FBCA Certificate Policy Change Proposal Number: 2025-03

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

Title: Clarify Background Checks, Activation Data/PIN Reset Requirements and Auditor and Assessor responsibilities

X.509 Certificate Policy For The Federal Bridge Certification Authority Version 3.6 October 25, 2024

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

Organization requesting change: CPWG

Change summary:

Clarify reinvestigation requirements for trusted roles in alignment with a corresponding change to Common.

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

Additionally, clarify the distinction between internal auditor trusted roles and third party or external independent auditors.

Background:

The FBCA CP defined a minimum reinvestigation requirement of 10 years; however, Common policy was silent on this requirement. This change aligns with proposed updates to the Common CP by clarifying the different personnel security determinations for federal employees and cleared contractors and provides reciprocity for meeting FPKI background check procedures and revinvestigations based on those determinations.

The FPKIPA support team received comments regarding activation data generation (specifically hardware token PIN reset) are defined for PIV-I, but may not appropriately reference available reset prerequisites defined in FIPS 201. This proposal seeks to incorporate requirements for PIN

resets by way of referencing the appropriate section in FIPS 201 while reducing direct definition of available options for biometric matching.

Additionally, 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

FPKIMA personnel acting in trusted roles must, at a minimum, undergo procedures necessary to be cleared at the TOP SECRET level.

CA personnel 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.

~~If a formal clearance is the basis for background check, the background refresh must be in accordance with the corresponding formal clearance. Otherwise, the background check must be refreshed every ten years.~~

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 Agencies: A successfully adjudicated Tier 1 investigation (such as a National Agency Check with Written Inquires (NACI)) or National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the minimum standards~~

~~specified above.~~

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.

6.4.1 Activation Data Generation and Installation

The activation data used to unlock CA or subscriber private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected, 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.**~~ Where the CA uses passwords as activation data for the CA signing key, at a minimum the activation data must be changed upon CA re-key or upon appointment of new administrator or operator trusted roles.

For Medium Assurance and above, RA and Subscriber activation data may be user-selected. The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 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.**~~

For PIV-I and highAssurance credentials, in the event activation data ~~must~~ can be reset by an issuer after a card is locked, ~~a successful biometric 1:1 match~~ authentication of the ~~applicant~~ subscriber ~~against the biometrics collected in Section 3.2.3.1~~ is required. This ~~biometric 1:1 match~~ authentication must be conducted ~~by an RA, self-service portal that authenticates the user via the biometric, a trusted agent of the issuer~~ 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.**

1.3.11. Other Participants

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

1.5.3. Person Determining CPS Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The FPKIPA is responsible for asserting whether the FBCA CPS conforms to this CP. Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).

In each case, the determination of suitability must be based on 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 is optional. Any job rotation frequency and sequencing procedures must provide for continuity and integrity of the CA services.

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 ~~security~~ 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. Auditor~~s~~ 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,.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The external independent auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the CA ~~compliance~~ external independent auditor must be thoroughly familiar with the requirements which the applicable CP imposes on the issuance and

management of their certificates. The ~~compliance~~ external independent auditor must perform such compliance audits as a regular ongoing business activity.

For the FBCA, in addition to the previous requirements, the external independent auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The FPKIMA must identify the ~~compliance~~ external independent auditor for the FBCA.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The ~~compliance~~ external independent auditor either must be a private firm, that is independent from the entity being audited, or it must be sufficiently organizationally separated from that entity 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 an ~~compliance~~ external independent auditor meets this requirement

8.4. TOPICS COVERED BY ASSESSMENT

The purpose of an external independent compliance audit of a PKI must be to verify that ~~it~~ a CA and its RAs ~~is~~ are operating in accordance with a CPS that meets the requirements of the applicable CP, as well as any MOAs between the PKI and any other PKI. Components other than CAs may be audited fully or by using a representative sample.

If the 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.

A full compliance audit for the PKI covers all aspects within the scope identified above.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the ~~compliance~~ external independent auditor finds a discrepancy between how the FBCA is designed or is being operated or maintained, and the requirements of this CP, the MOAs, or the applicable CPS, the following actions must be performed:

- The ~~compliance~~ external independent auditor must document the discrepancy and provide a copy to the FPKIMA;
- The FPKIMA will provide a copy of the discrepancy documentation to the FPKIPA Chair;
- The FPKIMA will report findings and corrective action to the FPKIPA;
- The FPKIMA must determine what further notifications or actions are necessary to meet the requirements of this CP and the MOAs, and then proceed to make such notifications and take such actions without delay.

- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may direct the FPKIMA to take additional actions as appropriate, including temporarily halting operation of the FBCA.

When the Entity ~~compliance~~ external independent auditor finds a discrepancy between how the Entity CA is designed or is being operated or maintained, and the requirements of the Entity CP, any applicable MOAs, or the applicable CPS, the following actions must be performed:

- The ~~compliance~~ external independent auditor must document the discrepancy;
- The ~~compliance~~ external independent auditor must notify the responsible party promptly;
- The Entity PKI must determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MOA provisions. The Entity PKI must proceed to make such notifications and take such actions without delay.

When the FPKIPA receives a report of audit deficiency from an Entity PKI, the FPKIPA may direct the FPKIMA to take additional actions to protect the level of trust in the infrastructure.

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

Implementation Date: Immediate upon publication

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 31, 2024
Date comment adjudication published:	March 14, 2025