FBCA Certificate Policy Change Proposal Number: 2017-04

To:	Federal PKI Policy Authority (FPKIPA)
From:	Chi Hickey, Co-Chair, FPKIPA
Subject:	Proposed modifications to the Federal Bridge Certificate Policy
Date:	April 3, 2017

Title: How Long Can PIV-I Card Stock Be Used Once They Are Removed From the GSA Approved Products List?

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.30, October 5, 2016

Change Advocate's Contact Information: chi.hickey@gsa.gov

Organization requesting change: FPKI Policy Authority

Change summary: Clarifying the period of time PIV-I card stock that has been removed from the GSA Approved Products List can be used.

Background:

The primary objectives of the FIPS 201/FICAM Testing Program are to:

- Provide a common government-wide testing capability for ICAM products and services;
- Provide FIPS 201 compliance, consistency, and alignment of commercially-available products and services with the requirements and functional needs of government ICAM implementers;
- Update and maintain the GSA Approved Products List (APL); once products and services have passed FIPS 201/FICAM conformance testing; they are listed on the APL
- Ensure availability, security, interoperability, and choice among vendor products to support various ICAM components; and
- Coordinate interaction with the ICAM vendor community to improve the inclusion of requirements into product offerings; and services that have been demonstrated to perform successfully.

Standardization of PIV and PIV-I Card issuance greatly contributes to achieving the objectives of interoperability across PIV and PIV-I Card Issuer implementations. For all

organizations to accept the PIV and PIV-I Cards of other organizations, one set of interoperable components must be used across organizations.

This change proposal provides additional guidance to PIV-I issuers about how to deal with card stock that has been removed from the APL.

Specific Changes

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

6.2.1 Cryptographic Module Standards and 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). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA. 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.

Estimated Cost:

There may be a cost associated with this change due to unused card stock no longer authorized for use and the labor for reissuance if required due to critical vulnerability.

Implementation Date:

This change is a clarification and is effective upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates:

Date presented to CPWG: April 3, 2017
Date change released for comment: May 17, 2017
Date comment adjudication published: June 1, 2017