White Paper

Realizing the HSPD-12 Interoperability Vision:

Increase Efficiencies and Establish Collaboration Across Federal Identity and Credential Management Implementations

ATARC Identity Management Working Group

April 2022

ATARC

Advanced Technology Academic Research Center

Table of Contents

Disclaimer: This Guidebook was prepared by the members of the ATARC Identity Management Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with.

1 Executive Summary

This paper seeks to highlight the persistent challenges present within the Federal Government about the redundant issuance and validation of Personal Identity Verification (PIV) credentials to federal employees and contractors and provide several recommendations to address them. These challenges are: (1) multiple PIV credentials issued to one person, (2) siloed and incompatible PIV card issuance, and (3) lack of efficiency to leverage enrollment processes across federal agencies. These challenges are often highlighted when multiple PIV cards are provided to a single person from disparate organizations—such as, a federal employee on-detail away from their home agency or when a federal employee or contractor simultaneously supports two or more agencies. Organizational policy decisions and limitations to successfully implement a technical solution appear to be the driving cause of these challenges. The effect is an increase in costs for the federal PIV issuance systems; wasteful and redundant identity verification services; increased work for technical staff to maintain multiple chains of trust within their identity management store; and an increased risk of compromising identity data.

The Advanced Technology Academic Research Center (ATARC) Identity Management Working Group will support its recommendations for these challenges by seeking industry input to demonstrate potential solutions, with the goal of modernizing backend PIV issuance mechanisms and PIV-enabled systems. Subsequently, these technology demonstrations in the ATARC Identity Management Laboratory could potentially support policy revisions that improve process efficiencies in agency PIV programs and realize the intent of HSPD-12.

2 Background

Homeland Security Presidential Directive 12 (HSPD-12) established the requirement for a "… mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors"[1]. It stipulates how the identity credentials are to be used, with interoperability in both physical and logical access. In response to this directive, the National Institute of Standards and Technology (NIST) released the Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. One of the goals of FIPS 201 was to describe specifications to support technical interoperability of the PIV credentials among Federal agencies and departments[2]. Since the release of FIPS 201, agencies have responded by implementing internal policies and practices resulting in parallel enrollment processes, physical access solutions that do not meet the interoperable intent, plus an increase in the overall cost of maintaining the PIV infrastructure along with the logistical challenge of maintaining multiple cards. Further, there are more than 10 hosted PIV enrollment services with redundant enrollment data (e.g., fingerprints, photos, and personal identifiable information). These PIV enrollment services maintain little to no communication between their respective databases to help improve inter-organizational trust and PIV card interoperability. The Office of Management and Budget (OMB) is aware of these challenges and has since then issued memoranda OMB M-11-11, OMB M-19-17, and OMB M-22-09 with the aim of clarifying the requirements. OMB M-19-17 states "Agency processes shall accept and electronically verify PIV credentials issued by other agencies. This is equally applicable for local and physical access where another agency's employee has been provisioned access"[3]. Despite these memoranda, the vast majority of federal agencies continue to deploy systems with no ability to accept other agencies' PIV credentials. According to the USAccess Program, that accounts for slightly less than half of all PIV cards in circulation, there are at present 3,362 PIV card holders that have two (2) or more valid PIV credentials with two (2) or more agencies. The duplication of PIV cards stems from various scenarios. For example, some contractors or federal employees support multiple agencies. The lack of credential interoperability or reuse to support these agencies, results in customary practices to issue them a different PIV credential from each agency supported. If the federal employee or contractor is working a long-term assignment at another agency, their multiple PIV credentials (PIV/PIV-I) will be concurrently valid.

A second scenario is a federal employee who takes a new job at a different agency. This creates the situation of undergoing another enrollment process to obtain a new PIV card while having a valid one—often with months or years of validity still left on the valid card. Yet, that credential will be revoked as a new PIV card is issued representing the affiliation with the new agency. Is organizational affiliation worth the reissuance of an identity credential when a federal employee or contractor possesses a current and valid PIV card? The number of PIV credentials that are revoked "early" for this reason is many orders of magnitude greater than agencies' efforts to make credentials interoperable.

[1] https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-8.html

[2] https://csrc.nist.gov/publications/detail/fips/201/2/final

[3] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

3 Purpose

This paper seeks to: (1) describe the challenges occurring with the Federal Government's implementation of HSPD-12, and the growing operational cost incurred by agencies not complying with policy and standards, and (2) provide recommendations that will result in internal government efficiencies and effectiveness for identity management enrollment and provisioning practices.

In response to these identified challenges, the ATARC Identity Management Working Group will look to showcase solutions in the ATARC Identity Management lab that will demonstrate the feasibility for agencies to leverage one PIV card per person across the entirety of the federal landscape.

4 Identified Challenges

4.1 One person:Many PIV cards

In the majority of cases, agencies currently issue an agency or department affiliated PIV or PIV-I card to any external federal employee or contractor, independent of whether that individual is a current and valid PIV cardholder from another agency. While the reasons for this are many, the most common is insufficient infrastructure to support physical and logical validation of the PIV card electronically against all PIV card issuers. This lack of cross-agency interoperability is in direct contrast to the objectives identified in HSPD-12, whereas the resulting PIV card was to be a “Secure and Reliable forms of identification” and “can be rapidly authenticated electronically.” By not being able to reliably validate an existing PIV card, or in many cases check for whether an individual is a current, valid PIV cardholder, agencies are forced to require issuance of their own affiliated PIV card which can work with their existing infrastructure.

4.2 PIV card issuers as silos

As directed through HSPD-12, NIST was asked to create an interoperable and trustworthy enrollment record format that could be reused and transferred between PIV issuers. Through this direction, NIST has seen three revisions of the FIPS 201 framework released. Despite this framework, issuers today act in isolation without sharing information between issuance systems and corresponding backend databases. To date, no PIV card issuer has implemented a solution consistent with this guidance and shared an enrollment package with any other PIV card issuers. As an extension of its FIPS 201 guidance, NIST created SP 800-156[4] with its introductory purpose stating the following:

> *The chain-of-trust offers process efficiencies because a PIV Card can be re-issued based on the most current chain-of-trust record, and more importantly, can avoid having to repeat the identity proofing and re-registration (re-enrollment) process. Departments and agencies that implement a chain-of-trust will also be able to transfer the record to another agency or to a service provider, so that the receiving agency or service provider can use the record to issue a PIV Card rather than re-enroll an applicant. This Special Publication provides the representation of a chain-of-trust for import and export between PIV Card issuers.*

As defined through these NIST publications, a critical component of the enrollment package is background verification status and final investigative status. By failing to adopt a compliant chain-of-trust enrollment record, an element identified specifically within the 800-156 NIST special publication, agencies have incurred higher than necessary costs for the issuance and lifecycle management of their PIV cardholder population. These costs are typically incurred through the lost time and material cost associated with requiring current and valid PIV cardholders to physically report to a PIV issuance station to receive an additional PIV card. Arguably, the largest source of cost is the incremental background check. Having an ability to let a current valid background check stand, and be available for validation, for

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-156.pdf

any agency with need of this information would improve interoperability, and lead to a significant reduction in the costs.

4.3 Inefficiency drives non-compliance

Many agencies have been slow to implement FICAM compliant and interoperable systems. As such, the FIPS 201 goal of implementing a “one person:one PIV card” paradigm has not yet been achieved due to budget, logistical, technical, and administrative constraints that are unique to each agency. The impact from these constraints is an agency’s increase in cost and time to manage the identity of a single person using multiple PIV cards rather than establishing both technical and process interoperability using a centralized chain-of-trust. Further, these constraints drive inefficiencies and non-compliance that are reflected in how federal employees and contractors gain physical and logical access to federal facilities and systems. For example, the use of Physical Access Control Systems (PACS) to access federal facilities were not PKI-based before the initial release of FIPS 201. Visual inspection, non-cryptographic authentication modes, and continued reliance on less secure proximity-based RFID (radio frequency identification) technology has persisted at various posts throughout the last decade and a half instead, despite the advancements in compliant PIV-based PACS validated entry control points.

In addition to the challenges prevalent within interagency PACS validation, Logical Access Control Systems (LACS) have seen similar inefficiency challenges. These specific LACS interoperability issues are not in scope within this document, but their existence shares equal rooting to the same challenges driving multiple PIV card issuance and should therefore be acknowledged. These challenges are especially important in consideration of the current Administration’s goals and policies driving towards zero trust architecture. The ATARC Identity Management Working Group will address these PIV LACS interoperability challenges in a future publication.

5 Market Opportunity

There is a need to reduce the number of times an individual's Personally Identifiable Information (PII) is captured so only a single PIV record is created. Also, there is a need to increase interoperable trust of a single PIV record for government-wide use.

Federal departments and agencies present an opportunity to reduce operating and personnel costs, as well as a potential reduction in the exposure of PII data. All PIV card issuers should be mandated to leverage NIST SP-800-156 complaint Credential Management Systems (CMS). While OMB and NIST have defined and mandated an interoperable PIV issuance infrastructure, such infrastructure does not exist today, and many technical barriers exist preventing easy cross-agency validation and determination of an individual's PIV cardholder status across the Federal Government. Therefore, **we recommend a process should be established at the Federal Public Key Infrastructure Policy Authority (FPKIPA) to facilitate secure requests for enrollment records among issuers**. Such an establishment should combat siloed PIV issuance and allow agencies and departments the ability to validate and trust the issued PIV credentials from other PIV issuance providers.

Industry has also seen value in reducing silos created through proprietary issuance systems. Work has been done to examine each interface involved in the entire PIV issuance process. There are two efforts underway which COTS (commercial-off-the-shelf) technology manufacturers are following and beginning to implement:

The OSIA framework (https://secureidentityalliance.org/osia-about)

The MOSIP API (https://www.mosip.io/)

As of the writing of this paper, there is effort to converge these two efforts. This should allow for even greater flexibility of intermingling the various components of identity enrollment and credential issuance. **We recommend advancing these efforts to enable one enrollment station with any other credential management system**. NIST SP 800-156 provides data interoperability among entire credential enrollment systems. These efforts are providing interoperability among the technical components that handle the data.

This opportunity to update and modernize the backend PIV framework, to break down the existing issuance silos, reduce, and ultimately, eliminate the number of individuals carrying multiple PIV cards, will see greater recognition of the original vision of HSPD-12.

6 Next Steps

The ATARC Identity Management Working Group is providing this white paper for a 60-day comment period, seeking feedback from government and industry stakeholders. We will leverage this feedback, in addition to the recommendations noted, to demonstrate the ability to implement this proposed modernization approach through outreach to industry, and establishment of the ATARC Identity Management Laboratory. The lab will provide practical demonstration of government or commercial off-the-shelf (GOTS/COTS) solutions to facilitate agency compliance with FIPS 201.

7 Authoritative References

7.1 Guidance

Title	Description
FIPS 201-3	This is the standard for federal agencies to implement HSPD-12.
800-156	This is a special publication on how federal agencies can establish a chain-of-trust record to facilitate the exchange of PIV card enrollment data.

7.2 Directive & Memoranda

Title	Description
HSPD-12	This is a directive that directs federal agencies to implement standardized badging to include security principles.
OMB M-11-11	This memorandum affirms the importance to implement HSPD-12 within federal agencies and clarifies requirements.
OMB M-19-17	This memorandum re-affirms HSPD-12 as the way to implement standardized badging and encourages federal agencies to leverage PIV credentials with other authentication form factors.
OMB M-22-09	This memorandum lays out the strategy for federal agencies to improve on enterprise identity and access controls.