HSPD-12/PIV Credential Solution Migration Planning

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

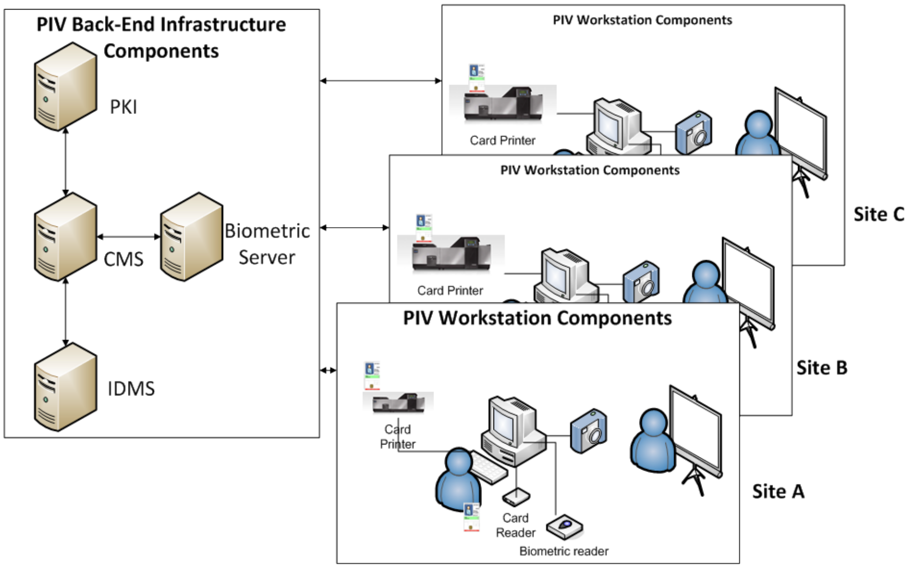
[3] http://csrc.nist.gov/publications/PubsSPs.html

[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


PIV Back-End Infrastructure Components
PKI
CMS
Biometric Server
IDMS
PIV Workstation Components
Card Printer
PIV Workstation Components
Card Printer
PIV Workstation Components
Card Printer
Card Reader
Biometric reader
Site C
Site B
Site A

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 HSPD-12 PIV AND PIV-I SOLUTION TRANSITION APPROACH

Agencies that consider solution transition to new PIV Providers, or to more economically advantageous PIV operating models, should incorporate specific elements into transition plans. Additionally, planning where the Agency seeks to preserve sunk cost investments must ensure:

1) Rights to data are in place and allow for the extraction of Agency owned data to place that data under Agency control and management.
2) Existing solution will remain available for the period of transition required to allow for the options identified above to be properly engaged.
3) Legacy service provider who offers turnkey capabilities to the Agency will be required to continue KMA responsibilities as per the Federal PKI Common Policy, for the full data retention period as required in Section 5.5.2 of that policy.

With these items in place, transition plans can be engaged to migrate to new service Providers.

2.1 <u>Preparation Efforts</u>

Establishment of a transition plan is imperative for success in any IT program. Failing to plan is planning to fail! A is a nominal level of effort (LOE) should be planned to investigate dependencies or barriers to transition success. The investigative analysis needs to examine:

- Existing contract language to determine the rights of the Agency
- Clear identification of what the Agency can ask of a current service Provider to support a transition.
- Configuration data for both CMS and PKI to aid in configuration of a target transition environment.
- Assessment of the deployed capability (e.g., credentials, use cases, geographic distribution footprint, etc.) to allow for new operating plans and so logistic processes can be put in place to address user-focused service needs and overall service continuity.

This information is used as an input to Target Solution Setup for transition activities, to align manpower in a manner that efficiently addresses transition needs, and to minimize cost impacts to the Agency from the transition effort.

2.2 <u>Coordination Efforts</u>

Coordination efforts are managed where each Actor/Role is provided their respective sets of responsibilities to accomplish transition. A major assumption for transition is that any incumbent vendor/service Provider will not be eager to support a transition process. Therefore, coordination will involve minimum touch points with that vendor and will seek to reduce both LOE and coordination requests to the maximum extent possible. Coordination should be accomplished with only "necessary" information to permit successful solution transition, addressing transition dependencies such as:

- Network configurations required to reconstitute services in a target environment
- Information to support "sizing" of hosting capability to ensure minimum requirements are met for supporting service capabilities
- Application specific configurations for CMS, PKI, and where an impact exists, with the IDMS, to ensure configurations meet existing service and technical "standards" in place with current capabilities

- A review of a PIV or PIV-I card to identify configurations that may exist and that need continued support in the end-product
- Migration considerations introduced by Policies, Standards, or other guidance

The coordination activities should incorporate the appropriate subject matter experts (SMEs) that offer insight into the application architecture, integration approaches, and technical/operational dependencies for fully integrated PIV solution capabilities. These efforts will benefit from appropriately skilled Identity and Access Management (IAM) SMEs that have a firm understanding of Federal Identity Credential and Access Management (FICAM). Though initial costs associated with SME participation may seem unnecessarily high, the dividends provided to the effort are immeasurable. The SME participation will curtail the refactoring, re-evaluation, and repeat analysis of facts associated with all aspects of the current and target solution, and the steps being taken to successfully accomplish a migration/transition across Providers.

2.3 Target Solution Setup

Any measure of success for setting up a target solution will depend on several factors, which can influence cost, schedule or performance based upon that service's design and the flexibility it offers with its PIV Issuance capability. Examples of impact drivers include:

- Capability to address Agency specific business processes or service needs that are Optional in the FIPS 201-1 Standard need to be considered in any Target Service that already exists, to validate that it can be supported;
- Any business process or service needs that results in a change to the PIV product (i.e., PIV or PIV-I Cards) such as data elements stored in the card's ICC, printed elements that are placed on the card, etc.
- Any customizations resulting from adjustments from common PIV workflow processes that incorporate business units or stakeholders in PIV enrollment and approval processes
- Any concessions or adjustments made to enhance performance of current service Providers, which are undocumented or "forgotten" but may impact newly identified service Providers

Most of these considerations should be addressed as a function of Coordination Efforts, and will yield a set of requirements for the Target Solution setup. These configuration and setup requirements are best managed by an HSPD-12 Integrator that demonstrates the experience and capability of HSPD- 12 solution construction (as opposed to a strategy consulting firm or a COTS product vendor, who each normally lack the technical depth and experience to address this need).

Core COTS product setups can typically be accomplished in less than 30 calendar days, once hardware and hosting capabilities are in place to support them. The specific configurations of an end-to-end solution can normally be accomplished from within 30 to 60 days. This timeframe is inclusive of basic product testing to validate the installation baselines. Therefore, Agencies can realistically expect a Target Solution capability in place within a 90 day period. In parallel to these activities, an appropriate Security Accreditation process will be required as a measure of proper compliance to security policy (e.g., Federal Information Security Management Act (FISMA), Agency Security Policy, etc.). These efforts can be accomplish in accordance with the Agencies normative scheduling and cost impacts. It is important to note that my leveraging an already certified PKI SSP, the certifications of these service providers can be leveraged within the accreditation process, and therefore the System Security Boundary can typically be established around the CMS and IDMS components with respect to the back end infrastructure capability. The workstation footprints can remain unaltered with a re-established capability and therefore any security accreditations should not realize an impact from any adjustments to the back-end of the core solution. Where changes to the workstations are required, typically these can be addressed as a minor change event, and should not require full re-accreditation with the modified/adjusted target state of the solution.

2.4 Service Testing

Testing is a known best practice and it is imperative to incorporate this into any transition plan. There are core elements of service testing that should be accomplished as part of planned activities, which include:

- The test environment should be in place with sufficient time to remediate any problems with the target service implementation.
- Agencies should have a full validation of the functional capability of a target environment, which addresses all Agency defined requirements and Use Cases. Use case testing should include current and new users, and each step of Card Services should be validated in the testing (e.g., enrollment, registration, issuance, printing, card/certificate update, etc.).
- Testing needs to address critical design and performance needs such as performance testing with a selected PKI provider. Testing should consider known issues in CMS to PKI performance such as ensuring that network latency does not impose timeout issues between the CMS and the PKI Certificate Authority.
- Round trip testing for a fully functional target system should be done prior to engaging in actual production migration efforts. This will ensure that migration activities can be accomplished succinctly, by reducing the complexity of the effort to mere data migration point A to point B.
- Fully exercise the workstation components that interact with the back-end infrastructure components to validate that no changes or updates are required in the distributed capability that the Agency relies upon to service customer needs

Other elements of testing will likely be incorporated into these needs, based on the outputs from previous activities and coordination. An appropriately skilled SME should assist any Test Manager in the development of test scripts, to ensure that all functionality is properly exercised in the target Service environment.

2.5 Migration Activities

Migration activities can typically occur for an Agency over a weekend. Migration schedules are predominately driven by the volume of data to be migrated. Within the Federal government only GSA's USAccess solution and VA's PIV System are of sufficient size to warrant added steps to address "management of big data".[9] Migration activities address the preservation of production

[9] These two Federal solutions are known to manage in excess of half a million users each, and introduce alternative concerns that have to be addressed as a function of large volume data management. The VA's PIV System is also

data as it moves from the original Provider A to the new Provider B. It should be noted that Provider B can be the Agency itself, and it is only used as a point of reference. The most important production data to preserve includes the “Live” CMS Database (from the production CMS) and the TK Keys from the production HSM that services the CMS. Once the data is migrated and its integrity validated, a simple set of functional tests should be run to validate that the expected capabilities and performance are addressed by the target solution.

Consistent with best practices, the Target Solution environment should provide a Production, Pre-Production/Quality Assurance, and Test/Development environment. These environments are utilized with normal change and configuration management processes that are engaged over time to address solution changes or updates, and to preserve the integrity of the Production instances of the Target Solution. An added best practice is continuity of operations and disaster recovery capabilities, which will ensure compliance with Directives such as Federal Continuity Directives #1 and #2. This offers the Agency a redundancy in the production capability in the event of single-site service disruption. These considerations can realistically be addressed holistically over time (e.g., COOP, COG, DR), as a measure of Agency risk acceptance. This is an important consideration in recognition that service adoption may suffer from strained Program operating budgets or technical capabilities initially, when considering solution migration. Therefore, Agencies can opt to accept the risks associated with immediately transitioning solutions, so long as a clear set of plans are in place to address a Plan of Action and Milestones (POA&Ms) that will be identified as a function of the security accreditation process. Program Offices can therefore adopt the operating budgets over time to address these critical needs, and remove some of the business and technical burdens associated with accomplishing a transition to a new Provider solution or capability.

2.6 Service Enablement or Cut Over

Based on all previous steps, the Agency should have a functional Target System/Service, all production capabilities in place, and validation from testing that the services are ready for cut over with production grade data. This assumes that appropriate security accreditations are in place for the now Target Solution environment. The service cut over event should be as simple as making a network change, such as modifying DNS entries to point to new IP addresses and updated URLs. The replication of these changes can occur in less than 24 hours and the Agency will effectively be operating on the new Target solution.

2.7 Production Support Services

Agencies must consider the solution maintenance and operational needs as a function of Program planning and management. These considerations are common for any Production capable solution. Depending upon the operating model adopted, the Agency or a Services Vendor/Provider may retain responsibility for certain aspects of a production solution. Some considerations of direct migration relevance that should be included in program plans include:

- **User Guidance and Training Needs –** Any impacts to the users that are realized as a function of solution migration should be incorporated into user focused documentation, training, or education that ensures that the user is appropriately advised as to how to continue to engage services.

poorly maintained and suffers from significant data quality concerns and other operational risks that introduce a host of other major migration concerns which require specialized knowledge and technical capabilities to fully address.

- **Certificate Rekey Instructions** – this is a potential need that may need to be addressed as a function of solution migration. The instructions should identify how users can engage in a Certificate Update process to refresh the PKI capabilities of their current Production PIV/PIV-I cards, such that the Agency can fully migrate from legacy PKI or PIV service offerings to the newly established capabilities. This strategy would include plans for scheduling users to the appropriate locations to engage in an Update to their cards, and serves as a cost reduction activity for the Agency to fully engage in cessation of existing Provider capabilities. Once the last user has been migrated, there are no further policy conflicts or constraints from terminating current service contracts with existing Providers.

3 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*.

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.

3.1 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.