Personal Identity Verification Interoperable (PIV-I) Certification Process

Federal PKI Policy Authority
Certificate Policy Working Group

Version 1.0
March 8, 2011

Table of Contents

1. Introduction

The Personal Identity Verification Interoperability (PIV-I) guidance is intended to facilitate the issuance of identity credentials by organizations that are interoperable with Federal PIV-conformant systems and can be trusted by Federal organizations. In order to achieve this level of trust, PIV-I credentials must include digital credentials from a certification authority cross-certified with the Federal Bridge Certification Authority (FBCA) at the Medium Hardware Level of Assurance or above whose cross certificate relationship includes the PIV-I policy object identifiers (OID).

The Federal government has established a PIV-I cross certification list for entities that have demonstrated the ability to provide digital credentials that meet the expectations of the PIV-I guidance by demonstrating comparability with the appropriate FBCA policies.

This PIV-I guidance is intended to provide the background information and activities related to the cross-certification process for prospective PIV-I providers, resulting in inclusion on the PIV-I cross certification list. It also describes requirements that must be met to maintain cross-certification.

Questions related to this document should be directed to idmanagement@gsa.gov.

1.1. Document Overview

This document is constructed in three sections:

- *PIV-I Cross Certification Overview* describes the components of a PIV-I program and the partitioning of responsibilities;
- *PIV-I Cross Certification Requirements* describes the steps that entities must perform to become a PIV-I provider and approved for inclusion on the PIV-I cross certification list. This section identifies the requirement documents that must be considered as part of this process;
- *PIV-I Post-Acceptance Process* describes the steps a PIV-I provider must perform to maintain certification.

1.2. Roles and Responsibilities

Federal PKI Policy Authority (FPKIPA)

The Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.

Federal PKI Certificate Policy Working Group (CPWG)

The Federal PKI Certificate Policy Working Group (CPWG) reviews the prospective PIV-I provider documentation for cross-certification of the PIV-I provider with the Medium Hardware/PIV-I requirements in the X.509 Certificate Policy (CP) for the

Federal Bridge Certification Authority (FBCA) and makes recommendations for cross-certification to the FPKIPA. The CPWG is comprised of representatives from organizations that are members of the Federal PKI Policy Authority (FPKIPA).

Identity, Credential, and Access Management (ICAM)
The Identity, Credential, and Access Management (ICAM) lab performs PIV-I card interoperability testing. A favorable recommendation from the CPWG (after successful card interoperability testing) will be presented to the FPKIPA members for a vote to approve the applicant as a PIV-I provider at their earliest convenience.

2. PIV-I Cross Certification Overview

2.1. PIV-I Components

The PIV-I provider must implement five distinct components: Certification Authority (CA); Registration Authority (RA); Card Management System (CMS); Repository; Archive and Online Certificate Status Protocol Server (for those PIV-I providers that support PIV-I authentication and/or PIV-I card authentication). While there are many ways to architect, deploy and manage these components, the responsibilities of the components are described below:

- The CA issues X.509 certificates and certificate revocation lists (CRL) that conform to FBCA Medium Hardware/PIV-I;
- The RA performs identity proofing for prospective certificate subjects in a manner that conforms to FBCA Medium Hardware/PIV-I;
- The CMS issues PIV-I cards;
- The Repository publishes CA certificates and CRLs; and
- The Archive provides long term secure storage for certificates and CRLs issued by the CA, CA and RA electronic and physical audit logs, audit results, and policy documents.
- The Online Certificate Status Protocol (OCSP) servers provide the revocation status of X.509 certificates

2.2. PIV-I Provider & External Entities

The FPKIPA does not limit outsourcing of specific PKI services by the PIV-I provider. For example, the Registration Authority responsibilities may be outsourced to an external organization. However, the responsibility for the continuing conformance of the Registration Authority remains between the organization and the PIV-I provider.

2.3. PIV-I Cross Certification Process

PIV-I cross certification with the Federal Bridge Certification Authority (FBCA) is an adjunct to the process for cross certification with the FBCA at Medium Hardware, and is comprised of the same six primary activities:

- Application for Cross Certification
- Policy Mapping
- Technical Testing
- Audit Review
- Memorandum of Agreement
- Cross Certification

Entities previously cross certified with the FBCA at Medium Hardware may utilize the Legacy PIV-I process (refer to footnotes 1 and 2) to add PIV-I to their current cross certificate agreement. All others must complete the full cross certification process for FBCA cross certification at Medium Hardware and PIV-I.

This will be discussed in detail in the following section.

3. PIV-I Cross Certification Requirements

3.1. Application for Cross Certification

The first step in achieving PIV-I cross certification with the FBCA is to submit an application to the FPKIPA. The application template is available at: http://www.idmanagement.gov/fpkipa/documents/fpkipa_application.doc[1]

The application must indicate that FBCA Medium Hardware cross certification is sought in addition to PIV-I cross certification.

Upon receipt, the FPKIPA will review the application and make a determination as to whether cross certification is in the best interest of the U.S. Federal Government. The Applicant will be notified of the FPKIPA's decision. Those whose applications have been approved will move into the mapping and technical testing phase.

Organizations whose applications are rejected by the FPKIPA may request a written decision and an interview with the FPKIPA for reconsideration.

3.2. Policy Mapping

The FBCA Certificate Policy includes specific requirements pertaining to PIV-I. PIV-I service providers must achieve comparability with the FBCA Medium Hardware policy as part of the PIV-I alignment. Entities should familiarize themselves with the following documents prior to beginning the mapping process:

- X.509 CP for the Federal Bridge Certification Authority (FBCA)
- PIV Interoperability for Non-Federal Issuers
- Criteria and Methodology for Cross Certification with the FBCA or C4CA

[1] Entities cross certified with the FBCA at Medium Hardware at the time of application may use the PIV-I Application template located at: http://www.idmanagement.gov/documents/PIVI_NFI_Application.doc

- X.509 Certificate and CRL Extensions Profile for PIV-I Cards;

Each PIV-I provider must submit the following in order to initiate the mapping process:

- X.509 CP governing the PKI that will provide the PIV-I service formatted according to RFC 3647
- X.509 Certification Practices Statement (CPS) that implements the associated Certificate Policy
- Completed mapping matrices available at: http://www.idmanagement.gov/fpkipa/documents/FPKI_CertificationApplicantRequirements.docx[2]
- Any additional documentation referenced in either the CP or the CPS that is required to determine mapping comparability.

The Federal PKI Certificate Policy Working Group (CPWG) will review the PIV-I mapping matrices to determine their overall satisfaction of alignment with the FBCA CP. Questions or concerns that cannot be answered by consulting the supporting documentation provided with the matrix will be referred back to the applicant for resolution. If necessary, the CPWG will invite the applicant to a meeting to resolve open issues. In some cases, the applicant may be asked to provide copies of additional documents cited in the CP, where these are considered critical to resolving particular issues or concerns. This is an iterative process and may be repeated several times before successful completion. Any areas of concern will be discussed with the PIV-I provider and resolved prior to providing a mapping recommendation to the FPKIPA.

Once the review has been completed successfully, the PIV-I Technical Testing will be scheduled.

The PIV-I provider shall operate their PKIs in a manner that ensures continuing alignment with the FBCA CP. Each PIV-I provider shall develop and operate their systems according to a CPS governing operation of its PKI. The PIV-I provider's CPS must be in compliance with their Certificate Policy.

3.3. Technical Testing

The PIV-I applicant must successfully complete technical testing in accordance with the PIV-I Test Plan. Technical testing can occur at any time after the initial mapping review activity has completed. The purpose of technical testing is to validate the ability of a PIV-I candidate to issue PIV-I cards that meet the test requirements. This test requirement goes beyond the testing conducted for FBCA Medium Hardware and is required of all applicants.

[2] Entities cross certified with the FBCA at Medium Hardware at the time of application may use the PIV-I Legacy mapping matrices located at: http://www.idmanagement.gov/fpkipa/documents/PIVI_Legacy_Mapping_Matrix.doc

At a minimum, PIV-I providers who operate under the PIV-I program must support smart cards conforming to NIST Special Publication 800-73-3 and listed on the FIPS 201 Evaluation Program Approved Products List (APL).

If the PIV-I applicant does not successfully complete the requirements of the PIV-I Test Plan, the applicant will be provided with a list of criteria that were not met. Depending upon the severity of the issues, the FPKIPA may choose from the following options:

- If the issues are judged to be minor, the FPKIPA may accept a written attestation that the issues have been corrected and approve the technical testing; or
- The PIV-I applicant repeats some portion or all of the Technical Testing.

If remediation requires a change to the applicant's CP, the CPWG will require an update to the compliance audit.

Successful PIV-I implementation is dependent on the Card Management System (CMS). As a result, the CMS must be identified during the testing process. Organizations that plan to utilize multiple CMS products shall submit at least one test card associated with each CMS for testing. Once complete, the approved PIV-I provider shall list their approved CMS(s). New testing shall be performed whenever a new CMS is to be instantiated in association with a specific PIV-I provider.

Upon successful completion of the PIV-I Test Plan, the results are reported to the FPKIPA.

3.4. Audit Review

To provide assurance of that their CP and CPS reflect their operations, PIV-I providers must submit a compliance audit from a qualified, independent, third party auditor, in accordance with Section 8 of the FBCA CP, that establishes:

- The PIV-I provider CPS is in compliance with its Certificate Policy;
- The PIV-I PKI, excluding customer responsibilities, is operated in compliance with the CPS.

For an initial audit review, operational compliance may be determined by a Day Zero Audit, which covers all aspects of the PKI operations except issuance and management of end user certificates.

The PIV-I provider and their third party auditor should consult the *Auditor Letter of Compliance, Compliance Audit Requirements* for guidance on preparing the audit letter to the FPKIPA.

3.5. Memorandum of Agreement

Once all of the above criteria have been successfully completed, the Federal PKI Certificate Policy Working Group will submit a recommendation to the Federal PKI Policy Authority to cross certify with the applicant at the identified levels of assurance, including PIV-I. Upon a favorable vote, the applicant and the Chair of the Federal PKI

Policy Authority shall complete the Memorandum of Agreement (MOA) citing each organization's rights and responsibilities associated with the cross certification.

3.6. Cross Certification

Once the MOA is complete, the Federal PKI Management Authority (FPKIMA) and the applicant will coordinate the steps necessary to issue the cross certificates.

The entity will then be added to the approved PIV-I Provider List at:
http://www.idmanagement.gov/drilldown.cfm?action=pivi_cross_cert

4. PIV-I Post-Acceptance Process

The Triennial Compliance Audit Guidance mandates yearly compliance audits performed by a competent, independent third party. The PIV-I provider has ongoing audit and analysis responsibilities to ensure that the PKI continues to operate at the appropriate level of trustworthiness.

The PIV-I provider shall submit a compliance audit letter each year covering PIV-I operated components for as long as they continue. If a PIV-I provider is determined to be out of compliance, it shall submit a remediation plan to the CPWG for consideration. Failure to submit an annual compliance audit letter, or findings that indicate the PIV-I provider is out of alignment with the FBCA CP, will result in removal from the PIV-I cross certification list and/or revocation of the cross certificates.

5. Glossary

Access Control	The process of granting or denying requests to access physical facilities or areas, or logical systems (i.e., computer networks or software applications). See also "logical access control system" and "physical access control system".
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Affiliated Organization	Organizations that authorize affiliation with subscribers of PIV-I certificates.
Applicant	Any organization seeking to participate in the Federal Certified PKI Personal Identity Verification Interoperability (PIV-I) program.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authentication	The process of establishing confidence in the identity of users or information systems.
Authorization	The process of giving individuals access to specific areas or systems based on their authentication.
Biometric	A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.
Cardholder Unique Identifier (CHUID)	The PACS Implementation Guidance [PACS] defines the CHUID data object; this description is refined in NIST SP 800-73. The PIV Card shall include the CHUID as defined in NIST SP 800-73. The CHUID includes an element, the Federal Agency Smart Credential – Number (FASC-N), which uniquely identifies each card. The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation. The PIV FASC-N shall not be modified post-issuance.
Card Management System (CMS)	The Card Management System is responsible for managing smart card token content.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	Lists maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Compliance Analysis	Independent review of documentation and operations to ensure the systems are operated in accordance with their governing documentation.
Day Zero Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, on the core PKI Service Offering. This review does not include the operational aspects associated with the issuance of credentials to end users since these operations have not been initiated at the time of the Day Zero Audit.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
Operational Capabilities Demonstration (OCD)	Evaluation process to determine the ability of the applicant service to perform a set of prescribed functions.
Personal Identity Verification (PIV)	Term referring to the HSPD-12 compliant identity credential issued to all Federal employees and select Federal contractors.
PIV-Interoperable (PIV-I) providers	Providers of PKI Services that have successfully completed the review and evaluation activities described in this guidance.
Public Key Infrastructure	A set of policies, processes, server platforms, software, and

(PKI)	workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system component that provides a service in response to requests from clients.
Smart Card	Any pocket-sized card with embedded integrated circuits that allows storage and retrieval of information. For the purposes of this document, a smart card is a dual-interface card, allowing both contact and contactless access to a microprocessor that contains, among other features a cryptographic engine capable of generating strong asymmetric key pairs.

6. References

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.idmanagement.gov/documents/HSPD-12.htm

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST Special Publication 800-63 Version 1.0.2: Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

NIST Special Publication 800-73-3: Interfaces for Personal Identity Verification (4 Parts)
http://csrc.nist.gov/publications/PubsSPs.html

NIST Special Publication 800-76-1: Biometric Data Specification for Personal Identity Verification
http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

NIST Special Publication 800-78-3: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

NIST Special Publication 800-79-1: Guidelines for the Accreditation of Personal Identity Verification Card Issuers
http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf

NIST Special Publication 800-104: A Scheme for PIV Visual Card Topography
http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29_2007-final.pdf

NIST Special Publication 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

OMB M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-05.pdf

OMB M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf

Personal Identity Verification Interoperability for Non-Federal Issuers
http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

Request for Comments (RFC) 3852: Cryptographic Message Syntax (CMS)
http://www.ietf.org/rfc/rfc3852.txt

Request for Comments (RFC) 4122: A Universally Unique IDentifier (UUID) URN Namespace
http://www.ietf.org/rfc/rfc4122.txt

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3
http://www.idmanagement.gov/iab/documents/PACS.pdf

X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards
http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

Personal Identity Verification Interoperable (PIV-I) Frequently Asked Questions (FAQ)
http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf