COMMON Certificate Policy Change Proposal Number: 2023-04

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Updates to audit and archive records supporting assignment of trusted roles
Date: June 2023

Title: Appointment of Trusted Roles

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.4 April 7, 2023

Change Advocate's Contact Information:
Jimmy Jung | Phone: 703-851-6813
Jimmy.jung@slandala.com

Organization requesting change: CPWG

Change summary: Clarify the requirements for the appointment of Trusted Roles

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Additionally, an outdated reference to the PIV-I Profiles document is being deprecated in this policy and it will now reference the Common Profiles.

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.

5.4.1. Types of Events Recorded

At a minimum, each audit record must include the following (either recorded automatically or manually for each auditable event):

- What type of event occurred;
- Date and time when the event occurred;
- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure; and
- Identity of any individuals, subjects, or objects/entities associated with the event

…

- MISCELLANEOUS:
    - ~~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

5.5.1. Types of Events Archived

CA archive records must be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data must be recorded for archive:

- Certificate Policy

…

- ~~Appointment of an individual to a Trusted Role (to include KRA/KRO)~~
- Record of an individual being added or removed from a trusted role, and who added or removed them from the role.

6.1.7. Key Usage Purposes

The use of a specific key is constrained by the Key Usage extension in the X.509 certificate.

…

Certificates that assert id-fpki-common-pivi-contentSigning must include a critical Extended Key Usage extension that asserts only id-fpki-pivi-content-signing {2.16.840.1.101.3.8.7} (see [~~PIV-I Profile~~CCP-Prof]).

…

APPENDIX B: REFERENCES

~~PIV-I Profile~~	~~X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-pivi.pdf~~

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