



FBCA CP Change Proposal Number: 2011-03

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA Certificate Policy
Date: January 18, 2011

Title: Change to the FBCA CP to clarify key generation location for PIV-I Key Management certificates

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.22, January 24, 2011.

Change Advocate's Contact Information:

Name: Deb Gallagher
Organization: GSA
Telephone number: 202-604-5733
E-mail address: deborah.gallagher@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This change proposal corrects an inconsistency in the FBCA CP relating to the generation of PIV-I Key Management certificate keys.

Background:

PIV-I Card testing found a difference in the policy requirements for the Key Management certificate on a PIV-I card versus the Key Management certificate on a PIV card. Further investigation revealed a technical inconsistency with the requirements for the Key Management certificate key generation in the FBCA CP.

NIST SP 800-73, section **3.2.4, X.509 Certificate for Key Management** states:

The X.509 Certificate for Key Management and its associated private key, as defined in FIPS 201, support the use of encryption for the purpose of confidentiality. This key pair may be escrowed by the issuer for key recovery purposes.

However in the FBCA CP, Section 6.1.1.2, ***Subscriber Key Pair Generation*** states:
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.

The PIV-I certificate profile requires all PIV-I Key Management certificates to include a PIV-I Hardware certificate policy. This would preclude the ability for the CA to generate encryption keys on behalf of the subscriber enabling the CA to escrow the Key Management certificate's private key.

Specific Changes:

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

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS approved method or equivalent international standard.

For PIV-I Hardware certificates, to be used for digital signatures and/or authentication, and PIV-I Card Authentication certificates, subscriber key generation shall be performed on hardware tokens that meet the requirements of Appendix A. For all other certificates issued aAt 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.~~

6.2.3.4 Escrow of Subscriber private encryption and dual use keys

Subscriber private dual use keys shall not be escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1.

~~No stipulation with respect to escrow of subscriber private encryption keys.~~

Estimated Cost:

There is no cost expected for Federal Agencies. This change would allow PIV-I issuers to provide escrow services for PIV-I Key Management certificates. Each PIV-I issuer would need to weigh the estimated cost of being able to provide this service.

Risk/Impact:

There is no risk associated with making this change. The risk of not making the change means PIV-I issuers may not be able to escrow and recover Key Management keys leading to the potential risk of subscribers' inability to decrypt essential information.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

Not Applicable.

Approval and Coordination Dates:

Date presented to CPWG: January 18, 2011

Date presented to FPKIPA: January 20, 2011

Date of approval by FPKIPA: January 28, 2011