FPKIPA

Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2022-01A

To: Federal PKI Policy Authority (FPKIPA)
From: Federal PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Federal PKI Common Policy Framework Certificate Policy
Date: August 26, 2022

Title: Updates to Archive Retention Period Section of Common Policy

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy for the Federal PKI Common Policy Framework Version 2.2, December 1, 2021*

Change Advocate's Contact Information:
Organization: FPKI Certificate Policy Working Group
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This proposal incorporates changes to Section 5.5.2 of Common Policy based on the input of CPWG. The changes lend specificity to the archive record retention periods, assisting RAs, or other archiving elements, to understand what artifacts need to be archived, and for how long in certain scenarios. The aim of this change is to ensure Certification Authorities (CAs) have appropriate traceability for their certificate issuances.

Specific Changes:
Insertions are underlined; deletions are in ~~strikethrough~~.

5.5.2. Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

CAs will maintain all archived records related to that CA, in an accessible fashion, for 3 years after CA expiration or CA termination.

Individual records associated with certificate request authorization, certificate revocation, subscriber authentication, or subscriber certificate acceptance must be maintained for a minimum of 3 years after the subject certificate expiration date. Issuance of new certificates with extended validity periods (i.e., renewal, rekey or modification) supported by existing subscriber authentication records (i.e., authentication using an existing valid certificate) will result in a new retention period for those initial records, based on the new certificate expiration date.

Practice Note: Archive records can be retained for as long as business purposes require; however, this policy does not waive any organizational policies that may require the destruction of such records or otherwise limits their retention periods.

Practice Note: If the archive records are maintained separately from the CA, communication processes may be required to determine when archive records are no longer needed based on related public certificates.

National Archives and Records Administration General Records Schedules [NARA GRS], 5.6 Item 120, defines required enrollment chain-of-trust records, and archive retention periods related to credentials issued in support of HSPD-12.

~~Otherwise~~ RA system operations audit records ~~to~~ that include any IT resources ~~systems~~ that facilitate RA functions, must maintain relevant archives for a minimum of 3 years after RA system replacement or termination.

Change Impacts:

- RAs will have to review recommended archive retention periods against their current policies and practices; overall the change:
  - may extend the period which RAs may need to maintain records regarding certificate lifecycle operations (request, revocation, suspension, etc.)
  - may not require RAs archive process changes

Estimated Cost: Unknown

Implementation Date: November 1, 2022 (aligns with Common v2.2 implementation date)

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: January 25, 2022, reintroduced May 24, 2022
Date change released for comment: February 18, 2022, resubmitted June 3, 2022
Date comment adjudication published: June 3, 2022