HSPD-12/PIV Credential Solution Migration Feasibility

When considering management and technical challenges associated with migrating from one service provider to another within solution lifecycles, there are a number of critical concerns within Homeland Security Presidential Directive -12 (HSPD-12) or PIV Credentialing solutions (inclusive of HSPD-12 related technical solutions[1]). To fully address these challenges, Agencies must engage comprehensive planning and technical assessments, or Agencies risk significant impact to business-enabling technical services (for their user constituency) and even greater impact to IT investment management. Investment concerns include considerations to "sunk costs", service continuity, and operational costs required to succeed in transition activities/effort.

1 BACKGROUND

Following the publication of HSPD-12, the National Institute of Standards and Technology (NIST) published the standard with Federal Information Processing Standard 201-1 (FIPS 201)[2]. This standard was augmented with additional technical and operational guidance through the NIST 800 Series Publications[3]. These documents provide a definition for the base components and operational processes that must comprise an HSPD-12 solution. Subsequent to the publication of these standards, the Federal CIO Council published guidance in May 2009 related to PIV interoperability[4]. This publication serves as definition for PIV-Interoperable (PIV-I) credentials for non-Federal issuers (NFIs) such as State, Local, other Jurisdictional governments and private sector or commercial organizations.

The Federal CIO Council outlined the parameters that will allow Federal government reliance (trust) in PIV-I identity cards. It identifies that PIV-I credential are required to technically comply with PIV specifications so as to technically interoperate with Federal government PIV systems. It also requires trust elements in the processes associated with issuing PIV-I credentials. A PIV-I credential requires a commensurate level of stringency and rigor in the operational processes of enrollment, registration, and issuance as PIV credentials. Any PIV-I based solution further requires the technical solution meet the same specifications as outlined by the NIST for PIV credentials. Therefore, any organization supporting issuance of PIV-I credentials should consider this background as equally applicable to their technical solutions and operating environments.

1.1 Technical Solution

PIV credential issuance solutions involve a complex mix of technologies that work collaboratively to deliver a PIV identity card as a productized output. PIV solutions can also serve as the most authoritative source of organizational Identity data, which can be leveraged to add value to other business needs and services.

These technical solutions can be described best in terms of the back-end infrastructure and the PIV workstation components of the solution. As to the back-end infrastructure, the core server-side components include the Card Management System (CMS), the Public Key Infrastructure (PKI) services, the Identity Management System (IDMS), and the Biometric Management

1 Solutions such as PIV Interoperable (PIV-I) or PIV Compatible (PIV-C) solutions as well

2 http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

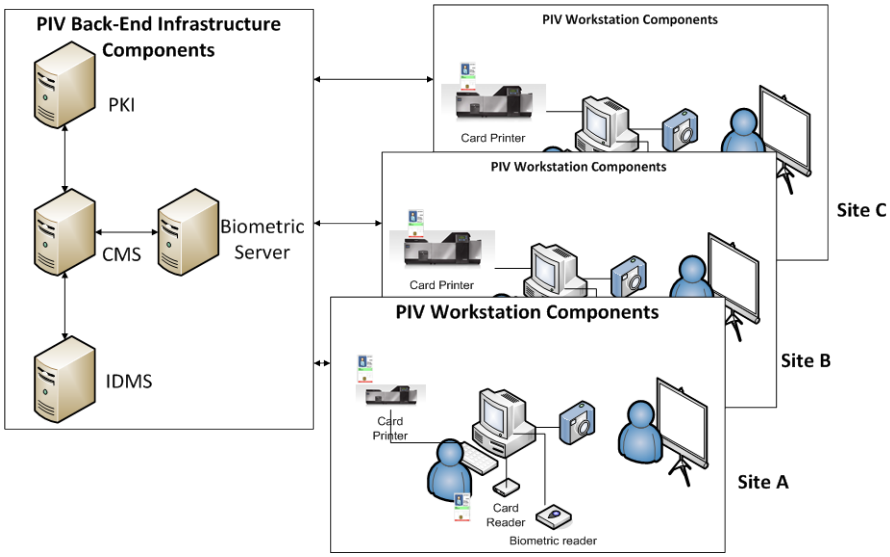
3 http://csrc.nist.gov/publications/PubsSPs.html

4 Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers, May 2009 (http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf)

Service. These core server-side components are typically COTS products which are authorized or certified on the HSPD-12/PIV Approved Product List (APL)[5]. Together, these core technologies comprise the PIV Card Issuance and Management Subsystem as defined in FIPS 201-1 Section 3.1.2.

As for the PIV workstation components, there are integral technologies that comprise an interoperable workstation-based solution that can work appropriately with the back-end infrastructure capability/services that are established by or on behalf of the Agency. This component of a PIV/PIV-I solution incorporates software that interacts with the back-end infrastructure over agreed upon service interfaces. Typically, this interaction is primarily between the workstation (and its software) and the back-end infrastructure's IDMS. In some cases, there can be interaction directly to the CMS component as well, depending on the design of the solution. The workstations are comprised of peripherals, plug-ins, and software such as: biometric capture devices, smart card reader devices, digital camera devices[6], biometric software plug-ins, etc. In some cases, there is a local PIV credential issuance capability[7], although other paradigms support a "bureau of printing" approach that distributes the PIV or PIV-I credential for activation upon receipt[8]

1.2 Operational Processes



The operational processes of PIV/PIV-I must comply with FIPS 201-1 Part 1 and NIST 800-79 process controls. They require comprehensive background checks to be performed for any potential credential holder. They also require an appropriate separation of duty from authorized "roles" that can process credentials for issuance. These roles work across the Enrollment, Registration, and Issuance phases of the credential issuance process. These process controls are in place to ensure appropriate trust can be asserted in identity of a PIV or PIV-I card holder when the card is presented to physical or logical access points to authorize appropriate access. The operational processes of PIV/PIV-I are enforced within the IDMS products within back-end infrastructure solution components.

5 http://fips201ep.cio.gov/apl.php

6 Devices that capture a Card Applicant's photo that will be incorporated into the resulting PIV/PIV-I identity card credential

7 Specifically, there is a smart card printer local to the Issuance facility, such as in the case of the VA's PIV System solution

8 i.e., the card is mailed to the recipient and subsequently activated by them with appropriate process controls in place to bind the credential to the person, such as in the GSA USAccess credential solution approach.

2 VENDOR LOCK TRANSITION CHALLENGES

Technology solutions operate within a solution lifecycle that involve input of data, manipulation of data, and storage of data (as part of solution archive capabilities). That is to say that any technical service provided by an Agency will manage data within several operating states. Herein resides the complexity with HSPD-12 solution transition.

HSPD-12 based solutions utilize services of a federally-recognized or certified PKI Shared Service Providers (SSPs). PKI is used to provide certificates that are embedded in the logical processing chip of the credential (i.e., the gold Integrated Circuit Chip (ICC) on the smart card). The policies of Federal PKI introduce very specific constraints that must be considered as a factor of PIV solution transition. The most significant issue is the role a CMS product fulfills, which is to serve as the PKI service's PKI Registration Authority (RA)[9]. Federal PKI requires SSP services be sustained as a measure of ensuring government-wide trust in authorized PKI services, and PIV credentials rely on these trust services as a factor of the trust and assurance they provide for Agencies.

Additionally, there are security designs within CMS COTS products that impose constraints to technology portability and migration. A CMS application's security model will restrict relationships of issued PIV cards to specific PKI SSP providers. In addition, CMS will protect PIV and PIV-I smart card stock used for issuance by way of a Transport Key (TK)[10]. This means that any issued credential is "locked" to a current PKI SSP as well as to a particular instance or implementation of the CMS platform (*operating under the assumption that this problem statement was not considered as a function of solution design and implementation*).

2.1 PKI Vendor Lock Issue

The impact associated with absence of the PKI service would be a loss of any ability to service certificates loaded onto production PIV/PIV-I credentials. Absence of the PKI service can be caused by PKI SSP contract termination or expiration. The loss of an ability to revoke PKI certificates that are resident on production PIV/PIV-I cards introduces a policy conflict within the Federal PKI Common Policy[11]. Historically, this policy conflict has been identified by PKI SSPs during contract re-negotiations, which in essence instills "vendor lock" to their services. Service providers extoll this non-obvious PKI policy conflict when an Agency makes a determination to consider alternative solutions that offer better economic models or improved solution performance. This issue becomes more obvious when the Agency starts planning for solution migration to alternative offerings (or services) from other industry providers. Only then do Agencies realize that the costs to migrate from Provider A to Provider B will require a continuation of PKI SSP services to address certificate management needs (e.g., revocation capabilities and management of archived certificates that are integral to PKI SSP Key Management Archive (KMA) responsibility[12]).

9 The PKI RA is the trusted role that can interact with the SSP's Certificate Authority to requests, modify, renew, or revoke certificates.

10 A Transport Key is an asymmetric cryptographic key that protects the Card Stock from being intercepted and used to produce a fraudulent PIV or PIV-I Card, and these are required as a part of the PIV standard.

11 X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf)

12 PKI SSPs are obligated as part of their Certificate Practice Statement (CPS), Registration Practice Statement (RPS), and more directly as part of their Key Recovery Practice Statement (KRPS) to appropriately manage the archive of data encipherment (e.g., encryption) keys for a retention period of 10.5 or 20.5 years (depending upon the level of assurance and trust asserted in the certificate consumed/used by Agencies).

PKI SSPs are also quick to identify that they are under no obligation to provide KMA services to Agencies or commercial organizations for free. Though the data may be the property of the government (or the Agency), this does not imply that services to manage this data are expected to be provided at no cost. Since the KMA concern is non-obvious, and most concentrations within contract/acquisition approaches seek to **enable** enrollment and issuance capability, the long-term key archive management needs or the revocation capabilities for production certificates are typically not incorporated into contract language or program operating budgets as a function of addressing solution transition needs.

Agencies quickly find themselves in a "vendor lock" situation, and discover that they planned insufficient program budgets to adopt transition strategies to lower cost or better performing/better fit solution to meet Agency needs. This is because they must address costs for continuation of service with current Providers, while they adopt new costs for an alternate Provider as a function of any considerations for transitioning.

2.2 CMS Platform Lock Issue

The very design of a secure CMS platform introduces constraints on technology or service mobility. These issues are difficult to resolve, since solutions portability run counter to the very security protections designed and offered within a properly configured CMS COTS solution.

CMS application architectures are designed to be very secure, and they offer robust controls to protect Card Stock from fraudulent use (should it be intercepted), as well as a secure binding of issued cards to digital credential service providers (i.e., PKI services). This provides added protections against man-in-the-middle attacks for soon-to-be trusted credentials, and are designs embedded into best-of-breed CMS solutions for issued/production cards. These constraints should never be considered a design flaw a CMS COTS application, but a security benefit that should be expected from a robust CMS platform implementation. These "portability challenges" are further exacerbated by their use of strong asymmetric cryptography which serves as the enforcement mechanism that protects both Card Stock and integrated card components (i.e., digital PKI credentials used within the smart card).

When an Agency seeks to migrate to a new service provider for PIV/PIV-I issuance services, they discover barriers to transition strategies once these technical design elements of the CMS platform are discovered. The specific set of barriers includes:

- A sunk cost in current PIV Card Stock used by the current PIV issuance provider, which is locked to a specific CMS platform by use of the TK that protects the supply line of trusted card stock.
- A strong binding between the smart card holder/user and their PKI credentials, which therefore locks the user to a specific PKI SSP that issues those credentials for continued certificate management services
- Agencies do not normally plan program budgets to address cost needs for sustaining exiting CMS platforms while migrating to newly established CMS platforms.

PIV and PIV-I credentials typically have a three year life, which implies that Agencies would need to absorb costs for operating two CMS platforms as a function of transition to a new Provider. Seemingly, an existing CMS production solution would need to be maintained until the last PIV/PIV-I user is migrated to any newly established CMS provider/capability; while in parallel Agencies develop issuance strategies to new PIV/PIV-I providers to transition users to new services from the newly established Provider capability. This revelation results in a massive

business constraint, which is the introduction of significant cost for maintaining two PIV/PIV-I issuance capabilities. The results of which are increased burdens on Program Offices, and introduction of unplanned funding challenges as a function of service sustainment, and the potential of imposing training/education demands on serviced populations (i.e., the users) that can further drive transition complexity and cost.

The security features of CMS also increase management burden when adopting a new PKI SSP to service existing PIV/PIV-I user populations. The implementation of a new PKI SSP relationship to the CMS component/platform is a solution feature from any industry-leading CMS COTS product, wherein the CMS platform can readily integrate several PKI services as a measure of its service flexibility. However, existing card populations (i.e., users) will continue to require PKI services from existing PKI SSPs to permit certificate/key revocation capabilities when considering the transitioning of users to newly established SSP services. This binds PIV/PIV-I programs to services of existing PKI SSPs (as previously indicated in the *PKI Vendor Lock Issue*).

The results of these identified transition issues are increased program management, technical sustainment, and user education needs that typically result in a business decision that make it cost prohibitive to adopt alternative business models or Provider solutions, so an Agency can enjoy the benefits of economic competition with PIV/PIV-I outsourced solutions. In essence, the very design from standards for PIV can work counter to business flexibility, due to non-obvious technical and business constraints imposed when an Agency adopts a specific service Provider.

3 VIABLE HSPD-12 AND PIV-I TRANSITION OPTIONS

Despite the seemingly impossible challenges of PKI and CMS constraints, Agencies do have options to engage in low cost transition approaches for migrating from one PIV/PIV-I service Provider to another. To fully understand these options requires a significant amount of subject matter expertise in HSPD-12 and all of its related technologies. However, options can be described in business terms that can be more readily understood as a function of transition planning. Though there are costs associated with transition from Provider A to Provider B, costs can be manageable depending on a number of existing contract factors and with availability of some program budget to fully address needs for solution transition.

Core to any transition consideration is an understanding of contractual rights of the Agency. It is imperative that the Agency retain the rights-to-data for any certificates, keys, cards, or technical platform controls are in place for their PIV or PIV-I solution. This means that, though a turnkey solution may be "owned" by the Provider/Vendor, the data remains as "owned" by the Agency.

In this contractual relationship, the turnkey vendor is merely the data steward of data that belongs to the Agency. For Federal and State level government Agencies, these contractual clauses and controls are almost always in place, wherein the rights-in-data clauses protect the Agency interest and mitigate the risk of data ownership being transitioned to a technology service provider[13]. With the proper establishment of data ownership in place, the Agency is able to engage in transition strategies that are further outlined in the following sections.

13 Agencies that are unsure of their rights to data should verify their rights with their internal General Counsel or legal departments, to validate that they do indeed have the ownership over data that pertains to the Agency users or customers.

3.1 The Importance of CMS "Ownership"

The most critical technical element of PIV/PIV-I solution transition is ownership, possession, and management of the CMS. The operative word in CMS is from the "M" which is the abbreviation for "Management". A CMS is the lifeblood of a PIV/PIV-I issuance capability, and inability to secure this asset will result in an inability to fully transition services without a total loss of sunk cost investments. Where an Agency has the capability to migrate the CMS to their control, there are options that become available to preserve existing sunk cost investments in deployed capabilities and solutions. A best-in-class **HSPD-12 Integrator** can engage options to preserve sunk cost investment in PIV/PIV-I thought re-establishment of the CMS under Agency control. This permits forward looking integrated solutions that can preserve 100% of Agency sunk costs in PIV/PIV-I, and permit models of economic advantage with new service Providers at a lower overall cost, as opposed to abandoning investments in issued trusted credentials.

3.2 Addressing PKI Certificate Archive Concern with PIV Cards

Some Agencies utilize services of PIV or PIV-I credentials with other business services. Of particular interest is use of PKI with email, or what is known as Secure Email or S/MIMEv3[14] based email. Where PIV/PIV-I credentials are used as an enabling technology for secure email services, there are additional business needs that must be addressed with regard to PKI encryption keys stored within the PKI SSP's KMA service. Agencies that do not extract these archived keys from the KMA can perform a denial of service event on their user populations who leverage these keys to engage secure email capabilities/services.

To address this need, CMS can be configured to permit legacy PKI data encipherment certificates/keys to be stored in PIV "PKI containers" to ensure accessibility to users. To exploit the capability of extracting keys from a PKI SSP requires a PIV Card configuration with Java Applets in smart card that permits insertion of archived keys into "PKI containers" on the Card. Enabling this capability requires a deeper understanding of specific configurations of the Agency PIV Card profile, which can be seen within the CMS platform. An assessment of whether the PIV Card profile could be modified to allow use of PKI archive certificate containers on updated cards can be done by a certified CMS and HSPD-12 integrator vendor to determine viability of this potential business option. Where it is deemed infeasible to modify the card profile(s), the remaining option can be obtrusive to large enterprise customers, since it requires decryption of all existing mail messages, and re-encryption of those messages using updated PKI encipherment keys/certificates when they are made available to the end user/PIV card holder.

4 VENDOR QUALIFICATIONS

Any vendor that wants to succeed in the management, planning, sustainment, or operations of HSPD-12 (*as well as ICAM*) technical frameworks must be dedicated to engaging industry and keeping pace with the evolution or changes associated with these technologies.

The GSA has established a certification program that reviews capabilities of industry vendors, and which results in a certification in HSPD-12 capabilities across a number of service categories. This program was established as a result of Directives such as: *OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* and *OMB M-06-18 Acquisition of Products and Services for Implementation of HSPD-12*.

14 S/MIMEv3 is the industry standard for enabling secure-email services, and it standards for Secure Multipurpose Internet Mail Extensions version 3.

Important to note with regard to certified vendors is the Service Category they are assigned, ensuring that a *Certified Systems Integration Services and Products* vendor is used for these efforts. This is because the other categories of service (e.g., *Activation and Finalization Services and Products, Card Management and Production Services and Products, Enrollment and Registration Services and Products, Systems Infrastructure Services and Products*) are not as directly applicable to the experience, capability, and talent needed to succeed with migration and transition efforts. The *Certified Systems Integration Services and Products* vendors are more apt to address the integration requirements, end-to-end solution expertise, and direct technical capabilities needed for migration success.

Federal acquisition rules and laws require the use of Qualified or Certified vendors to address HSPD-12 related work efforts. Agencies can opt to engage the GSA Schedule 70 within Special Item Number 132-62 to acquire these resources or at a minimum must utilize the certified labor as listed on the ID Management web site (www.idmanagement.gov) within the acquisition process.

4.1 White Paper Author

LS3 Technologies is an organization that has been dedicated to the advancement, use, and practical application of HSPD-12 and ICAM for more than a decade. We specialize in researching, reviewing, and assessing each of the component technologies that comprise ICAM and HSPD-2 solutions. We dedicated significant corporate resources to finding and retaining talented industry experts that share a similar interest in investing themselves in these technologies to offer best-in-class solutions for our customers. Our best-in-class service capabilities have addressed the solution design, development, integration, and operational sustainment needs of PIV and FICAM for a decade.

LS3 Technologies, a valued partner, minority woman-owned 8(a) certified and Small Disadvantaged Business, specializes in full lifecycle IT solutions. Clients benefit from our solid reputation for rapidly and successfully implementing best-in-class practices, processes, and systems. We strive to offer an accelerated return on our customers' time and investment. We carefully select each team member to ensure the resources each provides matches or exceeds expectations of our customers. Our teams of experienced critical thinkers are results-oriented people that cover the full spectrum of the IT industry, with specialized focus areas dedicated to success in individual tasks, yet integrated to keep their eyes on the end state desired. Our cross-functional management approach permits emphasis of strengths within each team member while ensuring a collaborative and inclusive atmosphere for achieving results and making progress.