COMMON Certificate Policy Change Proposal Number: 2012-04

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modification to the COMMON Certificate Policy
Date: August 14, 2012

Title: Operate Common Policy CA Offline

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.19 June 22, 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: Detail and clarify the Common Policy CA's CRL issuance policies to ensure Offline Root CA operations are permitted

Background:

The Federal Common Policy Certification Authority (FCPCA) is the trust anchor for digital certificates for Personal Identity Verification (PIV) credentials and for commercial relying parties that trust federal government credentials. As the trust anchor for the federal government, the FCPCA root certificate is distributed by commercial vendors as a publicly-trusted root certificate.

The past year has seen multiple high profile attacks against trust infrastructures - from the RSA Security hack to the Dutch DigiNotar CA breach. FPKI CA compromise could result in forgery of PIV or PIV-Interoperable (PIV-I) credentials that would allow undetected access by adversaries. Compromise of a root CA cannot be addressed simply by revoking a certificate; the CA's root certificate must be removed from all relying party trust stores. This is a relatively difficult task, with no means to confirm that all relying party trust stores have been covered.

The FCPCA root certificate is distributed to relying party applications throughout the FPKI Community and to the general public via various COTS vendor (e.g., Microsoft,

Adobe, and Apple) applications. In response to the recent attacks commercial venders are introducing additional requirements for CAs to be included in their trust stores.

Mozilla is considering adding the following rule:

> "The root is expected to be offline, the intermediate certificates online."

The CABForum is considering the following:

> "Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks:

Microsoft has added the following rule:

> "All root certificates distributed by the Program must be maintained in an offline state – that is, root certificates may not issue end-entity certificates of any kind, except as explicitly approved from Microsoft."

In addition to complying with commercial vendor requirements, operating the FCPCA offline reduces the opportunities for the FCPCA to be compromised, therefore minimizing the risk of relying party applications needing to remove the FCPCA root certificate from trust stores.

The FPKIMA is planning to move the FCPCA offline due to the security benefits. Although the Common Policy CP does not explicitly state the requirements for FCPCA CRL validity periods or issuance frequencies, this change proposal would explicitly allow the FCPCA to be operated in an offline manner with 31 day CRLs, similar to legacy Federal Root CAs.

Specific Changes:

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

4.9.7. **CRL Issuance Frequency**

…

CAs operating as part of the Shared Service Providers program that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). ~~For l~~Legacy Federal PKI~~s only,~~ root CAs and the Common Policy Root CA that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 31 days, and the *nextUpdate* time in the CRL may be no later than 32 days after issuance time (i.e., the *thisUpdate* time).

Delta Mapping: Not Applicable

Estimated Cost:

The cost is internal to the FPKIMA

Implementation Date:

This change will be implemented within 12-24 months of 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:	June 21, 2012, July 17, 2012, August 2, 2012
Date presented to FPKIPA:	August 14, 2012
Date of approval by FPKIPA:	TBD