COMMON Certificate Policy Change Proposal Number: 2025-02

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Clarifications on Background Checks, CA terminations, PIN Reset and Auditor roles
Date: April 9, 2025

Title: Clarify Trusted Role Background Reinvestigation Timelines, CA Termination Requirements, Activation Data/PIN Reset Requirements, and auditor role distinctions

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.10 February 14, 2025

Change Advocate's Contact Information: fpki@gsa.gov

Organization requesting change: CPWG

Change summary:

Clarify reinvestigation requirements for trusted roles.

Additionally, clarify requirements and associated processes for CAs planning to terminate operations to better convey FPKI requirements.

Streamline PIN reset requirements by removing information redundant to FIPS 201 and providing the appropriate standards reference.

Finally, clarify the distinction between internal auditor trusted roles and external independent auditors throughout the policy.

Background:

The FPKIPA support team received comments regarding inconsistencies between the Common CP and the FBCA CP as it relates to requirements for periodic reinvestigations for trusted roles. Specifically, the minimum requirement of a 10 year periodic reinvestigation is necessary for FBCA trusted roles, but Common is silent on any similar requirements. Although many federal employee trusted roles may be subject to security eligibility and associated personnel security

continuous evaluation, commercial SSP trusted roles currently have no defined minimum reinvestigation requirements. This proposal seeks to provide parity on that minimum reinvestigation requirement, and it updates colloquial personnel security terminology to be more accurate and consistent with current times and aligns with the current Standard Form (SF) 85.

Given recent SSP decommissionings, current policy requirements surrounding CA termination in Section 5.8 have been found to require additional organization for clarity and updates to account for preferred termination practices while also removing policy requirements surrounding CA signing key transfers upon complete PKI service termination. This section is being modified and expanded to define standard CA decommissioning requirements, expected processes and termination artifacts, for both individual CA cessation of operations and full PKI service terminations.

Additionally, FBCA requirements on activation data generation (specifically hardware token PIN reset) are not accounted for in Common policy for the appropriate credential types (e.g., PIV, common PIV-I, common-high). This proposal seeks to incorporate requirements for PIN resets by way of referencing the appropriate section in FIPS 201 provided issuers offer PIN reset capabilities.

Finally, some aspects of policy leverage duplicative terminology for internal trusted role auditors and third party assessors used for annual FPKIPA reviews. This change seeks to deconflict that terminology overlap to reduce potential confusion of these distinct auditor roles.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~, and moves to a location are **bolded red** (where they are moved from are ~~**bolded red strikethrough**~~**.**

5.3.2. Background Check Procedures

Trusted Roles must receive a favorable adjudication after undergoing a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence, and
- Law Enforcement~~, and~~
- ~~References~~

The period of initial investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified.

Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968], or equivalent.

For Federal employees and cleared contractors:

- a national security eligibility (i.e., Confidential or above) is granted after positive adjudication of a Tier 3 or Tier 5 investigation,
- a suitability determination is granted after positive adjudication of a Tier 2 or Tier 4 investigation, and
- a PIV credential eligibility is granted after a positive adjudication of a Tier 1 investigation.

An active national security eligibility, suitability determination, or PIV credential eligibility fulfills the background check procedure requirements and continued maintenance of those determinations fulfills any reinvestigation requirements.

In all cases, the reinvestigation period for a Trusted Role background check must not exceed 10 years. If a Trusted Role's national security eligibility, suitability determination, or PIV eligibility is ever suspended or revoked during their appointment, all CA accesses must be revoked until the security eligibility, suitability determination, or PIV eligibility is reinstated or a separate investigation is completed and adjudicated.

Practice Note: For Federal organizations, continuous evaluation (CE) processes, where utilized, replace the need for periodic reinvestigations. Currently, CE is in use for national security eligibility recipients, and are planned for inclusion of the other determination types.

5.8. CA OR RA TERMINATION

~~Whenever possible, the FPKIPA must be notified at least two weeks prior to the termination of a CA operating under this policy. For emergency termination, CAs must follow the notification procedures in Section 5.7.~~

~~When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys must be surrendered to the FPKIPA. This Section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).~~

~~Any issued certificates that have not expired, must be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates must be generated. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be destroyed or taken offline, designated as "not in use", and protected as stipulated in Section 5.1.2.1.~~

~~Prior to CA/KRS termination, the CA/KRS must provide archived data to an archive facility as specified in the CPS/KRPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.~~

A CA cessation of operation is when a PKI service provider makes the determination that a specific active CA or set of CAs will no longer be required to be in operation; however, the PKI service maintains their relationship to the FPKI. There can be several reasons for a CA cessation of operation, such as replacement by another CA, migration to newer technologies, or organizational restructuring.

A PKI termination is when an organization that operates a CA or a series of CAs within the scope of this policy wishes to completely discontinue their PKI services and terminate their agreement(s) with the FPKI. This requires that all operational CAs within their PKI service offering be terminated.

Practice Note: Emergency CA certificate revocations following an incident are distinct from CA termination actions. See Section 5.7 for incident response procedures.

When an organizational RA function operating under this policy terminates operations, the RA must archive all audit logs and other records prior to termination and destroy its private keys ~~upon termination~~ as specified in the CPS/RPS.

5.8.1. CA Cessation of Operation

The FPKIPA must be notified at least two weeks before a CA that is operating under this policy ceases operations.

When a CA ceases operations prior to the expiration of all of its issued certificates, the PKI must:

- inform all impacted customers of the CAs cessation of operations, using a communication method specified in the CPS,
- generate and publish a final CRL,
- ensure the final CRL is available, via established public repository URLs, for all relying parties until the validity period of all issued certificates has passed, and
- migrate CA records to an archive or government customer, as specified in the CPS.

The final long-term CRL must:

- include serial numbers of all unexpired subscriber certificates, and
- assert a nextUpdate time beyond the validity period of all issued certificates

Once the final CRL has been issued, the private signing key of the impacted CA(s) must be destroyed or taken offline and protected as stipulated in Section 5.1.2.1.

5.8.2. PKI Termination

The FPKIPA must be notified at least ninety (90) days before any organization terminates their operations, unless otherwise specified in their FPKIPA Memorandum of Agreement (MOA). The PKI Provider must coordinate with the FPKIPA to document the responsibilities of each party and a timeline of events associated with the PKI termination.

When a PKI is terminating, the FPKIPA co-chairs will:

- Inform FPKIPA members of the intent of a PKI to terminate, either in written email communications or during standard monthly meetings, and provide status updates as needed,
- Update the FPKI notifications posted to FPKIPA public repositories with the intent to revoke the impacted CA(s) and provide a tentative timeline in the description of the notice for relying party situational awareness,
- Draft an MOA with the PKI service provider to document responsibilities and a timeline of events.

When a PKI is terminating they must:

- advise all customer organizations of its termination using a communication method specified in the CPS,

- coordinate with the FPKIPA to finalize the stipulations in the termination MOA and execute the agreement,
- generate and publish final CRL(s) by the dates stipulated in the MOA,
- ensure final CRL(s) are available, via established public repository URLs, for all relying parties until the date for CRL maintenance defined in the MOA has passed, and
- migrate CA records to an archive or government customer as specified in the CPS or the established MOA.

The final long-term CRL(s) must:

- include serial numbers of all unexpired subscriber certificates, and
- assert a nextUpdate time beyond the validity period of all issued certificates

Once the final CRL(s) have been issued, the private signing key(s) of the terminating CA(s) must be destroyed or taken offline and protected as stipulated in Section 5.1.2.1.

PKIs using a phased termination, where they plan to operate in "maintenance mode," must continue to conform with all relevant aspects of this policy (e.g., audit logging and archives) until full termination. "Maintenance mode" CAs have ceased issuing new certificates while continuing to actively maintain revocation related operations. In these scenarios, the scope of their annual reviews may be reduced via their FPKIPA MOA.

6.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple ~~parties~~ trusted roles holding that activation data). The strength of the CA activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 3 in [FIPS 140], see Section 6.2.1. **~~If the activation data must be transmitted, it must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.~~**

RA and Subscriber activation data may be user-selected. The strength of the RA activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140], see Section 6.2.1. The strength of Subscriber activation data must meet or exceed the requirements for authentication mechanisms stipulated in [FIPS 140] for the associated cryptographic module level listed in Section 6.2.1. **~~If the activation data must be transmitted, it must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.~~**

For all PIV, common-PIV-I, and common-high credentials, in the event activation data can be reset by an issuer after the card is locked, authentication of the subscriber is required. This authentication must be conducted in accordance with FIPS 201, Section 2.9.3.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

- memorized;
- biometric in nature;
- contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates, or
- physically recorded and secured at the level of assurance associated with the activation of the cryptographic module, and stored separately from the cryptographic module.

Practice Note: For [FIPS 140] Level 2 and higher modules, the protection mechanism should include an ability to temporarily lock the account or terminate the application, after a predetermined number of failed login attempts to protect against repeated guessing attacks.

Activation data that is **transmitted, must be** transmitted **via an appropriately protected channel, and** be **distinct in time and place from the associated cryptographic module.**

1.3.8. Other Participants

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as external independent compliance auditors.

Participating agencies that do not operate a PKI directly must identify one or more Agency Points of Contact (POC) as liaisons to the issuing PKI and the FPKIPA.

1.5.4. CPS Approval Procedures

CAs issuing under this CP are required to meet all requirements. The FPKIPA will not issue waivers.

The FPKIPA makes the determination that a CPS complies with this policy. The CA and RA must operate under an approved CPS. RA practices are documented in the CPS or an associated Registration Practices Statement (RPS). In each case, the determination process must include an external independent ~~compliance~~ auditor's results and recommendations. See Section 8 for further details.

5.3.5. Job Rotation Frequency and Sequence

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor trusted role must not audit their own work from a previous role.

5.4.8. Vulnerability Assessments

…

Practice Note: The audit data should be reviewed by the auditor trusted role for events such as repeated failed actions, requests for privileged information, attempted access of system files, requests for escrowed keys, attempted access of escrowed keys, unauthenticated responses, and other suspicious or unusual activity. Auditors trusted roles should check for continuity of the audit data.

5.5.3. Protection of Archive

Only Auditor trusted roles, as described in Section 5.2, or other personnel specifically authorized by the CA are permitted to add or delete records from the archive. Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The contents of the archive must not be released except in accordance with Sections 9.3 and 9.4, or under circumstances described in the approved CPS.

…

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The external independent auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. The external independent ~~compliance~~ auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the external independent auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The ~~compliance~~ external independent auditor either must be a private firm that is independent from the entities (CA and RAs) being audited, or it must be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an agency inspector general. To ensure independence and objectivity, the ~~compliance~~ external independent auditor may not have served the entity in developing or maintaining the entity's CA facility or Certification Practices Statement. The FPKIPA may determine whether a ~~compliance~~ external independent auditor meets this requirement.

Each agency is responsible for identifying and engaging a qualified ~~compliance~~ external independent auditor ~~of agency operations implementing aspects of this CP~~.

8.4. TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit must be to verify that a CA and its RAs comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation must be subject to compliance ~~audit~~ inspections. Components other than CAs may be audited fully or by using a representative sample.

If the ~~compliance~~ external independent auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the ~~compliance~~ external independent auditor or FIPS 201 Evaluation Program testing finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions must be performed:

- The discrepancy must be documented;
- The responsible party must be notified; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate agency.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The FPKIPA will develop procedures for making and implementing such determinations. A compliance audit, or FIPS 201 Evaluation Program testing, may be required to confirm the implementation and effectiveness of the remedy.

8.6. COMMUNICATION OF RESULTS

On an annual basis, CAs operating under this policy must submit an annual review package to the FPKIPA. This package must be prepared by the CA's PMA, in accordance with the FPKI Annual Review Requirements document. The package must include an assertion that all PKI components have been audited including any components that may be separately managed and operated. The report must identify the versions of this CP and the CPS used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

Each agency must provide a~~n Auditor~~ Letter of Compliance signed by the external independent auditor for those PKI components that it operates to its issuing CA or directly to the FPKIPA.

Estimated Cost: No additional direct costs are expected to be incurred by any other parties as a result of this change proposal.

Implementation Date: November 1, 2025

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	January 28, 2025
Date change released for comment:	December 27, 2024
Date comment adjudication published:	March 14, 2025