COMMON Certificate Policy Change Proposal Number: 2013-03

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the COMMON Certificate Policy
Date: November 13, 2013

Title: Require PIV Cards to be on the GSA Approved Products List (APL) Prior to Issuance

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.21, December 18, 2012

Change Advocate's Contact Information:
Name: Chi Hickey
Organization: GSA FIPS 201/FICAM Testing Program
Telephone number: (202) 501-1881
E-mail address: chi.hickey@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Require Cards for PIV to be on the GSA Approved Products List

Background:

The GSA FIPS 201/FICAM Testing Program is the central hub for information related to product testing, approved products, and lab certification. It provides a comprehensive evaluation capability to support the selection and procurement of qualified products and services for the implementation of a federated and interoperable ICAM segment architecture.

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.

The FIPS 201/FICAM Testing Program has recently uncovered interoperability issues with components such as cards that were formerly, but no longer listed on the APL. For example, testing highlighted interoperability issues of installed card readers with Type B Cards. This resulted in GSA no longer requiring readers to work with Type B in order to be approved and listed on the APL. Consequently, cards that only support Type B technology are not listed on the APL. In order to maximize interoperability across the FPKI, PIV Card Issuers should only use PIV Cards listed on the APL.

OMB Memos M-05-24 and M-06-18 require the use of products listed on the APL. This change proposal will provide the ability to enforce the requirement as part of the PKI Audit Review.

Specific Changes:

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

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140-2]. Cryptographic modules shall be validated to a FIPS 140 level identified in this section.

In accordance with FIPS 201, the relevant NIST Guideline for PIV Card Issuers (PCI) is NIST SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, which utilizes various aspects of NIST SP 800-37 and applies them to accrediting the reliability of PCIs.

CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

PIV Cards are PKI tokens that have private keys associated with certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth. PIV Cards shall only be issued using card stock that has been tested and approved by the FIPS 201/FICAM Testing 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/FICAM Testing Program), one populated, representative sample PIV Card shall be submitted to the FIPS 201/FICAM Testing Program for testing.

Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the authentication policies (id-fpki-common-authentication or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

CSSes that provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CSSes that do not provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

10. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
APL	Approved Products List (APL) http://www.idmanagement.gov/approved-products-list-apl
NIST Special Publication 800-79	http://csrc.nist.gov/publications/PubsSPs.html

11. ACRONYMS & ABBREVIATIONS

CMS	Card Management System
PCI	PIV Card Issuer

Delta Mapping: Not applicable

Estimated Cost: There should not be a cost associated with this change as PIV issuers should already be using the APL.

Implementation Date: This change is a clarification and is effective upon approval by the FPKIPA and incorporation into the Common Policy CP.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	November 19, 2013; December 5, 2013
Date presented to FPKIPA:	March 11, 2014
Date of approval by FPKIPA:	March 18, 2014