Common Policy 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 Common Policy Certificate Policy
Date: 8/13/13

Title: Common Policy 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 U.S. Federal Common Policy Framework (FCPCA) Version 1.21, December 18, 2012

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 Common Policy CP which were flagged during the FPKIMA Annual Audit as either contradictory with the FBCA CP or contradictory to current best practices.

- Clarify division of responsibilities between trusted roles, 5.2.1

- Clarify meaning of "all Security Audit logs, 5.4.1

- Allow audit logs to be removed from production site once reviewed, 5.4.3

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 Common Policy CP.

1) 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.

2) Section 5.4.1 "All security auditing capabilities of the CA operating system and CA applications required by this CP shall be enabled during installation." Enabling ALL security auditing capabilities of the CA operating system could have significant performance impact. For example if Audit object access is enabled for all access of every object the log could grow exponentially as log entries are written for every permissible access for every object touched. If this language was changed to agree with the FBCA CP that only the security auditing capabilities required by the CP must be enabled, this could be limited to auditing access to objects related to the CA.

3) Section 5.4.3 requires audit logs remain on site for at least two months. The FBCA CP allows audit logs to be removed after they have been reviewed, if the review takes place more frequently than every two months.

Specific Changes:

Insertions are <u>underlined</u>, deletions are in ~~strikethrough~~:

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 will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. 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 primary trusted roles defined in this policy are Administrator, Officer, Auditor, and Operator. Individual personnel shall be specifically designated to the four roles defined below.~~

<u>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.)</u>

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

2. *Officer* – authorized to request or approve 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.

The roles required for each level of assurance are identified in Section 5.2.4. These four roles are employed at the CA, RA, and CSS locations as appropriate. 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.

5.2.1.1 Administrator
The administrator role shall be responsible for:
- Installation, configuration, and maintenance of the CA and CSS (where applicable);
- Establishing and maintaining CA and CSS system accounts;
- Configuring certificate profiles or templates;
- Configuring CA, RA, and CSS audit parameters;
- Configuring CSS response profiles; and
- Generating and backing up CA and CSS keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer
The officer role shall be 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 shall be responsible for:
- Reviewing, maintaining, and archiving audit logs; and

- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and CSS (where applicable) are operating in accordance with its CPS.

5.2.1.4 Operator

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

5.4.1 Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications <u>required by this CP</u> shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

5.4.3. Retention Period for Audit Log

Audit logs shall be retained on-site ~~for at least 2 months~~ <u>until reviewed,</u> in addition to being archived as described in section 5.5. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

Estimated Cost:

There is no cost expected to implement this change. The proposed changes clarify language in the Common Policy 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 Common Policy 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: 8/13/13
Date of approval by FPKIPA: 8/13/13