FPKIPA
Federal Public Key Infrastructure Policy Authority

FBCA Certificate Policy Change Proposal Number: 2019-01

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Allow Offline FBCA
Date: February 28, 2019

Title: Allow Offline FBCA

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)
Version 2.34, 4 October 2018

Change Advocate's Contact Information:
Name: India Donald
Organization: FPKI Management Authority
E-mail address: india.donald@gsa.gov

Organization requesting change: FPKIMA

Change summary: Allow the FBCA to be operated in an off-line status.

Background:

When the Federal Bridge CP was originally written, the FBCA risk assessment highlighted the need for the FBCA to issue CRLs at least every 24 hours. Since that time, the operational risks of the FBCA have changed as well as the number of connected affiliates.

- 16 (4 Bridges and 11 NFI) CAs connected to the FBCA. Only 5-8 CA Certificates are issued every year by the FPKIMA.
- 3 of 4 Bridge PKIs are operated off-line.
- 7 of 11 NFI CAs are operated off-line.

This change proposal is to allow the FBCA to issue a 31-day CRL if it is operated in an off-line manner while still allowing it to operate on line with a 24 hour CRL.

In addition, the current CP requires the FBCA to be rekeyed every 3 years with a maximum of 6 years for its key lifetime. Operating the FBCA off-line with longer CRLs minimizes the use of the private key and therefore the risk of key compromise from overuse. Therefore, it was suggested that an off-line FBCA may be allowed a 10-year key lifetime with the ability to use its private key to sign new certificates for 6 years similar to other intermediate CAs in the FPKI.

Specific Changes:

Insertions are underlined, deletions are in strikethrough:

4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request involving an FBCA-issued certificate, the FPKIMA shall authenticate the request and apprise the FPKIPA. The FPKIPA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the FPKIPA shall direct the FPKIMA to revoke the certificate. The FPKIMA shall give prompt oral or electronic notification to the FPKIPA co-chairs and all previously designated officials in all entities having a Principal CA with which the FBCA interoperates.

If a revocation is due to a certificate or systems compromise or an Entity Principal CA violation of the Memorandum of Agreement with the FPKIPA, the FPKIMA will notify previously designated officials in all entities having a Principal CA with which the FBCA interoperates.

4.9.7 CRL Issuance Frequency

For this CP, CRL issuance encompasses both CRL generation and publication.

~~For the FBCA, the interval between CRLs shall not exceed 24 hours.~~

For the FBCA and Entity CAs, see the table below for issuing frequency of routine CRLs. CRLs may be issued more frequently than specified below.

Table 4 FBCA and Entity CA CRL Issuance Frequency

Assurance Level	Max Interval for Routine CRL Issuance	
	Online	Offline
Rudimentary	No Stipulation	No Stipulation

Basic	24 Hours	31 Days
Medium (all policies)	24 Hours	31 Days
PIV-I Card Authentication	24 Hours	31 Days
High	24 Hours	31 Days

~~For Entity Principal CAs that are operated in an off-line manner routine CRLs may be issued less frequently than specified above if the CA only issues:~~
CAs may be operated in an offline manner if the CA only issues:

- CA certificates
- (optionally) CSS certificates, and
- (optionally) end user certificates solely for the administration of the principal CA.

However, the interval between routine CRL issuance shall never ~~not~~ exceed 31 days.

6.3.2 Certificate Operational Periods/Key Usage Periods

If operated online, the FBCA shall limit the use of its private keys to a maximum of three years for certificate signing and six years for CRL signing. If the FBCA is operated offline, its private key may be used for a maximum of six years for certificate signing and ten years for CRL signing. CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.

Estimated Cost: There is no estimated cost for this change.

Implementation Date: At the discretion of the FPKIMA.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	February 25, 2019
Date change released for comment:	March 4, 2019
Date approved by FPKIPA:	April 9, 2019