The Case for Personal Identity Verification (PIV) and Personal Identity Verification-Interoperable (PIV-I) identity credentials

AFCEA International
Cyber Committee - Sub Committee - Assured Identity
WHITE PAPER SERIES TOPIC # 1

Table of Contents

I Introduction

The federal government is making strides to implement identity management activities that will streamline the citizen user experience connecting to electronic government information and services. They want to make the experience with online government services more convenient and less susceptible to fraud and identity theft while enabling federal agencies to gain cost savings in any function that requires the use of a login credential. In spite of some guidance from Office of Management and Budget (OMB) and rising numbers of Personal Identity Verification (PIV) credentials being issued by the Federal agencies, there are many challenges with completing the vision of Homeland Security Presidential Directive 12 (HSPD-12)[1]. Among the remaining challenges in the National Strategy for Trusted Identities in Cyberspace (NSTIC)[2] vision, particularly for business-to-government (B2G) transactions is the adoption of PIV-Interoperable (PIV-I) credentials for both Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS) applications This paper will highlight several of these challenges, discuss options for resolution and provide recommendations on a way ahead for federal and commercial sector consideration for using PIV-I to enhance and secure B2G transactions .

II Background

Use of electronic systems enabling our government to conduct transactions reliably with its' citizenry and suppliers has expanded along with the speed and capability of computers, networks, software applications and mobile devices. Conduct of transactions between government and business was facilitated using system-issued identity credential, commonly known as a "userid and password". Over the last 10 years the idea of an electronic claim of identity (or "userid and password") used to access electronic systems across the Internet did not advance until the introduction and use of smart cards that included Public Key Infrastructure (PKI) certificates. The driving factor for using the PKI technology is its ability to mitigate fraudulent use of an identity credential.

The Department of Defense (DoD) began to move to stronger forms of electronic or digital identity in 2001 with the establishment of their smartcard-based credential, the Common Access Card. The federal government followed suit in 2004and established their requirement for a digital Identity for federal employees and government contractors with the

[1] HSPD 12: *Policy for A Common Identification Standard for Federal Employees and Contractors*, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm)
[2] National Strategy for Trusted Identities in Cyberspace (NSTIC), http://www.nist.gov/nstic/about-nstic.html

issuance of HSPD-12. Very recently, with guidance and direction from the White House in the NSTIC, the federal government has established a national strategy that uses a range of digital identity credential types that will meet the needs of a diverse set of audiences that are using electronic government services. The strategy includes making on-line identity credentials available for all citizens, promoting privacy by reducing the likelihood of fraudulent credential use or identity theft and allowing the growing online culture to operate more securely and with greater convenience and efficiency. Progress towards use of digital identities in all of these areas is advancing, albeit at different rates in different agencies.

There has been a huge increase in the populations of users interacting with web-based processes that provide services from government agencies. For example, citizens have one web site (USAJOBS) to use to apply for a job in any government agency. There are also numerous types of citizen to government transactions that are now conducted online including interactions with the Social Security Administration, and applications for government backed student loans. Within the federal government, government agencies have adopted online collaboration tools and networked systems that enable federal employees to work more effectively and efficiently conducting the business of government in paperless processes. All these online activities are predicated on using a digital credential to make an initial claim of identity that is used to gain access to the electronic resource.

HSPD-12 established a credentialing standard for federal agency employees and designated contractors. This left many government partners that frequently entered federal facilitates or transacted electronic business with federal agencies ineligible for a Federal Information Processing Standard (FIPS) 201[3] compliant identity credential. to close this gap, the General Services Administration's Office of Government-wide Policy and the Federal PKI Policy Authority developed the Personal Identity Verification –Interoperable (PIV-I) standard for identity credentials. The PIV-I standard credentialing rules and processes are documented in the Federal Bridge Certification Authority's (FBCA, aka "the Federal Bridge") certificate policy[4]. The FBCA is the government certifying authority for all identity credential providers that issue PIV-I identity credentials[5]. The PIV-I credential was designed to be interoperable with PIV enabled systems and is electronically verifiable as a claim of identity from the user. The FBCA monitors and publishes the list of all currently certified PIV-I providers. In addition, DoD lists all FBCA certified PIV-I providers[6] that have been approved for use by DoD information systems and physical access control systems (PACS) that operate at DoD facilities.

To spur adoption and use of both PIV and PIV-I identity credentials within the within the Executive branch of the Federal government, the Office of Management and Budget (OMB) has directed OMB memo 11-11 to push federal agencies toward using these stronger digital identities. The recent GAO report, "*Personal ID Verification Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*"[7] identifies that while OMB has outlined the way forward to take advantage of the federal identity credential, PIV, implementation within many agencies demonstrates that they are not effectively or efficiently using the PIV credential in identity-reliant processes like authentication to electronic and web-based systems. The GAO report verifies that there are a myriad of barriers to making use of PIV quality identity credentials in federal agency online business processes.

III The Benefits of Strong Identity Credentials

---

[3] FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[4] Federal CIO Council, *Personal Identity Verification Interoperability for Non-Federal Users*, May 2009, NFI PIV-I, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf
[5] http://www.idmanagement.gov/pages.cfm/page/IDManagement-PIVI-cross-certification
[6] http://iase.disa.mil/pki-pke/interoperability
[7] GAO Report 11-751, *Personal ID Verification Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, September 2011, http://www.gao.gov/new.items/d11751.pdf.

By understanding the benefits of strong identity credentials we can better analyze and understand what are the barriers to implementing the use of PIV or PIV-I credentials. There are several issues inhibiting near term use of PIV and PIV-I. In the following paragraphs, the benefits of strong identity credentials are presented. .

For the purposes of this paper, "strong Identity credentials" are credentials that meet or exceed the e-authentication assurance level 4 requirements, as stated in NIST Special Publication 800-63 -1[8]. PIV and PIV-I meet or exceed all those requirements.

The first benefit is use makes an agency's IT systems more efficient and can enhance the security posture of the organization. PIV and PIV-I credentials are less vulnerable to compromise and fraudulent use by bad actors because public key cryptography eliminates the use of "shared secrets"[9]. Third-party credential service providers (CSP) facilitate the identity proofing, registration and card issuance with audited identity and credential management systems, relieving those functions from an information system operator. The cryptography and protocol make PKI-based identity credentials immune to phishing, eavesdropping, replay or man-in-the-middle attacks. A CSP's audited compliance with standardized proofing, registration and issuing processes demonstrate that credentials were created under secure and repeatable conditions can be trusted by information system operator. Information system owners/operators can outsource the credential issuance function and re-focus their staff into more critical missions.

> The DoD has seen the benefits of this effort. Successful intrusions to DoD unclassified networks had declined 46 percent due to CAC use.
> ~ Lieutenant General (Retired) Charles E. Croom, 2007 DISA Partnership Conference

these and

A second reason for using strong identity credentials is that their use can lead to reducing the number of identity credentials a single person needs to have. Each agency and commercial partner can purchase identity credentials for their employees from approved CSPs. Because all approved credentials are interoperable (can be trusted by the other agencies or partners) federal and commercial employees are "credentialed" only once. This significantly reduces the requirement for credential issuance at each physical facility or each web-based IT system. Reduced local credential issuance translates to reduced costs for agencies and IT systems.

A third reason for using strong credentials is the cost of issuing and maintaining (resetting PINs or replacing lost credentials) the identity credential is shifted from the information systems owners that accept the credential to the users that need the credential to identify themselves. This is akin to how consumers shifted from using retail company credit cards (e.g. Gulf, Texaco or Montgomery Ward) to using a VISA or MasterCard. VISA identity proofs the cardholder during the card application process, and then issues a personalized card to the VISA patron. Retail stores save the expense of operating and maintaining credit departments or making collections; which was not part of the retail company's core business. Most information system owners are not cognizant of credential issuance and maintenance costs. Information system owners need to be educated that use of PIV or PIV-I could cut helpdesk costs significantly, by avoiding frequent password resets.

The last and maybe most overlooked benefit from using credentials like the PIV or PIV-I is leveraging digital signatures created from digital identity credentials to boost the bottom line of a business or the efficiency of a government

[8] NIST Special Publication 800-63-1, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[9] FIPS 196, "Entity Authentication Using Public Key Cryptography" , http://csrc.nist.gov/publications/fips/fips196/fips196.pdf

business function. Digital credentials facilitate changing a business function from a paper–based to a paperless one. Converting to a paperless process with electronic work flow saves the costs of handling or moving paper for every transaction, saves time and money by reducing cycle time to conduct a single transaction, and saves money by eliminating the paper storage costs necessary to support auditing and compliance reviews. . The Defense Travel System (DTS) is a specific example of how the DoD has taken advantage of this benefit of digital identity credentials. The paper-based travel expense business process was converted to a paperless process, saving millions of dollars and making the travel expense reporting and reimbursement process more efficient.

IV Discussion on Challenges - Barriers to PIV implementation:

An understanding of the potential benefits of "PIV quality" (PIV and PIV-I) credentials should help to shed light on why there are barriers to adopting them extensively across the federal IT environment. We have identified three primary barriers to extensive PIV and PIV-I adoption. They are lack of education, failure to realize the business value to organizations, and trust/shared security.

Education:

Issue: Across the public and private sectors, information system owners do not know or understand why adoption of PIV and PIV-I is important.

Discussion: The current perception is that the security of commonly practiced authentication methods using traditional user id and passwords is "good enough". This perception continues because evidence that credential fraud has been a contributing factor in sensitive data exfiltration is not widely published in public sources. What is recognized and acknowledged by most security professionals is that the ability to fraudulently use userids and passwords has increased tremendously over the past twenty years and the profitability from using stolen identity data is almost unlimited. For any federal agency or commercial company, the cost of remediating the loss of stolen data or stolen identities (i.e., Personal Identity Information) is extremely expensive (e.g., TRICARE data breach, Nov 2011[10]). The cost of remediation from data loss is not budgeted for and not considered in the cost/benefit analysis of system upgrades. With greater education and discussion in government and security forums about using strong authentication methods, information system owners (in both government and industry) can discover how to avoid the consequences of information or PII loss by using strong identity credentials that are far less vulnerable to commonly used attacks.

The "good enough" perception has to be changed at many different levels within organizations. Authentication and access control are executed at the network and/or system level and are arguably the weakest link in the organization's computer network defense in depth scheme. System owners/operators need to understand how their authentication process participates in the organization's network defense operations. Authentication of strong identity credentials needs to be viewed as a tool in the cybersecurity "toolbox" on par with certification and accreditation, intrusion detection, computer asset configuration and patch management. Leadership must appreciate that strong authentication is critical to executing effective access control and access control is rudimentary when combating cybersecurity threats. The DoD has "Eliminate Anonymity" as one of their key cybersecurity goals yet it is not understood how anonymity negatively impacts agency mission operations.

[10] Matthew Schwartz, "Worst Data Breaches of 2011," *Information Week*, December 28, 2011, http://informationweek.com/news/security/attacks/232301079.

The GAO report[11] indicates that PIV and PIV-I adoption is far less extensive than was expected. Industry adoption is also moving at a much slower pace presumably because return on investment considerations drive business' decisions.. We have to educate system owners about how they can have trust in and use PIV and PIV-I credentials to the fullest extent.

Recommendation:

Institute communications campaigns across each organization. Mount an agency-wide campaign to advertise the benefits of using PIV and PIV-I. Use internal communications media such as newsletters, bulletin boards, and electronic kiosks. Users should be given examples of how these credentials can be more convenient and simplify their interactions with logical and physical access situations. This will institute a bottom-up demand to use these credentials. Highlight to system owners the potential cost savings of no password resets and the potential cost avoidance by not issuing and maintaining individual system–issued credentials to their user base. Advertise the systems that are ready to accept or are moving to accept these credentials. Give rollout dates for when they will be accepted. Tie in the use of PIV and PIV-I with individual information security training, highlighting PIV/PIV-I use as a security enhancing best practice.

As part of the campaign, provide senior leadership short decks that can be incorporated into speeches and briefs to groups within the agency, at government forums and trade and technical conferences or in periodicals. Provide "sound bites" for seniors to use that demonstrate the acceptance of these credentials within their organization.

Highlight acceptance by individual organizations within the agency to build "friendly completion" between sub-organizations.

Business Value

Issue: Federal agency system owners are not directly motivated to innovate or change by improving the overall return on investment (ROI) of their system operations. They are constrained by operating budgets that are planned and approved in multi-year cycles. They have not planned for expanding the types of credentials used in their system into the operating budgets.

Discussion: functional communities (e.g., logistics, intel community, procurement and acquisition) operating within federal agencies have a wide variety of user communities (commercial vendors, contractors, citizens, state and local government officials and employees, academics, researchers, students, etc.) Each functional activity has a different motivation for obtaining a quantifiable return on investment from their activity's automated information systems. Adoption of strong identity credentials will be quicker in some communities of interest and take longer in other communities. Identifying and realizing the benefit of PIV and PIV-I use in the business process can take extensive analysis or even a business crisis. The transition to use of only PIV and PIV-I credentials for authentication to DoD's JPAS system[12] illustrates the complexity of issues that constitute "business value".

Part of the calculation of business value is consideration of cost to implement and operate. For both PIV and PIV-I credentials, cost considerations include both infrastructure costs and credential issuance and maintenance costs.. With PIV or PIV-I, system functionality must be adapted to interface and use the smartcard data, and workstation systems must be retrofitted to use card readers and middleware. Additionally systems may require custom programming to map PKI credentials to user accounts. That cost is partially off-set by the PIV or PIV-I credential issuer absorbing the issuance and credential maintenance costs, not the system owner.

[11] GAO Report 11-751, *Personal ID Verification Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, September 2011,

[12] Lesson's Learned about the JPAS conversion can be obtained from the DoD's Defense Manpower Data Center CIO.

Realizing value has often been a barrier to implementation of many new technologies that over time have become commonplace. An example of one such technology is the banking industry's ATM card and system. When ATM systems were first introduced, many of the same barriers to adoption existed that are hindering the adoption of "PIV quality" smartcards today. The barriers to adoption were the customers' uncertainty about the security of the ATM and both the customers and the bank's aversion to change. While the ATM system won initial converts for its banking convenience, it reached wider adoption by realizing additional value for both consumers and banking service providers.

A PIV-based authentication, authorization and revocation model[13], when properly implemented, can enable both increased security and enhanced user convenience - partly by overcoming the vulnerabilities and unwieldiness of the user/password tokens, and partly by simplifying the user experience (a single card and PIN used in any logon/entrance situation). As in the banking analogy, ultimately the convenience of the walk up ATM over the alternative of waiting in teller lines during "banking hours" helped to overcome the barriers of using the new technology.

Federal agencies must assess how to bring greater value to their mission-centric and business services for employees and "business" partners that use PIV or PIV-I credential solutions. The additional confidence in the identity asserted with the PIV quality credential can be the ingredient in the service delivery process that can make the mission-centric services more effective and business or support services more efficient and the overall posture more secure. In many European and Asian nations, a PIV-I like citizen credential forms the basis for receiving citizen services including health care, social services (unemployment benefits and government assistance), facilitates the processing of citizen information on applications (for business licenses), payment of fees (parking tickets), and other identity-specific services. As an example, federal agencies could streamline the student loan or research grant application process if applicants used a PIV-I credential to log in to the service portal. By tying "PIV quality" solutions into a broader set of business processes and benefits, the potential value of smartcard-based identity technologies becomes more apparent and creates additional user demand beyond the inherent improved security.

Recommendation:

Mandates to adopt PIV and PIV-I have led to spotty and sporadic implementations and don't drive users or system owners to assess opportunities for their wider use. Therefore Government should incentivize agencies and systems to innovate and adopt solutions that use of strong identity credentials in business processes. Incentives should drive agencies to harness the business value available through use of these credentials.

Trust and Shared Security

Issue: A major factor in building trust in other credential alternatives is overcoming the risks associated with credential use. Because of unfamiliarity with recently approved PIV-I issuers, system owners don't realize that there are other authentication 'log on' options for their users. They are familiar with RSA Secure ID fobs, but, are not well-informed about how users can obtain PIV-I credentials or how they can use the PIV-I for authentication.

Discussion: In the majority of today's mission and business IT environments, the perception is that the traditional login/password authentication and authorization mechanism is sufficient to ensure authorized access. Similarly, in the banking industry, the prevailing perception was security measures were good enough, assuming that tellers knew their customers by name/sight. In reality, as a bank's customer base grew, the teller-customer transaction became increasingly anonymous thereby circumventing the presumed security practices. To reach the "good enough" level of security assurance in many of today's systems, IT system owners create and manage their own logon/passwords and adopt password management rules that target only vulnerabilities associated with password length, complexity, and aging . As

[13] FIPS *201*, csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

the sophistication of attackers increased, "best practice" password management did not address more sophisticated phishing, pharming or spyware attacks.

The trustworthiness (some use the term "trust model") of system–issued passwords is built around reliance on a system operator's disciplined implementation of credential issuance best practices. System owners could not rely on ("place trust in") another system's registration or identity proofing without knowing that specific procedures that were followed. Additionally, without the "issuing" system's token assignment database, "relying" systems had no way to verify the logon credentials issued by another system.

The trustworthiness or trust model used for all "PIV quality" credentials addresses each of the trust generating elements: registration, identity proofing, credential verification and timely credential revocation. PIV quality credentials are issued by third party issuers that comply with a written set of procedures that prescribe registration, identity proofing, PKI certificate generation and distribution, and credential revocation. Because all PIV and PIV-I issuers follow a standardized set of operating rules and demonstrate their compliance through periodic audits, they can prove the trustworthiness of the credentials and confidence level (assurance level) of the identity asserted by the credential. As system owners understand the elements of trust that make these credentials trustworthy, they can incorporate this trust model into the risk management framework used to accredit and operate IT systems within federal agency IT.

This trust model is the basis for verifying third-party issued credentials across networks and organizations. However, it is foreign and unfamiliar to many system owners. This, in part, is why government mandated PIV and PIV-I credential use is suffering poor adoption rates.

Obtaining identity credential interoperability with PKI is complicated. Implementing PKI-based trust requires a high level of technical knowledge to be applied to technology interfaces, policy, process, governance, and trust reciprocity. Both PIV and PIV-I credentials conform to the PKI certificate policy of the Federal Bridge. Because of this, "PIV quality" credentials are all trustable (and interoperable) and their PKI trust chains can be verified. Any system owner can verify the status of the certificates by using the trust reciprocity mechanism that is established and supported by the Federal Bridge certification process. The basic trust verification procedures are the same regardless of which issuer created the credential, although there are technical challenges associated with choice of unique identifiers used by any particular relying system.

Beyond the technology aspects, the ATM analogue can again serve as the model for how to expand the use of interoperable credentials. In the banking industry, the companies formed agreements through intermediaries (Plus, Cirrus) to negotiate and agree on interoperability issues, including penalties for non-compliance. For PIV and PIV-I the Federal Bridge Certification Authority serves as the governance body for PKI-based interoperability for the government and defense industry base. Other identity federations such as Kantarra, OpenID, FiXs, and Open Identity Exchange (OIX)provide a similar type of governance for identity credentials that are assertion-based (e-Authentication assurance levels 1& 2, and non-PKI level 3. Discussions of these governance groups and processes are beyond the scope of this particular paper.

Recommendation:

Agencies should develop and implement policy that calls for system owners to use PIV and PIV-I credentials from the FBCA list of issuers.

The recommendation is for this policy to establish performance objectives for system owners and agency compliance to HSPD-12.

V Summary and Conclusion

The federal government is committed to taking advantage of expanding on-line capabilities and efficiencies, but vulnerabilities exist with electronically identifying government workers. This paper discusses the PIV and PIV-I credentials, the benefits of these electronic identities, the implementation challenges that they present, and the steps to overcome the acknowledged challenges.

Expanding education, identifying the business value, and increasingly knowledge about the trustworthiness of the credentials are the three critical issues to improve PIV and PIV-I adoption.

Increasing adoption across the federal agencies including the DoD and commercial industry partners will result in significant cost savings for the federal government. Raising the acceptance levels for these third party credentials will also have a major impact on improving security and information sharing between agencies.

The next step identified requires a broad government and industry dialog over the three critical issues. Through this discourse, the group can narrow the issues and jointly identify solutions that are easily understood and implemented using a common strategy. This approach should facilitate analysis and planning for each agency's particular situation and populations of online users.

Our goal remains to help improve compliance with the vision and intent of HSPD-12 while improving the state of the network and trusted interaction among government and industry partners.