



**FBCA Certificate Policy Change Proposal Number: 2010-03**

**To:** Federal PKI Policy Authority  
**From:** PIV-I Tiger Team  
**Subject:** Proposed modifications to the Federal Bridge Certificate Policy  
**Date:** May 11, 2010  
**Title:** Certificate Policy Updates to Address PIV-I

**Version and Date of Certificate Policy Requested to be changed:**

X.509 Certificate Policy for the Federal Bridge Certification Authority, Version 2.15, April 8, 2010.

**Change Advocate's Contact Information:**

Name: Chris Loudon (PIV-I Tiger Team Co-Chair)  
Organization: Protiviti Government Services (on behalf of GSA)  
Telephone number: 703-447-7431  
E-mail address: [chris.loudon@pgs.protiviti.com](mailto:chris.loudon@pgs.protiviti.com)

**Organization requesting change:** Federal PKI Policy Authority

**Change summary:** The Personal Identity Verification – Interoperable (PIV-I) Tiger Team has coalesced requirements for Non-Federal Issuers (NFIs) of PIV-I Cards. A subset of the requirements applies to PIV-I certificates. Since an NFI of a PIV-I Card must be cross-certified with the Federal Bridge at the Medium Hardware Assurance Level, the FBCA Certificate Policy (CP) must be revised to incorporate applicable PIV-I requirements, in the form of policy statements. This document lists the proposed updates (e.g., additions, changes) to the FBCA CP for that purpose.

**Background:** In November 2009, the GSA commissioned a PIV-I Tiger Team to search all applicable Federal government documents for requirements pertaining to PIV-I Cards. The team reviewed source such as PIV-I for Non-Federal Issuers, FIPS 201, NIST SP 800-63, and NIST SP 800-79. PIV-I requirements across a number of categories were found (e.g., certificates and keys, security, algorithms, ID proofing). The requirements ensure NFIs issue PIV-I Cards that can be trusted by the Federal government and that are interoperable with Federal government PIV systems.

## Issue

FPKI CPs are evolutionary documents that continue to grow and change as new understanding and insight is gained by the Federal sector. As a result of the Federal government's desire to expand the universe of identity cards that can interoperate with Federal government PIV systems in a controlled, trustworthy manner, the FBCA CP must be revised to address relevant aspects of PIV-I Cards.

### **Specific Changes:**

**Specific Changes:** Specific changes are made to the following sections:

Insertions are underlined, deletions are in ~~striketrough~~:

### **1. Introduction**

This Certificate Policy (CP) defines ~~seven~~ ten certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent ~~five-six~~ different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High) for public key certificates. The level of assurance refers to 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.

Personal Identity Verification Interoperable (PIV-I) policies for PIV-I Hardware, PIV-I Card Authentication, and PIV-I Content Signing are for use with PIV-I smart cards (see Appendix A for more information).

[...]

### **1.2 Document Identification**

There are ~~seven-ten~~ policies specified at six different levels of assurance in this Certificate Policy, which are defined in subsequent sections.

[...]

The FBCA policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

fbca-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
---------------------------------	---------------------------

[...]

<u>id-fpki-certpcy-pivi-hardware</u>	::= { fbca-policies 18 }
<u>id-fpki-certpcy-pivi-cardAuth</u>	::= { fbca-policies 19 }

<u>id-fpki-certpcy-pivi-contentSigning</u>	<u>::= { fbca-policies 20 }</u>
--	---------------------------------

[...]

The requirements associated with the mediumHW-CBP policy are identical to those defined for the Medium Hardware Assurance policy, with the exception of personnel security requirements (see Section 5.3.1).

The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in Appendix A.

In addition, the PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

**1.3.1.7 Certificate Status Servers**

[...] OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy. Entity CAs that issue PIV-I certificates must provide an OCSP responder.

**1.3.3 Card Management System (CMS) [NEW SECTION]**

The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the PIV-I policies only. Entity CAs issuing PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix B. In addition, the CMS shall not be issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

**1.3.5 Affiliated Organizations [NEW SECTION]**

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

**1.4.1 Appropriate Certificate Uses**

[...] To provide sufficient granularity, this CP specifies security requirements at ~~five~~ six increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High. [...]

Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. <u>This level of assurance includes the following certificate policies: Medium, Medium CBP.</u>
<u>PIV-I Card</u>	<u>This level is relevant to environments where risks and</u>

<u>Authentication</u>	<u>consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical.</u>
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. <u>This level of assurance includes the following certificate policies: Medium Hardware, Medium Hardware CBP, PIV-I Hardware, and PIV-I Content Signing.</u>

[...]

### 3.1.1 Types of Names

[...]

The table below summarizes the naming requirements that apply to each level of assurance.

Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
-------------	--

[...]

<u>PIV-I Card Authentication</u>	<u>Non-Null Subject Name (see practice note) and Subject Alternative Name.</u>
----------------------------------	--

[...]

PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

*cn=Subscriber's full name, ou=Affiliated Organization Name,{Base DN}*

For certificates with no Affiliated Organization:

*cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}*

PIV-I Content Signing certificates shall clearly indicate the organization administering the CMS.

For PIV-I Card Authentication subscriber certificates, use of the subscriber common name is prohibited.

PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

*serialNumber=UUID, ou=Affiliated Organization Name,{Base DN}*

For certificates with no Affiliated Organization:

*serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}*

### 3.1.2 Need for Names to Be Meaningful

[...]

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation for the FBCA.

Entity CAs must specify rules for interpreting names in Subscriber certificates in the Entity CP or a referenced certificate profile. (The rules may be simply a description of naming conventions.)

Rules for interpreting PIV-I certificate UUID names are specified in RFC 4122.

### 3.2.2 Authentication of Organization Identity

Requests for FBCA, ~~or~~ Entity CA, or Subscriber certificates in the name of an Affiliated Organization shall include the organization name, address, and documentation of the existence of the organization. [...]

### 3.2.3 Authentication of Individual Identity

PIV-I Hardware certificates shall only be issued to human subscribers.

#### 3.2.3.1 Authentication of Human Subscribers

[...]

**For the Basic and Medium Assurance Levels:** An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

**For PIV-I Certificates:** The following biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76] (see Appendix A):

- An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and

- Two electronic fingerprints to be stored on the card for automated authentication during card usage.

The table below summarizes the identification requirements for each level of assurance.

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address

[...]

<p>Medium (all policies)</p>	<p>Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License).</p> <p>Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the “<i>FBCA Supplementary Antecedent, In-Person Definition</i>” document.</p> <p><u>For PIV-I, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID).</u></p> <p><u>For PIV-I, the use of an in-person antecedent is not applicable.</u></p>
----------------------------------	---

[...]

### 3.3.1 Identification and Authentication for Routine Re-key

[...]

Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in table below.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, <u>Authentication</u> and Encryption Certificates
-----------------	--

[...]

<p>Medium (all policies)</p>	<p>Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.</p>
----------------------------------	---

<u>PIV-I Card Authentication</u>	<u>Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.</u>
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration.

#### 4.9.1 Circumstances for Revocation

[...]

Entity CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

For Certificates that express an organizational affiliation, Entity CAs shall require that the organization must inform the Entity CA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the Entity CA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with an Entity CA such that it no longer provides affiliation information, the Entity CA shall revoke all certificates affiliated with that organization.

[...]

#### 4.9.2 Who Can Request Revocation

[...]

Entity CAs that implement certificate revocation shall, at a minimum, accept revocation requests from subscribers. Entity CAs that issue certificates in association with Affiliated Organizations shall accept revocation requests from the Affiliated Organization named in the certificate.

Requests for certificate revocation from other parties may be supported by Entity CAs. Note that an Entity Principal CA may always revoke the certificate it has issued to the FBCA without any Federal PKI Policy Authority action.

#### 4.9.3 Procedure for Revocation Request

[...]

Entity CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Where subscribers use hardware tokens, but excluding PIV-I certificates, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- [...]

~~For PIV-I and~~ in all other cases not identified above, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

Entity CAs (or delegate) shall collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid, whenever possible. Entity CAs (or delegate) shall record destruction of PIV-I Cards.

#### 4.9.7 CRL Issuance Frequency

[...]

For Entity CAs, see the table below for issuing frequency of routine CRLs. CRLs may be issued more frequently than specified below.

**Table 1 Entity CA CRL issuance Frequency**

<b>Assurance Level</b>	<b>Maximum Interval for Routine CRL Issuance</b>
------------------------	--

[...]

Basic	24 hours
<u>PIV-I Card Authentication</u>	<u>24 hours</u>

[...]

#### 4.9.9 On-line Revocation/Status Checking Availability

If on-line revocation/status checking is supported by an Entity CA, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.9.7.

For PIV-I certificates, CAs shall support on-line status checking via OCSP [RFC 2560].

#### 4.9.12 Special Requirements Related To Key Compromise

[...]

For Entity CAs, when a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

<b>Assurance Level</b>	<b>Maximum Latency for Emergency CRL Issuance</b>
Rudimentary	No stipulation
Basic	24 hours after notification
<u>PIV-I Card Authentication</u>	<u>18 hours after notification</u>
Medium (all policies)	18 hours after notification

[...]

## 5.1 PHYSICAL CONTROLS

[...]

All the physical control requirements specified below apply equally to the FBCA and Entity CAs, CMSs, and any remote workstations used to administer the CAs except where specifically noted.

### **5.1.2.4 Physical Access for CMS Equipment [NEW SECTION]**

Physical access control requirements for CMS equipment containing a PIV-I Content Signing key shall meet the CA physical access requirements specified in Section 5.1.2.1.

## 5.2.4 Separation of Roles

[...]

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Assurance Level	Role Separation Rules
[...]	
<u>PIV-I Card Authentication</u>	<u>Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Role separation duties follow the requirements for Medium assurance below.</u>
Medium (all policies)	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, <u>CMS</u> , and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

[...]

## 5.4.1 Types of Events Recorded

[...]

All security auditing capabilities of the FBCA or Entity CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

<b>Auditable Event</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; <u>PIV-I Card Authentication</u></b>	<b>High</b>
------------------------	--------------------	--------------	---	-------------

[...]

#### 5.4.2 Frequency of Processing Log

[...]

For the FBCA, the FPKI Management Authority shall explain all significant events in an audit log summary.

<b>Assurance Level</b>	<b>Review Audit Log</b>
Rudimentary	Only required for cause
Basic	Only required for cause
<u>PIV-I Card Authentication</u>	At least once every two months <u>Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity</u>
Medium (all policies)	At least once every two months Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

#### 5.5.1 Types of Events Archived

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

<b>Data To Be Archived</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; <u>PIV-I Card Authentication</u></b>	<b>High</b>
----------------------------	--------------------	--------------	---	-------------

[...]

## 5.5.2 Retention Period for Archive

[...]

This minimum retention period for these records is intended only to facilitate the operation of the FBCA and the entities' CAs.

Assurance Level	Minimum Retention Period
Rudimentary	7 Years & 6 Months
Basic	7 Years & 6 Months
<u>PIV-I Card Authentication</u>	<u>10 years &amp; 6 months</u>
Medium (all policies)	10 Years & 6 Months

### 6.1.1.2 Subscriber Key Pair Generation

[...]

At the High and Medium Hardware assurance levels, subscriber key generation shall be performed using a validated hardware cryptographic module. For Medium and Basic assurance, either validated software or validated hardware cryptographic modules shall be used for key generation.

For PIV-I Card Authentication certificates and PIV-I Hardware certificates, subscriber key generation shall be performed on hardware tokens that meet the requirements of Appendix A.

### 6.1.5 Key Sizes

[...]

- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

All end-entity certificates associated with PIV-I shall contain public keys and algorithms that conform to [NIST SP 800-78]

The FBCA shall not issue a cross-certificate with a validity period extending beyond 12/31/2010 to any Entity Principal CA unless all of the following conditions apply:

[...]

### 6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

[...]

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements,

except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Entities are encouraged at all levels of assurance to issue Subscribers two key pairs, one for key management and one for digital signature and authentication.

PIV-I Content Signing certificates shall include an extended key usage of *id-fpki-pivi-content-signing* (see [PIV-I Profile]).

### 6.2.1 Cryptographic Module Standards & Controls

[...]

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA, CMS & CSS	Subscriber	RA
-----------------	---------------	------------	----

[...]

Medium	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
<b><u>PIV-I Card Authentication</u></b>	<u>Level 2 (Hardware)</u>	<u>Level 2 (Hardware)</u>	<u>Level 2 (Hardware)</u>
Medium Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

For hardware tokens associated with PIV-I, see Appendix A for additional requirements.

#### **6.2.4.5 Backup of PIV-I Content Signing Key [NEW SECTION]**

Backup of PIV-I Content Signing private signature keys may be required to facilitate disaster recovery. In which case, PIV-I Content Signing private signature keys shall be backed up under multi-person control.

### 6.2.8 Method of Activating Private Keys

For the FBCA and Entity CAs that operate at the Medium, Medium Hardware, or High level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.

In addition, PIV-I Content Signing key activation requires the same multiparty control established for the Entity CA (see Section 5.2.2).

The Subscriber must be authenticated to the cryptographic module before the activation of any private key (s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered). \_

For PIV-I Card Authentication, user activation of the private key is not required.

### **6.3.2 Certificate Operational Periods/Key Usage Periods**

The FBCA shall limit the use of its private keys to a maximum of three years [...] use of subscriber key management private keys is unrestricted.

PIV-I subscriber certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside.

For PIV-I, CSS certificates that provide revocation status have a maximum certificate validity period of 31 days.

### **6.4.3 Other Aspects of Activation Data**

No stipulation.

For PIV-I, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by a trusted agent of the issuer.

## **6.7 NETWORK SECURITY CONTROLS**

[...]

Entity CAs, RAs, CMSs, directories, remote workstations used to administer the CAs, and certificate status servers shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

[...]

### **7.1.2 Certificate Extensions**

For all CAs, use of standard certificate extensions shall comply with [RFC 3280].

Certificates issued by the FBCA shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Certificates issued by Federal Entity CAs operating at High, Medium Hardware, and/or Medium Assurance shall comply with [FPKI-Prof].

Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile].

<p><u>Practice Note: For Entity CAs that issue PIV-I certificates, the associated CSS certificates will also comply with [PIV-I Profile].</u></p>
---

### 7.1.3 Algorithm Object Identifiers

[...]

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

[...]

ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

For PIV-I, signature algorithms are limited to those identified by NIST SP 800-78.

## 8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The FBCA, Entity Principal CAs, CMSs, and RAs and their subordinate CAs, CMSs, and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, PIV-I Card Authentication, and Medium Assurance, and at least once every two years for Basic Assurance. [...]

### 9.4.3 Information not deemed Private

Information included in FBCA certificates is not subject to protections outlined in Section 9.4.2.

For Entity CAs, certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).

### 9.6.1 CA Representations and Warranties

[...]

A non-federal entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of a non-federal entity's certificate policy by the Federal PKI Policy Authority is not a substitute for due care and mapping of certificate policies by the non-federal entity.

For PIV-I, Entity CAs shall maintain an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

### **9.6.5 Representations and Warranties of Affiliated Organizations [NEW SECTION]**

Affiliated Organizations shall authorize the affiliation of subscribers with the organization, and shall inform the Entity CA of any severance of affiliation with any current subscriber.

## 10. BIBLIOGRAPHY

[...]

- FIPS 186-2      Digital Signature Standard, January 27, 2000.  
<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>
- FIPS 201      Personal Identity Verification (PIV) of Federal Employees and Contractors  
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
- FOIACT        5 U.S.C. 552, Freedom of Information Act.

[Http://www4.law.cornell.edu/uscode/5/552.html](http://www4.law.cornell.edu/uscode/5/552.html)

[...]

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NIST SP Interfaces for Personal Identity Verification (4 Parts)

800-73 <http://csrc.nist.gov/publications/PubsSPs.html>

NIST SP Biometric Data Specification for Personal Identity Verification

800-76 [http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1\\_012407.pdf](http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf)

NIST SP Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)

800-78

<http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf>

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.

[http://snyside.sunnyside.com/cpsr/privacy/computer\\_security/nsd\\_42.txt](http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt)  
(redacted version)

[...]

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PIV-I Profile X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link:

[http://www.idmanagement.gov/fpkipa/documents/pivi\\_certificate\\_crl\\_profile.pdf](http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf)

PKCS#12 Personal Information Exchange Syntax Standard, April 1997.

<ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf>

[...]

## 11. ACRONYMS & ABBREVIATIONS

[...]

<u>AID</u>	<u>Application Identifier</u>
CARL	Certificate Authority Revocation List

CMS Card Management System

COMSEC	Communications Security
--------	-------------------------

[...]

GPEA	Government Paperwork Elimination Act of 1998
GSA	<u>General Services Administration</u>
<u>HTTP</u>	<u>HyperText Transfer Protocol</u>
<u>HSM</u>	<u>Hardware Security Module</u>

IETF	Internet Engineering Task Force
------	---------------------------------

[...]

ITU-TSS	International Telecommunications Union – Telecommunications System Sector
---------	---

<u>LDAP</u>	<u>Lightweight Directory Access Protocol</u>
-------------	--

MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity Principal CA)
-----	--

[...]

NSTISSI	National Security Telecommunications and Information Systems Security Instruction
---------	---

<u>OCSP</u>	<u>Online Certificate Status Protocol</u>
-------------	---

OID	Object Identifier
-----	-------------------

PIN	Personal Identification Number
-----	--------------------------------

<u>PIV-I</u>	<u>Personal Identity Verification – Interoperable</u>
--------------	---

PKCS	Public Key Certificate Standard
------	---------------------------------

[...]

U.S.C.	United States Code
--------	--------------------

<u>UPN</u>	<u>User Principal Name</u>
------------	----------------------------

<u>UUID</u>	<u>Universally Unique Identifier (defined by RFC 4122)</u>
-------------	--

WWW	World Wide Web
-----	----------------

[...]

[...]

## 12. GLOSSARY

[...]

Activation Data Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Affiliated Organization Organizations that authorize affiliation with Subscribers of PIV-I certificates

Applicant The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

[...]

## **Appendix A – PIV-Interoperable Smart Card Definition [NEW SECTION]**

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements shall apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2. PIV-I Cards shall conform to [NIST SP 800-73<sup>1</sup>].
3. The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].
5. PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:
  - a. conforms to [PIV-I Profile];
  - b. conforms to [NIST SP 800-73]; and
  - c. is issued under the PIV-I Card Authentication policy.
6. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
9. The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
  - a. Cardholder facial image;
  - b. Cardholder full name;
  - c. Organizational Affiliation, if exists; otherwise the issuer of the card; and
  - d. Card expiration date.

---

<sup>1</sup> Special attention should be paid to UUID requirements for PIV-I.

10. PIV-I Cards shall have an expiration date not to exceed 5 years of issuance.
11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.
12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].
13. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

### **Appendix B – Card Management System Requirements [NEW SECTION]**

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Audit log files shall be generated for all events relating to the security of the CMS shall be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

The CMS shall have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, all certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

**Estimated Cost:**

There is no cost expected for Federal Agencies as the changes create a new policy under which Non-Federal Issuers can issue PIV-I Credentials.

Issuers that do not require Affiliated Organizations to send notification of affiliation status changes may incur costs to implement the practice.

**Implementation Date:**

For PIV-I policies, this change will be effective immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

All other Issuers that do not require Affiliated Organizations to send notification of affiliation status changes have one year to implement the practice.

**Prerequisites for Adoption:**

There are no prerequisites.

**Plan to Meet Prerequisites:**

There are no prerequisites.

**Approval and Coordination Dates:**

Date presented to CPWG: April 1 and 20, 2010

Date presented to FPKIPA: May 11, 2010

Date of approval by FPKIPA: May 13, 2010