FBCA Certificate Policy Change Proposal Number: <2016-01>

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 16 December 2015

Title: Subscriber Private Key Protection for Multiple Keys or Key Holders

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: Scott Rea
Organization: CPWG
Telephone number: 801-701-9636
E-mail address: Scott.Rea@DigiCert.com

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Adding guidance for protection of Medium assurance private keys when multiple keys are co-located or when stored on behalf of others (e.g. some implementations of Group certificates or subscriber keys stored "in the cloud").

Background:

FBCA CP 6.2.1 Cryptographic Modules

The following are the rated FIPS140 crypto modules required for FBCA Medium Assurance:

- CA/CMS/CSS = Level2 Hardware;
- Subscriber = Level1;
- RA = Level2 Hardware

A question arises in respect to Group certs, and specifically, where a single entity holds a collection of Group certs.

Under the current FBCA policy, a Medium level certificate only has to be protected at FIPS140 L1 by the Subscriber, however any other trusted role in the PKI that uses/requires a Medium credential is required to have FIPS140 L2 Hardware to protect the private key – this potentially seems like a gap in trust assurance. Under the CA/CMS/CSS/RA situations, there is a proscribed higher requirement for key protections, presumably because there is greater risk due to the ability to affect multiple credentials under those scenarios. Therefore, when a Custodial subscriber key store (where a single entity holds a collection of keys for subscriber certificates) is implemented, there is a higher risk associated with compromise and the crypto module requirement should be commensurate with the level of risk. This change proposal provides additional guidance to increase the protection of private keys in Custodial Subscriber Key Stores.

Specific Proposals

Add New Section 6.2.1.1:

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber. Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware. In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

Glossary

Custodial Subscriber Key Stores	Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.

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 after the full review currently underway.

Prerequisites for Adoption:

CAs will need to update their CPS and Subscriber Agreements to require Subscribers who utilize a Custodial Subscriber Key Store to utilize FIPS140 L2 or greater cryptographic modules and appropriate authentication to those devices.

Plan to Meet Prerequisites:

N/A.

Approval and Coordination Dates: *<These dates will be inserted by the CPWG>*

Date presented to CPWG:	3 September 15, 3 December 2015, and 7 January 2016, 4 February 2016, 15 March 2016
Date presented to FPKIPA:	12 April 2016, 10 May 2016
Date of approval by FPKIPA:	<TBD by the CPWG>