functions as defined by the HR LOB Target Requirements for SSCs are not mandated. If the SSC chooses to offer services for any of the non-core sub-functions, they must meet the applicable mandatory requirements at the time such services are provided to the customer. Customer agencies may seek non-core functions from an SSC, but are not mandated to do so.

This approach allows agencies at their discretion to select services as needed to increase their focus on agency mission activities and the strategic management of human capital.

OPM expects the HR LOB to help the Federal Government realize the potential of electronic government, significantly enhance human resources service delivery for civilian employees of the Executive Branch, and realize program objectives that were established in FY 2004, as shown in Table 1:

Table 1 – HR LOB Strategic Goals and Objectives

Objectives	Goals
Improved Management Improve the governmentwide strategic management of human capital	▪ Faster decision making ▪ More informed policy making ▪ More effective workforce management ▪ Improved resource alignment with agency missions
Operational Efficiencies Achieve or increase operational efficiencies in the acquisition, development, implementation and operation of human resources management systems	▪ Improved servicing ratio/response times ▪ Reduced cycle times ▪ Improved automated reporting
Cost Savings and Cost Avoidance Achieve or increase cost savings and cost avoidance from HR solution activities	▪ Reduced duplicative software/ hardware/operations/labor resources ▪ Increased competitive environment
Improved Customer Service Improve customer services	▪ Increased accessibility to client and value ▪ Improved communication and responsiveness ▪ Enhanced quality ▪ Enhanced timeliness ▪ Enhanced accuracy ▪ Enhanced consistency

1.2 HR LOB Enterprise Architecture

HR LOB has developed enterprise architecture in compliance with the Federal Enterprise Architecture guidelines. HR LOB has completed and published the five reference models as follows, Business Reference Model (BRM), Data Model (DM), Service Component Model (SCM), Performance Model (PM), and Technical Model (TM), through the collaborative efforts of many HR professionals across government agencies. These enterprise architecture models are some of the primary sources of requirements for identity and authentication management within the HR LOB context.

The HR LOB Technical Model refers to identity and authentication in two ways. First, identity and authentication are referred to in the Component Framework Service Area (CFSA). The

CFSA consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. Security services defined in the CFSA include identity and authentication services such as digital signature, encryption, role definition, biometrics, two-factor identification, and access control.

Second, the Technical Model defines standards profiles including security profiles. The primary purpose of the standards profile is to provide inputs to the architect during the development process to populate the architecture with technologies and products that meet HR LOB requirements. Another use of the standards profile is to help ensure that solution providers get a clear statement of the technical requirements for the development of HR LOB solutions. Also, the security services standards profile view in the Technical Model defines applicable standards for encryption, certificates/digital signature, role definition, access control, authentication, and single sign-on.

1.3 Overview of HR LOB Identity and Authentication Reference Model

A reference model provides definitions and a formal structure for describing the implicit and explicit concepts and relationships in a domain and defines the framework for understanding significant relationships among the entities in that domain. Based upon this definition, the IARM objectives are:

- Establish a common understanding of identity and authentication concepts within the HR LOB context;
- Define a common language for HR LOB subject matter experts and implementers to formulate requirements for the systems;
- Facilitate identification of the priorities for architectural specifications and provide a minimal set of requirements; and
- Establish a high-level concept of operations for implementing E-Authentication in a standardized, consistent manner.

It is important to understand that though the IARM defines and describes standards, components, and services that facilitate reuse and interoperability, it does not recommend or endorse any vendor products. This reference model is not a Solution Architecture or a Segment Architecture document. It does not contain “as-is” or “to-be” system descriptions, or component models.

Lastly, the IARM makes no statements or implications about what organization structure should be instituted to support and exploit the technology, or which individuals should have particular roles, and what processes should be implemented to leverage the technology.

1.4 HR LOB Identity and Authentication Reference Model (IARM) Recomended Uses

The IARM should be used in the following ways:

- For compilation and validation of existing documentation about Identity and Authentication **as applicable to HR LOB**;
- To share with appropriate system owners and agency points of contact, and for establishing a common understanding among system owners of E-Authentication and the value it provides for agencies;
- To understand important concepts and relationships of identity and authentication elements in the HR LOB domain;
- To discover common identity and credential attributes required by OPM systems and define a standard OPM identity and credential dataset that is composed of common attributes and system specific attributes;
- To identify priorities for E-Authentication solution architectural specifications;
- To develop a solution and/or segment architecture for implementing E-Authentication in a standardized, consistent manner for governmentwide HR systems; and
- To provide feedback to the ICAM sub-committee regarding HR LOB authentication and identity attributes and the Information Exchange Package[1] that agencies and governmentwide system owners can use to achieve data integration, data standardization, and work flow integration.

1.5 HR LOB Identity and Authentication Reference Model Guiding Principles

There are five primary guiding principles for the IARM that emphasize its different aspects. These principles are:

- **Focus:** The primary focus of this reference model is the HR LOB and E-Authentication issues related to the governmentwide HR systems managed by OPM. The scope of this reference model is to address identity authentication, which is a process of establishing a degree of confidence in an individual's identity. This excludes service, network, session, and system authentications.
- **Easy to Interpret:** The IARM enables users to rapidly interpret its contents and place it within their own context. In addition, the IARM uses well-defined terms, and provides examples to enable users to distinguish between distinct but related ideas or concepts.
- **Traceability:** The IARM serves as an architectural foundation; therefore, it is well documented. By establishing traceability, users can check that this IARM covers their critical areas of interest and all applicable areas of policy.
- **Usability:** The IARM helps end-users, system developers, solution providers, and other technical personnel communicate with each other across domain and technology boundaries.
- **Independence:** By definition, the IARM is not tied to a specific application architecture, design, or implementation. Therefore, it is implementation and technology agnostic. Users and providers must be able to map their application requirements and technologies to the IARM regardless of how or when developed.

[1] Information Exchange Package (IEP) is a XML instance that contains the transaction or message-level data passed between two information systems.

1.6 Structure of the Document

The document is organized as follows:

***Chapter* 1** provides introductory information about the HR LOB Identity and Authentication Reference Model and sets the stage for the rest of the document.

***Chapter* 2** describes the high-level requirements for HR LOB identity (or identification) and authentication. Identification requirements are typically insufficient by themselves, but they are necessary prerequisites for authentication requirements. Essentially, authentication is dependant on identification.

Chapter 3 provides the details of identity and authentication related standards, their relevance and applicability to governmentwide HR systems.

Chapter 4 describes the details of the identity "object", its attribute types and attributes, Personally Identifiable Information (PII) attributes, and service components required for identity description.

Chapter 5 promotes a common understanding of authentication terminology as related to the HR LOB. This chapter also addresses different issues and concerns raised by the workgroup members regarding authentication and presents a view that is most relevant to HR LOB. It also addresses considerations for integrating authentication into OPM-managed HR IT systems.

***Chapter* 6** presents the Identity Credential and Access Management high-level diagram, and describes the potential HR LOB Identity and Authentication Solution architecture at a conceptual level, defined as architecture building blocks.

Chapter 7 describes high-level considerations and general guidance for implementation planning and solution architecture development for an E-Authentication solution for government wide HR systems managed by OPM.

Chapter 8 provides a list of all reference materials used in developing this document.

1.7 Audience

The HR LOB Identity and Authentication Reference Model is intended for use by system owners, IT managers, procurement officials, program and project sponsors, technical and system architects, security architects, systems integrators, vendors, service providers, and supporting contractors operating or interested in the HR LOB domain.

2.0 Identity and Authentication Requirements

Identity is a notion that is broadly and intuitively used and its meaning seems to be clear to everyone. Identity is related to the existence of objects, their uniqueness and distinctness from other objects. A person's identity is who or what that person is, his/her attributes such as name, date of birth, eye color, height, weight, profession, occupation, etc. Very often people are asked to prove their identity. Identity may be proven by an individual in a number of ways; for example, fingerprint, signature, or simply by showing their driver's license can prove an individuals identity. The most important aspect to keep in mind about identity is that identification requirements are everywhere, and they are increasing.

2.1 Identity and Authentication Basics

Identity is both a "real-world" concept and a digital construct. It is the dynamic collection of all attributes related to a specific entity, be it a person, enterprise, or object. An identity is what allows one entity to be distinguished from another. Digital Identity is defined as "*data that uniquely describes a person or a thing (called the subject or entity in the language of digital identity), but also contains subjects' relationships to other entities*.[2]" Identity spans many different contexts and purposes, for example, people have multiple individual identity relationships (one with the employer, one with the bank, possibly several with the many different parts of government). There are also role-based identities – a by-product of current employment, or position. Personal identities are more complex than just a person's name, driver's license number, or fingerprint.

Authentication is an essential element of information system security requirements. It is the process of confirming the identity of a user (or in some cases, a machine) that is trying to log on or access technology resources. Essentially, authentication is dependant on identification. Therefore, identification requirements are necessary prerequisites for authentication. The typical objectives of authentication are to validate and verify that an identity is representative of a specific person or their claims and avoid compromising security to an impostor.

It is easy to confuse authentication with authorization, which is another element to be considered in regards to information systems security. While authentication verifies the user's identity, authorization verifies that the user has the correct permissions, rights, and qualifications to access the requested resource. The term **identity authentication**, as it is used throughout this reference model, refers to the process whereby an organization establishes its degree of confidence in an assertion that a person is who they claim to be. Ultimately, the underlying idea is that authentication occurs before authorization.

2.2 Requirement Drivers

Given that authentication and identification are distinct but related concepts, it is important to understand the interplay between them. It is essential to develop authentication systems whose

[2] "How can a Person's Digital Identity be managed and protected?: Peter Topalovic, SEP 707: Dec 14 2007"

strength (and often therefore whose intrusiveness into privacy) is in line with the security needs of and threats to the resources being protected.

Business drivers relevant to identity and authentication include:

- The need to protect the assets and services that serve the agency and support its operations;
- Legal and regulatory compliance including the rules and policies imposed by regulatory entities;
- Direct or indirect loss (financial, credibility, etc.) to the business as a result of a security incident such as identity theft or data theft;
- Need to protect sensitive personal information;
- Different levels of authentication required by different applications; and
- Interoperability of authentication, authenticated identities, and related attributes across diverse target systems or domains.

2.3 Identity Requirements

Identification requirements are everywhere, and increasing in number and complexity. In the online digital environment, however, the identity challenges are greater, since identification demands are becoming more frequent. The Federal Identity Management Handbook provides implementation guidance for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with Homeland Security Presidential Directive (HSPD)-12 and Federal Information Processing Standards (FIPS) 201. Personal information collected for employee and contractor identification purposes must be handled in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a). Also, identity and identification requirements must be consistent with privacy requirements, which may require the anonymity of users. These requirements should **not** be specified in terms of the types of security architecture mechanisms that are typically used to implement them.

HSPD-12 establishes control objectives for secure and reliable forms of identification. Federal departments and agencies should implement governmentwide identity proofing, registration, and issuance functions that accomplish the following:

- Identification is issued based on sound criteria for verifying an individual employee's identity;
- Identification is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Identification can be rapidly authenticated electronically; and
- Identification is issued only by providers whose reliability has been established by an official accreditation process.

An identity assertion in this context should have the characteristics listed in the following table:

Table 2—List of Identity Assertion Characteristics

Characteristic	Description
Accessible	Available when required
Assignable	Assign when needed by trusted authority after properly authenticated request
Atomic	Single data item—no sub-elements having meaning
Concise	As short as possible
Content-free	Does not depend upon content of other fields in the record
Controllable	Only trusted authorities have access to linkages between encrypted and non-encrypted identifiers
Have Longevity	Designed to function for foreseeable future with no known limitations
Secure	Can encrypt and decrypt securely
Standard	Compatible if possible with existing or emerging standards
Unambiguous	Minimizes risk of misinterpretation such as confusing the number zero with letter O
Unique	Identifies one and only one individual
Universal	Able to support every living person for the foreseeable future
Usable	Can be processed by both manual and automated means
Verifiable	Can determine validity without additional information

These characteristics can be interpreted as the following implementation requirements:

- All users must have a unique and individual identity;
- Identity must never be shared, transferred or used by more than one person;
- The identity should also be non-forgeable so that one person cannot impersonate another;
- An identifier should contain only alphabetic and numeric characters and should not contain any special characters;
- Technical identity systems MUST only reveal information identifying a user with the user's consent; and
- The system must also protect the user against deception, verifying the identity of any parties who ask for information.

2.4 Authentication Requirements

Authentication is the process where an entity provides the proof that validates who it is claiming to be. In many cases it is technically accurate to separate identification and authentication into two distinct processes. However, the importance of selecting an environment-appropriate authentication method is arguably the most crucial decision in designing secure systems. The following are some of the factors that should be considered when designing or selecting an authentication system:

- Authenticate only for necessary, well-defined purposes;
- Minimize the scope of the data collected;
- Minimize the retention interval for data collected;
- Minimize the intrusiveness of the process;
- Minimize the personally identifiable information collected;
- Ensure that the use of the system is audited and that the audit record is protected against modification and destruction; and
- Provide means for individuals to check on and correct the information held about them that are used for authentication.

The assurance level of an authentication mechanism depends on the extent of protections against abuse, and hence on whether it can be effectively repudiated by the entity concerned. OMB guidance, *E-Authentication Guidance for Federal Agencies*, OMB 04-04 defines four levels of authentication (Levels 1 to 4), in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance (weakly authenticated) and Level 4 is the highest (strongly authenticated). National Institute of Standards and Technology Special Publication (NIST SP) 800-63 provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. Also, NIST SP 800-63 defines technical requirements for each level of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions. This technical guidance can be summarized as follows:

- For low-impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable;
- For some moderate-impact information systems where potential impact is only inconvenience, distress, or some financial loss, tokens that meet Level 2, 3, or 4 requirements are acceptable but all other moderate-impact systems, tokens that meet Level 3 or 4 requirements are necessary; and
- For high-impact information systems, tokens that meet Level 3 or 4 requirements are mandatory[3]

Organizations should note that different combinations of authentication methods can have different characteristics. For example, the overall authentication strength of a compound

[3] Burr, Bill; Polk, Tim and Dodson Dona; National Institute of Standards and Technology (NIST). *Special Publication 800-63: Electronic Authentication Guideline.*

authentication method depends not only on the authentication strength of each component but also on *how* they are combined. The Federal Identity, Credential, and Access Management (FICAM) Implementation and Roadmap Guidance document describes transition activities associated with the implementation of the target identity, credential, and access management (ICAM) segment architecture.

The following table provides a summarization of the high-level requirements for E-Authentication:

Table 3—High-Level Requirements

High-Level Requirement	Summarization
Practical	Easy to use and non-intrusive
Appropriate level of security	With respect to both the cost and sensitivity of the system
Location Transparency	Ability to authenticate remote users
Protocol Insensitivity	Assurance that those authentication systems and various servers interoperate
Appropriate Level of Privacy	Lower-level users should be restricted from seeing higher- level data
Reliability	All data should be trustworthy. This is a must, because intrusion into an authentication system can be the foundation for access to mission-critical resources
Auditability	Accountability must be ensured. This means making logs at various levels and tracking and protecting these logs
Manageability	Easy to manage – meaning that users/licenses/certificates should be easily added, updated, or deleted
Federation support	Must support federation identity management requiring confidence in the partner organization. The federation provides a standardized means for allowing agencies to directly provide services for trusted users that they do not directly manage. A *federation* is defined as a "group of two or more trusted partners with business and technical agreements that allow a user from one federation partner to seamlessly access information resources from another federation partner in a secure and trustworthy manner.

3.0 Standards and Best Practices

The growth in distributed computing and a continued increase in computer crime have led to legislation and regulations that have established the legal requirements for identity management, authentication, and data security. The various network security standards outlined by the American National Standards Institute (ANSI), Federal Information Processing Standards (FIPS), and the International Organization for Standards (ISO) have undergone extensive peer review and represent the strongest security design thinking available. Use of standards-compliant identity and authentication systems provide the best assurance of high quality and strong security for both personal information and transaction data.

The National Institute of Standards (NIST), Office of Management and Budget (OMB), and other Federal entities has promulgated a number of E-Authentication and identity management standards and requirements. Also driving Federal authentication requirements is Homeland Security Presidential Directive/HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 directed the promulgation of a new Federal standard for secure and reliable identification issued by Federal agencies for their employees and contractors. The HSPD-12 initiative provides a common, standardized identity credential that enables secure, interoperable online transactions.

3.1 Standards Applicability

Standards and best practices should be adopted to achieve improved security and interoperability, and assurance of continued availability of service. Exceptions to standards and best practices may be considered only when a non-conforming technology is essential to fulfill an organization's role and mission.

It is with a holistic understanding of the identity and access management environment that the Chief Information Officers Council established the Identity, Credential, and Access Management Subcommittee (ICAMSC) with the charter to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. A document[4] has been developed in support of the ICAM mission to provide a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs.

3.2 Mandatory Standards

The HR LOB Shared Service Centers (SSC) and agencies are responsible for implementing and administering E-Authentication programs consistent with Federal policies and guidance to ensure electronic transactions conducted by the SSC provide the appropriate level of assurance and protection. Federal Information Processing Standards (FIPS) 200, *Minimum Security*

[4] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 1.0, October 2009

Requirements for Federal Information and Information Systems, states that organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the guidance provided in NIST SP 800-53.[5]

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, defines security control IA-2, User Identification and Authentication, as follows:

> "Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems.[6]"

For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter, which is considered to offer sufficient protection, NIST SP 800-63 guidance should be applied as required.

3.3 Open Standards

The HR LOB will use open standards wherever possible when attempting to standardize any component of HR LOB Enterprise Architecture such as data entities, attributes, information exchange packages, or service components. Open standards are standards made available to the general public and are developed, approved, and maintained via a collaborative consensus-driven process. An open standards-based architecture for identity management and authentication helps to lower total cost of ownership while providing maximum flexibility and choice. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. The deployment and the use of solutions and products based upon open standards provides flexibility and vendor independence.

There are a number of organizations that create and publish open standards for identity and authentication. The major organizations that are actively developing identity and authentication related open standards are the following:

- **American National Standards Institute (ANSI)** – ANSI is a voluntary standardization organization whose purpose is to administer and coordinate standardization efforts in the private sector.

[5] Some organizations may use other documents for guidance instead of NIST publications. For example, Department of Defense may use guidance such as DOD Information Assurance Certification and Accreditation Process.

[6] Ross, Ron, et al; National Institute of Standards and Technology (NIST). *Special Publication 800-53: Recommended Security Controls for Federal Information Systems*. February 2005. Page 4.

- **National Institute of Standards (NIST)** – NIST, publisher of the Federal Information Processing Standards (FIPS), was formed under the Information Technology Management Reform Act (Public Law 104-106) and authorizes the Secretary of Commerce to approve standards and guidelines for Federal computer systems.
- **International Standards Organization (ISO)** – ISO is a worldwide federation of national standards bodies from some 140 countries whose mission is to promote the international development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements, which are published as international standards.
- **World Wide Web Consortium (W3C)** – The W3C's purpose is to develop interoperable technologies (standards, specifications, guidelines, software, and tools) for the Internet.
- **Open Authentication Standards Initiative** – The Initiative for **Open Authentication (OATH)** (http://www.openauthentication.org) is a collaborative effort of IT industry leaders aimed at providing reference architecture for universal strong authentication across all users and all devices over all networks. OATH-compliant vendors support innovation and encourage consumer adoption while providing interoperable services without the cost, complexity and vendor-lock of proprietary solutions.
- **The Liberty Alliance Project** – The Liberty Alliance Project is a global consortium for open federated identity and Web services standards. It is focused on developing open specifications for interoperable strong authentication. Liberty has specified an open standard for federated network identity that is intended to support current and emerging network devices, offering a secure way to control digital identity information. The Liberty Alliance Identity Federation Framework (ID-FF) Version 1.2 Specifications are now part of SAML v2.
- **OASIS (Organization for the Advancement of Structured Information Standards) --** OASIS consists of identity management platforms and technical committees whose principal interest include: Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), Service Provisioning Markup Language (SPML), eXtensible Resource Identifier (XRI), and Web Services Security (WS-Security).

Key standards and protocols for identity and authentication are:

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors -- This standard defines a reliable, governmentwide PIV system for use in applications such as access to federally controlled facilities and information systems. This standard specifies a PIV system within which common identification credentials can be created and later used to verify a claimed identity. The standard also identifies Federal governmentwide requirements for security levels that are dependent on risks to the facility or information being protected.

Security Access Markup Language (SAML) -- SAML 2.0 is now considered the dominant framework for browser-based identity federation. SAML defines an **eXtensible Markup Language** (XML)-based framework for security and identity communication between systems

and is security infrastructure independent in that it does not rely on any particular architecture such as Public Key Infrastructure, Kerberos or Lightweight Directory Access Protocol. It does not, however, standardize all aspects of security management, dealing with the secure communication of identity information. An *assertion* is a piece of data produced by a SAML authority referring to either an act of authentication performed on a user, attribute information about the user, or authorization permissions applying to the user with respect to a specified resource. SAML describes data format in XML as well as protocol for exchanging authentication and authorization information between security systems.

Security Provisioning Markup Language (SPML) -- Security Provisioning Markup Language (SPML) is an XML-based framework specification for exchanging user, resource, and service provisioning information. SPML is being developed with consideration of the following provision-related specifications: Active Digital Profile (ADP), eXtensible Resource Provisioning Management (XRPM), and Information Technology Markup Language (ITML).

eXtensible Access Control Markup Language (XACML) -- XACML is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. Also, XACML is a security standard which allows developers to write and enforce information access policies, making it a key component in the development of authorization infrastructures and a foundational step in the creation of federated authentication environments.

The XACML specification describes both an access control policy language (which allows developers to specify who can do what and when), and a request/response language, which expresses queries about whether a particular access should be allowed, and describes the answers to those queries.

WS-* -- Is a collection of specifications describing mechanisms for authentication, authorization, policy, and security within single domains and across multiple domains in order to enable secure web services. It is intended to be a "composable" architecture in that selected elements can be implemented to support organizational requirements. It includes such aspects as WS-Trust, WS-Federation, WS-Policy, and WS-Security.

3.4 Best Practices

A **best practice** is a technique, method, process, activity, incentive, or reward that is believed to be more effective at delivering a particular outcome than any other technique, method, process, etc., when applied to a particular condition or circumstance. Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people[7]. Some of the best practices for identity and authentication management followed in the information systems security industry are summarized below.

[7] "Best practice - Wikipedia, the free encyclopedia."

- **Establish sound identity and authentication policy:** Identity management is more than simply permitting a user to log on; it controls what that user can do, similar to putting boundaries on where a person can go once in a building. Like building security, identity management is the most essential form of information protection that agencies use. Yet, it also is among the information security practices that are least used or properly implemented. Beyond the technology, agencies need policies for ensuring that user identities and authentication are managed properly. All authentication techniques used should be governed by policy (e.g., password policy, remote access policy, certificate policy). Therefore, a comprehensive authentication policy, which dictates the use of mechanisms or practices to validate user identity per system and/or application should be developed and documented.
- **Monitor access:** Consistent monitoring of how resources are accessed by employees and contractors is a good practice to detect improper usage of identity and breaches in authentication. It is a good design-principle to externalize identity management and authentication. Every application or business service having its own identity management and authentication leads to a suboptimal solution, more overhead, and greater chance for security breaches.
- **Use open standards to promote interoperability:** Open standards promote interoperability using security (identity and authentication) standards such as LDAP(S), HTTPS, SAML, XML, DSIG, WS-Security (WSS), and other WS-* standards. This results in secured services being reused by (both internal and external) heterogeneous infrastructures. Next to technical standards there are also a number of security reference architectures, principles, and guidelines that organizations can leverage, for example, using a centralized identity management repository. This avoids duplicate user management and possible inconsistencies.
- **Define and manage limited set of authentication levels:** Define a limited set of authentication levels and differentiate on information (password), possession (token, physical key, text message to a phone), and attribute (voice, fingerprint) as mechanisms for authentication. Use multi-factor authentication when a strong password policy causes users to take actions which weaken security such as writing passwords down; or causes users to constantly forget passwords.
- **Perform enterprise risk-analysis before implementing single-sign on:** Most organizations promote Single Sign-on (SSO) to improve user-friendliness and provide for better user-experience. However, SSO can create vulnerability by making a single entry mechanism the key to access multiple applications. If one is compromised, all are compromised. To mitigate this risk, organizations must ensure passwords are changed regularly; lost or stolen authenticators are promptly reported and cancelled; and invalid credentials do not allow access to the system to keep authentication mechanisms effective.
- **Manage stakeholders:** ICAM implementation roadmap defines stakeholder management and accreditation as two important practices that should be followed for identity, credential, and access management. It is critical to identify all stakeholders, not just those who may be positively affected by the project. The stakeholders affected may include employees, unions, application owners, industry partners, system integrators, user

populations, solution providers, partners, and other affiliates. These stakeholders will likely have very different viewpoints that may conflict with one another or the program objectives. Therefore, stakeholder management and collaboration is essential to incorporate a holistic approach for ICAM implementation.

- **Obtain security accreditation:** Accreditation is an important aspect of any ICAM initiative not only because of the security and regulatory requirements, but also because of the scheduling and cost impacts resulting from the process. Accreditation provides accountability for adverse impacts that might occur as a result of a security breach, thus challenging responsible parties to implement the most effective security controls allowable within resource constraints.

4.0 Identity Considerations

Identity is information about an entity (person). When physical identity is represented using a digital format it is known as electronic or digital identity. In this document, "identity" refers to "digital identity". Establishment of an identity typically begins with collecting identity data as part of an on-boarding process. An identity is typically comprised of a set of attributes that when aggregated uniquely identify a user within a system or an organization. Today, many application owners and program managers create an identity in order to enable application-specific processes. The most important characteristic of an identity is that it is referential. An identity is not a person; it is only a reference to a person.

4.1 Identity Overview

Identity begins with an assertion (explicit or implicit) that one is a certain person or has a certain characteristic, and is not someone else with other characteristics (authentication). It is relational, including that which a person says about himself and that which others say about that person (reputation or accreditation). Identity is a context-sensitive and multidimensional concept. Yet many identity solutions seem to assume a simple, monolithic model architected on the assumption of a universal identity that can be used for all interactions. Individual identities are more complex than just the name, driver's license number, or fingerprint. Rather, identity is the synthesis of many factors that are constantly changing and evolving.

An **identifier** is unique; it identifies a distinct person, place, or thing within the context of a specific namespace. An identifier is *an attribute that uniquely represent*s *an entity within a specific context*. An identifier is also referred to as *name, label,* and *designator*. One identity can have multiple identifiers, for example, a person has a Social Security Number (SSN) and can have an employee ID number as well. Each identifier is meaningful only in a specific context or namespace, and can reasonably be thought of as having a <thing identified, identifier> pair.

Identifiers are building blocks of identification. These are facts that distinguish people and identities from one another (same as characteristics or attributes used for sorting or categorizing entities). Identifiers are classified as follows:

- **Something-you-are:** Inherent characteristics (mostly) attached to physical body, e.g. DNA. These are known as biometrics and are further categorized into physiological and behavioral.
- **Something-you-are-assigned:** Socially defined titles such as names and addresses. These identifiers are not unique and are subject to change.
- **Something-you-know:** Some distinct knowledge such as password, or mother's maiden name. Known as epistemetric identification, the knowledge of a person is compared to what he/she is supposed to know given her alleged identity (Fact-Checking).
- **Something-you-have:** Possessing some distinct item such as an identity card (also called 'token'). Tokens are physical objects that help identify their bearer (e.g., driver's license, access cards, etc.).

A certificate is an electronic data structure used to identify an individual, a server, a company, or some other entity, and to associate that individual's identity with a public key and an associated private key. Like a passport, a certificate provides generally recognized proof of an entity's identity. Today, even though it was not originally intended to be used that way, the SSN is commonly used as a personal identifier and authenticator throughout the country and all levels of government. However, other attributes such as the Federal Agency Smart Credential – Number (FASC-N) are being promoted as a unique alternative for employee identification. The FASC-N is part of the Cardholder Unique Identifier (CHUID) and is the primary identification string to be used on all government issued credentials. The CHUID is designed to provide the basis for interoperable identification of individuals and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. Ultimately, the full FASC-N has 17 separate fields, and does not include SSN.

Authorizations allow the individual to access system resources. These are not identity attributes but authorization may depend upon the value of an identity attribute. For example, an identity attribute value "Active" may have different authorization than that of "Retired". Authorization is assigned by an authorization authority and depends upon system access policies.

There are different types of identities based upon their context and usage. *Role-based identities* are based upon the job, position, or responsibilities. Equally, there are *group identities* ranging from families through to companies. The concept of *enterprise identity* covers those specific aspects of the digital representation within the context that the enterprise needs to manage. Enterprise identity could cover Personally Identifiable Information (PII), roles, relationships, accounts and related access, physical assets and privileges/entitlements.

Federated identity is another important concept used in Services-Oriented Architecture (SOA) environments. Federation is the mechanism that enables the portability of identity attributes across autonomous security domains. To an individual user, *federated identity* means the ability to associate various application and system identities with one another. In information technology terms, federated identity means the virtual reunion, or *assembled identity*, of an individual's user information (or principal), stored across multiple distinct identity management systems. Federated identity is the "glue" that enables Internet Single Sign On to occur across many identity providers and service providers.

4.2 Identity Attribute Types

An **attribute** is a characteristic associated with an identity. An attribute can be **intrinsic** (i.e., belongs by nature), or **extrinsic** (i.e., acquired from the outside). Examples of intrinsic attributes include race, eye color, biometrics (e.g., fingerprints). Examples of extrinsic attributes include family name, first name, and address. An attribute can be **persistent** or **temporary**. Examples of persistent attributes include height, eye color, and date of birth. Examples of temporary attributes include address, employer, and organizational role. A SSN is an example of a long-lived attribute. Some biological attributes are persistent (e.g., fingerprints); some change over time or can be changed (e.g., hair color).

Identity attributes can be classified into many different types based upon the usage and view point as follows:

- Profile attributes
- Credential attributes
- Provider-specific attributes
- Transactional attributes

Profile attributes are the information specific to the user identity that establishes uniqueness of the person. These are name (first or given name, middle name, surname, or last name), SSN, and employee ID. In addition, other related characteristics such as e-mail and home address, birth date, and telephone number, but may not be primarily tied to authentication or authorization decisions, are included in profile attributes. Identity profile attributes also include preference or personalization attributes such as a user's frequent flier number, location information, preferences, and subscription information (e.g., newspaper, magazine, etc.). This information may be used as part of secondary user identity validation (e.g., as part of a lost password recovery process)[8].

Credential attributes or authentication credentials are the information used to authenticate an identity. This information is bound to a user's identifier such as a logon or user name. The authentication credentials themselves are represented by data such as a password or a one-time-generated PIN number from hardware token. These credentials are presented by a user as part of the authentication process, which proves (i.e., authenticates) the user's claimed identity. This implies that to authenticate a user, a federation business partner must have a copy of the user's authentication credentials, or some other means of validating the user's authentication credentials. Thus, current models of authentication require a distinct identity data model, meaning that each federation business partner has a copy of the user's authentication credentials[9].

Provider specific attributes include both transactional and profile attributes that are relevant for a given user at a given service provider; these attributes have not been shared with other service providers. A user's provider-specific attributes are distinct attributes that are not shared across federation business partners and are not required to be managed through a provisioning solution across business partners. Examples of provider-specific transactional attributes may include a user's buying history maintained with an online auction house and the bonuses (free shipping) associated with this user's transaction history[9].

Transactional attributes include information that describes a user and his affiliations and entitlements. This information is bound to a user's identifier. This may include groups that the

[8] "Federated Identity Management." *The Business Forum - Executive Meetings, Conferences, Business Luncheons - Round Table Discussions - World Information*.

user belongs to or roles that he can assume. This data may also include additional identifiers (e.g., customer ID number, 401K account number, frequent flier status level, health care number, supplier ID, or billing or credit card number, etc.), specific organizational roles (e.g., HR manager, stock broker, benefits administrator, primary care physician, executive, supervisor, travel exception approver, etc.). This information is often used as part of authorization/access control decisions at the transactional level (e.g., can this HR manager update this employee's personnel evaluation). In general, a user's transaction attributes are not common across all identity and service providers, and only some of these attributes are relevant to multiple identity/service providers[9].

4.3 Identity Attributes

Attributes are the core unit of identity data. They have many representations in many systems as data elements, but refer to a single piece of information that represents some characteristics of an identity. To support business-to-business service provision, a person may have one or more credentials in one authentication domain. Identity attributes must support multiple credentials. Clearly distinguishing different types of attributes like profile versus credential will clarify use of data, help meet privacy legislation, and ease the introduction of new authentication techniques to replace passwords.

The following table provides a list of attributes associated with identity that are typically required for authentication.

Attribute Name	Attribute Type	HR LOB DRM Code Table Name	Backend Attribute Interface Specs	Remarks
Given Name	Profile	Person Name Given	PersonGivenName	
Middle Name	Profile	Person Name Middle	PersonMiddleName	
Surname	Profile	Person Name Family	PersonSurname	
Name Prefix	Profile	Person Name Prefix	*	
Name Suffix	Profile	Person Name Suffix	PersonNameSuffixtText	
Unique Identifier	Profile	Employee ID	*	
Social Security Number	Profile	Person Social Security Number	*	
Gender	Profile	Person Gender Code	PersonSexCode	

[9] "Federated Identity Management." *The Business Forum - Executive Meetings, Conferences, Business Luncheons - Round Table Discussions - World Information*.

[*] At this time there is no data for the related field.

Attribute Name	Attribute Type	HR LOB DRM Code Table Name	Backend Attribute Interface Specs	Remarks
Date of Birth	Profile	Person Date of Birth	PersonBirthDate	
Citizenship	Profile	Person	PersonCitizenshipCode	
User Id	Credential	*	*	May have multiple instances
Password	Credential	*	*	May have multiple instances
Password Expiration Date	Credential	*	*	
FASC-N	Credential	*	FASC-N	
Fingerprint Image	Credential	*	FingerprintImage	
Face-Photo Image	Credential	*	Photo	
Digital Signature Certificate	Credential	*	DigitalSignatureCertificate	
Card Authentication Certificate	Credential	*	CardAuthenticationCertificate	
Organization Affiliation	Credential	Employee Organization ID	OrganizationalAffiliation	
PIV card Issue Date	Credential	*	CardIssueDate	
PIV card Expiration Date	Credential	*	CardExpirationDate	

Table 3 – List of Identity Attributes

4.4 Personally Identifiable Information

OMB has issued several memoranda to provide Federal agencies guidance on the protection of Personally Identifiable Information (PII) entrusted to them. For example, OMB memorandum M-07-16 states that safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public; however, all PII is not considered sensitive. The Department of Homeland Security (DHS) defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. It further defines Sensitive PII as personally identifiable

information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual[9].

OMB memorandum M-06-19 defines sensitive PII as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual[10]."

Essentially, information containing name, SSN, alien registration number (A-Number), or biometric identifiers about a person is considered sensitive PII. The following information is also considered sensitive PII when grouped with a person's name or other unique identifier, such as address or phone number:

- Citizenship or immigration status;
- Medical information;
- Driver's license number;
- Passport number;
- Full date of birth;
- Authentication information such as mother's maiden name or passwords;
- Portions of SSN's such as last four digits; and
- Financial information such as account numbers.

Additionally, the context of the PII may determine if it's sensitive, such as a list of employee names with poor performance ratings.

4.5 Identity Service Components

The FICAM Roadmap and Implementation Guidance document describes the following identity service areas:

Identity Proofing: Provides capabilities of verifying necessary and sufficient information (e.g., identity history, credentials, and documents) for establishing an individual's right to a claimed identity; initiates a chain of trust in establishing a digital identity and binds it to an individual.

Vetting: Provides capabilities for the collection, examination, evaluation, and establishment of verified credentials and attributes.

Adjudication: Provides the capability of reviewing identity vetting results and determining eligibility for an identity credential.

[9] "Safeguarding PII" Homeland Security, The DHS Privacy Office – Presentation
[10] Evans, Karen. "Office of Management and Budget." *OMB memoranda M-06-19*, July 2006

Digital Identity Lifecycle Management: Supports the process of establishing and maintaining the attributes that comprise an individual's digital identity; support general updates to an identity such as a name change or biometric update.

Identity Attribute Discovery: Maps pathways and creates indexes or directories that allows identification of Authoritative Data Sources (ADS) within identity data.

Linking/Association: These are the processes of linking one identity record with another across multiple systems; activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to an automated or interactive process; used in conjunction with Authoritative Attribute Exchange. Linking/Association services provide capabilities for managing the account linking based upon a common unique identifier for the user, which can be bounded with the internal, local user identity at the service provider.

Authoritative Attribute Exchange: Provides the capability to connect various ADS's and share identity and other attributes with the shared infrastructure.

In addition to the above services, in a federated identity model, one or more dependant parties and service providers enter into a trust together, where assertions made by one party are recognizable and verifiable by the other parties. Federation protocols and standards, such as SAML, Liberty ID-FF, and WS-Federation, allow for identity information to be transferred across domain contexts. Therefore, the following additional services may be needed to manage context sensitive identity information that is exchanged. These services are:

Identity/Attribute Mapping Services: Define attributes to be shared and the mapping of them between the two partner systems. In distributed systems, identities are communicated and transformed in a variety of ways. Identity mapping services are used to manage these relationships when identity attributes, are mapped onto other principals.

Trust Services: Ensure the security of connections, transport, messages and tokens.

Integration Services: Aggregates identity-related information from multiple data-sources based upon a meta-directory. A meta-directory is a centralized service that joins and rationalizes identity data from multiple databases and directories in an organization. Identity integration services are typically needed when an organization has multiple directories or identity stores. Since each of these directories contains a subset of all the information about a user, identity integration services can help by creating an aggregate view of the information from all the identity stores. Identity integration services create this aggregate view by pulling identity information from a variety of authoritative sources, such as existing directories, HR and accounting applications, e-mail directories, and various databases.

Identity Data Synchronization Services: Synchronizes identity data across a wide range of heterogeneous apps, directories, databases, and other stores.

Identity Runtime Services: Virtualizes the authoritative source of the identity information so the developer does not have to know implementation details about where and how the identity information is stored. The typical runtime services provided by an identity abstraction layer can include query services for applications to query the abstraction layer to validate and exchange identity information; as well as communication services to encapsulate, negotiate, transform, and propagate identity information.

5.0 Authentication Considerations

In theory, authentication is relatively simple: A user provides some sort of credentials, a password, smart card, fingerprint, or digital certificate, which identifies that specific user as the individual who is authorized to access the system. There are, however, many methods and protocols which can be used to accomplish this. Regardless of the method, the basic authentication process remains the same.

Traditionally, authentication has been defined by different authentication factors, corresponding to the different credentials used. The following demonstrates some of the factors and their corresponding credentials:

- Something known only to the user — like a password;
- Something held by only the user — for example, a token, such as a One-Time Password (OTP), or an identity card; and
- Something inherent only to the user — that is, a biological or behavioral biometric trait, such as face topography, a fingerprint, or typing rhythm.

Authentication is the process of establishing confidence in the truth of some claim. Also, it is important to note that both identifiers and attributes can be authenticated. The following is a list of examples of different software and hardware authentication methods:

- User name and password
- Personal Identification Number (PIN)
- X.509 digital certificates
- One-time passwords
- Biometrics (fingerprint, iris scans, etc.)
- Smart cards
- Electronic passport
- Hardware tokens

However, all these techniques are not equally robust. The most robust techniques (needed for highly secure applications) use cryptographic mechanisms to protect user credentials and authentication sessions while credentials are transferring across the network.

5.1 Authentication Taxonomy

More and more organizations are looking for authentication methods that are stronger than one-factor credentials such as simple passwords. During the past few years, the variety of authentication methods has increased significantly, making it more difficult for organizations to do the following:

- Select new authentication methods that are appropriate for their needs; and
- Ensure like-to-like comparisons of different authentication products and services.

For organizations to resolve the difficulties with authentication methods, it is imperative that there is a thorough understanding of the authentication taxonomy. Organizations should know the different processes and phases of authentication, as well as the components and assurance levels necessary to meet their requirements. The following terms provide a brief description of those processes, phases, components, and assurance levels:

Identity authentication—is the process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual. For example, verification of the password associated with a Hotmail account authenticates an identity (foo@example.com) that may not be possible to link to any specific individual. Identity authentication happens in two phases:

- An identification phase, during which an identifier to be authenticated is selected in some way (often the identifier is selected by a claimant); and
- An authentication phase, during which the required level of confidence is established (often by challenging the claimant to produce one or more authenticators supporting the claim that the selected identifier refers to the identity).

Attribute authentication—is the process of establishing an understood level of confidence that an attribute applies to a specific individual. Attribute authentication happens in two phases:

- An attribute selection phase, during which an attribute to be authenticated is selected in some way; and
- An authentication phase, during which the required level of confidence is established, either by direct observation of the individual for the purpose of verifying the applicability of the attribute or by challenging the individual to produce one or more authenticators supporting the claim that the selected attribute refers to the individual.

Identity Proofing—is the process of validating the claimed identity of an individual. It is central to a secure and authoritative process for the issuance and use of identity credentials. Identity proofing can be accomplished through a variety of processes that establish a history of identity by collecting identity information (e.g. personal, demographic, and biographical information); validating the accuracy and legitimacy of the information collected by conducting a face-to-face interaction; and/or verifying the validity of identity source documents against third-party databases.

Level of Assurance—describes the degree of certainty that the user has presented a valid set of identifier attributes (credentials, etc.) that refer to his or her identity. In this context, assurance is defined as: the degree of confidence in the vetting process used to establish or validate the identity of the individual to whom the credential was issued. Therefore, to establish a degree of confidence, the person who accepts the credential should have assurance that the provider is the individual to whom the credential was issued.

Assertion based authentication typically addresses lower levels of assurance (i.e., levels 1 and 2) where PINs and passwords are used by end users. The end user authenticates to a selected

Credential Service (CS), which in turn asserts their identity to the appropriate Relying Party (RP). Certificate based authentication typically addresses higher levels of assurance (i.e., levels 3 and 4) where X.509 digital certificates in a Public Key Infrastructure (PKI) are used by end users. Certification Authorities issue X.509 certificates to end users. The end user authenticates to a selected CS, which in turn asserts the end user identity to the appropriate RP. In general, the Federation leverages Federal Public Key Infrastructure (FPKI) efforts, such that FPKI-compliant credentials can be used at the higher identity assurance levels.

Authentication Service Component (ASC)—is an E-Authentication infrastructure implemented as a federated architecture. The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards, and policies. The ASC accommodates assertion-based authentication and certificate-based authentication. Assertion-based authentication uses passwords and PINs. Certificate-based authentication uses PKI certificates. Technical details of the ASC are described in the document "Technical Approach for the Authentication Service Component" published by the GSA.

5.2 Two Factor / Multi Factor Authentication

Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of an individual. In contrast, single factor authentication (SFA) involves only a user ID and password. In two-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

Federal agencies classify electronic transaction into 4 levels that are needed for authentication assurance according to the potential consequences of an authentication error.

- Level 1
  - Single factor: often a password; password must be masked
  - Types of tokens allowed: Passwords and PINs, Soft crypto token, One-time password device, and Hard crypto token
  - Protected against on-line guessing and replay
  - Moderate password guessing difficulty requirements
- Level 2
  - Single factor
  - Requires secure authentication protocol
  - Fairly strong password guessing difficulty requirements
  - Types of tokens allowed: same as Level 1
  - Protected against on-line guessing, replay, and eavesdropping
- Level 3
  - Multi-factors required either a single multi-factor token or multi-token solutions
  - Must resist eavesdroppers
  - Types of tokens allowed: only Soft crypto token, one-time passwords, and Hard crypto token

  - Protected against on-line guessing, replay, eavesdropping, verifier impersonation, active network attacks, and man-in-the-middle attack[11]
- Level 4
  - Types of token allowed: Only hard crypto token
  - Protection against on-line guessing, replay, eavesdropping, verifier impersonation, active network attack, man-in-the-middle attack, session hijacking, and malicious host software

There are three ways of authenticating an individual, based on what are known as the factors of authentication: something the individual knows, something the individual has, or something the individual is. Each **authentication factor** covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.[12]

Security research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

- The **ownership factors**: Something the user **has** (e.g., wrist band, ID card, security token, software token, phone, or cell phone)
- The **knowledge factors**: Something the user **knows** (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))
- The **inherence factors**: Something the user **is** or **does** (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

Each authentication factor when used alone has inherent weaknesses that can be exploited. Strong authentication is achieved by using two or more authentication factors.

Multifactor authentication uses a combination of two or three different ways to authenticate an identity. The first is based on something known to the user, usually a password, but can also include your response to a challenge question, known as Knowledge Based Authentication. The second is based upon something held by the user. This could be a physical device, for example, a smart card with a chip in it or a hardware token that generates one-time-only passwords. The third is based upon something inherent to the user, as indicated by some biometric such as a fingerprint or an iris scan. Almost every multifactor approach uses a password, and then combines this with the second or the third factor or both[13].

[11] Man-in-the-middle Attack – NIST SP 800-63: An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.
[12] Authentication Factor explanation from the Wikipedia
[13] eWEEK. "What Is Multifactor Authentication? - Finance IT from eWeek." *Technology News, Tech Product Reviews, Research and Enterprise Analysis - eWeek*.

A true or an ideal two-factor system requires that the two authentication factors both be compromised before security can be breached. It also requires that the compromise of one factor not help an attacker to compromise the other factor more easily. Otherwise, it would defeat the purpose of using two authentication factors in the first place. While these requirements seem fairly self-evident and obvious, they are seldom met in real-world systems.

However, many users favor convenience to security, so they choose passwords that can be easily compromised. To address this issue, multifactor authentication uses a combination of components to provide secure access to network resources. These components include a device that the user has, such as a biometric characteristic or hardware token, and something the user knows, such as a PIN. Smart cards are an increasingly popular form of multifactor authentication.

Multifactor authentication is expensive. The initial outlays for tokens, password generators, biometrics and even authentication servers are high, while ongoing support costs often outstrip the already high help-desk costs for retrieving and resetting passwords. The problem is that the deployment of multifactor authentication, even in the financial sector, is not organized. Most online banking security considers details of a user's computer as an additional authentication factor, tracking things like the user's IP address, browser, and software settings. If those aren't recognized, users face challenge questions. An attacker could spend five minutes on a Facebook page, however, and figure out answers to most of these questions. Within the broader enterprise market, adoption is painfully slow, and it's mostly token-based. End users balk at tokens, though, because they're easily lost or forgotten. There are a few promising trends, however. Tokens are moving from hardware to software, and the idea is spreading that they should be embedded in things people carry already.

5.3 Single Sign-on Considerations

Single sign-on is the mechanism that enables the user to sign in just once and have access to all the needed resources. Its benefits include increased productivity and ease of use. Single Sign-On (SSO) is of particular importance because it removes the user's burden of remembering many passwords and the security breeches created when the user writes down her passwords. Services may require different levels of authentication, and re-authentication may be required before access can be granted to the user. SSO is therefore not always possible and the Liberty Alliance uses the term *"Simplified sign-on"* rather than SSO. With Microsoft CardSpace, *"Reduced sign in"* is used since the user is offered the possibility to select in the appropriate ID card containing the required credentials for authentication.

SSO is often touted as a solution to reduce or eliminate costs associated with the multiple-password problem. This gets to be very confusing for a couple of reasons. First, SSO is a very ambiguous term and means something different to different people. Second, the typical SSO approaches hide, rather than eliminate, the use of multiple passwords. This means that the majority of the administrative costs involved in managing user IDs are directly related to managing multiple passwords.

In an ideal SSO solution a user is only prompted once for a user ID and password and never prompted again, no matter what resources on which systems are subsequently accessed by the user directly or through client/server or multi-tier applications. Enterprise risk analysis for each application, each network, and each device being used to access the enterprise i.e., workstation, PDA, laptop, etc., need to be done before implementing single sign-on.

It is worth noting that with SSO, the user may still have several identities for different services and it is always possible to reverse the process and demand appropriate log-in for each service separately. SSO is not the same as E-Authentication; it is one of the capabilities facilitated by E-Authentication.

5.4 Integration Considerations

Governmentwide HR systems managed by OPM have their own distinct authentication mechanisms and establish their own user ID and password for authorization and access control. The level of authentication required by all governmentwide HR systems managed by OPM is not the same; different OPM systems require different levels of authentication. OPM does not have a single standardized process for E-Authentication; each OPM system follows different authentication process. There is no interoperability among different authentication products and systems.

There are two fundamental approaches for integrating identity and authentication in such a diverse environment. One approach is called *Front-end integration*, a technique that tries to present users with a single unified application that will act as an authentication "front-end" for all governmentwide HR systems. This approach usually employs some kind of SSO facility. Credential/password vault type of systems that implement SSO should not be used because they violate NIST SP 800-63 listed threats such as password replay and man-in-the-middle attacks. The implementation of SSO may be quite straightforward for web applications and very complex for legacy applications.

Another approach is to integrate user management procedures in different systems. This usually means the automation of user account creation and modification, centralization of user databases, etc. This may require modification to the legacy systems and Commercial Off The Shelf (COTS) packages which may be difficult. In addition, a centralized user identity database can create single points of vulnerability, which can cause a systemic or catastrophic failure of the entire system. For example, if the main digital identity repository is compromised, all transactions are suspect. It may also mean the reissue of all digital identities, in itself an almost overwhelming task when dealing with large populations.

According to the Gartner Research Report ID# G00152556, there are five distinct ways to integrate new authentication methods with multiple heterogeneous target systems (platforms and applications):

- Integrate directly with each system;
- Implement a proprietary authentication server or in-the-cloud service that is interrogated directly by each system;
- Integrate with a central security ticket service (such as Kerberos) issuing tokens that are consumed by each system;
- Integrate with a central identity repository that is interrogated directly by each system;
- Integrate with an Enterprise Single Sign-On (ESSO) product that brokers the native password authentication to each system[14].

No approach is ideal, but a hybrid approach such as a federated system may be more flexible. A federated system is one where a single digital identity can be used to access a number of services and systems, and a framework where security follows the transactions. Federation links disparate identity systems by securely exchanging identity information or credentials with partners, suppliers, customers, and other entities wanting to conduct business. While SSO is a key component of federated identity systems, they are, however, much more complex than a simple SSO component.

A federated identity system allows users to use a single set of credentials to access, not only organizational resources, but also resources of that organization's associates and partners. A key element is to separate the administration of the credentials from the numbers of relationships and identities in use. Administration of the credentials is distributed and devolved to the organizations within the federation.

The *Federal Identity Management Handbook*[15] has been developed in collaboration with the Federal Identity Credentialing Committee (FICC), Interagency Advisory Board (IAB), Federal Public Key Infrastructure Policy Authority (FPKIPA), and OMB. It is offered as an implementation guide for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with HSPD-12 and FIPS 201. The handbook provides specific implementation guidance on courses of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

[14] Gartner Research, Ways of Integrating New Authentication Methods Within a Heterogeneous Environment, October 30, 2007
[15] Federal Identity Management Handbook, US General Services Administration, September 2005

6.0 HR LOB Identity and Authentication Solution Architecture – CONOPS

A Concept of Operations (CONOPS) is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for a specific scenario. CONOPS identifies the relationship, dependencies, and desired interfaces envisioned between a new or upgraded system and other existing or planned systems. HR LOB Identity and Authentication CONOPS describes the elements/components that make up the solution architecture building blocks and presents these building blocks as a set of concepts and components, which is defined in the Federal Identity, Credential, and Access Management (FICAM) Implementation Roadmap document.

6.1 ICAM High-level View

The FICAM Roadmap and Implementation Guidance document describes the high level view of identity and access management. The roadmap defines three main functional areas for identity and access management as shown in the following diagram. These areas are: Identity Management, Credential Management, and Access Management. This high-level view of ICAM depicts the interdependencies between each area, which are combined to create an enterprise solution. The activities performed in one area are leveraged and built upon in the others. Identity management includes the processes for maintaining and protecting the identity data of an individual over its lifecycle.

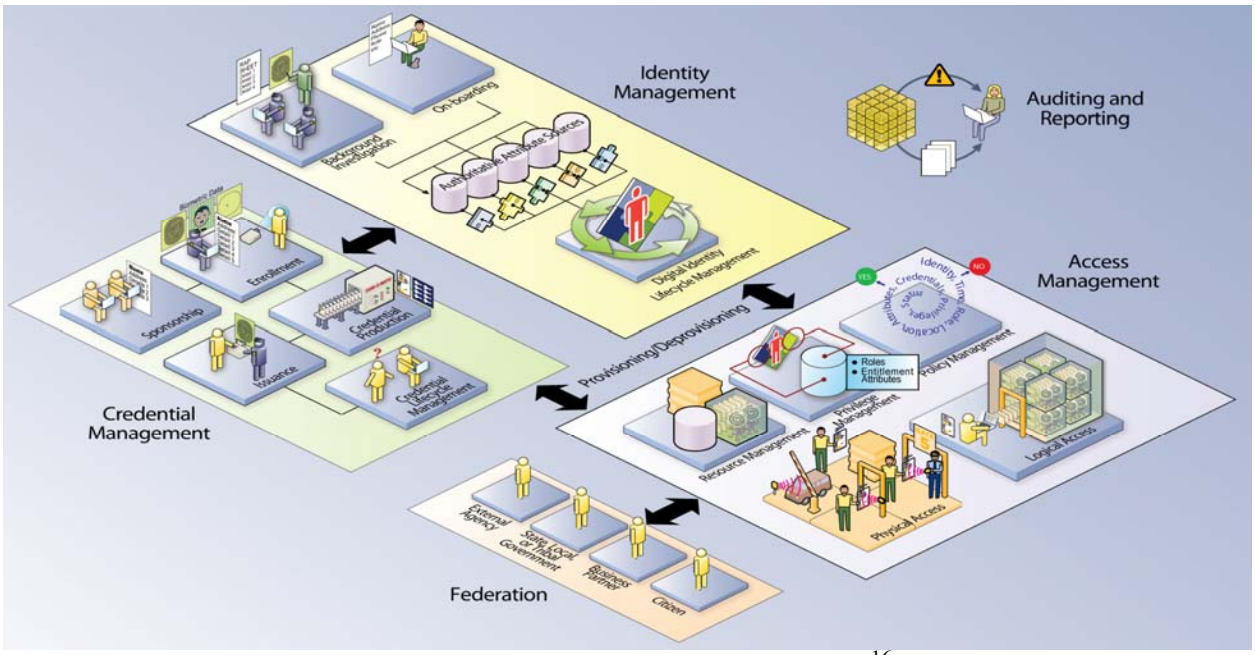

Figure 1 -- ICAM High-level Overview[16]

[16] FICAM Roadmap and Implementation Guidance Version 1.0

Establishment of a digital identity typically begins with collecting identity data as part of an on-boarding process. This digital identity may then be provisioned into applications in order to support physical and logical access (part of Access Management, discussed in Section 2.1.3) and deprovisioned when access is no longer required.

Credential management supports the lifecycle of the credential itself. In the Federal Government, examples of credentials are smart cards, private/public cryptographic keys, and digital certificates. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM.

Access management is the management and control of the ways in which entities are granted access to resources. The purpose of access management is to ensure that the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials. A key aspect of access management is the ability to leverage an enterprise identity for entitlements, privileges, multi-factor authentication, roles, attributes and different levels of trust.

6.2 HR LOB Identity and Authentication CONOPS

Conceptually, the authentication process is simple. User requests are intercepted by the authentication proxy for identification of the user and authentication of the user's claimed identity allowing access to secured applications. The authentication proxy verifies credentials with the security services and upon validation directs the request to secured applications. If the credentials are not verified it redirects the request back to the login page. The detailed use case scenario and process flow for providing the high-level steps for authenticating and authorizing a user to grant logical access to systems, applications, and data is described in section 4.10, *Granting Logical Access*, in the FICAM Roadmap and Implementation Guidance document. Some of the assumptions for authenticating an internal user (federal employee or contractor) described in this use case scenario are:

- The process to provision users into an application and establish access control policies and lists are performed prior to the start of the process flow based upon applicable policy and guidance;
- Processes for granting access to internal users are based upon use of the PIV card; and
- Target process flows reflect the use of a centralized Logical Access Control System (LACS) within an agency. However, control over access policies should still remain with application owners.

In addition to the assumptions made in the use case scenario for granting logical access to the applications data described in the FICAM Implementation and Roadmap Guidance document, governmentwide HR systems managed by OPM have the following technical characteristics:

- Secure Sockets Layer (SSL) will be used to secure the HR Identity and Authentication data;
- Authorization will be handled by each application and will be based upon a defined subject, security policy, and Security Access Grouping;
- Database authorization will be handled by the database management system;
- Authorization may not occur until identification and authentication have already occurred;
- Auditing will be available across all tiers and all log sources;
- Authentication across organizational boundaries is determined through risk assessment and mutually agreed upon identity proofing methods appropriate to the information being transmitted or data accessed;
- Identity proofing is the responsibility of the employee's agency;
- Authentication credentials will be encrypted in transit using appropriate encryption or hashing; and
- Appropriate authentication services will be configured and used on the web tier and utilize SSL for credential passing.

Data access rules for the governmentwide HR systems depend upon the assessed assurance level as follows:

- Level 1: No User ID or password requirements
- Level 2: Single factor authentication mandatory (User ID/Password)
- Level 3/4: Two factor authentication required over all networks. (User ID/Password + digital certificates, or one-time passwords)

Each User must be identified and authenticated before being authorized to access any data on the system. The following diagram shows the high-level CONOPS for E-Authentication of government wide HR systems:

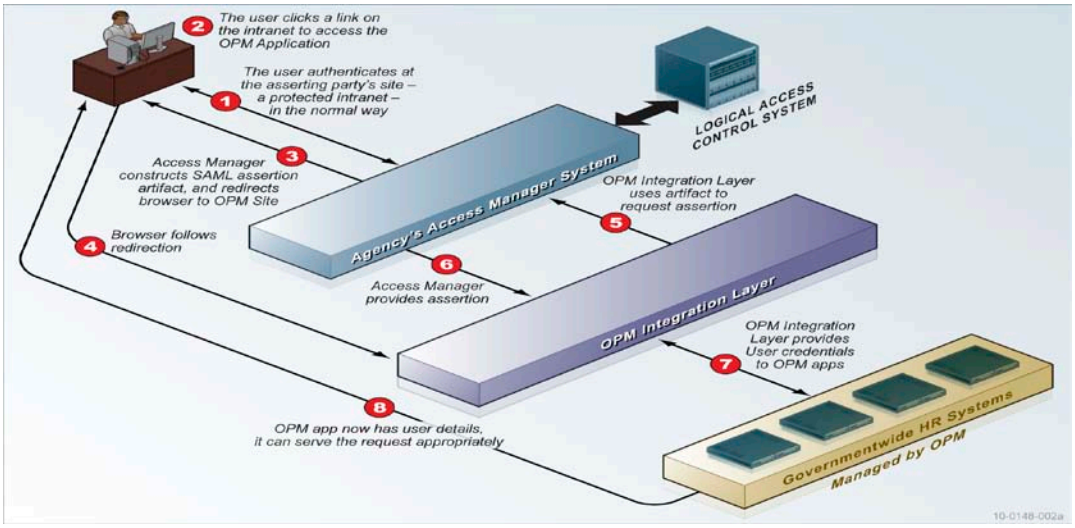

Figure 2 -- HR LOB E-Authentication High-level CONOPS

6.3 Use of Personal Identity Verification (PIV) Card

The PIV card is an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV cards are interoperable with and trusted by all Federal government relying parties. Effective use of identity cards requires an identifier that is unique across all identity cards. Lack of a unique identifier may result in incorrect access control decisions. The PIV card includes a Federal Agency Smart Credential - Number (FASC-N) to uniquely identify it, and thus avoid identifier namespace collisions. However, FASC-N is not a unique employee identifier for Federal employees—it is unique within the card issuing agency.

A PIV card consists of many sophisticated security technologies that have not been fully understood and adopted despite being in the market for years. Therefore, implementation of the PIV card requires careful planning, well-defined strategy, and end-user training. One of the most promising uses for PIV cards is to reduce the number of passwords end users must remember to authenticate to different web based applications. The PIV card is supported by a well-defined data model. It defines mandatory data elements and does not restrict issuers from *adding* additional applications and data. But issuer specific data is not considered interoperable across agencies. Ultimately, a PIV card is a very powerful tool that:

- Enables trust in identity of bearer of the token
- Enables a range of security models
  - Logical/Physical
  - Biometrically enhanced
  - Integrity with issuer signatures
- Enables range of transactional options depending on facility and system/network security requirements

One of the biggest challenges of successfully implementing PIV cards is understanding the value of the card. In numerous instances, the end user receives their PIV card without any high level explanation of what the card is and its expected usage. The result is the end user perceives the card as just a "badge replacement" and does not understand the card is part of a security infrastructure upgrade that will drastically help to improve and streamline their identification and authentication efforts. Without a fundamental understanding that the card will be used to protect the end user's identity and their agency, they will be less likely to use the card as intended.

FIPS 201, section 6 defines a suite of identity authentication mechanisms that are supported by the PIV card, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. The PIV card bears a number of visual and logical credentials. Depending upon the specific PIV credentials used to authenticate the holder of the PIV card to an entity that controls access to a resource, varying levels of assurance that the holder of the PIV card is the owner of the card can be achieved. Security of the ID credential issued to an

employee or contractor is achieved by full compliance with the mandatory requirements of FIPS 201. Specific safeguards include:

- Card issuing authority is limited to providers with official accreditation pursuant to NIST SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*;
- Sensitive card data is encrypted and stored on the card;
- Employees are alerted to the importance of protecting the card; and
- Card expiration date is within 5 years from issuance.

7.0 Solution Design and Implementation Considerations

Designing and implementing an identity and authentication solution is a complex project that requires clear goals, detailed planning, and a good understanding of an organization's requirements. Organizations may have to change the way they do business once they integrate the identity, authentication, and access management components into their application security architecture and security profile. Different authentication assurance levels are needed for different types of transactions. Any identity and authentication solution must ensure compliance with the Gramm-Leach-Bliley Act (GLBA), federal guidelines, and other applicable privacy laws.

An E-Authentication implementation approach should not depend upon a single proprietary solution. Solution product components must interoperate and controls must be implemented to protect privacy of personal information. Once an individual is issued with a valid credential there are a number of points in the E-Authentication process that need to be secured or managed to reach a high level of assurance that the person using the valid credential is who they claim they are. These points form a chain of trust. Electronic identity authentication at assurance level 4 using a valid credential should have mechanisms to the extent that effective technology is available to ensure acceptable levels of security at all these links in the process. Strong authentication must be coupled with the corresponding appropriate level of encryption for the information in storage and whilst traveling across untrusted networks (e.g. the Internet).

PIV card usage and deployment challenges include:

- Integrating card issuance with back-end directory and provisioning functions;
- Integrating smartcards with desktops, applications, and building access;
- Life cycle card management;
- Providing a flexible, easy to implement authentication system that meets the needs of your organization and your clients;
- Assuring data owners that only appropriately authenticated end users have access to data.

A successful identity and authentication solution depends on interoperability among different systems and applications, including the sharing of authentication and authorization information, as well as maintaining the consistency of identity information.

Interoperability and portability are strengthened by standards. Standards related to authentication and authorization processes emerged in recent years. They are often dependant on a directory services infrastructure and combined together they provide methods to support the identity and authentication solution. The most well known standards are:

- **eXtensible Markup Language (XML)** – provides an implemented and standard way to describe any type of data and to share them
- **Security Assertions Markup Language (SAML)** – allows exchange of identities (used for authentication and authorization processes)

- **Security Provisioning Markup Language (SPML)** – allows organizations to securely set up user interfaces for Web services and applications by letting enterprise platforms such as Web portals, application servers, and service centers generate provisioning requests within and across organizations
- **XML Key Management Services (XKMS)** – allows Public Key Infrastructure (PKI) enabling applications
- **X.500** – a series of standards that describe the functionality and interoperability of autonomous centralized identities data stores

Identity and authentication governance is another critical aspect in any solution implementation. Governance is defined as the processes and procedures by which an identity and authentication solution operates. An important aspect of the identity and authentication strategy is that identity data used in enterprise provisioning and de-provisioning processes, authentication and authorization decisions must come from enterprise approved authoritative identity sources. In addition, changes to the identity data must be approved by an identity data governance committee before any changes are made. Changes to the authentication mechanisms and routine maintenance, need to follow a clear set of change management governance policies. A clear set of password management policies must also be established. Identity and authentication polices should include rules for applying authentication mechanism hot fixes and rules for immediate identity termination.

When implementing authentication mechanisms in either an existing or new system, there are two considerations that merit special attention. Firstly, the security and authentication design must start early in the lifecycle process. Most users and stakeholders do not typically view the implementation of additional security requirements as value added from their perspective of accomplishing a functional mission. Many, at best, consider security to be a necessary annoyance. This dilemma emphasizes the need for a change management initiative to be in place when implementing authentication measures. The process needs to start early enough to reach the customers in time to allow for questions and for the users of the capability to develop a clear understanding of what is, and is not, going to happen. This is especially important if this is the first PIV implementation for an organization. Also, users may need basic instructions on how to use their PIV card. Many will have forgotten their PIN, having never used it. Also, some organizations may need time to deploy the PIV readers and software to be able to use the PIV card.

The second consideration is about implementing organization specific local security rules and policies. This is important in a large geographically dispersed implementation such as DoD or NASA. In addition to headquarters policy, many local level organizations have implemented extensions to security and use policy that can adversely impact, or completely prevent a successful implementation of authentication mechanism at their site. For example, if a local security officer has determined that their best practice is to close their firewall to anything not on their white-list of known good applications, a new authentication process using new ports is not going to work. Therefore, it is important to establish a communications outreach effort that

includes local level network, security, and management personnel to make them aware of what is being implemented and how it will interact with their environment.

It is important to verify network and communications capabilities such as bandwidth, routing, existing protocols, etc., prior to the implementation of E-Authentication capabilities. Some installations pass though geographic locations that do not support high quality communications. Other facilities are located in parts of the world where the communications conduits may not be particularly secure from monitoring or attack. This may or may not affect the decision to implement in these locations, but it is important to consider this issue and make an informed choice.

Other implementation considerations are, but not limited to:

- Transition roadmap as described in the FICAM Roadmap and Guidelines while implementing new ICAM segment architecture[17]
- Evolving nature of current technical standards (e.g., SAML 2.0)
- Varying levels of technical understanding and infrastructure among agencies
- Identification and protection of sensitive PII
- Managing and reporting the status of lost/forgotten card requests/approvals, certificate revocation, key escrow and recovery operations
- Cost of PIV card administration
- Supervising Change Management issues
- Managing technical interoperability caused by a wide variety of logical control application interfaces and network connectivity

[17] FICAM Roadmap and Guidance Version 1: Section 5 - Transition Roadmap and Milestones

8.0 References

"Best practice - Wikipedia, the free encyclopedia." *Wikipedia, the free encyclopedia*. N.p., n.d. Web. 25 June 2010.

Best Practices in Authentication: White Paper by RSA Security, ABP-WP-0905

Bolten, Joshua B., Director, Office of Management and Budget (OMB). *M-04-04: EAuthentication Guidance for Federal Agencies*. December 16, 2003

Burr, Bill; Polk, Tim and Dodson Dona; National Institute of Standards and Technology (NIST). *Special Publication 800-63: Electronic Authentication Guideline.* April 2006

Bush, George W., President of the United States of America. Homeland Security Presidential Directive/HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004.

Cameron, Kim. The Laws of Identity, An introduction to Digital Identity - the missing layer of the Internet.

CIO Council, Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version1.0, October 30, 2009.

E-Authentication Federation Architecture 2.0 Interface Specifications, Version 1.0.0, May 4, 2007, GSA

E-Authentication Federation Adopted Schemes, Version 1.0.0, May 4, 2007, GSA

Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard by United States Government Accountability Office

Electronic Government: Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards by United States Government Accountability Office

Enterprise Segment Architecture Report (ESAR), September 2009, Interim Version 1.3, an OMB publication

Evans, Karen. "Office of Management and Budget." *OMB memoranda M-06-19*. N.p., 12 July 2006. Web. 25 June 2010.

eWEEK. "What Is Multifactor Authentication? - Finance IT from eWeek." *Technology News, Tech Product Reviews, Research and Enterprise Analysis - eWeek*. N.p., 11 Sept. 2007. Web. 25 June 2010. Interview with Mark Diodati, Identity and Privacy Strategies analyst for the Burton Group.

"Federated Identity Management." *The Business Forum - Executive Meetings, Conferences, Business Luncheons - Round Table Discussions - World Information*. N.p., n.d. Web. 25 June 2010.

Federal Identity Credentialing Committee, Federal Identity Management Handbook, September 2005

Gartner Research, A Taxonomy of Authentication Methods: Quick- Reference Outline, February 29, 2008, ID Number G00155585

Gartner Research, Ways of Integrating New Authentication Methods Within a Heterogeneous Environment, October 30, 2007, ID Number G00152556

GSA, E-Authentication Federation Adopted Schemes, V 1.0.0, May 4, 2007

HSPD12, Backend Attribute Exchange Architecture and Interface Specification, Version 1.0.0, May 15, 2008

HR LOB Business Reference Model Version 2.0, US Office of Personnel Management

HR LOB Data Model Version 1.0, US Office of Personnel Management
HR LOB Service Component Model Version 2.0, Office of Personnel Management
HR LOB Technical Model Version 2.0, Office of Personnel Management
HR LOB Target Requirements for Shared Service Centers Version 3.0, Office of Personnel Management
Identity and Access Management: Laying the Foundations for a Trusted Business Environment (A Report) by Butler Group © 2006
Information Security Handbook: A Guide for Managers (NIST Special Publication 800-100) by Pauline Bowen, Joan Hash and Mark Wilson National Institute of Standards and Technology (NIST) © 2006
Johnson, Clay, Director, Office of Management and Budget (OMB). *M-06-16: Protection of Sensitive Agency Information*. June 23, 2006.
Johnson, Clay, Director, Office of Management and Budget (OMB). *M-07-16*: Safeguarding Against and Responding to the Breach of Personally Identifiable Information. May 22, 2007.
Monteleone, Michael. Defense Civilian Personnel Data System (DCPDS) CAC Implementation Lessons Learned – Presentation at E-Authentication Workgroup meeting #7 on 10/28/2009
National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 200: Minimum Security Requirements for Federal Information and Information Systems*. March 2006. Page 65.
National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors.* March 2006.
OATH, An Industry Roadmap for Open Strong Authentication,
Polk, Tim. NIST E-Authentication Guidance, SP 800-63, NASA SEWP Security Symposium June 1, 2004
Privacy Impact Assessment for the Department of Justice, PIV card System, July 20, 2007
Silverman, M. Federal Authentication and Identity Management v1.0, NIH OCITA NRFC0022, August 2006
Ross, Ron, et al; National Institute of Standards and Technology (NIST). *Special Publication 800-53: Recommended Security Controls for Federal Information Systems*. February 2005. Page 4.
Safeguard PII, Homeland Security, The DHS Privacy Office Presentation
Technical Approach for the Authentication Service Component, Version 2.0.0, May 4, 2007, GSA
Timchak, Steve. E-Authentication Initiative – PKI What's Happening, February 14, 2003
Topalovic, Peter, How can a Person's Digital Identity be Managed and Protected?: An Inquiry into the social, ethical, and the political implications of digital entity, SEP 707: December 14 2007

Appendix – A

Glossary of Terms

ASSERTION: A piece of data produced by a *SAML authority* regarding either an act of authentication performed on a *subject*, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified *resource*.

ASSERTING PARTY: The system, administrative domain, or an organization that asserts information about a subject or identity. For instance, the asserting party asserts that this user has been authenticated and has given associated attributes.

AUTHENTICATION: Validation of identification credentials. This is a process where a person, device or a computer program proves their identity in order to access environments, systems, resources and information. The person's identity is a simple assertion, the login ID for a particular computer application, for example. Proof is the most important part of the concept and that proof is generally something known, like a password; something possessed, like your ATM card; or something unique about your appearance or person, like a fingerprint.

AUTHORIZATION: The act of granting a person or other entity permission to use resources in a secured environment. This is usually tightly linked to authentication. A person or other identity first authenticates and then is given pre-determined access rights. They now have the authority to take specific actions.

CREDENTIALS: Credentials are the components or attributes of identity that are assessed to prove a person, device, or computer program is who they claim to be. Common credential stores include databases, directories and smart cards.

DIGITAL CERTIFICATE: In general use, a certificate is a document issued by some authority to attest to a truth or to offer certain evidence. A digital certificate is commonly used to offer evidence in electronic form about the holder of the certificate. In PKI it comes from a trusted third party, called a certification authority (CA) and it bears the digital signature of that authority.

DIGITAL IDENTITY: Electronic Identity or Digital identity is the representation of identity in terms of digital information or online identity.

E-AUTHENTICATION: E-Authentication is a federal government secure on-line access authentication initiative.

FEDERATED IDENTITY: Federated identity is identity management with defined trust relations between independent principals.

IDENTITY: The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

IDENTIFICATION: The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

IDENTITY PROOFING: Identity proofing is the process of validating the claimed identity of an individual. It is central to a secure and authoritative process for the issuance and use of identity credentials.

LEVEL OF ASSURANCE: Level of Assurance describes the degree of certainty that the user has presented a valid set of identifier attributes (credentials, etc.) that refer to his or her identity.

PERSONAL IDENTITY VERIFICATION (PIV) CARD: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

RELYING PARTY: The system, administrative domain, or an organization that relies on information supplied to it by the asserting party.

SECURITY ASSERTION MARKUP LANGUAGE (SAML): SAML is a standard for exchanging XML-based authentication and authorization assertions between identity providers and service providers (assertion consumers).

SECURITY PROVISIONING MARKUP LANGUAGE (SPML): SPML is an XML-based framework for exchanging user, resource and service provisioning information between cooperating organizations.

Appendix – B

List of Abbreviations

Acronym	Description
ADS	Authoritative Data Source
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BAE	Backend Attribute Exchange
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CSP	Credential Service Provider
DHS	Department of Homeland Security
DOB	Date of Birth
DoD	Department of Defense
EA	Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FICC	Federal Identity Credentialing Committee
FIWG	Federation Interoperability Working Group
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal Public Key Infrastructure Policy Authority
FSAM	Federal Segment Architecture Methodology
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
HR	Human Resources
IAB	Interagency Advisory Board

IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ID	Identification
IDP	Identity Provider
LACS	Logical Access Control Systems
LDAP	Lightweight Directory Access Protocol
NIEM	National Information Exchange Model
NIST SP	National Institute of Standards and Technology Special Publication
OASIS	Organization for the Advancement of Structured Information Standards
OIDF	OpenID Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control Systems
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Registration Authority
SAML	Security Assertions Markup Language
SPML	Security Provisioning Markup Language
SOAP	Simple Object Access Protocol
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Appendix – C

List of Standards

- FIPS 112
- FIPS 186
- FIPS 199
- FIPS 200
- FIPS 201
- Advanced Encryption Standard (AES)
- NIST Special Publication 800-53
- NIST Special Publication 800-63
- NIST Special Publication 800-73
- NIST Special Publication 800-87
- X.509 CRLs
- Backend Attribute Exchange (BAE) Specifications
- LDAP v.2 and v.3;
- XML
- Security Assertion Markup Language (SAML) version 2.0
- eXtensible Access Control Markup Language (XACML)
- Security Provisioning Markup Language (SPML) version 2
- Web Services Description Language (WSDL) version 2.0

United States
Office of Personnel Management
Chief Information Officer
1900 E Street, NW
Washington, DC 20415

CIO/HRITT/IARM/082010