FBCA Certificate Policy Change Proposal Number: 2015-02

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Align PIV-I Card Life with FIPS 201-2
Date: 24 November 2015

Title: Align PIV-I Card Life with FIPS 201-2

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.27, December 2, 2013

Change Advocate's Contact Information:

Name: Matt King
Organization: CPWG
Telephone number: 410-271-5624
E-mail address: matthew.king@protiviti.com

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: FIPS 201-2 allows 6 year PIV cards to align with two full certificate life cycles. Several PIV-I issuers requested PIV-I be allowed the same flexibility.

Background:

At the time PIV-I was added to the FBCA CP, FIPS 201 had the restriction that the maximum life span of a PIV card was 5 years. PIV-I aligned with this requirement, but added it to the FBCA CP. FIPS 201-2 was modified in section

2.8 PIV Card Issuance Requirements

…

+ The PIV Card shall be valid for no more than six years.

This proposal is to allow the same change with PIV-I cards.

In addition, a requirement to perform annual testing on PIV cards to ensure correct population of the cards was added the Common Policy CP in 2014. This change proposal will add the same annual testing requirement for PIV-I cards.

Specific Proposals

6.2.1 Cryptographic Module Standards & Controls

…

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting policies mapped to PIV-I hardware or PIV-I-cardAuth. PIV-I Cards shall only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

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

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 for certificate signing and six years for CRL signing. CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 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.

Subscriber public keys in certificates that assert the id-fpki-pivi-content-signing OID in the extended key usage extension have a maximum usage period of nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-certpcy-pivi-contentSigning certificate shall be later than the expiration of the id-fpki-certpcy-pivi-hardware and id-fpki-certpcy-pivi-cardAuth certificates

APPENDIX A – PIV-INTEROPERABLE SMART CARD DEFINITION

10. PIV-I Cards shall have an expiration date not to exceed ~~5~~ 6 years of issuance.

Estimated Cost:

There is no cost expected to implement this change.

Implementation Date:

This change will be effective immediately upon approval by the FPKIPA and incorporation into the FBCA Certificate Policy.

Prerequisites for Adoption:

PIV-I issuing CAs may need to modify their Certificate Management System configuration. No PIV-I cards should need to be re-issued to meet this requirement as it is simply extending the maximum lifetime.

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates:

Date presented to CPWG:	3 December 2015
Date presented to FPKIPA:	8 December 2015
Date of approval by FPKIPA:	12 December 2015