Personal Identity Verification (PIV) Cards as Federated Identities – Challenges and Opportunities

Sarbari Gupta
Electrosoft
11417 Sunset Hills Road, Ste 228
Reston, VA 20190
703-437-9451x12

sarbari@electrosoft-inc.com

ABSTRACT

In this paper, we describe the challenges in using Personal Identity Verification (PIV) cards and PIV-like cards as federated identities to authenticate to US Federal government facilities and systems. The current set of specifications and policies related to the implementation and use of PIV cards leave a number of gaps in terms of trust and assurance. This paper identifies these gaps and proposes approaches to address them towards making the PIV card the standardized, interoperable, federated identity credential envisioned within Homeland Security Presidential Directive 12 (HSPD-12).

Categories and Subject Descriptors

K.6.5 {Management of Computing and Information Systems]: Security and Protection

General Terms

Management, Security, Standardization.

Keywords

Authentication, Smart cards, PKI, Assurance, Federal Bridge Certification Authority, Authorization.

1. BACKGROUND

Homeland Security Presidential Directive 12 (HSPD-12) entitled "*Policy for a Common Identification Standard for Federal Employees and Contractors*" was issued in 2004 to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors [1] that:

"+ Is issued based on sound criteria for verifying an individual employee's identity

+ Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation

+ Can be rapidly authenticated electronically

+ Is issued only by providers whose reliability has been established by an official accreditation process."

In response, the National Institute of Standards and Technology (NIST) published Federal Information Processing Standard (FIPS) 201 – "*Personal Identity Verification (PIV) for Federal Employees and Contractors*" [2] and several related Special Publications (found at http://csrc.nist.gov/piv-program) with detailed specifications on issuance and deployment of PIV cards to their personnel. The latest version of this standard is FIPS 201-1 published in March, 2006.

The goal of this standard is to support an appropriate level of assurance in conjunction with efficient verification of the claimed identity of an individual seeking physical access to Federal facilities and electronic access to government information systems. The PIV card is a smart card based digital identity container with a collection of identity credentials that provide graduated levels of assurance regarding the identity of the holder of the card.

When implemented and deployed by Federal agencies, the PIV card is envisioned to provide the attributes of security, authentication, trust and privacy using this commonly accepted identification credential.

1.1 PIV Documentation

NIST has published a suite of documents in support of PIV. These are identified below.

FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors. This document specifies the physical card characteristics, storage media, and data elements that make up the identity credentials resident on the PIV card.

SP 800-73-2: Interfaces for Personal Identity Verification (4 parts). This document specifies the interfaces and card architecture for storing and retrieving identity credentials from a smart card.

SP 800-76-1: **Biometric Data Specification for Personal Identity Verification**. This document describes technical acquisition and formatting specifications for the biometric credentials of the PIV system.

SP 800-78-1: **Cryptographic Algorithms and Key Sizes for Personal Identity Verification**. This recommendation identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, and message digest algorithms, and

IDtrust '09, April 14-16, 2009, Gaithersburg, MD
Copyright 2009 ACM 978-1-60558-474-4…$5.00.

specifies mechanisms to identify the algorithms associated with PIV keys or digital signatures.

SP 800-79-1: Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers. This document provides guidelines for accrediting the reliability of issuers of Personal Identity Verification cards that collect, store, and disseminate personal identity credentials and issue smart cards.

SP 800-87-1: Codes for the Identification of Federal and Federally-Assisted Organizations. This document provides the organizational codes necessary to establish the PIV Federal Agency Smart Credential Number (PIV FASC-N) that is required to be included in the FIPS 201 Card Holder Unique Identifier (CHUID).

SP 800-104: **A Scheme for PIV Visual Card Topography**. This document provides additional recommendations on the Personal Identity Verification (PIV) Card color-coding for designating employee affiliation.

SP 800-116: **A Recommendation for the Use of PIV Credentials in Physical Access Control**. This document describes a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal government facilities and assets.

1.2 PIV CREDENTIALS

The PIV card contains a number of mandatory and optional data elements that serve as identity credentials with varying levels of strength and assurance. These credentials are used singly or in sets to authenticate the holder of the PIV card to achieve the level of assurance required for a particular activity or transaction. A Personal Identification Number (PIN) is required to activate the card for privileged operations.

The mandatory credentials on the PIV card are:

- Cardholder Unique Identifier (CHUID)
- PIV Authentication Private Key and X.509 Certificate
- Biometric Object with cardholder fingerprints

The optional elements on the PIV card are:

- PIV Card Authentication Key (CAK) and X.509 Certificate (if CAK is asymmetric)
- PIV Digital Signature Private Key and X.509 Certificate
- PIV Key Management Private Key and X.509 Certificate
- Cardholder Facial Image

The reader is directed to [2] for further details on any or all of these credentials.

2. U.S. FEDERAL PKI and FIPS 201

In this section, we present a brief overview of the related Federal PKI policies to aid the understanding of the core thoughts presented in this paper.

The "*X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)"* defines seven certificate policies to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent different assurance levels indicating the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself. Of these, the *Medium-HW* policy is of relevance to this paper.

The "*X.509 Certificate Policy for the U.S. Federal PKI (FPKI) Common Policy Framework*" governs the public key infrastructure component of the Federal Enterprise Architecture. It incorporates six specific certificate policies of which two are of direct relevance to this paper: *id-CommonAuth* or *id-CommonHW*.

FIPS 201-1 requires the PIV authentication certificate loaded on a PIV card to be issued under the *id-CommonAuth* or *id-CommonHW* policies or under a policy that is equivalent to the FBCA *Medium-HW* policy.

FIPS 201-1 includes a detailed set of requirements related to identity proofing, registration processes and security controls required to securely store, process, and retrieve identity credentials from the card. In many cases, the requirements levied by FIPS 201-1 are more stringent than the requirements stemming from one or both of the FPKI policies mentioned above. For the purposes of this paper, it is important to recognize the elements where the requirements of FIPS 201 differ from the policy requirements of these two FPKI policies. These are summarized in the table below:

Table 1 - Differences in Requirements

FIPS 201-1	***id-CommonAuth or id-CommonHW* policies**	**FBCA *Medium-HW* policy**
NACI has to be initiated for Interim PIV card. NACI has to be completed for full scope PIV card.	NACI not required for regular applicants. Only CA personnel are required to undergo background checks.	NACI not required for regular applicants. Only CA personnel are required to undergo background checks.
FBI fingerprint check required.	Fingerprint check not required. Biometric collected for potential dispute resolution purposes.	Fingerprint check not required.
Facial image collected at registration.	Facial image not collected if some other biometric is collected.	Facial image not collected.
The applicant must appear in person at Registrar at least once prior to issuance.	Remote registration allowable; applicant may avoid in-person encounter prior to issuance.	Remote registration of applicant possible through existing subscriber with a valid certificate at the same level; applicant may avoid in-person encounter prior to issuance.

FIPS 201-1	***id-CommonAuth or id-CommonHW* policies**	**FBCA *Medium-HW* policy**
Two forms of original identity source documents from list in Form I-9 presented in original form. At least one must be a government issued picture ID.	One government issued identification document which includes or can be linked with biometric data of applicant.	One Federal government issued picture ID or two non-Federal IDs one of which is a picture ID.
Only designated sponsors can submit request for PIV card for an applicant.	Anyone with a valid credential issued under id-CommonAuth policy can act as a sponsor.	No requirement for a sponsor for an applicant.
Role separation implies that at least two authorized individuals need to be involved prior to issuance of card to applicant.	Only one authorized individual involved prior to issuance of credential to applicant.	Only one authorized individual involved prior to issuance of credential to applicant.
Identity proofing and registration process self-accredited by head of agency.	Third party audit required for authorization to operate CA.	Third party audit required for authorization to operate CA.
Card activated via PIN.	Card activated by passphrase, PIN or biometric.	Card activated by passphrase, PIN or biometric.

3. PIV AUTHENTICATION MECHANISMS

Chapter 6 of FIPS 201-1 provides a series of authentication use cases that can be supported using the electronic credentials resident on a PIV card. They are presented here to facilitate the reader's understanding of subsequent sections of this paper.

- CHUID – The cardholder is authenticated using the signed CHUID data element on the card. The PIN is not required. This mechanism is useful in environments where a low level of assurance is acceptable and rapid contactless authentication is necessary.
- CAK – The PIV card is authenticated using the Card Authentication Key in a challenge response protocol. The PIN is not required. This mechanism allows contact or contactless authentication of the PIV card without the holder's active participation, and provides a low level of assurance.
- BIO – The cardholder is authenticated by matching his or her fingerprint sample(s) to the signed biometric data element in an environment without a human attendant in view. The PIN is required to activate the card. This mechanism achieves a high level of assurance and requires the cardholder's active participation is submitting the PIN as well as the biometric sample.
- BIO-A – The cardholder is authenticated by matching his or her fingerprint sample(s) to the signed biometric data element in an environment with a human attendant in view. The PIN is required to activate the card. This mechanism achieves a very high level of assurance when coupled with full trust validation of the biometric template retrieved from the card, and requires the cardholder's active participation is submitting the PIN as well as the biometric sample.
- PKI – The cardholder is authenticated by demonstrating control of the PIV authentication private key in a challenge response protocol that can be validated using the PIV authentication certificate. The PIN is required to activate the card. This mechanism achieves a very high level of identity assurance and requires the cardholder's knowledge of the PIN.

In each of the above use cases, except the symmetric CAK use case, the source and the integrity of the corresponding PIV credential is validated by verifying the digital signature on the credential. The entity signing the credential objects resident on a PIV card is called a PIV Signer. The PIV Signer has a special certificate under the Common Policy Framework; however, in legacy and cross-certified PKIs under the Federal Bridge environment, the PIV Signer can use a digital signature certificate issued under policies equivalent to the Federal Bridge CA (FBCA) Medium-HW and High policies.

3.1 Decomposition of PIV Authentication and Authorization

Identity credentials issued to conform to the PIV standard and related specifications can support a number of mechanisms for authentication of the user as described above. Assuming that technical interoperability have been achieved, the authentication of the holder of a PIV card can be decomposed into a series of activities as described below:

- Credential Integrity Validation – the relying party (RP) needs assurance that the identity credential is not tampered
- Credential Source Authentication – the RP needs to determine the identity and trustworthiness of the issuer of the credential
- Issuer Authority Verification – the RP needs to verify that the issuer of the credential has the authority to issue PIV credentials
- Credential Status Check – the RP may need to check that the identity credential is currently valid and not revoked
- Proof-of-Possession Check – the RP may require the user presenting the PIV card to prove that he or she is the rightful owner of the PIV card

The table below illustrates how each of the credentials present on a PIV card support the above decomposition steps.

Table 2 - CHUID Authentication

Activity	Details of execution
Integrity Validation	CHUID signature validated
Source Authentication	CHUID Signer certificate trust path validated to trust anchor
Issuer Authority Check	*id-PIV-content-signing* asserted within *extendedKeyUsage* extension of Signer certificate, or, explicit trust of CHUID Signer certificate/key
Status Check	Revocation check of PIV Authentication certificate (if practical)
Proof-of-Possession	-

Table 3 - CAK Authentication

Activity	Details of execution
Integrity Validation	CHUID contents used in CAK derivation (possibly[1])
Source Authentication	Issuer key used in CAK derivation (possibly[1])
Issuer Authority Check	Explicit trust of PIV card issuer as authoritative (possibly[1])
Status Check	Backend channel status queries (if practical)
Proof-of-Possession	PIV card presented can perform challenge response to prove control of a CAK that matches derived/registered CAK

Table 4 - Biometric Authentication

Activity	Details of execution
Integrity Validation	Biometric object signature validated
Source Authentication	Biometric Signer certificate trust path validated to trust anchor
Issuer Authority Check	*id-PIV-content-signing* asserted within *extendedKeyUsage* extension of Signer certificate, or explicit trust of CHUID Signer certificate/key
Status Check	Revocation check of PIV Authentication certificate (if practical)
Proof-of-Possession	User provides PIN to activate PIV card; provides biometric sample which is matched to biometric object on card

Table 5 - PKI Authentication

Activity	Details of execution
Integrity Validation	PIV Authentication certificate signature validated
Source Authentication	PIV authentication certificate trust path validated to trust anchor
Issuer Authority Check	Certificate issuer asserts *id-Common-HW* policy, or, explicit trust of certificate issuer certificate/key
Status Check	Revocation check of PIV Authentication certificate
Proof-of-Possession	User provides PIN to activate PIV card ; uses private key on card in challenge response scheme to match PIV Authentication certificate

Following successful completion of some or all of the steps above, the RP knows the identity and a set of attributes of the PIV cardholder with varying degrees of certainty and assurance. The next step is to determine whether the cardholder can be granted access to the requested physical or logical resource. This access control decision is typically based on one of the following models:

- Identity-based access – the identity of the authenticated subscriber determines the authorization that may be granted. This model is appropriate when very fine-grained access provisioning and access revocation is required. For example, a specific Federal employee who is on detail to another agency for an extended period may be provisioned access based on their FASC-N.
- Role- or Group-based access – authorization is determined based on whether the identity is part of a broader group or set or individuals. This model is useful for rapid access provisioning and de-provisioning of groups of users. For example, all users from a particular agency may be provisioned access rapidly by allowing access to anyone whose PIV agency code matches the target agency.
- Attribute-based access - various other attributes (or combinations thereof) are evaluated to determine the authorization for the PIV cardholder. These attributes may be retrieved from the PIV card or from attribute authorities through backend channels. This model is useful to establish specific criteria for access without limiting access to specific individuals or groups. For example, users who are from a particular agency and whose NACI has been completed successfully may be granted access to a resource.

4. PIV COMPATIBLE AND PIV INTEROPERABLE CARDS

As the Federal government rolls out PIV cards for Federal employees and contractors, various other segments of government (e.g., state and local) and industry are also adopting the standards specified for PIV cards. These organizations desire to interoperate with Federal agencies. To this end, the Federal Identity Credentialing Committee (FICC) defined two new categories of identity credentials that are functionally and technically similar to

[1] A possible symmetric CAK implementation could use the CHUID and Issuer key as inputs to derive a unique CAK for each PIV card.

PIV cards, and may be accepted for access to Federal facilities and systems [4].

The primary challenges in making these non-Federally issued identity credentials interoperable are that non-Federal organizations cannot:

1) Satisfy the requirement to conduct a National Agency Check with Inquiries (NACI) on Subscribers
2) Issue digital certificates under the Common Policy Framework
3) Create Federal Agency Smart Credential Numbers (FASC-N) since these numbers include an Agency Code that is only capable of supporting Federal agencies.

PIV-Compatible cards conform to the technical specifications for PIV but do not support the trust and assurance of PIV cards.

PIV-Interoperable cards conform to the technical specifications for PIV and additionally have been issued in a manner that supports trust by Federal relying parties. Specifically, these cards must include an authentication certificate issued by a provider cross-certified with the Federal Bridge certification authority (FBCA) at *Medium-HW* policy and require subscriber registration through an identity proofing process that satisfies NIST SP 800-63 Level 4 requirements.

5. PIV CREDENTIALS AS FEDERATED IDENTITIES - CHALLENGES

A federated identity supports portability of identity information across disparate security domains. This allows users of one security domain to obtain services from a second security domain without the need for each domain to administer redundant identities for the same user. In promoting a “Government-wide standard for secure and reliable forms of identification”, HSPD-12 inherently envisions the use of the PIV card for access to various Federally controlled facilities and information systems. Thus, an implicit goal of HSPD-12 is to facilitate the use of the PIV card as a federated identity across the Federal government.

When an agency accepts credentials on PIV cards or PIV-like cards issued by organizations outside of their own agency, it constitutes a use case of “federated identity”. [Note that using local agency PIV cards for authentication and authorization is not considered federated use.] There are at least three scenarios of federated use of PIV or PIV-like cards as described below.

- Non-local Agency PIV cards – An agency allows the use of PIV cards issued by other Federal agencies as a means of authentication and subsequent authorization to agency controlled facilities and systems.
- PIV-Interoperable cards – An agency allows the use of PIV-Interoperable cards as defined by the FICC for authentication and authorization to agency controlled facilities and systems.
- PIV-Compatible cards - An agency allows the use of PIV-Compatible cards as defined by the FICC for authentication and authorization to agency controlled facilities and systems.

The challenges in accepting identity credentials as federated identities in each of the above scenarios are described the sections below.

5.1 Non-Local Agency PIV Cards

In accordance with HSPD-12 and FIPS 201, only Federal agencies can issue PIV cards to Federal employees and contractors. HSPD-12 requires that agencies “require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.” As agencies deploy PIV-enabled authentication mechanisms for physical and logical access, they need to evaluate the risks posed by acceptance of PIV cards issued by other agencies.

HSPD-12 requires that PIV cards be “issued only by providers whose reliability has been established by an official accreditation process.” NIST has published SP 800-79-1, “Guidelines for the Accreditation of Personal Identity Verification Card Issuers” to serve as a framework for accreditation [3]. However, accreditation is essentially an agency’s internal risk-based decision to authorize operation of a system. In the context of HSPD-12, accreditation is the subjective process of determining whether a PIV card issuer is compliant with FIPS 201-1 and related specifications. Each agency applies its own level of rigor to the compliance checking to determine whether their PIV card issuer can be accredited. FIPS 201-1 does not require an independent audit of the issuance and management processes for PIV cards. While the PKI credentials resident on the PIV card are issued through an infrastructure that mandates an independent annual audit, the additional requirements that pertain to a PIV card are never subjected to an independent audit.

The decision to accept PIV cards issued by other Federal agencies becomes even more complicated because HSPD-12 does not apply uniformly to all Federal agencies. HSPD-12 states that only “executive departments and agencies” need to implement a program in compliance with the directive. Effectively, this implies that Federal government organizations that are outside the executive branch are not mandated to implement HSPD-12 compliant programs. Although not required to do so, many of these non-executive branch agencies have decided to implement identity credentials technically equivalent to PIV cards (including PKI certificates issued through the Common Policy Framework for Subscribers as well as PIV Signers) – however, many of the process-oriented requirements of FIPS 201-1 are not being followed by these agencies since they are not required to comply with HSPD-12. Typically, these same agencies have decided not to accredit their issuance systems using the framework in NIST SP 800-79-1. As a result, while the PIV cards from these agencies are technically indistinguishable from PIV cards issued by executive branch agencies that have followed all required processes, they are, in essence, inferior in terms of the vetting and due diligence and hence do not have the same level of assurance.

Another concern in using the CHUID and biometric objects on the PIV card as a basis for authentication is that the integrity and source of these objects have to be verified through validation of the signature on the CHUID and biometric objects as described earlier. When the PIV card is issued by an agency that obtains PKI certificates through the Common Policy Framework, the PIV content signing certificate is clearly distinguishable through the presence of the *id-CommonHW* policy identifier and an extended key usage of *id-PIV-content-signing*. However, when the PIV card issuer is using a legacy branch of the Federal PKI (e.g., one that is directly cross-certified with the FBCA) there is no obvious way to differentiate a PIV content signing certificate from a regular signature certificate issued under a policy equivalent to the FBCA *Medium-HW* policy.

In essence, it is entirely possible that a regular user who has a digital signature certificate asserting the equivalent of *Medium-HW* policy within the FBCA trust environment, can create PIV-like cards with digitally signed fictitious CHUIDs – a Federal relying party that verifies the signature on this type of CHUID would typically consider the CHUID to be trustworthy since the signer's certificate can be validated through the FBCA; yet, this is clearly a scenario that needs to be detected by the relying party to prevent fraudulent CHUIDs being used to gain access. It may be noted that only trusted Certification Authorities (CAs) can issue the PIV authentication certificate, so this credential is not vulnerable to the same type of weakness as the signed CHUID and biometric objects.

The above concerns are summarized below.

Table 6 - Risks of Non-local Agency PIV Cards

Scenario	Risk
Independent audit of compliance not required by HSPD-12; only internal risk based accreditation using SP 800-79-1.	Agencies accepting non-local PIV cards don't have assurance about the rigor of the SP 800-79-1 accreditation.
HSPD-12 mandate does not apply to non-Executive branch agencies.	Agencies accepting PIV cards from non-Executive branch agencies have little assurance of compliance with HSPD-12
Agencies with legacy PKI don't have a mechanism to indicate authorized PIV object signers	Agencies accepting PIV cards from Issuers that use legacy PKI certificates have a low level of assurance in the integrity of the CHUID and BIO objects on the card.

The mitigation strategies to address the identified concerns are as follows:

- A relying party agency may analyze the issuing agency's NIST SP 800-79-1 accreditation process and assessment results. The former may additionally require targeted assessments of the latter agency's PIV issuance activities to more adequately identify the risks of accepting the issuing agency's PIV cards.
- A relying party agency that wants to allow CHUID and BIO authentication for PIV cards issued by another Federal agency, can import the PIV Signer certificates from the second agency as trusted certificates (after careful vetting of the second agency's processes related to issuance of the CHUID and biometric objects); this would ensure that only signed PIV objects from verified non-local PIV Signers are accepted for identity authentication purposes.
- A relying party agency may only accept PKI based authentication for holders of non-local PIV cards.

5.2 PIV-Interoperable Cards

As mentioned earlier, PIV-Interoperable cards are required to include an authentication private key and certificate that can be validated through the FBCA under *Medium-HW* policy. Additionally, NIST SP 800-63 Level 4 registration requirements need to be met by PIV-Interoperable cards.

Since the authentication certificate on the PIV-Interoperable card is issued under a policy equivalent to the *Medium-HW* policy of the FBCA, the assurance provided by this certificate (and corresponding private key) is very high. However, if the relying party desires to use the CHUID, biometric or CAK credentials loaded on the PIV-Interoperable card, the assurance level quickly drops off to nearly nothing. This is because the *Medium-HW* policy of the FBCA or requirements for Level 4 identity proofing under NIST SP 800-63 do not include the collection of biometrics during subscriber registration, nor do they include any form of background checking or role separation during registration and issuance.

Additionally, for the same reasons described in the previous section on PIV cards issued through legacy PKIs, there is no way to distinguish that the signer of the CHUID or biometric is an authoritative signer rather than just another user with a digital signature certificate within the FBCA environment. In summary, the CHUID and biometric credentials on a PIV-Interoperable card have little or no assured association to the identity asserted within the authentication certificate on the same card. Relying party agencies deciding to utilize PIV-Interoperable cards need to exercise the utmost discretion in choosing to use the CHUID, BIO and BIO-A authentication mechanisms with PIV-Interoperable cards.

The above concerns are summarized below.

Table 7 - Risks of PIV-Interoperable Cards

Scenario	Risk
No independent audit or SP 800-79-1 accreditation required for PIV-Interoperable cards	Agencies accepting PIV-Interoperable cards have little assurance of compliance with HSPD-12.
No mechanism to identify authorized signers of data objects on PIV-Interoperable cards.	Agencies accepting PIV-Interoperable cards have a low level of assurance in the integrity of the CHUID and BIO objects on the card.

The mitigation strategies to address the identified concerns are as follows:

- A relying party agency may require that the issuer of PIV-Interoperable cards demonstrates that it has performed a thorough assessment of their issuance facility and processes based on the NIST SP 800-79-1 guideline and are willing to make the results of the assessment available for review.
- A relying party may wish to include the certificate of the PIV Signer for each approved PIV-Interoperable

card issuer as an explicit trust anchor rather than accepting any Medium-HW signing certificate through the FBCA – this limits the acceptable signers of CHUID and biometric objects.

- A relying party agency may wish to perform background checking (such as NACI) on the subjects of PIV-Interoperable cards prior to allowing them access to federal facilities and systems.
- A relying party agency may only accept PKI based authentication for holders of PIV-Interoperable cards.

While these techniques definitely hinder interoperability, an agency with a low risk tolerance level may wish to employ one or more of these to allow the controlled acceptance of PIV-Interoperable cards as federated identities.

5.3 PIV-Compatible Cards

PIV-Compatible cards suffer from all of the assurance related drawbacks of PIV-Interoperable cards. In addition, there is no basis for trusting any of the digitally signed credentials on the card. Relying party agencies wishing to accept PIV-Compatible cards for access to facilities and systems should exercise the utmost caution and perform out of band due diligence of issuance processes and trustworthiness of the credentials on the PIV compatible card.

6. STRATEGIES TO IMPROVE ASSURANCE IN FEDERATED IDENTITY USING PIV AND PIV-LIKE CARDS

In Section 5, we discussed assurance related challenges in using PIV and PIV-like cards issued by external organizations and related mitigation options. This section offers some additional strategies to promote the use of PIV and PIV-Interoperable cards as federated identities.

In the near term, we recommend that the Office of Management and Budget (OMB) establish a clear policy that requires Executive branch agencies to conduct a thorough accreditation of their PIV card issuers prior to issuance of PIV cards; agencies should also be required to report their PCI accreditation activities to the OMB on a yearly basis. Likewise, we recommend that OMB establish policy that PIV and PIV-like cards that are accepted as a basis for allowing access to Federal facilities and resources, are issued by accredited issuers (in accordance with SP 800-79-1). This creates an environment where non-Executive branch agencies and commercial PIV-Interoperable card issuers would undergo SP 800-79-1 accreditation if they wish their cards to be accepted by other federal agencies.

In the long-term, it may be worth investigating whether the cost of implementing a third-party audit and compliance regime for issuers of PIV, PIV-Interoperable and PIV-Compatible cards can be balanced against the improved security and ease of federation between the digital identities of government and commercial organizations. This would be very similar to the work being done by the Liberty Alliance Identity Assurance Expert Group in the context of the assurance levels for electronic authentication.

7. STRATEGIES FOR RAPID ELECTRONIC AUTHENICATION OF NON-LOCAL PIV AND PIV-LIKE CARDS

HSPD-12 establishes policy for secure and reliable forms of identification that can be “rapidly authenticated electronically.” When using non-local PIV or PIV-like cards, this becomes difficult since the types of authentication mechanisms that allow for rapid authentication – namely, CHUID, CAK, BIO, BIO-A – have little or no assurance. The PKI authentication mechanism is the only one that provides a reasonable level of assurance, however, this requires contact readers, PIN use, and possible fetching of online revocation lists. In this section, we describe a novel approach to rapid electronic authentication of non-local PIV and PIV-like cards.

Consider the scenario where an employee of Federal Agency A needs to work at the facility of Agency B for six or more months. This scenario occurs very often when agency employees are on detail to another agency. One very effective way to allow this non-local person rapid but secure authenticated access to Agency B’s physical facilities may be use a hybrid PKI-CAK scheme. In a “Visitor Enrollment” step at Agency B, the employee of Agency A can present their PIV card to the physical security group. The latter employs tools (like the PIV Trust Validation Tool being developed by NIST) to perform a thorough validation of all of the credentials on the non-locally issued PIV card, including the CHUID, biometric object and PKI credentials. The tool performs full path validation and revocation checking of all digital certificates needed to validate the credentials on this PIV card. The cardholder validates that they know the correct PIN to activate the PIV card, and his or her biometric samples match those stored on their PIV card. At the end of the Visitor Enrollment step, Agency B has a high degree of assurance that the cardholder is the genuine owner of the PIV card presented and that the credentials on the card are trustworthy and unmodified. As the last step of the Visitor Enrollment step, a series of random challenge strings (perhaps five to ten) are issued to the PIV card and the CAK is invoked to generate responses to each challenge string. The challenge-response pairs are stored along with the cardholder’s unique FASC-N as a part of the physical access control database (PACS-DB).

Following the Visitor Enrollment step, when this non-local individual needs to enter Agency A’s facilities, the contactless reader at the entry point will likely detect that the CHUID is not for a local subscriber. In this case, the PACS-DB record for that CHUID will be retrieved, and one of the stored challenges (selected randomly) will be issued to the visitor’s PIV card and the CAK invoked to respond. The received response will be compared to the stored response for that challenge string, and on a successful match, the visitor will be considered adequately authenticated. The FASC-N associated with that PACS-DB challenge-response pair will then be used for the authorization decision for the targeted facility. Since this CAK based challenge response scheme can be performed with a contactless reader without PIN submission, it allows for painless, rapid and secure authentication of the visitor. The assurance of this scheme can be further raised through additional mechanisms such as:

- Periodic revocation checking of all registered visitors to eliminate the need to do revocation checking in real-time

- Adding biometric authentication of the cardholder to match stored biometric objects (collected during the registration step)

The above scheme is most rapid when a symmetric CAK is present on the external PIV card, but works with a asymmetric CAK as well. Certificate path development and validation in real-time is eliminated in the scheme since it is done during the Visitor Enrollment step – occasional revocation checking is done in the background to validate the current status of the certificates within the PACS-DB. When the visitor presents their PIV card for authentication and access to a facility, the CAK is invoked with known challenge response pairs to establish the identity of the cardholder; additional assurance can be achieved by requiring cardholder biometric matching with the enrollment record.

Let's consider the use of PIV-Interoperable and PIV-Compatible cards by non-local individuals that need access to Agency A facilities for longer than six months. A similar Visitor Enrollment step can be followed which validates all of the credentials on the card and records the unique GUID of the card, biometric objects, and challenge-response pairs generated by invoking the CAK on the card. Additionally, a background check on the visitor may be performed if needed. Once the Visitor Enrollment record is completed, the visitor can use their PIV-like card for rapid but secure authentication for access to Agency A facilities.

8. CONCLUSION

In this paper, we discussed a number of trust and assurance issues related to the use of non-local PIV cards and PIV-like cards as federated identity credentials. We presented a number of strategies to improve the assurance in the credentials carried in these non-local cards. We also presented a novel approach to higher assurance authentication of long-term visitors to a Federal facility through the use of a thorough Visitor Enrollment step that records challenge-response pairs for the CAK on the card.

9. ACKNOWLEDGMENTS

My thanks to Nabil Ghadiali and Dennis Bailey on supporting the refinement of the thoughts presented in this paper through lengthy discussions.

10. REFERENCES

[1] The White House. August 2004. Policy for a Common Identification Standard for Federal Employees and Contractors. Homeland Security Presidential Directive/Hspd-12. DOI= http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[2] National Institute of Standards and Technology, March 2006. Federal Information Processing Standard (FIPS) Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.

[3] National Institute of Standards and Technology, June 2008. NIST Special Publication 800-79-1, Guidelines for the Accreditation of Personal Identity Verification Card Issuers.

[4] Spencer, J. 2008. Beyond HSPD-12: Interoperability with non-PIV Credentials. Office of Governmentwide Policy, Federal Identity Credentialing Committee. Presentation at Federal Information Assurance Conference 2008.