FBCA Certificate Policy Change Proposal Number: 2023-03

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Updates to audit and archive records for trusted role assignment and key/certificate operational periods
Date: June 2023

Title: Appointment of Trusted Roles and updates in Section 6.3.2

X.509 Certificate Policy For The Federal Bridge Certification Authority Version 3.0 October 19, 2022

Change Advocate's Contact Information:
Jimmy Jung | Phone: 703-851-6813
Jimmy.jung@slandala.com
and
India Donald
india.donald@gsa.gov

Organization requesting change: Slandala and FPKIMA

Change summary: Clarify the requirements for the appointment of Trusted Roles, increase Root CA certificate private key and certificate lifetimes, and remove incorrect restriction on private keys associated with cross-certificates

Background:
The current policy requires the appointment of Trusted Roles to be archived, but does not actually require trusted roles to be appointed, except when discussing archive materials. The term "appointment" carries a formal connotation and may not reflect the typical practice of logging the training and authorization of personnel as opposed to a formal documented memo, signed and filed indicating the "appointment."

Additionally, when the table in 6.3.2 was added for Certificate Operational Periods and Key Usage Periods, we were overzealous in specifying validity periods for all certificate types. Issuing a cross certificate to an existing CA does not change the validity period of its private key.

In addition, prior to the FBCA CP v3.0 update, the maximum lifetime for a Root CA certificate was 37 years and there was no maximum certificate period specified for cross-certificates, although 3-years was the usual.

This limitation on the cross-certificate lifetime caused unnecessary issues whenever the FBCA had to perform a rekey, as the cross-certificates with the Federal Common Policy first had to be renewed. Therefore, the current cross-certificates issued between the FCPCAG2 and the FBCAG4 were issued with an expiration date matching that of the FBCAG4, a little over a 9-year validity period.

Provided established cryptoperiods are followed, the increase in the maximum life of the Root CA certificate and private key does not increase risk to the FPKI as cross certificate validity and revocation status can be modified to limit trust in the other root CAs as determined by the FPKIPA.

Specific Changes:

Insertions are underlined, 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 personnel 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. An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

~~Trusted Role appointments must be documented and archived as defined in Section 5.4 and Section 5.5.~~

5.4.1. Types of Events Recorded

…

Auditable Event	Rudimentary	Basic	Medium, PIV-I, High
MISCELLANEOUS			
~~Appointment of an individual to a designated Trusted Role~~ Record of an individual being	X	X	X

added or removed from a trusted role, and who added or removed them from the role			

5.5.1. Types of Events Archived

…

Auditable Event	Rudimentary	All Other Policies
~~Appointment of an individual to a designated Trusted Role~~ Record of an individual being added or removed from a trusted role, and who added or removed them from the role (to include KRA/KRO)	X	X

6.3.2 Certificate Operational Periods and Key Usage Periods

A CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Key	Private Key	Certificate
Root CA certificate (self-signed)	~~20~~ 30 years	~~20~~ 30 years
Federal Bridge CA certificate	10 years	10 years
Intermediate/Signing CA certificate	10 years	10 years
~~Cross Certificate~~	~~3 years~~	~~3 years~~
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
PIV-I Card Authentication	3 years	3 years
PIV-I Content Signing	3 years	9 years*

Code Signing	3 years	8 years
OCSP Responder	3 years	120 days
Device	3 years	3 years

Estimated Cost: None

Implementation Date: Immediately upon CP publication.

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG: April 10, 2023
Date change released for comment: May 19, 2023
Date comment adjudication published: May 26, 2023