COMMON Certificate Policy Change Proposal Number: 2024-03

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Updates in response to 2023 FPKI Compliance Audit
Date: January 9, 2024

Title: Certificate Policy Clarifications

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.6 November 3, 2023

Change Advocate's Contact Information: india.donald@gsa.gov

Organization requesting change: FPKIMA

Change summary: Clarify the language in CP based on 2023 FPKI Annual PKI Compliance Audit

Background:

Prior to the 2.0 rewrite of the Common Policy CP section 1.1.4 Interoperation with CAs Issuing under Different Policies clearly stated that the FPKI relied on the policy mapping with the FBCA to achieve interoperability with PKIs operating under their own CP. When the rewrite to version 2.0 was looking to remove the term "Legacy Federal PKIs" the language was over simplified and lost the language about interoperability relying on the FBCA for policy mapping.

In addition, the requirement in section 4.9, "For CAs operating under this policy, the FPKIPA must be notified at least two weeks prior to the revocation of a CA certificate, whenever possible." appears to contradict the first sentence of 4.9.5 "CAs will revoke certificates as quickly as practical upon receipt of a revocation request."

This change proposal clarifies language in the CP to match current practice.

Specific Changes:

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

1.1.4. Interoperation with CAs Issuing under Different Policies

PKI interoperation with CAs that issue under different policies will be achieved through cross-certification with the Federal Bridge Certification Authority (FBCA). Federal Government agency CAs may ~~perform~~ obtain a cross-certificate from~~ion with~~ either the Federal Common Policy CA or Federal Bridge CA at their discretion. In all cases, the CA's Certificate Policy is mapped with the FBCA CP for comparability and the policy mapping approved by the FPKI Policy Authority.

Interoperability may also be achieved through other means, such as trust lists.

4.9.5. Time within which CA must Process the Revocation Request

CAs will revoke subscriber certificates as quickly as practicable ~~practical~~ upon receipt of an authenticated revocation request. Revocation requests must be processed before the next required CRL issuance as specified in Section 4.9.7, excepting those requests received within two hours of the next required CRL issuance. Revocation requests received within two hours of CRL issuance must be processed before the following CRL is published.

Routine CA certificate revocation must be completed within an agreed time following receipt of an authenticated revocation request. If the revocation is due to a compromise or emergency, the time to revoke must adhere to the requirements of Section 4.9.12.

Estimated Cost: None

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	10/24/2023
Date change released for comment:	10/18/2023
Date comment adjudication published:	11/28/2023