THE REALIZED VALUE OF THE FEDERAL PUBLIC KEY INFRASTRUCTURE (FPKI)

BY

IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT SUB COMMITTEE (ICAMSC)

JANUARY 29, 2010

VERSION 1.0.0

Document Owner	Identity, Credential and Access Management Sub-Committee (ICAMSC)
Contact	Fpki.webmaster@gsa.gov
Document Title	The Realized Value of Federal PKI

Revision History Table

Date	Version	Description	Author
7/10/09	0.2.0	Incorporation of Comments from DoS, DoD, CertiPath	PGS (Judy Fincher and Dave Silver)
7/13/09	0.2.1	Review and edit	PGS (Judy Fincher)
9/3/09	0.2.2	Incorporate comments from Judy Spencer, DoE, DHS, USPS, GSA, NIST, Booz Allen Hamilton	PGS (Dave Silver)
9/14/09	0.2.3	Revised per Judy Spencer	Judy Spencer, PGS
9/21/09	0.2.4	Revised per Judy Spencer action items	PGS (Dave Silver)
9/23/09	0.2.5	Joint editing session with Judy Spencer	Judy Spencer, PGS
9/25/09	0.2.6	Revised per meeting with Judy Spencer	Judy Spencer, PGS
10/7/09	0.2.7	Revised Section 2.4.1 per new CertiPath input.	PGS (Dave Silver)
10/26/09	0.2.8	Revised per external comments.	PGS (Dave Silver)
11/3/09	0.3.0	Revised per review of external comments with Judy Spencer.	Judy Spencer, PGS
11/9/09	0.3.1	Revised per final internal review	PGS
11/24/09	0.3.2	Revised per GPO and State Department feedback	GPO, State Department
1/29/10	1.0.0	Approved version for publication	General Publication

Acknowledgements	Judy Spencer (GSA), Judy Fincher (PGS), Tim Pinegar (PGS), Dave Silver (PGS), David Cooper (NIST), Brant Petrick (GSA), Jim Degenford (A&N Associates for DoD), John Cornell (GSA), Rebecca Nielson (Booz Allen, Hamilton, for DoD), Evan Olson (DoE),Mark Stepongzi (USPS), Scott Rae (Dartmouth), Robert Schlecht (GSA)

Table of Contents

Tables

Figures

Executive Summary

In June 2000, the Federal Public Key Infrastructure (FPKI) Steering Committee published *The Evolving Federal Public Key Infrastructure*, a report that described the FPKI activities at that time.

Since that paper was published, new government identity management initiatives designed to take advantage of public key technology emerged that expanded the original FPKI scope. The emergence of government-wide electronic authentication and identity management guidelines, mandates, and standards has greatly facilitated government-wide interoperability of credentials and PKI adoption. For example, Homeland Security Presidential Directive 12 (HSPD-12) has driven large scale issuance of Personal Identity Verification (PIV) credentials to all Federal employees and contractors, which has made PKI more prevalent in the Federal government. At the end of fiscal year 2009, the deployment of PIV cards across the Federal enterprise exceeded 60% of the workforce, with 22 Federal credential issuance infrastructures operational nationwide; and multiple industry participants on the GSA Approved Products and Services List.

This report updates the previous report by relating how the FPKI has evolved to meet increasing Federal identity management demands. In addition, this report discusses how value-rich PKI technology may further support growth of trusted electronic transactions within the Federal government, and between the Federal government and external entities that include state and local governments, the business community, and the American public.

Continued PKI growth within the Federal government was spurred by Federal agencies needing strongly authenticated, trusted transactions: a) within the Federal agency; b) between itself and other Federal agencies; and c) with external entities (e.g., business partners, state and local governments, constituents).

Vendors have responded to increasing PKI demands by producing public key enabled commercial-off-the-shelf (COTS) products that enable the Federal community, state and local governments, industry, and other national governments to deploy PKI technology in ways that add significant value to business process (e.g., greater efficiencies) and security (e.g., increased protection for assets). PKI qualitative benefits include:

1. Strong digital signature;
2. Support for technical non-repudiation;
3. Strong authentication;
4. Strong Encryption; and
5. Trusted interoperability between disparate systems.

PKI quantitative benefits (measured by return on investment) include:

1. Synergy with HSPD-12;
2. Multi-factor authentication;
3. Network security; and
4. PKI-enabled applications.

Federal agencies and cross-certified external PKIs have access to the aforementioned benefits. For example, the Department of the Treasury's PKI is used by many Federal

Bureaus to protect trillions of dollars per year by providing strong authentication, encryption, and digital signature services.

The future of PKI is closely tied to the increased emphasis on identity management and cyber security both by industry and government. As organizations become more conscious of their cyber security needs, they increasingly recognize the value of Public Key solutions for providing the technology to attain their identity management and data security goals. The inclusion of public key credentials on PIV identity cards ensures that there is widespread availability of these basic tools for strong identity assurance and data protection within the Federal government. The extension of trusted identity credentials to State and local governments through the Department of Homeland Security-sponsored First Responder Authentication Credential (FRAC) and Transportation Workers Identity Credential (TWIC) programs has raised interest in Public Key solutions in other state and local electronic business activities In addition, the adoption of Public Key technology within industry is becoming more widespread. In many cases, this interest has been generated by the high-level of interest in the FIPS 201 standard for PIV Cards and the desire to have identity management processes that are interoperable with Federal systems. The two industry-sponsored PKI Bridges, CertiPath and SAFE-BioPharma, are examples of the burgeoning interest in public key technology displayed by the private sector, and these investments are indicative of an intention to further expand public key technology usage within and between these communities and the Federal government. It is easy to envision PKI as a tool for enhancing cyber security, providing improved services to the American public, and helping move government and industry to a secure, paperless environment, as well as providing positive identity management.

The deployment of PIV Cards makes strong PKI credentials increasingly ubiquitous. An estimated 5.8 million Federal government employees and contractors will rely on the PKI in their PIV Cards for both physical and logical access to government resources. The recently released *PIV Interoperability for Non-Federal Issuers* document, providing guidance to non-Federal entities on achieving technical interoperability and trust with Federal systems designed to utilize PIV Cards will further expand PKI credential ubiquity to state and local governments, industry, and commercial activities.

Section 5, Case Studies, relates actual PKI uses and benefits. PKI beneficiaries include Federal agencies, business and commerce, and other governments. The case studies highlight multiple PKI uses and significant qualitative and quantitative benefits.

1 Introduction

In June 2000, the Federal Public Key Infrastructure (FPKI) Steering Committee published *The Evolving Federal Public Key Infrastructure*, a report that described the FPKI activities at that time. The report detailed efforts by individual Federal agencies to develop and deploy their own PKIs and described the activities undertaken by the FPKI Steering Committee to enable interoperability of these disparate PKIs through implementation of the Federal Bridge Certification Authority (FBCA). In addition, the report discussed the FBCA concept and design from its inception to a proof-of-concept prototype.

In September 2002, following successful demonstration of the FPKI bridge concept, the FBCA went operational with four (4) charter Federal agencies. The FBCA continues to operate under the management of the General Services Administration (GSA) with policy oversight provided by the FPKI Policy Authority (FPKIPA). With the increased Federal government attention to Identity Management issues, the FPKI Steering Committee was superseded by the Federal Identity Credentialing Committee (FICC), which was recently incorporated into the Identity, Credential, and Access Management Sub Committee (ICAMSC). Today, the FBCA's primary role is to enable interoperability between FPKI domains, and to enable Federal interoperability with non-Federal PKIs. The current list of cross-certified CAs includes seventeen government and business entities representing millions of users (see Appendix B - Entities Cross-Certified with the FBCA).

Since the FBCA became operational, new government identity management initiatives have emerged that rely on public key technology. The initiatives listed below have expanded the original FPKI scope. Today the FPKI includes four (4) Certification Authorities (CAs): the FBCA, the Federal Common Policy Framework CA (COMMON), the E-Governance CAs (EGCA), and the Citizen and Commerce Class Common Certification Authority (C4CA).

This report updates *The Evolving Federal Public Key Infrastructure* by relating how the FPKI has evolved to meet increasing Federal identity management demands. Industry has responded to increasing PKI demands by producing public key-enabled commercial-off-the-shelf (COTS) hardware and software products, thus adding value to Federal agency business and security processes. Section 5, Case Studies, relates the experiences of some Federal agencies employing PKI technology, and the qualitative and quantitative benefits realized from those experiences.

Finally, this report discusses how PKI technology supports growth of trusted electronic transactions within the Federal government, and between the Federal government and external entities that include state and local governments, the business community, and the American public.

2 The New Federal PKI Landscape

Continued PKI growth within the Federal government was spurred by Federal agencies needing strongly authenticated, trusted transactions: a) within the Federal agency; b) between itself and other Federal agencies; and c) with external entities (e.g., business partners, state and local governments, constituents). This is the “bottom up” approach predicted in *The Evolving Federal Public Key Infrastructure*. Government mandates concerning the adoption of a holistic approach to electronic authentication provided additional impetus to the continued growth of the Federal PKI.

2.1 New Standards and Mandates

The emergence of government-wide electronic authentication and identity management guidelines, mandates, and standards has greatly facilitated government-wide interoperability of credentials and PKI adoption.

The Office of Management and Budget (OMB) memorandum, *Streamlining Authentication and Identity Management within the Federal Government,* published July 3, 2003, instructs Federal agencies to “buy-not-build” PKI to the maximum extent possible. Likewise, OMB memorandum M-05-05, *Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services*, published December 20, 2004, identifies the Shared Service Provider (SSP) Program as a source for Federal agencies to obtain PKI services. The SSP Program provides strong government oversight of commercial-managed service providers, which results in cost savings, benefits associated with contractor-provided services, and risk mitigation. In addition, the SSP Program ensures PKI services consistent with current electronic signature law and policy.

In December 2003, OMB issued memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, which established four levels of identity assurance for the authentication of electronic transactions. It soon became clear that achievement of M-04-04 levels of assurance 3 and 4 requires PKI support. The four (4) M-04-04 levels of assurance are:

- Level 1: Little or no confidence in the asserted identity’s validity.
- Level 2: Some confidence in the asserted identity’s validity.
- Level 3: High confidence in the asserted identity’s validity.
- Level 4: Very high confidence in the asserted identity’s validity.

On August 27, 2004, President Bush signed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. Based upon this directive, in February 2005 the National Institute of Standards and Technology (NIST) issued *Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identity Verification of Federal Employees and Contractors*[1], which describes the minimum requirements for a Federal system to comply with the HSPD-12 mandate. These requirements include personal identity proofing, registration, and credential issuance. In addition, FIPS 201 requires Personal Identity Verification (PIV) Cards to contain PKI-based authentication data (one asymmetric key pair and one corresponding digital certificate) for high-

[1] FIPS 201-1, the first revision of FIPS 201, and currently applicable standard, was issued in March 2006.

confidence physical and logical access to Federal facilities and systems. Further, these PIV-authentication certificates must be issued under the COMMON Policy.

2.2 The Evolving FPKI

The FPKIPA develops Federal PKI policy and provides operations oversight. The FPKIPA is "an interagency body established under the Chief Information Officers (CIO) Council to enforce digital certificate standards for trusted identity authentication across Federal agencies, and between Federal agencies and outside bodies such as universities, state and local governments, and commercial entities."[2] The primary FPKIPA mission is to provide a solution for strong authentication, digital signature capability, and confidentiality for data in transit and data at rest.

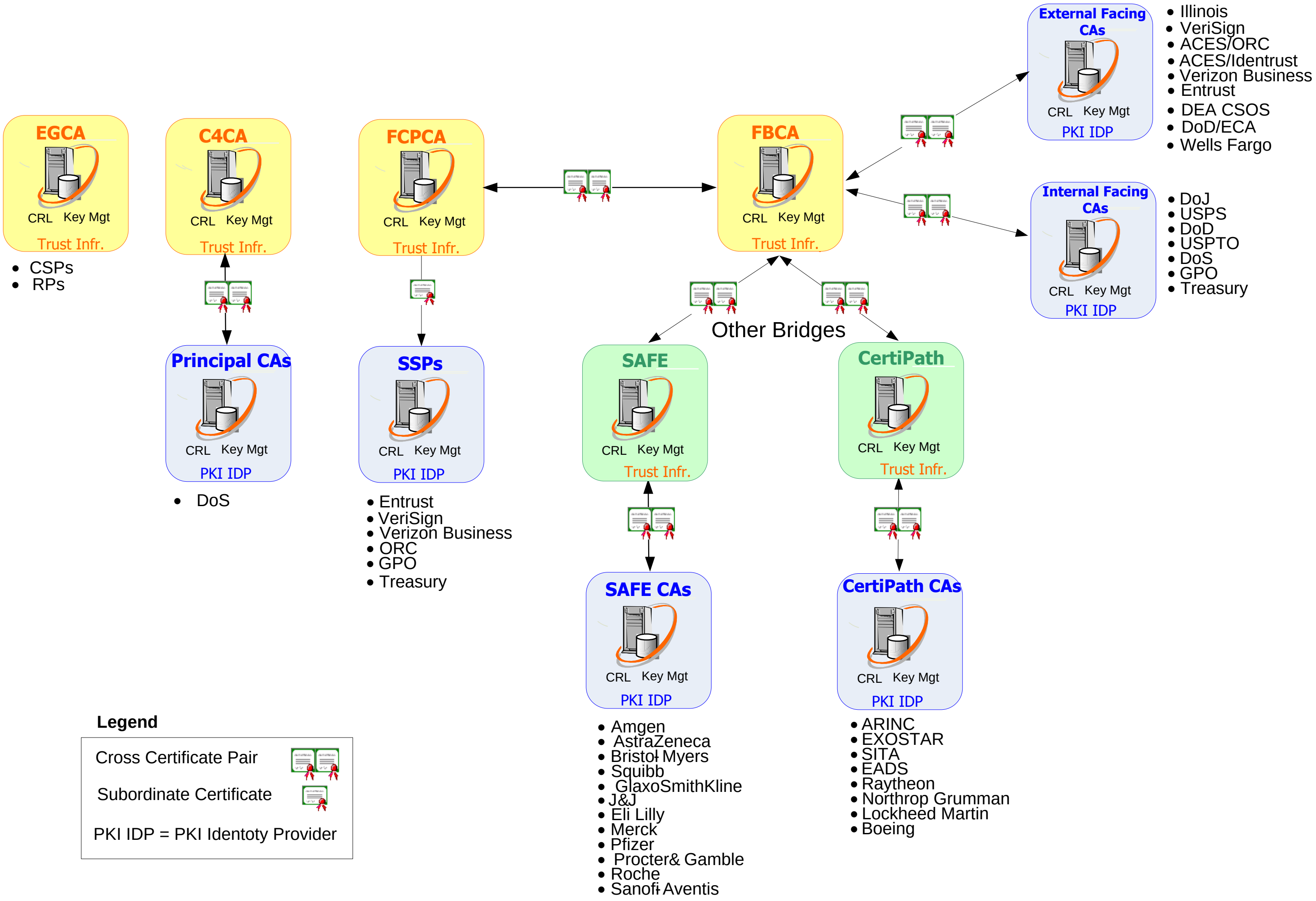
The Federal PKI Architecture (FPKIA) debuted in 2002 and included the FBCA and four cross-certified Federal agencies: United States Department of Agriculture (USDA)/National Finance Center, Department of Defense (DoD), Department of The Treasury (Treasury), and National Aeronautics and Space Administration (NASA). The other FPKIA components were added over time as the demand was identified.

Figure 2-1 depicts the current FPKIA[3]. The FBCA and COMMON are cross-certified with each other, while the E-Government Certification Authority (EGCA) and Citizen and Commerce Class Common Certification Authority (C4CA) stand alone.

[2] The FPKIPA Mission Statement

[3] At the time of this writing, Entrust and Verizon Business were not yet cross-certified with the FBCA. However, in anticipation of their cross-certification, they are being included in the paper.

Figure 2-1 FPKI Landscape as of September 2009



2.2.1 FBCA

Originally developed as a mechanism to facilitate interoperability between Federal agency enterprise PKI implementations, the FBCA's role has subsequently expanded to include external entities. Today, the FBCA is the identity trust hub[4] that enables peer-to-peer transactions between its member organizations, both Federal and non-Federal.

Federal agencies operating PKIs cross-certified with the FBCA are (see Appendix B - Entities Cross-Certified with the FBCA for cross-certification dates):

- Department of Defense (DoD);
- Department of State (DoS);
- Department of Justice (DoJ);
- Drug Enforcement Administration (DEA CSOS);
- Government Printing Office (GPO);
- Treasury;
- United States Postal Service (USPS); and
- United States Patent and Trademark Office (USPTO).

The FBCA is also cross-certified with the State of Illinois, and with two commercial PKI Bridges: CertiPath, which serves the Aerospace and Defense industry, and SAFE-BioPharma, which has established FBCA-comparable digital identity and signature standards for the pharmaceutical and healthcare industries. These partners have extended the reach of the FPKI well beyond its own boundaries. In addition, there are PKI service providers associated with the FBCA: Access Certificates for Electronic Services (ACES), for which GSA administers the Certificate Policy; and VeriSign, Entrust and Verizon Business, which are commercial service providers offering Federally-trusted credentials to U.S. state and local governments and business entities.

2.2.2 EGCA

To support levels of assurance 1 and 2, the FPKIPA developed the X.509 Certificate Policy for the E-Governance Certification Authorities. The EGCA issues PKI certificates to approved Credential Service Provider (CSP) and Federal Relying Party (RP) systems to enable mutual authentication, and therefore mutual trust. These credentials establish secure communication links between recognized and trusted entities. Since only approved CSP and RP applications have EGCA credentials, the ability for a non-trusted entity to impersonate either identity or intercept the transaction is eliminated.

2.2.3 COMMON

In April 2003, the CIO Council challenged the FPKIPA to establish an FPKI hierarchical trust anchor for all Federal agency CAs. The resulting *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* document and the instantiation of the COMMON Root CA represented the beginning of a new era in FPKI. On July 3, 2003, OMB released the policy memo *Streamlining Authentication and Identity Management within the Federal Government*,

[4] An identity trust hub comprises multiple organizations using comparable policies and procedures to authenticate the identities of its participants and to assert those identities across the entire federation.

which advised Federal departments and agencies to cease building enterprise PKI solutions and to acquire PKI services from commercial providers. Commercial SSPs were invited to apply for subordination to COMMON via Certification Practices Statement (CPS) mapping to the COMMON CP. Departments and agencies were then free to acquire services from one of these approved providers. COMMON provides a single trust anchor for Federal PKI transactions and interfaces with the external trusted PKI communities through a single cross certification between COMMON and the FBCA.

COMMON enhances the FPKI as follows:

1. Federal agencies can deploy digital credentials without having to operate and maintain an Enterprise PKI. Instead, they can acquire services from commercial providers,[5] thus saving their resources for Federal agency purposes.
2. Individual Federal agencies are relieved from the requirement to establish their own CPs and to map to the FBCA. On their behalf, the FPKIPA administers COMMON and manages cross-certification with the FBCA.
3. COMMON is the single trust root supporting interoperability within the Federal government. And because it is cross-certified with the FBCA, it enables public trust of government-issued certificates.
4. COMMON is public facing and has its root CA in an increasing number of COTS product trust stores. This facilitates Path Discovery and Validation (PD-Val[6]) because the route between the trusted pairs is more direct than when traversing the FBCA.
5. FIPS 201 identifies COMMON as the source of digital authentication certificates for the PIV credentials.

2.2.4 C4CA

C4CA is the U.S. Federal government's mechanism for enabling a PKI trust domain satisfying level of assurance 2. Its primary purpose is to ensure that "commercial grade" PKI implementations (e.g., those that do not aspire to the requirements for FBCA cross-certification) are not disenfranchised as identity solutions. Uptake of C4CA is somewhat limited. However, DoS has been approved for cross-certification with C4CA in anticipation of extending electronic services to citizens without commingling certificates with employees.

2.3 Legacy FPKI Participants

A "legacy FPKI" is a Federal agency PKI operated and maintained by a Federal agency and directly cross-certified with the FBCA, as opposed to obtaining PKI services and credentials from an SSP under COMMON. Current legacy FPKIs are DoS, DoJ, DoD, Treasury, USPS, USPTO, and GPO. These Federal agencies were early adopters of PKI whose systems pre-date the issuance of the 2003 OMB Memorandum requiring the use of shared providers.[7]

[5] In addition to the Commercial Providers, the Department of The Treasury and the Government Printing Office provide Common CP Certificate Services.

[6] PD-Val entails tracing the digital certificate back to the issuing CA for verification.

[7] See *Streamlining Authentication and Identity Management within the Federal Government*.

As the government-wide initiative for identity management evolves and in order to comply with the requirements of FIPS 201[8], legacy FPKIs must evolve to remain in step. In this vein, legacy FPKIs have taken steps to conform to FIPS 201 requirements in order to align themselves for the purpose of issuing PIV Authentication certificates[9]. Towards this, COMMON includes provisions specifically developed to ensure legacy FPKI implementations can be aligned (e.g. naming conventions). In addition, there are plans to transition legacy FPKIs from the FBCA to a direct peer-to-peer relationship with COMMON in order to further simplify trust paths within the Federal community.

2.4 External FPKI Partners

Currently, external FPKI partners associated with the FBCA include one state and two industry PKI bridges. In 2003, the State of Illinois became the first external entity to cross-certify with the FBCA.

However, it was the addition of the two commercial PKI bridges that significantly increased the FBCA external trust community.

2.4.1 CertiPath PKI Bridge

CertiPath is a commercial standards-based PKI bridge establishing interoperable trusted identity credentials within the Aerospace and Defense (A&D) industry. CertiPath takes organizational identity assurance to a higher level with the CertiPath Bridge. CertiPath certifies organizations to a common standard, enabling them to assert the identities globally – utilizing software-based digital certificates or certificates deployed on hardware tokens – such as smart cards – to gain logical access to sensitive intellectual property and physical access to secure locations and corporate offices. The CertiPath Bridge gives receiving organizations the confidence of knowing that the individual identities conveyed by their partners have at least the same level of assurance as those asserted by their own employees.

The CertiPath Bridge offers a secure and efficient means of exchanging information, eliminating the costly and complex process of individually mapping Internal PKI's and hardware tokens to establish trust with every other partner organization for collaboration. The resulting solution allows for truly scalable collaboration without the expense of issuing project-specific credentials to facilitate every interaction with a new customer, supplier or partner.

CertiPath provides externally portable organizational and individual identity assurance by certifying an organization's credentials – and those of their employees – meet the same globally accepted standards. CertiPath maps an organization's policy to the CertiPath policy to ensure adherence to the standards, essentially providing a trusted "seal of approval".

CertiPath was designed to be a geopolitically neutral mechanism, meeting globally accepted standards for Certificate Policies (CPs) and interoperability.

Modeled after the FPKI, CertiPath provides three (3) levels of services to its customers.

[8] See FIPS 201 Section 5.4.4.

[9] See *Implementing HSPD-12 using Legacy PKI Certificates*

1. The CertiPath Premium service offers a cross-certification service to commercial enterprises that operate and maintain a PKI under their own enterprise CP and CPS. Participants must go through a policy mapping exercise, similar to that of the FBCA, in order to ensure that their policies and procedures are comparable to those of the CertiPath CA and, therefore, that their identity credentials at the appropriate Level of Assurance are trustworthy.

   The CertiPath Premium Service allows policy and technical implementation flexibility, an ideal option for organizations that have one or both of the following:
   - A Complex internal organizational structure (i.e., multiple business units and geographies).
   - An existing PKI with credentials issued and in use.

   The Premium Service includes the mapping and cross-certification of each customer's policy points to those of the CertiPath Bridge. Premium Service customers can use multiple CAs – for example, one that issues credentials to each business unit or CAs that are geopolitically aligned across a global enterprise.

2. The CertiPath Standard Services offering is for enterprises who wish to operate Principal CAs subordinate to CertiPath's Standard Root CA. These participants must develop CPs and procedures that align with the CertiPath CP.

   For organizations that don't already have a Private Key Infrastructure (PKI) – or are ready to expand their collaborative network to include other companies and/or government agencies – CertiPath Standard Service provides an easy and cost-effective method of PKI deployment and management. An organization would assume CertiPath's existing policy as their own and use it to build the infrastructure so that it mirrors CertiPath's.

   The Standard Service is designed for organizations that do not have the requirement – or the resources – to define their own Certificate Policy (CP) or to set up subordinate CA's for various business units or programs. Standard Service customers inherit the CertiPath CP, freeing them from the time and expense of creating a CP from scratch – and giving them the confidence of knowing that their CP meets the CertiPath global standard.

3. The CertiPath Directory services offers hosting of cross-certificates of Enterprise CAs and certificates of the enterprise CAs certified by the CertiPath Common Root CA. It also hosts the current trust status for these organizations through publication of no longer trusted certificates to the Authority Revocation List.

In addition, the CertiPath Certified Credential Provider (3CP)^{TM} program offers certification of Service Provider CAs who can, in-turn, issue certificates to enterprise customers at Levels of Assurance that match their certification with CertiPath. There are three companies who are 3CP ^{TM} certified: Citibank, EXOSTAR, and SITA.

Through its certification with the FCBA, CertiPath allows A&D contractors to conduct highly secure business communications with the Federal government. Current CertiPath member CAs include Citibank, EXOSTAR, SITA, EADS, Raytheon, Northrop Grumman, Lockheed Martin, and Boeing.

2.4.2 SAFE-BioPharma Association PKI Bridge

SAFE-BioPharma™ is a non-profit association that developed and manages digital identity and signature standards for the pharmaceutical and healthcare industries. Organizations seeking to provide authentication and digital signature services and to become issuers of SAFE-BioPharma credentials must first cross-certify with the SAFE-BioPharma Bridge CA.

Current SAFE-BioPharma member CAs include: Amgen, AstraZeneca, Bristol-Myers Squibb, GlaxoSmithKline, Johnson & Johnson, Eli Lilly, Merck, Pfizer, Procter & Gamble, Roche, and Sanofi-Aventis.

2.4.3 State of Illinois

In 2003, the State of Illinois became the first non-Federal entity to cross-certify with the FBCA. The State of Illinois provides full PKI services to its constituents, including strong authentication, digital signatures, and encryption services. This includes encrypted background checks for schools, digitally signed water discharge monitoring forms from the Environmental Protection Agency, strong authentication to Medicaid recipient information, and digitally signed forms at a municipal police department.

Illinois is the first non-Federal government entity to be cross-certified at the medium-hardware level of assurance with the FPKI. This will allow for the issuance of First Responder Access Card (FRAC) credentials (following the PIV-I guidance[10]) to First Responders within Illinois. Using these strong authentication credentials, Illinois first responders (e.g., police, firefighters, paramedics) will have up-to-date identification which will allow them quick access to emergency or disaster sites. In addition, the check-in agent at the site will be able to review not only the cardholders identification information, but also training information, certifications held, and licenses the holder possesses. In this way, the responders will be allowed access to the site and directed to where they can be of the greatest assistance. Since these credentials follow the guidelines of the Department of Homeland Security (DHS), the expectation is that they would be accepted nationally when Illinois sends volunteers to assist at incidents in other jurisdictions.

2.5 SSP PKI “Clones”

PKI SSPs offer out-sourced FPKI and COMMON services to Federal agencies. Per COMMON, SSPs cannot use this relationship with COMMON to sell credentials to non-Federal entities in order to attain a trust relationship with the FPKI. As a result, several commercial providers approved as SSPs under COMMON have elected to cross-certify with the FBCA for the purpose of issuing certificates to external entities that can be trusted by the Federal community. The FPKIPA refers to these services as commercial “clones” of the SSP offering.

The first responder community FRAC and the transportation/port worker community (Transportation Workers Identity Card, or TWIC) are two such external entities desiring a PKI-

[10] See *Personal Identity Verification Interoperability for Non-Federal Issuers,* May 2009 http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf

based trust relationship with the Federal government. This interoperability with external entities via SSP "clones" is expected to grow as more organizations adopt public key solutions and seek relationships with the Federal community.

2.6 Partnership with Academia

The FPKI has a research partnership with the Higher Education community, sponsored by EDUCAUSE, a non-profit organization whose mission is to advance higher education by promoting the intelligent use of information technology. The Higher Education Bridge CA (HEBCA) is a test CA housed at Dartmouth College.

2.7 The Four Bridges Forum

The nation's four (4) leading PKI bridges have joined forces under a federation called the Four Bridges Forum (4BF). Its purpose is to raise awareness and promote use of a growing global infrastructure that enables trusted transactions across diverse communities of interest. 4BF includes the FBCA, CertiPath, the SAFE-BioPharma Association, and HEBCA.

3 The Realized Value of PKI

This section discusses the PKI qualitative and quantitative benefits to both Federal agencies and cross-certified external PKIs.

3.1 Qualitative Benefits of PKI

3.1.1 Strong Digital Signatures

Public Key technology is based on asymmetric key exchange. This means that each holder of a PKI credential has a unique key pair, one of which is kept secret (the private key) and the other of which can be shared (the public key). The private key is used by the credential holder to create signatures for documents and to assert identity during an attempt to gain access. The public key is then used by the relying party to verify the authenticity of the signature or the identity claim. The private key remains in the control of the credential holder and cannot be determined from the public key, thereby preventing spoofing. The trust in the identity asserted in the asymmetric key exchange process is provided by the strength of the binding between the public key and the identity asserted by its certificate. This binding is the responsibility of the public key infrastructure (PKI), the set of policies and procedures that govern the determination of identity and the binding of that identity to the public key. The FPKI policies provide a single consistent framework for trusting public key certificates within the Federal community and between the Federal government and its external partners.

The algorithms used to create digital signatures using public key technology are under constant attack, as are the keys themselves. For this reason, the size (length) of keys and the algorithms used to manipulate them is subject to constant review and refresh. NIST publication Special Publication 800-57, *Recommendation for Key Management* requires that key lengths currently in use by Federal agencies double by the end of 2010 to 2048-bit keys and the use of an improved secure hash algorithm (SHA-2) for performing cryptographic hash functions.[11] These requirements are reflected in FPKIPA policies.

In addition to the strength of the algorithms, the method of storage for the private keys contributes to the level of trust that can be placed in a transaction. Private keys can be stored in either software-based or hardware-based modules. Hardware-based private key storage provides better security and portability, which contribute to credential strength, and is not subject to the attacks that can undermine software-based modules. Hardware modules can take many forms, including smart cards, USB tokens, and smart phones.

When used within a federated model, digital signatures allow important business and regulatory transactions to occur in a fully electronic, secure environment. This eliminates the need to handle, copy, ship, and store paper documents. An example of the cost savings and enhanced security is the Federal government's transition to paperless processing. Federal government use of digital signatures to sign PDF files is widespread, as exemplified by the GPO. Use of PKI features such as digital signature is especially pertinent for digital-only content. The increasing demand from the Federal government is driving increased support for stronger algorithms in COTS products.

3.1.2 Support for Technical Non-repudiation

The use of digital signatures by the FPKI community supports legally-recognized technical non-repudiation (i.e., someone claiming that he or she did not sign). When a document is "digitally signed," the document's contents are incorporated into the signature. In order for the "signature" to validate, not only must the relying party use the public key that corresponds to the signer's private key, but in addition, the content of the document must not have changed since the signature was affixed. Digital signatures function as a unique identifier for an individual, much like a written signature, and also validate the contents of the signed document, which a written signature cannot do.

Legally speaking, technical non-repudiation requires a chain of evidence that links the individual to the signed document. PKI supports this requirement in two ways: first, only the individual whose private key corresponds to the public key used to validate the document can have signed the document, and second, successful validation indicates that the document contents were not tampered with subsequent to the application of the signature.

Digital signatures remain legally vulnerable to non-technical non-repudiations such as lack of legal capacity to contract (e.g., mental state) and forced/unintended signature (e.g., forced to sign, accidentally hit the "sign" button).

3.1.3 Strong Authentication

PKI credentials can be used in place of traditional forms of identity assertion (e.g., userid/password) in order to strengthen the access control process. In this case, the digital signature process is part of a challenge/response process. The access control system has a

[11] NIST SP 800-57 indicates that key size requirements will again increase to 3072-bit by the end of 2030, an eventuality for which the FPKI is already preparing.

record of all PKI certificates and corresponding public keys whose owners are permitted access to the system or facility. When the individual attempts to gain access (either by logging on to a system or network, or approaching a physical access terminal), a challenge is presented which is signed using the individual's private key. This signed challenge is verified using the stored public key and current certificate revocation list. If verification is successful, the individual's asserted identity is accepted, and access is granted.

New accounts are easily created by adding public keys and PKI certificates to the access control system. In the case of visitors carrying PKI certificates on their identity credentials, the PKI certificates can be validated to determine they were issued by a recognized authority and have not been revoked for any reason. In addition, a challenge/response process can verify that the credential carries the private key that corresponds to the public key associated with the PKI certificate, a process that requires the credential-holder to activate the private key using an access PIN, which comprises a two factor access control activity: something I have, something I know. Finally, this information can be used to request additional identity information through an attribute exchange mechanism. Using the capabilities of public key technology and infrastructure, credentials are validated readily as part of the access decision-making process.

An example of a strong authentication and access control mechanism that takes advantage of the capabilities of public key technology is the government-wide PIV Card mandated by HSPD-12, and its embedded PIV Authentication Key, whose use and authority is governed by the Federal Common Policy Framework. The PIV Card puts strong hardware-based authentication processes in the hands of every Federal employee and contractor. The recently released *PIV Interoperability for Non-Federal Issuers* guidance offers similar strong authentication capabilities and mutual trust to communities external to the Federal government through the federated environment.

3.1.4 Strong Encryption

Encryption is used to protect data at rest (e.g., computer hard drives, storage devices) and data in motion (e.g., transmission over the Internet, e-commerce, mobile telephones, e-mail). Traditional encryption processes use symmetric keys which must be shared in advance among all authorized entities in order to gain access to encrypted data. Therefore, symmetric keys must be kept well protected in order to protect the integrity of the encrypted data. When using PKI for encryption purposes, there are two distinct processes that may be implemented. In the first, the data is encrypted with the public key of the individual for whom it is intended. Once encrypted in this manner, it can be decrypted only with that individual's private key. In the second, the PKI is used as part of the process to securely share and store a symmetric key that is used to encrypt and decrypt the data. In both cases, the ability to access or compromise the key used to decrypt the information is greatly reduced.

Generally, the size of the cryptographic keys contributes to stronger encryption. Complying with technical standards and best practices for ensuring the continued strength of its encryption processes is the reason for FPKIPA replacement of 1024-bit keys with 2048-bit keys. Federal agencies are using PKI not only in the process of encrypting and decrypting data files, but also to compress and decompress those same files for transmission.

3.1.5 Trusted Interoperability between Disparate Systems

Organizations generally use unique internal policies and procedures to manage the identities of their employees and collaborating groups. These policies and procedures do not easily or efficiently align with the policies and procedures used by other organizations.

Federated PKI trust mechanisms, such as the FBCA and the other bridges that are partnering with it, allow trusted interoperability between disparate systems, greatly facilitating e-Commerce. The bridges negotiate common ground among the organization-unique internal policies and procedures, which in turn enables recognition, mutual trust, and acceptance of each others' identity credentials. And because the PKI credential is unique to its owner, not requiring 'shared secrets' or other exchange of information, this inter-organizational trust is readily extended to all of the individual credentials within a federated organization, whether used to enable secure e-mail exchange, digital signature, or access control activities. In this manner, CertiPath promotes interoperability between the aerospace industry and DoD over the Internet through use of its PKI bridge's relationship with the FBCA.

For the Federal community, the move to the COMMON trust root for PIV Cards has simplified the cross-organizational trust model, since all trust has been placed in the single policy and its Certification Authority. The COMMON trust root has been added to commercial product Root Stores further facilitating federated trust. The FPKI is also working with the other major browser organizations to install the COMMON trust root in their trust stores. This will further facilitate inter-organizational trust, both within the Federal community and between the Federal community and its external partners.

3.2 Quantitative Benefits of PKI

It is generally believed that an accurate determination of PKI return on investment (ROI) is difficult because effective PKI implementations are tightly integrated within larger business systems and processes. Therefore, it may be impossible to differentiate the ROI directly attributable to the use of PKI from the ROI of the overall system's effectiveness. However, it is helpful to quantify PKI ROI in terms of a) increased protection for government assets, b) greater efficiencies in doing business, and c) reduced costs. It can be demonstrated that improving trust in the Internet for the exchange of sensitive information results in lower cost, more streamlined communications, and accelerated process improvements, in part because digital transactions vastly reduce paper use.

For example, DoS has seen drastic reductions in Help Desk management costs by reducing its use of passwords in favor of PKI-enabled logical access control. For CY2002 through CY 2008, DoS has saved $8 million in password management costs.

Another example is the Department of the Treasury's PKI, which is used at many Bureaus, including Departmental Offices (DO), Bureau of Engraving and Printing (BEP), Bureau of the Public Debt (BPD), Financial Management Service (FMS) and the U.S. Mint. Collectively, the Treasury PKI is used to protect trillions of dollars per year by providing strong authentication, encryption and digital signature services to mission-critical applications such as the FMS Secure Payment System.

The following are PKI quantitative benefits provided to the Federal community by Federal PKI implementations.

3.2.1 Synergy with HSPD-12

The HSPD-12-driven, large-scale issuance of PIV Cards to all Federal employees and contractors will make Federal government use of PKI more prevalent. At the end of fiscal year 2009, the deployment of PIV cards across the Federal enterprise exceeded 60% of the workforce, with 22 Federal credential issuance infrastructures operational nationwide; and multiple industry participants on the GSA Approved Products and Services List. Full deployment is anticipated by the end of fiscal year 2010, making implementation of PIV-enabled physical and logical access systems the next major initiative.

In practice, PIV Cards are issued with the mandatory PKI credential, the PIV authentication key, and the three optional PKI credentials: card authentication key, digital signature key, and key management (encryption) key. It is expected that, in the future, all Federal users will be supplied with PKI credentials via the PIV Card. This ubiquity will enable large scale implementation of PKI-enabled solutions for access control, data protection, and business process streamlining; and results in greater logical and physical security for employees and contractors throughout the Federal government. Including PKI in the PIV initiative may be the single most important security enhancement in the history of the Federal government.

3.2.2 Multi-factor Authentication

Authentication systems are often categorized by the number of factors that they incorporate. PKI is an excellent component (factor) to multi-factor authentication. The three factors often considered as the cornerstone of authentication are:

- Something you know (e.g., a password);
- Something you have (e.g., an ID badge, a cryptographic key); and
- Something you are (e.g., a fingerprint or other biometric data).

The more factors incorporated into the authentication process, the stronger the authentication. For example, authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors.

PKI can contribute several factors. By default, PKI contributes something you have (the private cryptographic key). If the PKI software or hardware module housing the private key requires user activation, PKI also contributes either something you know (a password to unlock the module in order to access the private key) or something you are (a biometric to unlock the module to access the private key). Federal agencies are leveraging this multi-factor approach, typically using a password to unlock the software or hardware module to gain access to the PKI private key.

3.2.3 Network Security

3.2.3.1 Access Control

PKI-based authentication is becoming widely used as a primary factor for access control to critical Federal agency resources. This will become ubiquitous as HSPD-12 deployment and implementation increases. Today, the best metric indicating the value of PKI for network security is from DoD. DoD reports reduced network intrusion and penetration attacks where PKI is used in conjunction with the DoD Common Access Card (CAC). In an environment where one successful attack could cost tens of millions of dollars, the potential cost savings is significant.

> "CCL [CAC Cryptographic Logon (CCL)] implementation across DoD has resulted in a 46% reduction in successful NIPRNet intrusions," according to Lt Gen Charles Croom, Director, DISA and Commander, Joint Task Force-Global Network Operations at the AFCEA SpaceComm 2007 Conference."

3.2.3.2 Secure Tunneling

The FPKI community is benefiting from using PKI to secure communications, such as Virtual Private Networks (VPNs). VPNs use PKI certificates to establish a secure tunnel through which data can be transmitted across a public network, such as the Internet, without being subject to threats such as eavesdropping. By using secure tunneling, organizations avoid the risk and costs of data tampering or data theft during transmission. See Appendix A - Case Studies, for a detailed description of the DoS's use of PKI to establish VPNs.

The SAFE community, exemplified by Johnson and Johnson (J&J), also uses two-factor authentication (something you have, i.e., smart card-based PKI credential; something you know, i.e., access PIN) to authenticate to the network and create an Internet Protocol Security (IPSec) tunnel. Tunneling protocols may use data encryption to transport unencrypted (i.e., plain text) traffic over a public network (e.g., Internet) through an encrypted channel, thereby providing VPN functionality. IPSec has an end-to-end Transport Mode, but also can be operated in a Tunneling Mode through a trusted security gateway.

3.2.3.3 Single Sign-on

Single sign-on (SSO) allows a user to log in once and gain access to multiple independent systems (possibly with different authentication mechanisms) without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple systems. Using public key technology for achieving SSO applies a strong two factor identifier (PKI credential and its activation PIN) to the process. Once activated for an SSO session, the PKI credential can conduct the authentication activity for accessing additional resources on the network without additional user intervention. PKI does not operate the way industry defines SSO, but provides all the user benefits of SSO without requiring the extensive back-end coordination that traditional SSO solutions require. In addition, the use of PKI eliminates the need for ever-increasingly complicated passwords that must be changed at increasingly shortened intervals. SSO benefits utilizing PKI include:

1. Eliminating password fatigue (i.e., having to remember too many different user name and password combinations);
2. Reducing time spent re-establishing identity for the same individual;

3. Reducing IT costs by eliminating IT help desk calls concerning passwords;
4. Eliminating vulnerabilities associated with large password databases;
5. Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users; and
6. Centralized reporting for compliance adherence.

3.2.4 PKI-enabled Applications

PKI-enablement of applications is occurring in internal, Intranet-based, and Internet-based environments. The types of interactions vary greatly, from signing and encrypting e-mail, to access control processes. Once enabled, an application is able to process any public key certificate it receives and make a trust decision without relying on end-user cognizance. In addition to examining the PKI certificates for content and expiration date, PKI enablement includes the capability to perform trust path discovery and validation. This is the process of tracing the PKI certificates origins and relationships to determine whether it should be trusted. The goal is an unbroken chain of trust from the relying party to the issuing entity. Additionally, PKI-enabled applications must perform certification revocation checking to determine the specific certificate's current validity, i.e., it has not been revoked by the issuer prior to its expiration date.

For example, GPO PKI-enabled the Office of Federal Register electronic submission system (eDOCS). This provides significant benefits to submitting Federal agencies by avoiding courier charges and reducing cycle times. Federal agencies that submit large numbers of Federal Register announcements via the PKI-based electronic submission method can recoup costs within three to six months. In addition, PKI-enabled electronic submission provides a significant benefit to Continuity of Operations (COOP), whereby electronic documents can be easily replicated and sent to disaster recovery command centers instantly in contrast to paper documents that need to be copied and couriered to a disaster recovery site.

Another example is DoS PKI-enablement of the Consular Affair's Adoption Tracking Service and the Immigrant Visa Allocation Management System (IVAMS). This PKI-enablement of an Internet-based application provided DoS an annual cost savings of over $700,000 compared to the paper-based, manual processes previously employed. Not only did it reduce man hours, but it speeded up the response to the request from days to seconds.

4 The Future of PKI

The future of PKI is closely tied to the increased emphasis on identity management and cyber security both by industry and government. As organizations become more conscious of their cyber security needs, they increasingly recognize the value of public key solutions for providing the technology to attain their identity management and data security goals. The inclusion of public key credentials on PIV Cards ensures that there is widespread availability of these basic tools for strong identity assurance and data protection within the Federal government. The extension of trusted identity credentials to state and local governments through the DHS-sponsored FRAC and TWIC programs has raised interest in public key solutions in other state and local electronic business activities In addition, the adoption of Public Key technology within industry is becoming more widespread. In many cases, this interest has been generated by the high-level of interest in the FIPS 201 standard for PIV Cards and the desire to have identity management processes that are interoperable with Federal systems. The two industry sponsored Bridges, CertiPath and SAFE, are examples of the burgeoning interest in public key technology displayed by the private sector, and these investments are indicative of an intention to further expand public key technology usage within and between these communities and the Federal government. It is easy to envision PKI as a tool for enhancing cyber security, providing improved services to the American public, and helping move government and industry to a paperless environment, as well as providing positive identity management.

The deployment of PIV Cards makes strong PKI credentials increasingly ubiquitous. An estimated 5.8 million Federal government employees and contractors will rely on the PKI in their PIV Cards for both physical and logical access to government resources. The recently released *PIV Interoperability for Non-Federal Issuers* document, providing guidance to non-Federal entities on achieving technical interoperability and trust with Federal systems designed to utilize PIV Cards, will further expand PKI credential ubiquity to state and local governments, industry, and commercial activities.

4.1 PKI Technology is Mature

PKI technology is mature, as evidenced by the emergence of identity management and security standards that increasingly utilize PKI. For example, PKI functionality is an important component of SAML, Web Services Trust (WS-Trust), WS-Security, and Domain Name System Security (DNSSEC) to secure communications via encryption and digital signature.

4.2 PKI is being Globally Deployed to Protect the Internet

Another use of PKI is its inclusion as a central component in DNSSEC. The OMB has mandated that every U.S. Federal government IT organization use DNSSEC[12] to protect against Internet risks. DNSSEC is the addition of data authentication and integrity protection to DNS, using public key cryptography and a hierarchy of digital signatures.[13] DNSSEC protects the Internet from DNS-related attacks such as forged (or "spoofed") DNS data. This will assist Federal agencies in protecting systems when using the Internet, Intranets, and Extranets.

In the future, DNS servers will be required to verify digital signatures and establish "chains of trust" between previously unknown zones and a known secure zone (root, or some other pre-configured, trusted PKI). The DNSSEC specification is now complete and efforts are directed towards its deployment within the Federal government and globally.

4.3 Increased Industry Adoption of PKI

Use of PKI outside the Federal government is increasing at a steep rate, as evidenced by the advent of new bridge communities exemplified by the SAFE-BioPharma community and the CertiPath-supported Transglobal Secure Collaboration Program (TSCP), a consortium of the aerospace industry in Europe and the US.

[12] OMB M-08-23, *Securing the Federal government's Domain Name System Infrastructure*.

[13] Federal Register/Vol 73, No. 197/Thursday, October 9, 2008, p. 59608. "The DNS protocol is a critical component of the Internet infrastructure and is used by almost every Internet protocol-based application to associate human readable computer hostnames with the numerical addresses required to deliver information on the Internet."

Increased industry adoption is illustrated by the PKI capabilities embedded in COTS products. Such PKI visibility, prevalence, and scalability will continue to improve the PKI value curve over time because users will be able to readily and seamlessly take advantage of PKI. In time, PKI functionality will be ubiquitous, and therefore more accessible and tangible.
The incorporation of PKI into COTS products is an easy decision for developers because PKI is low risk to implement while providing high value-add. Embedding PKI into COTS products and utilizing it to secure VPNs and implement SSO, affords higher levels of security than riskier technologies that use passwords or PINs. In the future, COTS products based on open standards will incorporate PKI to support digital signature and encryption used to construct trusted message exchanges.

Currently, PKI is integrated into the following:

1. E-mail clients (digitally signing and encrypting e-mails);
2. Form signing software (digitally signing forms);
3. Root Stores of major internet browser and products;
4. Word processors and readers;
5. Internet browsers; and
6. Smart Identity Cards (e.g., DoD CAC, PIV Card, FRAC, TWIC) that move PKI into the physical and logical access control arenas.

The future PKI value curve will be steeper because PKI capabilities are becoming more accessible to more users through ubiquitous applications like browsers and word processors. In addition, Interoperable industry infrastructures such as 4BF and TSCP will further steepen the PKI value curve. More use in industry makes it easier for the Federal government to realize more value.

4.3.1 Organizational Response to FPKI and other Identity Management Initiatives

Wide PKI acceptance is also evident in the Federal CIO Council’s recent action to create a superstructure comprised of key Federal government identity management initiatives that previously worked independently. These initiatives and their underlying technologies have matured and converged. Combining them under one superstructure – called Identity, Credential and Access Management (ICAM) – facilitates a clear, consistent, unified picture of where Federal government identity management wants to go. Within this superstructure, PKI plays a prominent role as a provider of strong identity credentials.

4.3.2 The Future is Now

FPKI has much to celebrate as a technology that is coming into its own after many years of development and refinement. Nowhere is this clearer than in the DoS PKI programs, which include digital signatures, encrypted e-mail, code and macro signing, hard disk encryption, and secure VPNs. Moreover, DoS is PKI-enabling internal, Intranet-based, and Internet-based applications.

There is much left to do to fully and wisely implement PKI within the US Federal government. DoS and DoD are models for the many possible PKI applications. The advent of the PIV Card will enable improved business processes across the entire Federal enterprise building on the successes of DoS and DoD.

5 Case Studies

In March 2009, the FPKIPA asked its cross-certified members, including the CertiPath and SAFE Bridges, to provide ROI and other qualitative and quantifiable data on the realized value of FPKI within their organizations. Tables 5-1 and 5-2 are high-level summaries of the benefits identified in those case studies. The summaries illustrate the scope and extent of realized FPKI value by a variety of members (Federal agency, commercial, and bridge)[14].

Currently, eight Federal agencies operate their own PKIs: DoD, DEA, DoS, Treasury, GPO, DoJ, USPTO, and USPS. Four Federal agencies implemented their own PKIs, but subsequently acquired PKI services from SSPs. Other Federal agencies either acquire their Public Key certificates from the SSP program or they have an internal PKI that does not issue certificates outside the Federal agency.

Table 5-1 is a consolidated summary of qualitative and quantitative benefits realized by cross-certified members. The solid black dots indicate where a cross-certified member is benefiting from PKI use. Dollar signs indicate where the member provided financial impact information, either in dollars, percentages, or orders of magnitude. Benefits are grouped (e.g., Network Security encompasses strong authentication for access control, SSO, and VPN usage) into major areas of benefit.

Table 5-1 Qualitative and Quantitative Benefits of FPKI

Qualitative Benefits						Quantitative Benefits					
Cross-Certified Member	Strong Digital Signature	Support for Technical Non-Repudiation	Strong Encryption/ Decryption	Authentication	Interoperability	Network Security	Synergy with PIV	Multi-Factor Authentication	PKI-enabled Applications	Reduced Costs & Greater Efficiency	Multiple Levels of Security
CertiPath	●	●	●	●	●	●	NA		●	●	●
DoD	●	●	●	●	●	$●	●		●	●	●
DoS	●	●	●	●	●	$●	●	$●	$●	●	●
GPO	●	●	●	●	●		$●			●	●
SAFE (J&J)	●					●	NA				
State of Illinois	●	●	●	●			NA	Soon	●	$●	
Treasury	●		●	●	●	●			●		

Legend: NA: Not Applicable.
$: Member provided financial impact information, in $, %, or orders of magnitude.

Table 5-2 is a comprehensive summary of the uses and benefits realized by cross-certified members. The table illustrates a wide scope of use and many quantitative and qualitative benefits realized.

[14] Appendix A contains the case studies upon which Tables 5-1 and 5-2 are based.

Table 5-2 Comprehensive Summary of FPKI Member Case Studies

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
DoS	1. Encrypted and digitally signed e-mail. 2. Digital signing of data embedded on all U.S. electronic passports to prevent passport fraud and counterfeiting (Since inception in October 2006, over 34.9 million e-Passports). 3. Developing a classified PKI infrastructure to meet a demand from the intelligence community and other CNSS partner agencies. 4. VPN links used throughout the DoS for secure communication use the DoS PKI for securing the communication channels. 5. Signing all Java applets and ActiveX controls for use within the DoS OpenNet infrastructure. 6. Digitally sign macros used in the MS Office suite of applications. 7. Verify that all patches are digitally signed by the DoS PKI to ensure the integrity of all patches and system updates throughout the DoS. 8. Web certificates for DoS web sites that require secure authentication. 9. Smartcard access to The Immigrant Visa Allocation Management System (IVAMS). 10. Encryption for XML inquiries/responses between the DoS and DHS. 11. Secure user login via a web browser to support	1. Safeguards DoS browsers against running potentially harmful mobile code on the Department's network. 2. Reduction in trouble tickets. 3. Single sign-on together with strong authentication. 4. Secure both documents developed by the DoS, as well as those that come from outside agencies, and provide a security barrier against the use of malicious code that might be embedded in MS Office documents. 5. Data and software integrity. 6. Secure web site access. 7. Secure client and server authentication to provide non-email communications delivery to the desktop. 8. Secure communications. 9. Privacy of sensitive information (e.g., financial, investigative).	1. Following PKI deployments, password trouble tickets ratios for 2003 - 2005 ranged between 22-25%. Based on the cited results above, the monetary savings for a user community of 65,000 would be approximately $14.81 million in the first year based on a cost per call of $31. Although private sector market data was used, cost per call within the DoS varies on a quarterly basis. As of Q4 2008, average cost per call was $26.25. Assuming a reduction from 33% to 22% in total calls, and a cost reduction from $31 to $26.25, the cost savings is $7,882,875. 2. In 2008, the DoS PKI Program accounted for a 5.8% certificate recovery rate. In comparing the two methods of authentication, password authentication experienced nearly 6% more reset trouble tickets.	G-G G-B G-C	FBCA	1. The DoS issues each DoS employee and on-site contractor an enterprise PKI certificate. 2. Domestic deployments, including 16 field offices outside Washington, DC, are almost complete, and overseas deployments are currently complete at 145 posts (53%). To date, 29,313 active enterprise PKI certificates have been issued to individuals—19,150 using token-based PKI two-factor authentication, with an additional 8,462 web certificates (including 3,023 for IVAMS) issued. PKI hardware and software have been installed on 36,013 desktops, 18,769 at overseas posts. 3. By end of fiscal 2010, all domestic DoS employees and most overseas employees will be issued a PIV or limited-PIV ID. 4. In June 2008, 599 DoS PKI certificates had been generated, with an average request of about 5-10 per week. The VPN group estimated a rollout of ~1000 VPN devices by the end of 2008. 5. To date 8,462 DoS PKI web certificates have been provided. This number includes 827 for web servers and 489 for domain controllers. 6. DoS has provided 3,023 PKI certificates and smart cards for IVAMS that have a three year lifetime. DoS averages about

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
	international adoptions. 12. Encrypted e-mail service to the Bureau of Diplomatic Security. 13. Compress and encrypt post financial data files. 14. Working with the DoD to arrange secure access to DoD applications from the DoS network.		3. PKI-enablement of IVAMS provides an annual savings to US taxpayers of over $718,600 by reducing the time required to process requests for Visa numbers from days to less than an hour.			10-15 new requests a week. 7. The Consular Affair's Adoption Tracking Service is currently in the pilot stage with almost 200 adoption agencies participating.
GPO	1. Enterprise storage of work files while keeping the files encrypted and protected from other GPO personnel. Also extensively used in the ePassport manufacturing process GPO operates for the DoS. 2. Secure email used within the agency, and to secure email applied to certain business processes that would otherwise require manual and more costly or more time consuming methods. 3. Supported PKI-enablement of the Office of Federal Register electronic submission system (eDOCS). 4. Digitally sign its PDFs to ensure citizens have reasonable confidence that they have the GPO-distributed version of a document.	1. Data and work file privacy. 2. Significant cycle time reduction for some processes, thus improving service and customer satisfaction. 3. Citizens have reasonable confidence that they have the GPO-distributed version of a document. 4. PKI-enablement eDocs provides a significant benefit in COOP situations. 5. Strong barrier to fraud or forgery, and therefore provides a strong integrity seal for GPO. 6. Feedback to date from GPO constituents, customers, stakeholders and	1. Easy to use and operate, and cost effective. 2. Federal agencies submitting documents electronically via the Federal Register electronic submission system (eDOCS) avoid courier charges and have reduced cycle times. Those Federal agencies can recoup costs within 3 to 6 months.	G-G G-C	FCPCA FBCA	PKI has proven easy enough to use and operate, and cost effective, such that GPO is pleased with the outcome of PKI technology in support of the GPO agency mission.

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
		users (including the American library community) has been very positive and supportive.				
CertiPath	1. SecureEmail with S/MIME supported by "LDAP Proxies". 2. Convergence of PACS/LACS such that a "one badge" solution is realistic not only for one's organization but for visitors to the organization. 3. Digital identities of planes/avionics, ground stations and maintenance crews.	1. Key enabler for identity and verification anytime, anywhere in the world by any party. 2. Scalability due to PKI multiple levels of assurance that can be evaluated accurately by a relying party upon its receipt of the credential.		G-B B-B	FBCA	In virtually every circle CertiPath is in, PKI has long been a foregone conclusion and most of the time is now spent on working on how to make PKI based authentication events scale by means of federation. It feels like we should be well equipped to justify investments in PKI.
SAFE (J&J)	1. Two-factor remote access to the J&J network. 2. Secure e-mail. 3. Hard disk encryption 4. Adobe digital signatures for compliance with FDA requirements, and for other non-regulated business purposes. 5. SSL user authentication. 6. SSL web site certificates.	1. Strong authentication. 2. Strong electronic signatures that meet FDA requirements. 3. Strong encryption.	1. PKI is the least expensive and most extensible mechanism that meets strong authentication need. 2. Estimated net savings due to strong electronic signatures in excess of $1M annually, which will grow over time as such use grows, as we have already seen. 3. Strong encryption is the most cost effective way to prevent losing personal data or company data, causing potential damage to the company's reputation or economic interests.	G-B B-B	FBCA via the SAFE Bridge	J&J has an enterprise PKI with almost 90,000 subscribers (out of a total J&J workforce of about 120,000). J&J issues two PKI certificates to each subscriber: signature certificate and encryption certificate. Virtually all subscribers have their certificates on FIPS 140-2 level 2 (SafenetiKey 2032) hardware tokens.
State of Illinois	1. Accessing the Health &	1. Strong	1. Provides better	G-G	FBCA	1. The PKI initiative crosses

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
	Family Services Medi system to check on Medicare claims. 2. Accessing the Department of Aging web site to check on benefits for the elderly. 3. Filing electronic water discharge reports to the Environmental Protection Agency. 4. Accessing the City of Chicago's Health Alert Network system. 5. Providing encrypted background checks to schools, etc, using the Illinois State Police CHRI system. 6. Obtaining teacher education scholarship information via the ISAC "CollegeZone" web site. 7. Viewing filings and board opinions of the Pollution Control Board. 8. Securing email for Illinois State University. 9. Providing access to legacy applications through the Internet. 10. Kane County Circuit Clerk's office utilizing digital signatures on biometric flash drives for use by Judges. 11. Digitally signing internal forms by the Illinois Department of Transportation. 12. Providing digital signing and encryption capabilities for administrative personnel at Southern Illinois University at Carbondale. 13. Digital signing of police reports by the City of Rock	authentication. 2. Secure Encryption. 3. Digital Signing of documents.	service to our citizens and greater savings to the Agencies. 2. Enables secure physical access during emergencies.	G-C		almost all traditional demographic boundaries. We estimate that 85-90% of PKI users are normal citizens conducting business with various Governmental entities. Clients will be usually be over the age of 18, and can be either male or female. 2. The PKI environment has grown tremendously during the last twenty-four months. In May of 2003, we had issued approximately 5600 digital certificates; the count now stands at over 133,000 with an average monthly growth of over 900 certificates. We have more agencies that are implementing applications and taking advantage of not only the established authentication mechanism, but also the security and digital signature capabilities provided.

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
	Island. 14. Providing encrypted email for Central Management Services.					
DoD	1. Encryption and digitally signed e-mail. 2. Authentication to website information and stores. 3. Smart-card login to DoD networks. 4. Digital signature of forms. 5. Mobile code signing certificates 6. Device Certificates. 7. Group/role Certificates.	1. Ensure a safer work environment for all Federal employees and contractors. 2. Enhancement of the information assurance environment on the SIPRNET to support the Global Information Grid (GIG). 3. More secure method of network logon.	1. 99.9% system availability. 2. Ability to make PKI Certificate validity checks in near real time without having to download large CRLs from multiple CAs every day. 3. Reduction of network bandwidth demands and associated burdens on user processing assets. 4. Greatly reduces response times for mission operations. 5. Common process for network logon reduces need for passwords and the associated administrative overhead for lost or forgotten passwords, time lost and reduced operational tempo because of lost or forgotten passwords. 6. A 46% reduction in NIPRNET Intrusion Activity as a result of SCL implementation.	G-G		1. The DoD has issued over 15 Million CACs 2. There are currently over 500,000 software certificates issued by DoD, 3. 98% of DoD private web-servers are protected by DoD PKI issued software certificates. 4. Over 42,000 certificates are active on the Secret Internet Protocol Router Network (SIPRNET). 5. As of March 2009, the DoD has issued 1,739,710 PIV Cards. Additional improvements are planned for updated PKI certificate cryptographic algorithms and validation that will support HSPD-12 logical access requirements. 6. The DoD PKI has issued over 10,000 web-server certificates.
Treasury	1. Strong authentication. 2. Strong encryption. 3. Digital signature services.	1. Facilitating PIV interoperability. 2. Advanced system security. 3. Secure business	1. Avoid unnecessary costs. 2. Eliminate paperwork. 3. Create workflow	G-G	FBCA FCPCA	1. Many Federal Bureaus use Treasury PKI to protect trillions of dollars per year. 2. Integrating Treasury's PKI into the GSA MSO.

Organization	PKI Uses	Qualitative Benefits	Quantitative Benefits	Sectors Served	FPKI Cross-certifications	Scope/ Assessment of PKI Use
		transactions.	efficiencies. 4. Increase viability in the electronic Government marketplace. 5. Significant cost reductions by offsetting operating expenses; currently evaluating partnership opportunities with other Agencies to continue reducing costs.			3. Forging partnerships with other Agencies such as the NASA and the SSA through the GSA PKI SSP program.

Legend: G: Government, B: Business, C: Citizens

Appendix A - Case Studies

The following case studies were contributed by entities cross-certified with the FBCA. Each is presented in the original wording to accurately and completely convey real-world PKI uses and benefits[15].

A-1 *Case Study #1: Department of State*

Environment

The DoS issues each employee and on-site contractor an enterprise PKI certificate. The certificate allows the employee to send encrypted and digitally signed e-mail. All hardware and software have been approved for deployment on the OpenNet Plus system and are included in the Department IT baseline.

The DoS PKI Program Office includes a deployment team that handles PKI installations, training, and support. Domestic deployments, including 16 field offices outside Washington, DC, are almost complete, and overseas deployments are currently complete at 145 posts (53%). To date, 29,313 active enterprise PKI certificates have been issued to individuals—19,150 using token-based PKI/biometric two-factor authentication, with an additional 8,462 web certificates (including 3,023 for IVAMS) issued. PKI hardware and software have been installed on 36,013 desktops, 18,769 at overseas posts. The DoS PKI Registration Center issues, recovers, and revokes all PKI certificates. Tier 1 PKI troubleshooting issues are resolved by the IT Service Center. Tier 2 and Tier 3 PKI troubleshooting issues are forwarded to the PKI Registration Center for resolution.

The DoS PKI Program meets the requirements of Homeland Security Presidential Directive 12 (HSPD-12) through the Personal Identity Verification (PIV) PKI Certificate Authority (CA). To date, the PIV PKI has issued 50,692 PIV certificates in support of HSPD-12. By end of fiscal 2010, all domestic DoS employees and most overseas employees will be issued a PIV or limited-PIV ID. In some cases, local Post security requirements may override usage of PIV ID. The certificate on the ID card may be used by other agencies to strongly authenticate badge holders and provide interoperability among all U.S. agencies. Internally, DoS is working to leverage the PIV Authentication certificate for logical access.

The Machine Readable Travel Document (MRTD) PKI is a system of hardware, software, and policies that enable digital signing of data embedded on all U.S. electronic passports to prevent passport fraud and counterfeiting. This critical infrastructure is supported by the DoS PKI Program. Since its inception in October 2006, the MRTD system has digitally signed over 34.9 million e-Passports.

[15] Minor editing was done for presentation and consistency purposes, but no editing was done to content. Because each case study is in the contributor’s wording, the appearance of “different voices” is likely in this section.

In addition, the DoS PKI Program Office is currently developing a classified PKI infrastructure to meet a demand from the intelligence community and other CNSS partner agencies.

Implementations

Any application that leverages the Windows credential and uses PKI for smart card log-on leverages the PKI for Single Sign-on (SSO) to the application. The applications run the gamut from procurement software, e-Forms, and award submissions. DoS also has a few applications that use PKI exclusively because the application owner believed that they needed a stronger level of assurance.

The first year DoS had reliable and readily generated internal reports in this area was 2002, where the number of Universal Trouble Tickets (UTTs) relating to password management opened by the InfoCenter totaled almost one-third of the total tickets opened. Following PKI deployments, the ratios from the years 2003 through 2005 ranged between 22-25%. Based on the cited results above, the monetary savings for a user community of 65,000 would be approximately $14.81 million in the first year based on a cost per call of $31. Although private sector (e.g., Gartner Group, Meta Group) market data was used, the cost per call within the DoS varies on a quarterly basis. As of Q4 2008, the average cost per call was $26.25. Assuming a reduction from 33% to 22% in total calls, and a cost reduction from $31 to $26.25, the cost savings is $7,882,875.

Another indicator of the impact of DoS password consolidation and elimination can be measured from applications that still use username/password for authentication. InfoCenter password lockout reports show specific patterns regarding certain applications. While password management requests went down significantly in 2006 compared to previous years, applications that use passwords have escalated significantly. In 2008, the DoS PKI Program accounted for a 5.8% certificate recovery rate. In comparing the two methods of authentication, password authentication experienced nearly 6% more reset trouble tickets.

Virtual Private Network (VPN) links used throughout the DoS for secure communication use the DoS PKI for securing the communication channels. In June 2008, 599 DoS PKI certificates had been generated, with an average request of about 5-10 per week. The VPN group estimated a rollout of ~1000 VPN devices by the end of 2008. The VPNs use the PKI certificates to establish a secure tunnel in which data can be transmitted without eavesdropping.

The DoS PKI Program Office is responsible for signing all Java applets and ActiveX controls for use within the DoS OpenNet infrastructure. Only signed applets and controls are allowed to execute within the DoS web browser configuration. Before custom code can be released onto the network, the DoS PKI Office certifies the code as authentic with a digital signature. Without the digital signature, the code will not run. This safeguards DoS browsers against running potentially harmful mobile code on the Department’s network. Currently, there are 68 DoS applications that have been digitally signed with the DoS PKI, as well as 58 PKI installation packages.

The PKI Online Macro Signer (POMS) was initiated to provide an automated process to digitally sign macros used in the Microsoft Office suite of applications. This application can be used to secure both documents developed by the DoS, as well as those that come from outside agencies. Regardless of the source of the document, the application will help provide a security barrier against the use of malicious code that might be embedded in Microsoft Office documents. This application, which is still undergoing additional development and is in early pilot testing, currently operates as a client application. The final product, which will automatically sign Microsoft Office files and return them to their owners, will be a web-based application. POMS will resolve known, serious security deficiencies that currently exist on OpenNet with relatively little inconvenience for users.

DoS Patch Management is working with the DoS PKI Program Office to verify that all patches are digitally signed by the DoS PKI to ensure the integrity of all patches and system updates throughout the DoS.

In order to meet FDCC requirements, the DoS PKI Office has acquired a VeriSign certificate for code signing. The purpose of this certificate is to sign drivers and software that are trusted to run in the VISTA kernel. In those instances where driver support is no longer available, the DoS can now sign legacy XP drivers that have been proven to run in VISTA.

In order to support the single sign-on within the DoS to reduce the number and insecurity of passwords, the DoS PKI Program Office is working with various bureaus and posts to PKI-enable their existing Intranet applications. The DoS PKI Program Office has assisted application owners that require direct PKI-enablement of their applications (e.g., e-SCORE) as well as AD-enablement (e.g., iPost, InfoCentral, ITAB, ePhone), which allows for secure single sign-on using PKI. PKI-enablement of e-SCORE was completed by the application owner using a White Paper developed by the DoS PKI Program Office.

The DoS PKI Program Office supplies web certificates for DoS web sites that require secure authentication. To date 8,462 DoS PKI web certificates have been provided. This number includes 827 for web servers and 489 for domain controllers.

The SMART infrastructure uses DoS PKI certificates to ensure secure client and server authentication to provide non-email communications delivery to the desktop. The initial component to begin using the DoS PKI is the Live Communication Service (LCS), which SMART is using for secure instant messaging. PKI allows the LCS client to establish a secure connection to the LCS server, similar to that of a VPN.

The Immigrant Visa Allocation Management System (IVAMS) is an internet-based system used by DHS to request immigrant visa allocation numbers through a web interface, which acts as a repository for worldwide visa statistics. The DoS PKI has an agreement with DHS to generate certificates and provide smart cards for this system. To date, DoS has provided 3,023 PKI certificates and smart cards that have a three year lifetime. DoS averages about 10-15 new requests a week, in addition to the reissuance of the existing outstanding cards due to loss, lock-out, or expiration (approximately 25 per week). The DHS reimburses the DoS for the costs of certificates, hardware, and software in support of the IVAMS program. Additionally, the DoS experiences significant cost avoidance because of the PKI-enablement of this application. This PKI-enablement of this application provides an annual savings to US taxpayers of over $718,600 by reducing the time required to process requests for Visa numbers from days to less than an hour.

The DoS PKI Program Office offers support to Consular Affairs in several ways by:

1. Providing a means for the mobile Overseas Citizen Services Duty Officer to encrypt sensitive e-mails for the OCS staff assistant every morning;
2. Enabling encryption for XML inquiries/responses between the DoS and DHS; and
3. Providing the ability to encrypt and decrypt files with passport numbers between the DoS and the GPO for ePassport book production.

Consular Affair's Adoption Tracking Service (ATS) has leveraged the DoS PKI for secure user login via a web browser to support international adoptions. The ATS system is currently in the pilot stage with almost 200 adoption agencies participating. As the system matures, the number of accredited adoption agencies included in the program is expected to increase exponentially. The digital certificates sent to each adoption agency are administered through the DoS PKI Program Office.

The DoS PKI Program Office also provides encrypted e-mail service to the Bureau of Diplomatic Security (DS). PKI certificates have been issued to field agents who normally have no connection to OpenNet. These agents can now send sensitive information back to the DoS over the Internet via encrypted e-mail. There are no additional costs to the DoS associated with this effort.

The DoS PKI Program developed the FSI HR Awards Application, which is a web-based application used by FSI to digitally approve and sign awards for students using the DoS PKI. FSI assumed O&M costs for this application in 2004.

The DoS PKI Program Office is supporting the DoS Central Financial Management System in two important ways. Charleston is currently using the DoS PKI for secure communications outside the Department with ABN AMRO bank. In addition, the DoS PKI Program Office is assisting Charleston in leveraging the DoS PKI in a new development effort called COAST, the Consolidated Overseas Accountability Support and Toolkit application. This will use the DoS PKI to compress and encrypt post financial data files, and then decompress and decrypt those files at the FSC level to provide the security required for transmitting financial information and data. COAST is currently undergoing final testing, and is scheduled for release by the end of FY 2008.

The DoS PKI Program Office supplied the U.S. Embassy in Canberra with the capability to encrypt files with investigative information that they share with the Australian Federal police force. This capability used feature that was already built into the desktop software. The DoS PKI Program Office received IT-CCB approval to provide this capability DoS-wide. This tool allows the Department to secure Personally Identifiable Information (PII) both in motion and at rest.

The DoS PKI Program Office is currently working with the DoD to arrange secure access to DoD applications from the DoS network. By using the DoS PKI, selected DoD applications can now accept DoS PKI certificates for secure authentication. This means that DoD employees working overseas and domestically can securely access DoD sites from a DoS OpenNet terminal. Some of the sites currently available include:

- https://spottest.altess.army.mil/
- https://afecmo.gunter.af.mil
- https://gcss61.csd.disa.mil/gcssportal/
- https://drc010076.drc.com/jtims/index.jsp
- https://dadsdms@disa.mil
- https://jitcdod411.gds.nit.disa.mil
- https://www.av.dla.mil

This capability is key to Defense Attaché, Marine Security Guard, and other DoD personnel located at embassies and consulates worldwide. The DoS has also initiated an exploratory effort to allow these DoD personnel to directly use their DoD CAC cards to access the DoS

OpenNet network. If successful, this would not only enable acceptance of non-DoS certificates for logical access—assuming the individual has a DoS network account—but also significantly ease their access to needed DoD websites and applications, while at the same time eliminating the cost to us to provide a DoS PKI token and second smart card reader.

A-2 *Case Study #2: Government Printing Office*

Environment

PKI was chosen by the Government Printing Office (GPO) because it provides a strong barrier to fraud or forgery, and therefore provides a strong authentication seal for GPO. In addition, PKI is easy both for citizens and Internet end users to use, as well as for GPO to support administratively. These usability and operational support aspects were critical to GPO, its customers, and the American public. Over the past year (and some), the PKI technology has met these challenges. A PKI technical solution that was too burdensome to operationally administer and support for GPO personnel could not be supported by the agency. The GPO PKI project tested this extensively before production deployment in February 2008. Feedback to date from GPO constituents, customers, stakeholders and users (including the American library community) has been very positive and supportive. PKI has proven easy enough to use and operate, and cost effective, such that GPO is pleased with the outcome of this application of PKI technology in support of the GPO agency mission.

Implementations

The Government Printing Office (GPO) uses PKI to digitally sign the PDF documents it disseminates electronically to ensure citizens have reasonable confidence that they have the GPO-distributed version of a document. This is accomplished via a PKI digital signature and GPO Seal of Authentication graphic logo, which are embedded into certain GPO-published PDF documents. PDF was chosen as the first document format for this capability because of its open standards orientation, wide acceptance and adoption, and the existence of free PDF reader software so that no additional software costs to citizens is necessary. As more content becomes "born digital" and may not be destined for hardcopy printing (in which the source of publication is more tangible), this type of digital document authentication capability became part of the GPO agency strategic vision to ensure that GPO customers, stakeholders, citizens and the public can be confident in files bearing the GPO Seal of Authentication.

GPO has successfully supported PKI-enablement of the Office of Federal Register electronic submission system (eDOCS). This provides significant benefits to submitting Federal agencies in terms of avoiding courier charges and in reducing cycle times. Federal agencies that submit large numbers of Federal Register announcements via the PKI-based electronic submission method can typically recoup costs within 3 to 6 months. In addition, PKI-enablement of the electronic submission method provides a significant benefit in COOP situations.

The GPO also uses PKI to secure enterprise file storage, keeping designated files encrypted and protected from other GPO personnel. This capability is used extensively, along with PKI secure email, in the ePassport manufacturing process GPO operates in support of the Department of State’s passport program.

GPO uses PKI to secure email within the agency, and to secure email applied to certain business processes that would otherwise require manual and more costly or more time consuming methods. This has reduced cycle times significantly for some processes, thus improving service and customer satisfaction.

A-3 *Case Study #3: Department of Treasury*

Enterprise Solutions (ES) supports the decision to integrate Treasury's PKI with the GSA MSO, as there is significant value in so doing. The reasons for this belief are listed below:

Environment

Treasury is currently integrating their PKI with the GSA MSO for several reasons. Treasury began developing its PKI as an "early adopter" in 2000 to address a wide variety of business requirements. Since then, Treasury has dedicated a tremendous effort to fine-tuning and enhancing the effectiveness of the solution to its stakeholders. Further, its in-house personnel have developed an excellent command of the technology that is unparalleled in the Federal community. Put simply, PKI has become a core competency at Treasury, and is a symbol of significant pride and accomplishment.

The technological readiness of the solution to support PIV, combined with the sheer knowledge requisite for effective management of such technology, makes Treasury's PKI extremely well suited to support PIV goals, far better than other, less mature solutions.

As anyone who has implemented PKI knows, flexibility is the key to an effective infrastructure. Since Treasury's PKI is internally managed, components may be easily re-configured as Treasury's business requirements change. Indeed, Treasury has performed many such alterations in the past to accommodate its ever-changing environment. Additionally, Treasury frequently updates its PKI policies to maintain compliance with Federal policies while upholding Treasury's unique business interests.

From a strategic perspective, the benefits of such flexibility are obvious. Treasury will use PIV services in the near future, either to accomplish its own security goals or to meet Federal mandates. In doing so, Treasury must restructure its business environment to accommodate certificates issued to the PIV Card; however, this may be performed in a far easier manner with a solution that is capable of rapidly and efficiently meeting localized needs.

Treasury's PKI has an unquestionably excellent reputation throughout the Government, and stands as a shining example to other Federal agencies with an interest in implementing advanced security systems. As proof of its standing within the PKI space, the Department has forged partnerships with other Agencies such as the National Aeronautics and Space Administration (NASA) and the Social Security Administration (SSA) through the GSA PKI SSP program.

By sharing PKI resources, Treasury and its partners have realized significant cost reductions by offsetting operating expenses, and the Department is currently evaluating partnership opportunities with other Agencies to continue reducing its costs. More importantly, the tremendous forward momentum Treasury has gathered through this collaboration has led to an in-depth understanding of PIV-related technological and policy requirements, which has resulted in the successful deployment of "PIV ready" PKI systems for its partners. These are noteworthy advantages and will be leveraged to great effect in supporting the Department's own PIV solution.

Implementations

Digital certificates issued by Treasury’s PKI bear the Department’s “seal of trust.” Just as one may associate the United States dollar with the nation’s strong and stable economy, digital certificates with the Treasury name reflect a significant degree of trust.

As these certificates are used to secure business transactions, information contained within them may be traced to specific Treasury policies that indicate their trustworthiness. For example, these policies require a highly secure operating environment that is 100% U.S. Government owned and operated. Considering that Treasury’s PKI is used to secure highly sensitive financial systems, many of its policies are unique within the Federal environment, even amongst other Agencies with considerably secure PKI solutions.

Additionally, Treasury was one of the first four Agencies to establish a trust relationship with the FBCA, and continues to serve a prominent role in this community. This enables Treasury’s certificates to be trusted by other Agencies, supporting PIV interoperability goals and enhancing value across the Federal IT environment. The importance of trustworthiness will be increasingly apparent as Treasury’s PIV certificates become more commonplace and relied upon.

Usability

Today, Treasury issues digital credentials to its business community to lend security benefits to applications, meet Federal goals, avoid unnecessary costs, eliminate paperwork, create workflow efficiencies, and increase its viability in the electronic Government marketplace.

Currently, Treasury’s PKI is used at many Bureaus, including Departmental Offices (DO), Bureau of Engraving and Printing (BEP), Bureau of the Public Debt (BPD), Financial Management Service (FMS) and the U.S. Mint. Collectively, the PKI is used to protect trillions of dollars per year by lending strong authentication, encryption and digital signature services to mission-critical applications such as the FMS Secure Payment System (SPS).

By issuing Treasury PKI certificates to the PIV Card, the Department will benefit from a smoother, less costly integration with current and future applications reliant on PIV services.

A-4 *Case Study #4: CertiPath Bridge*

Environment

For Aerospace and Defense (A&D), open standards based PKI technology was identified as the key enabler for identity and verification anytime, anywhere in the world by any party. In A&D, CertiPath does not look at any one use case or data sharing scenario as justifying the cost of PKI. CertiPath sees some very good applications of PKI right now including:

- SecureEmail with S/MIME supported by "LDAP Proxies" that handle the issue of finding your recipients public key automatically. CertiPath had its first production usage of this in December 2008 between Northrop Grumman and the US DoD. The UK and NL MoD's as well as the other major integrators are bringing their infrastructures online and having them certified now
- Convergence of PACS/LACS such that a "one badge" solution is realistic not only for one's organization but for visitors to the organization. A visitor shows up, uses their organization issued badge with PKI digital certificate on it (i.e. private key challenge) and goes to a conference room where they logon to a visitor network.
- Digital identities of planes/avionics, ground stations and maintenance crews. Whether it is the avionics being provided from a supplier to the airframe manufacturer or the airline taking delivery of the plane, all of this is now utilizing digitally signed avionics code with a resigning during maintenance periods. When the plane is in the air, it must talk to ground stations or satellites when over water. This is essentially a Secure Sockets Layer (SSL) session. Today it is unencrypted - but with Secure ACARS, there will be a global network of stations and airplanes that all must authenticate to each other, each potentially having a credential issued by a different provider. Having a, very literally, portable identity, able to be trusted globally is crucial to this effort's success.

Implementations

Unique to PKI is the ability to have multiple levels of assurance that can be evaluated accurately by a relying party upon its receipt of the credential. This is absolutely essential to having a technology approach to address an extremely wide spread set of potential use cases. PKI today is used to encrypt IM sessions at extremely low levels of assurance while simultaneously, an end user uses medium-assurance hardware credentials to access extremely sensitive information (i.e., encrypt the entire hard drive). Scalability requires such flexibility and there are no other technologies with this level of adaptability - this might be justification enough for PKI.

In virtually every circle CertiPath is in, PKI has long been a foregone conclusion and most of the time is now spent on working on how to make PKI based authentication events scale by means of federation. It feels like we should be well equipped to justify investments in PKI.

A-5 *Case Study #5: SAFE (Johnson & Johnson)*

Environment

Johnson & Johnson (J&J) has an enterprise PKI with almost 90,000 subscribers (out of a total J&J workforce of about 120,000). J&J issues two PKI certificates to each subscriber: signature certificate and encryption certificate. Virtually all subscribers have their certificates on FIPS 140-2 level 2 (SafenetiKey 2032) hardware tokens. J&J is cross-certified with the SAFE Bridge CA, which is cross-certified with the FBCA. In addition, J&J uses CoreStreet On-line Certificate Status Protocol (OCSP) responders. J&J has a contract with Chosen Security for RFC 3161 trusted time stamp services when doing Adobe digital signatures.

Implementations

The principle uses of J&J PKI certificates are:

- Two-factor remote access to the J&J network (for authentication to the network to create an IPSEC tunnel);
- Secure e-mail (digital signatures and/or encryption);
- Hard disk encryption (about 10% deployed to date but growing),with the decryption private key on the user's hardware token used to start the boot process; using SecureDoc's product;
- Adobe digital signatures for compliance with FDA requirements, and for other non-regulated business purposes;
- SSL user authentication; and
- SSL web site certificates.

Currently, there are over 2,500 internal J&J web sites that use J&J SSL web certificates, thus saving the cost of having to purchase from an external source. There is no problem with trusting these web sites since they are internal, and the J&J root is in all of the J&J laptop/desktop CAPI key stores as a trusted root.

The realized value to J&J of using PKI is threefold:

1. Strong authentication - no "ROI" can be calculated for this element, it is just a matter of ensuring two factor user identity protection to guard against impersonation, and for a large enterprise, PKI is the least expensive and most extensible mechanism that meets that need;
2. Strong electronic signatures - "digital signatures" that meet FDA requirements. Again hard to calculate the ROI for this, but rough estimates are net savings in excess of $1M annually, which will grow over time as such use grows, as we have already seen.
3. Strong encryption - again no ROI can be calculated, but the prospect of losing personal data or company data, causing potential damage to the company's reputation or economic interests, is clearly significant, and use of PKI is again the most cost-effective and secure way to do this.

For example, in using hard drive encryption with SecureDoc, J&J does not have to worry about managing a separate set of passwords for booting - users just employ their PKI token. If the user loses their token, J&J can do a private decryption key recovery. In fact, many J&J users who travel extensively carry a backup PKI token containing only their private decryption key, so if their main PKI token, which has both the signature and decryption keys, were lost, stolen or destroyed, the backup PKI token is available to get the system booted. Once booted with the backup PKI token, J&J employs a recovery process to issue new keypairs/certificates.

A-6 *Case Study #6: State of Illinois*

Environment

The State of Illinois operates a Public Key Infrastructure (PKI) environment that provides authentication, encryption, and digital signature capabilities to all governmental entities that wish to use it. This service became operational in January of 2001. This infrastructure allows these agencies/entities to provide secure internet-enabled sites that allow a high-level of authentication to applications, secure encryption capabilities, and digital signing of documents, thus providing better service to our citizens and greater savings to the Agencies.

The PKI initiative crosses almost all traditional demographic boundaries. We estimate that 85-90% of PKI users are normal citizens conducting business with various Governmental entities. Clients will be usually be over the age of 18, and can be either male or female. The purpose of business will range from individuals filing a complaint with the Pollution Control Board to checking Medicare benefits with the Department of Health and Family Services.

A PKI environment is basically a trust environment. In order to issue certificates, we must be reasonably sure of the certificate holder's true identity. This is why the State of Illinois utilizes a stronger method of client authentication than most systems. This helps them ensure that when a certificate is presented to an entity for processing, the entity has a high level of assurance that the person is, in fact, who they say they are. This is important in combating such things as identity theft and Internet spoofing.

That environment has grown tremendously in Illinois over the past four years, as more and more agencies realize the importance of maintaining the integrity and security of their data, the opportunity to streamline online transactions and the ability to improve public access to their services. Since the statewide contract means that agencies don't have to build this capability themselves, they save money and time. In May of 2003, the State of Illinois had issued approximately 5600 digital certificates; the count now stands at over 133,000 with an average monthly growth of over 900 certificates. The State of Illinois have more agencies that are implementing applications and taking advantage of not only the established authentication mechanism, but also the security and digital signature capabilities provided.

In late December of 2003, the State of Illinois became the first State in the union to successfully cross-certify with the Federal government. This Federal entity, known as the "Federal PKI", paves the way for easier interaction between State and Federal agencies. To illustrate this, a proof-of-concept project was adopted and implemented. This project began in October of 2003, and concluded the week of April 26th, 2004. Participants in this proof-of-concept were the State departments of CMS and EPA, and the Federal entities of EPA, GSA, and various third party contractors. This project proved that interaction between State and Federal applications can be achieved via the Federal Bridge and Public Key Infrastructure.

Implementations

In the emergency preparedness arena, PKI technology enables the Illinois State Police to provide local public-safety entities access to the State Terrorism Information Center, the Chicago Department of Public Health to provide medical facilities with access to its Health Alert

Network, and the Illinois Terrorism Task Force to provide secure biometric credentials to first responders.

Using PKI, Medicaid providers locate client benefit information online, future teachers apply for financial aid via the Illinois Student Assistance Commission, and water treatment facilities submit their wastewater discharge monitoring reports with the Illinois EPA.

To date, 15 other states have contacted Illinois for advice about how they can use the technology to improve their own government operations. And CMS has been asked to speak about its success at a national Gartner Group conference in June.

Some of the current functions utilizing PKI are as follows:

- Accessing the Health & Family Services Medi system to check on Medicare claims.
- Accessing the Department of Aging web site to check on benefits for the elderly.
- Filing electronic water discharge reports to the Environmental Protection Agency. (This was the Federal/State proof-of-concept application)
- Accessing the City of Chicago's Health Alert Network system.
- Providing encrypted background checks to schools, etc, using the Illinois State Police CHRI system.
- Obtaining teacher education scholarship information via the ISAC "CollegeZone" web site.
- Viewing filings and board opinions of the Pollution Control Board.
- Securing email for Illinois State University.
- Providing access to legacy applications through the Internet.
- Kane County Circuit Clerk's office utilizing digital signatures on biometric flash drives for use by Judges.
- Digitally signing internal forms by the Illinois Department of Transportation.
- Providing digital signing and encryption capabilities for administrative personnel at Southern Illinois University at Carbondale.
- Digital signing of police reports by the City of Rock Island.
- Providing encrypted email for Central Management Services.

A-7 *Case Study #7: Department of Defense*

Environment

The DoD issues hardware-based PKI certificates to each DoD civilian employee, each military service member, and sponsored contractors. The primary implementation of the DoD PKI smartcard is effected by the issuance of the Common Access Card (CAC). The CAC is the standard hardware token for the Non-Classified Internet Protocol Router Network (NIPRNET). The CAC-based certificate supports a number of DoD applications as follows: 1) encryption and digitally signed e-mail, 2) authentication to website information and stores, 3) Smart-card login to DoD networks as a strong authentication replacement for passwords 4) digital signature of forms. The DoD has issued over 15 Million CACs. The DoD PKI also issues PKI software certificates to DoD users and web-servers. There are currently over 500,000 software certificates issued by DoD, and 98% of DoD private web-servers are protected by DoD PKI issued software certificates. Over 42,000 certificates are active on the Secret Internet Protocol Router Network (SIPRNET).

On April 9, 1999, the ASD (NII) consolidated the responsibility for the DoD PKI under a single PMO. This responsibility was assigned to the National Security Agency (NSA) with operational support from the Defense Information Support Agency (DISA). In response, NSA and DISA have established a central PMO that will ensure the DoD PKI supports validated and endorsed Public Key (PK)-enabled systems and applications that meet the broad spectrum of DoD mission and business needs. The DoD PKI maintains a Help Desk at Oklahoma City, OK. The Help Desk handles Tier 1 calls and forwards anything higher to the technicians located in Chambersburg. The Help Desk operates around-the-clock (24x7) services for PKI users at all levels and will take calls or e-mails from a DoD user/RA/LRA experiencing a problem with PKI.

In compliance with Homeland Security Presidential Directive 12/HSPD-12, the DoD began issuing its revised CAC in October 2006. Pursuant to the President’s mandate, the new HSPD-12 compliant card contains advanced technology, which will enhance the security of Federally controlled facilities and computer systems and ensure a safer work environment for all Federal employees and contractors. As of March 2009, the DoD has issued 1,739,710 PIV Cards. Additional improvements are planned for updated PKI certificate cryptographic algorithms and validation that will support HSPD-12 logical access requirements.

In addition, the DoD PKI Program Office is planning enhancements to its classified networks PKI infrastructure to support issuance of a hardware token for the SIPRNET. Hardware PKI certificates will enhance the information assurance environment on the SIPRNET to support the Global Information Grid (GIG).

Implementations

The DoD PKI is structured to support the rapid acquisition of mature technology and to take advantage of the steady pace of advances in technology available from industry. The DoD PKI, based on commercial industry standards, is being deployed as an evolutionary rollout in multiple increments and spirals to the existing infrastructure, introducing new features and capabilities in an orderly fashion, consistent with commercial technology progression. The implementation of future system capabilities will be introduced in parallel with existing operational capabilities. The implementation of these enhancements will be transparent to the existing user base.

The DoD PKI is engineered as a highly reliable system to support GIG mission critical applications and systems. The PKI system architecture provides robustness and scalability for certificate issuance, revocation management, key escrow, and sub-component system availability. The DoD PKI incorporates system redundancy to enhance failover and meet COOP requirements. The DoD PKI architecture includes the following: 1) a load balancing capability, 2) a switching architecture designed for network segmentation of traffic to reducing networking latency and improved performance, 3) Certificate Authority (CA) mirroring to provide efficient and effective recovery from hardware component failure. In addition, the DoD PKI is in the process of adding a second source of CAs to remove the dependency that the DoD currently has on a single vendor. The DoD PKI has incorporated a PKI enterprise authoritative capability to issue PKI certificates reflecting the unique identity of an entity. This capability is in the form of a unique number similar to the DEERS/RAPIDS Electronic Data Interchange Personal Identifier (EDI-PI). The permanence of the unique identifier of the certificate attribute supports the certificate discovery process on SIPRNet. The DoD PKI enterprise design delivers a reliable and high-performance DoD PKI with 99.9% system availability.

The DoD PKI incorporates a system monitoring function that detects anomalies and ensures rapid service restoration. The system monitor ensures CAs are available to issue certificates and CRLs properly. The system monitor function supports higher levels of assurance for DoD's GIG mission operations, and watches for behavior that could indicate unauthorized behavior within the infrastructure environment. The automated monitor function maintains awareness of the PKI system in a cohesive manner across registration centers (1500), CAs (16) and issuance portals (10).

Validation of DoD PKI certificates (for revocation) is required by relying parties to ensure the trustworthiness of any information PKI based information transaction. Relying parties must be able to determine in real time that a certificate is valid as the certificate is presented to the relying party for authentication.

In response to the requirement to support minimization of validation bandwidth utilization, the DoD has fielded a real time certificate validation capability, known as the Robust Certificate Validation Service (RCVS). RCVS implements a commercial standards-based capability known as OCSP. OCSP allows a client workstation, with appropriate OCSP software plug-in, to request the status of an individual PKI certificate at an Enterprise OCSP responder. The enterprise OCSP responder provides a response back to the client application in less than 1 second (depending on network performance) allowing it to make a validity decision about the PKI certificate received. While the RCVS solution still requires the CRL to be generated and published every 24 hours, and downloaded from Global Directory Service (GDS), the CRLs will no longer be required to be downloaded to the client workstation. Each RCVS node supports as many as 650,000 DoD client workstations. Full enterprise deployment of RCVS will include 6 NIPRNET nodes and 1 SIPRNET node.

All DoD users, to include applications such as PKI based network logon and Defense Travel Service (DTS), are able to make PKI Certificate validity checks in near real time without having to download large CRLs from multiple CAs every day. Moving to robust certificate validation mechanisms has the effect of reducing network bandwidth demands and associated burdens on user processing assets. In addition, robust certificate validation greatly reduces response times for mission operations. DoD operations have to maintain the ability to change or revoke each credential and every GIG resource has to be able to validate that each received credential is not forged or revoked. Furthermore, this reduces the potential misuse of invalid certificates if CRLs are updated in a timely manner.

Network logon is critical to virtually all electronic operations across the Department. Through a series of Communications Task Orders, the DoD has mandated the implementation of certificate-based network logon using the services of the DoD PKI for the network components as well as subscriber CACs. The Smart Card Logon (SCL), also called Cryptographic Logon, capability enables users to log onto their unclassified network using their Common Access Card (CAC) and associated Personal Identification Number (PIN) instead of a username and password. SCL provides the increased security of two-factor authentication by allowing users to access their network with something they have (their CAC with DoD issued certificates) and something they know (their PIN).

The current DoD implementation of SCL requires Microsoft Active Directory in the root domain. SCL requires DoD user workstations with DoD-approved Windows operating systems, smart card readers, drivers, and the appropriate version of middleware. The Active Directory account associated with each user is populated with Electronic Data Interchange Personal Identifier (EDI-PI) numbers associated with the user's CAC certificate.

Once users start using SCL to access their unclassified networks, they no longer need to remember their ever-changing and complex network passwords. SCL is a more secure method of network logon because the PIN is not stored on or transmitted over the network.

Today, information transactions on DoD networks include: business; logistics; personnel; medical; sensitive but unclassified information; command and control; and other sensitive information that requires strong identity management. Username/password-based network logon remains the weakest link in protecting critical electronic operations across the Department. DoD users and system administrators also benefit from having a common process for network logon that will reduce the need for passwords and the associated administrative overhead for lost or forgotten passwords, time lost and reduced operational tempo because of lost or forgotten passwords. Lt. General Croom, former DISA Director and Commander JTF-GNO- has cited a 46% reduction in NIPRNET Intrusion Activity as a result of SCL implementation.

The DoD PKI has issued PKI certificates to support all DoD private web-servers. A private web-server is defined as any web-server that restricts public access to all or some of the information it contains. The issuance of server certificates means that DoD Users accessing a web-server are assured that it is a valid DoD server and that sensitive information exchanged between the client and server is encrypted. The DoD PKI has issued over 10,000 web-server certificates.

To assist the DoD PKI community in the PK-enabling (PKE) of applications, the DoD PKI PMO established and maintains a PKE information sharing site on the Army Knowledge Online (AKO). The site maintains resources, FAQs and contact information for those DoD organizations seeking assistance for PK-enablement of DoD applications.

It is DoD policy that all PK-enabled applications be tested to ensure interoperability and compatibility with the DoD PKI. The Joint Interoperability Test Center (JITC) at Fort Huachuca provides testing of COTS and GOTS applications for the DoD and PKI vendor community. The JITC process consists of the following: 1) Review of the JITC assessment worksheet 2) analysis of the application 3) test execution, 4) analysis of data, and 5) on successful interoperability test completion of the certification letter. Over 75 COTS and GOTS applications have completed formal JITC interoperability certification.

Appendix B - Entities Cross-Certified with the FBCA

Cross-Certified Entity:	FBCA Assurance Level:	Cross-Certified Date:
Department of the Treasury	High	September 18, 2002
	Medium	September 18, 2002
	Medium Hardware	** August 14, 2007
Department of State	High	January 21, 2004
	Basic	** September 25, 2008
	Medium	** September 25, 2008
	Medium Hardware	** September 25, 2008
	High	** September 25, 2008
State of Illinois	Basic	** January 13, 2009
ACES/Digital Signature Trust	Medium	February 11, 2004
DoD External CA (ECA) *	Medium	** January 13, 2009
	Medium Hardware	** January 13, 2009
ACES/ORC, Inc.	Medium	** February 8, 2005
US Patent & Trademark Office	Medium	June 1, 2005
Wells Fargo *	Basic	** October 4, 2006
	Medium	** November 12, 2008
	Medium CBP	** November 12, 2008
	Medium Hardware	** November 12, 2008
	Medium Hardware CBP	** November 12, 2008
Government Printing Office	Medium	** December 13, 2005
	Medium Hardware	** February 12, 2008
Department of Justice	High	** December 15, 2005
CertiPath Bridge	Medium	** May 9, 2006
	Medium CBP	** May 9, 2006
	Medium Hardware	** May 9, 2006
	Medium Hardware CBP	** May 9, 2006
DEA CSOS *	Medium	June 13, 2006
United States Postal Service	Medium	** October 20, 2006
	Medium Hardware	** February 12, 2008

DoD Interoperability Root CA	Medium Hardware	** July 10, 2007
SAFE Bridge	Basic	May 20, 2009
	Medium CBP	** February 12, 2008
	Medium Hardware CBP	** February 12, 2008
VeriSign	Rudimentary	** December 19, 2008
	Basic	** December 19, 2008
	Medium	** December 19, 2008
	Medium Hardware	** December 19, 2008
Verizon Business	Basic	** March 10, 2009
	Medium	** March 10, 2009
	Medium CBP	** March 10, 2009
	Medium Hardware	** March 10, 2009
	Medium Hardware CBP	** March 10, 2009

Legend:

*** FBCA issued cross-certificate allowing one-way trust.**

**** This was the date the Federal PKI Policy Authority voted on and approved issuing a FBCA cross-certificate.**

Table accurate as of September 16, 2009.