Common Policy Change Proposal Number: 2009-01

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the Common Certificate Policy
Date: 5 February 2009

Title: Changes to Federal PKI Common Policy Framework CP to change the requirement for nextUpdate in Certificate Revocation Lists (CRL) published by legacy Federal PKIs.

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 – 1.5, 20 November 2008.

Change Advocates Contact Information:

Name: Morris Hymes
Organization: DoD
Telephone number**:** 410-854-4900
E-mail address**:** mahyme1@missi.ncsc.mil

Organization requesting change: Department of Defense

Change summary: This change proposal changes the requirement for legacy Federal PKIs to ensure legacy PKIs can issue PIV Authentication certificates. It exempts legacy Federal PKIs from the requirement to have *nextUpdate* be no more than 48 hours after thisUpdate in a CRL.

Background: FIPS 201 section 5.4.4 specifically requires legacy PKIs to begin asserting id-fpki-common-authentication in PIV Authentication certificates. Common Policy Change Proposal 2007-03 made a number of changes to allow this to happen but did not change the requirement in paragraph 4.9.7 for *nextUpdate* to be no later than 48 hours after *thisUpdate*.

Many relying party applications treat *nextUpdate* as "expired." In some cases (e.g., Microsoft Certificate Based Login), the application does not have an option to allow certificate revocation checking to be skipped. This can result in a denial of service if, for any reason, a new CRL is not available. Some legacy Federal PKIs are used in environments where the ability of a relying party to access CRLs is intermittent. In addition, operational experience has shown that, in some cases, it has taken longer than 48 hours to recover from a CA failure. In either case, any application that rejects a CRL that has passed "*nextUpdate*" will fail.

Specific Changes: There are two specific changes to Section 4.9.7 listed below. New text is underlined.

Section 4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

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 legacy Federal PKIs only, CAs 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).

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). For legacy Federal PKIs only, the *nextUpdate* time in the CRL may be no later than 180 hours after issuance time (i.e., the *thisUpdate* time).

Practice Note: Since many applications only check for a new CRL at nextUpdate, a longer nextUpdate time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer nextUpdate time also increases the potential of a replay attack to validate a newly revoked certificate. Where the CRL nextUpdate exceeds 48 hours, relying parties should consider these risks and take appropriate measures to mitigate the risk. For high-risk, sensitive Relying Party applications suggested measures include configuring a preference for OCSP by applications, pre-fetching CRLs at least every 18 hours, and use of other compensating controls.

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

Risk Impact:
See Practice Note above. Applications that rely solely on *nextUpdate* may require modification to mitigate the risk of the extended *nextUpdate* time. If available, OCSP should be the preferred method. There will be a period of time between the implementation of this change and the ability for Replying Parties to react. In addition, Relying Parties may not be aware of the change immediately and could be operating at risk. Legacy Federal PKIs implementing this change should make an effort to notify known Relying Parties.

Cost Impact:
There may/will be a financial cost for implementing mitigation of risk factors.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Common Policy Framework CP. This policy will be reviewed annually to determine if *nextUpdate* can be decreased from 180 hours, consistent with operational constraints.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:
Date presented to CPWG: December 16, 2008
Date CPWG recommended approval: February 5, 2009
Date presented to FPKI PA: February 10, 2009
Date of approval by FPKI PA: February 10, 2009