FBCA Certificate Policy Change Proposal Number: 2013-01

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 8/13/2013

Title: FBCA CP Clarifications recommended to the FPKIMA during the Annual PKI Compliance Audit

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.26, April 26, 2013

Change Advocate's Contact Information:

Name: Darlene Gore
Organization: FPKIMA
Telephone number: 703-306-6109
E-mail address: darlene.gore@gsa.gov

Organization requesting change: FPKIMA

Change summary: Clarify places in the FBCA CP which were flagged during the FPKIMA Annual Audit as either contradictory with the Common Policy CP or contradictory to current best practices.

- Allow modification of cross-certificates for corrections, 4.8.1
- Clarify division of responsibilities between trusted roles, 5.2.1

Background: During the last annual PKI Compliance Audit for the FPKIMA, the auditor made a few recommendations to make the FPKI Certificate Policies followed by the FPKIMA more consistent with each other He also pointed out a few places in the CPS that contradict the language in the FBCA CP but the CPS meets the intent of the CP and follow commercial best practices. It was recommended that the FPKIMA propose changes to the FBCA CP.

1) Under section 4.8.1 Circumstances for Certificate Modification, the FBCA CP states: "For the FBCA, certificate modification is performed if the Entity CA changes its name." The CP does not state that this is the only modification that is allowed and the FPKI CPS also allows the Entity POC to request a modified cross-certificate if there is a need to correct extension information. Examples for

this type of modification include, the addition of new certificate policies, a change to the name constraints, or other included extensions.

2) Section 5.2.1 defines four Trusted Roles and divides the responsibilities for operation of the PKI among them. However, the specific language used is contradictory to the terms used by some commercial CA products which can result in a PKI either having to define additional roles or violate the language. For example, for some CA products configuring a certificate profile or template is the same as issuing a certificate, but configuring certificate profiles is a responsibility listed as belonging to an Administrator even though there is another line that says Administrators do not issue certificates. The intent of this section is to ensure the operation of the CA is divided across more than one role, to ensure any malicious activity would require collusion. As long as this intent is met, and multi-party control is maintained for those specific activities that require multi-party control, i.e. CA key generation, CA signing key activation, and CA private key backup, a PKI should be allowed to divide operational functions by Trusted Role in the manner that best fits the terminology and the CA product in use.

Specific Changes:

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

4.8.1 Circumstance for Certificate Modification

~~For the FBCA, certificate modification is performed if the Entity CA changes its name.~~
The FBCA may modify a CA certificate whose characteristics have changed (e.g. assert new policy OID, CA name change). The new certificate may have the same or a different subject public key.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Entity CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain ~~user~~system accounts; configure ~~profiles and~~ audit parameters; and generate component keys.

2. *Officer* – authorized to request or approve ~~certificates or~~ certificate issuance and revocations.

3. *Auditor* – authorized to review, maintain, and archive audit logs.

4. *Operator* – authorized to perform system backup and recovery.

Administrators do not issue certificates to subscribers.

~~Some roles may be combined.~~ The roles required for each level of assurance are identified in Section 5.2.4. Separation of duties shall comply with 5.2.4, and requirements for two person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

~~The following subsections provide a detailed description of the responsibilities for each role.~~

~~*5.2.1.1 Administrator*~~

~~The administrator role is responsible for:~~
~~Installation, configuration, and maintenance of the CA;~~

~~Establishing and maintaining CA system accounts;~~

~~Configuring certificate profiles or templates and audit parameters, and;~~

~~Generating and backing up CA keys.~~

~~Administrators do not issue certificates to subscribers.~~

~~*5.2.1.2 Officer*~~

~~The officer role is responsible for issuing certificates, that is:~~
~~Registering new subscribers and requesting the issuance of certificates;~~

~~Verifying the identity of subscribers and accuracy of information included in certificates;~~

~~Approving and executing the issuance of certificates, and;~~

~~Requesting, approving and executing the revocation of certificates.~~

~~*5.2.1.3 Auditor*~~

~~The auditor role is responsible for:~~
~~Reviewing, maintaining, and archiving audit logs;~~

~~Performing or overseeing internal compliance audits to ensure that the FBCA or Entity CA is operating in accordance with its CPS;~~

~~*5.2.1.4 Operator*~~

~~The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media~~.

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance.

Two or more persons are required for CAs operating at the Medium (all policies), ~~Medium Hardware,~~ or High Levels of Assurance for the following tasks:

- CA key generation;

- CA signing key activation;
- CA private key backup.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.

Delta Mapping:

Table 5.1 Identification and Duties of Trusted Roles will need to be modified with the final wording of this change.

Estimated Cost:

There is no cost expected to implement this change. The proposed changes clarify language in the FBCA CP and bring it into alignment with current FPKIMA operational practice.

Implementation Date:

This change will be effective immediately upon approval by the FPKIPA and incorporation into 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:	6/6/2013
Date presented to FPKIPA:	8/13/2013
Date of approval by FPKIPA:	8/13/2013