COMMON Certificate Policy Change Proposal Number: 2021-02

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: September 28, 2021

Title: Updates to Audit and Archive Sections 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 2.1, May 18, 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 suggested changes to Sections 5.4 and 5.5 of Common Policy and other related references based on the input of the Audit and Archive Work Team that operated at the request of the CPWG. The Audit and Archive Work Team's proposed changes are aimed at clarifying the purpose of audit and archival records to support the security of CAs and RAs, and the reduction of operational burden where feasible. Additionally, minor administrative updates to the links in the references section were made to fix broken links due to idmanagement.gov platform migration.

Specific Changes: Due to format changes and the number of edits, updates are highlighted for CPWG and FPKIPA members in a redlined version of Common Policy Section extracts that follow this cover sheet.

Change Impacts:

- Audit logs must now be reviewed by the auditor every month as opposed to the former two month review period for all certificates of lower assurance than common-high, potentially increasing costs associated with internal auditors
- CAs are no longer required to archive all CRLs ever produced, potentially decreasing information storage burdens
- Updated archive retention periods and clarified the start of the archive period:

    - may extend the period which CAs currently archive some of their records, but may decrease others, depending upon the archival mechanism
    - may extend the period which RAs may need to maintain records regarding certificate lifecycle operations (request, revocation, suspension, etc.)
- Updated specifics for the protection of archived records now allows the flexibility to transfer records to new formats and storage media as long as integrity is verified, this may allow for the retirement of legacy hardware and software which could save departments or agencies from financial burden

Estimated Cost: Unknown

Implementation Date: November 1, 2022

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: August 4, 2021
Date change released for comment: September 1, 2021
Date comment adjudication published: September 28, 2021

5.4. AUDIT LOGGING PROCEDURES

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

~~Audit log files must be generated for all events relating to the security of the CA.~~ Audit records, must be generated for all events identified in Section 5.4.1 of this policy, and must be available during audit reviews and third-party audits. For CAs operated in a virtual machine environment, audit records must be generated for both the Virtual Machine ("VM")[1] and hypervisor. Where possible, the audit records must be automatically collected. Where this is not possible, a logbook, paper form, other physical or electronic mechanism must be used.

Audit record reviews should be performed using an automated process, and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities. Implementation and documentation of automated tools must meet the requirements of the CP such that relevant events and anomalies are identified. ~~For CAs, KEDs, and DDSs operated in a virtual machine environment (VME)[2], audit logs must be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e., hypervisor).~~

~~Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits.~~ Reviews may be performed manually for physical or non-electronic records and logs, or when the audit log is small enough to allow for a thorough manual review.

All anomalous events must be analyzed to determine the cause and to ensure that the system is operating correctly.

A record of the review, all significant events, and any actions taken as a result of these reviews must be explained in an audit log summary. This review summary must be retained as part of the long-term archive.

All KED audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely, and is not vulnerable to unauthorized use.

5.4.1. Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications required by this CP (including the KRS) must be enabled during installation~~.~~

[1] For the purposes of this policy, the definition of a virtual machine environment does not include cloud based solutions (e.g., platform as a service) or container type solutions (e.g., Docker), which are not permitted for any CA operating under this policy.

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

- ~~The type of event;~~
- ~~The date and time the event occurred;~~
- ~~A success or failure indicator when executing the CA’s signing process;~~
- ~~A success or failure indicator when performing certificate revocation;~~
- ~~A success or failure indication for requested KED actions;~~
- ~~The request source, destination, and contents for requests to the KED; and~~

  ~~The identity of the entity and/or operator that caused the 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.

~~A message from any source requesting an action requiring the use of a private key controlled by the CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.~~Any request or action requiring the use of a private key controlled by the CA is an auditable event.

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) must be recorded.

Practice Note: Events related to CA certificate issuance may be different from those related to subscriber certificate issuance

The CA and KRS must record all ~~applicable~~ events identified in the list below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented with physical logs as necessary.

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - ~~Obtaining a third-party time-stamp~~
- IDENTIFICATION AND AUTHENTICATION:
  - ~~Successful and unsuccessful attempts to assume a role~~Platform or CA application level authentication attempts
  - The value of maximum authentication attempts is changed

  - Maximum authentication attempts unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from smart card login to password~~from password to biometrics~~

- ~~LOCAL~~ DATA ENTRY AND OUTPUT:
  - ~~All security-relevant data that is entered in the system~~Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented

- ~~REMOTE DATA ENTRY:~~
  - ~~All security-relevant messages that are received by the system~~

- ~~DATA EXPORT AND OUTPUT:~~
  - ~~All successful and unsuccessful requests for confidential and security-relevant information~~

- KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)

- PRIVATE KEY LOAD AND STORAGE:
  - ~~The loading of Component private keys~~The loading of CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates
  - All access to certificate subject private keys retained within the CA for key recovery purposes

- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - ~~All changes to the trusted public keys, including additions and deletions~~Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)

- ~~SECRET KEY STORAGE:~~
  - ~~The manual entry of secret keys used for authentication~~

- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)

- CERTIFICATE REGISTRATION:
  - ~~All certificate requests~~All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process

- CERTIFICATE REVOCATION:

    - ~~All certificate revocation requests~~All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process

- CERTIFICATE STATUS CHANGE APPROVAL:
    - ~~The approval or rejection of a certificate status change request~~All records related to certificate status change request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process
- CA CONFIGURATION:
    - Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.
- ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT:
    - All changes to the certificate profile
- ~~REVOCATION PROFILE MANAGEMENT:~~
    - ~~All changes to the revocation profile~~
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
    - All changes to the certificate revocation list profile
- MISCELLANEOUS:
    - Appointment of an individual to a designated trusted role

      Practice Note: If multiparty control is implemented via team separation, these records must include team appointment specifics.

    - ~~Designation of personnel for multiparty control~~
    - Installation of the operating system
    - Installation of the CA
    - Installing hardware cryptographic modules
    - Removing hardware cryptographic modules
    - Destruction of cryptographic modules
    - System startup
    - Logon attempts to CA applications
    - Receipt of hardware / software
    - Attempts to set passwords

  - Attempts to modify passwords
  - Backing up CA internal database
  - Restoring CA internal database
  - ~~File manipulation (e.g., creation, renaming, moving)~~Records of manipulation of critical files (e.g. creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation
  - ~~Posting of any material to a repository~~The date and time any CA artifact is posted to a public repository
  - Access to CA internal database
  - All certificate compromise notification requests
  - Loading tokens with certificates
  - ~~Shipment of tokens~~Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)
  - Zeroizing tokens
  - Re-key of the CA
  - Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating system
    - Patches
    - Security profiles

- PHYSICAL ACCESS / SITE SECURITY:
  - Personnel access to room housing CA
  - Access to the CA server
  - Known or suspected violations of physical security

- ANOMALIES:
  - Software error conditions
  - Software check integrity failures
  - ~~Receipt of improper messages~~
  - ~~Misrouted messages~~
  - ~~Network attacks (suspected or confirmed)~~
  - Equipment failure
  - Electrical power outages
  - Uninterruptible power supply (UPS) failure
  - ~~Obvious and significant n~~Network service or access failures that could affect certificate trust
  - Violations of certificate policy

  - Violations of certification practice statement
  - Resetting operating system clock

5.4.2. Frequency of Processing Log

~~For CAs that issue certificates under id-fpki-common-high, the audit log must be reviewed at least once every month. For CAs that do not issue certificates under id-fpki-common-high, the audit log must be reviewed at least once every two months.~~ Audit records must be reviewed at least once every month for CAs that issue certificates under this policy. ~~KRS audit log processing frequency shall align with the CA audit log processing frequency described above.~~CSS, CMS, IDMS and KRS audit log processing frequency shall align with the CA audit log processing frequency described above.

~~Such reviews may be performed manually or by an automated process, and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities. A statistically significant portion of the security audit data generated by the CA or KRS since the last review must be examined. This amount will be described in the CPS or KRPS.~~

~~All KED audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely, and is not vulnerable to hacking or unauthorized use. The objective of audit log reconciliation is to ensure that all actions are being made by authorized parties and for legitimate reasons. All significant events must be explained in an audit log summary. Actions taken as a result of these reviews must be documented.~~

5.4.3. Retention Period for Audit Log

Audit ~~logs~~ records must be ~~retained~~ accessible ~~on-site~~ until reviewed, in addition to specific records being archived as described in Section 5.5.

5.4.4. Protection of Audit Log

~~System configuration and operational procedures must be implemented together to ensure that:~~

- ~~Only authorized individuals and systems have read access to the logs;~~
- ~~Only authorized auditors may archive audit logs; and,~~
- ~~Audit logs are not modified.~~

System configuration and operational procedures must be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified before review.

Collection of the audit ~~logs~~ records from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

~~For RA, the authorized individual must be a system administrator other than the RA.~~For RA systems, the individual authorized to move or archive records may not hold an RA Trusted Role.

~~Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).~~ Procedures must be implemented to protect audit records from deletion or destruction before they are reviewed as described in Section 5.4.2. ~~Security audit data must be moved to a safe, secure storage location separate from the location where the data was generated.~~To protect the integrity of audit records, they must be transferred to a backup environment distinct from the environment where the audit records are generated.

5.4.5. Audit Log Backup Procedures

Audit ~~logs~~ records and audit summaries must be backed up at least monthly. ~~A copy of the audit log must be sent off-site on a monthly basis.~~

If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section 5.4.4. The backup procedure may be automated or manual, but must occur no less frequently than the audit log review described in Section 5.4.2.

The process for transferring the audit records to the backup environment must be documented.

5.4.6. Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system or KRS. Automated audit processes must be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations must be suspended until the problem has been remedied.

5.4.7. Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8. Vulnerability Assessments

~~CAs and KRSs must perform routine self-assessments of security controls.~~ CAs must perform routine vulnerability assessments of the security controls described in this policy.

Self-assessment of controls and control effectiveness (e.g., FISMA) must be performed in accordance with the frequency determined by the risk rating of the CA.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessment must be documented.

Practice Note: The ~~security~~ audit data should be reviewed by the ~~security~~ auditor 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. ~~Security~~ A~~a~~uditors should check for continuity of the ~~security~~ audit data.

5.5. Records Archival

~~CAs and KRSs must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.~~

The primary objective of the CA archive is to prove the validity of any certificate (including those revoked or expired) issued by the CA in the event of dispute regarding the use of the certificate.

The primary objective of the KRS archive is reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of key recovery requests
- Validation of the identity of the recipient of an escrowed key;
- Verification of authorization to obtain the escrowed key copy;
- Verification of transfer of custody of escrowed keys to an authorized Requestor; and
- Establishment of the circumstances under which a copy of the escrowed key was provided.

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:

- ~~CA Authority To Operate~~
- Certificate Policy
- Certification Practice Statement / Key Recovery Practice Statement
- Contractual obligations and other agreements concerning operations of the CA or KRS
- System and equipment configuration
- Modifications and updates to system or configuration
- ~~Certificate requests~~All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process
- All certificates issued and/or published
- Record of re-key
- ~~Revocation requests~~All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process

- Subscriber identity authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates ~~(if applicable)~~
- Subscriber agreements
- Documentation of receipt of tokens
- ~~All CRLs issued and/or published~~
- Other data or applications to verify archive contents (e.g., key escrow software)
- ~~Compliance Auditor reports~~Audit summary reports generated by internal reviews and documentation generated during third party audits
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- ~~All changes to the trusted public keys, including additions and deletions~~Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components such as CMS, RA, etc.
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role (to include KRA/KRO)
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement / Key Recovery Practice Statement

5.5.2. Retention Period for Archive

~~For CAs that issue certificates under id-fpki-common-high, records must be kept for a minimum of 20 years and 6 months without any loss of data.~~

~~For CAs that do not issue certificates under id-fpki-common-high, records must be kept for a minimum of 10 years and 6 months without any loss of data.~~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.

National Archives and Records Administration General Records Schedules [NARA GRS], 5.6 Item 120, defines other required RA chain-of-trust records, and archive retention periods.

Otherwise RA operations, to include any IT systems that facilitate RA functions, must maintain relevant archives for 3 years after RA system replacement or termination.

5.5.3. Protection of Archive

~~Only authorized users are permitted to write to, modify, or delete the archive. Archived records may be moved to another medium.~~ Only Auditors, 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.

Archive media must be stored in a safe, secure storage facility geographically separate from the CA using procedures approved by NARA or according to agency-specific policy. The transfer process between the backup environment and archive location must be documented.

~~Applications required to process the archive data must be maintained for a period that equals or exceeds the archive requirements for the data.~~In order to ensure that records in the archive may be referenced when required, the CA must do one of the following:

- Maintain the hardware or software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-Stamping of Records

~~CA or KRS archive records must be automatically time-stamped as they are created.~~ CA archive records must have accurate time-stamps when they are added to the archive.

The time precision must be such that the sequence of events can be determined.

The CPS or KRPS must describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6. Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner, but must be documented in the associated CPS/KRPS.

5.5.7. Procedures to Obtain and Verify Archive Information

Copies of records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

Procedures, detailing how to create, verify, package, transmit, and store the CA/KRS archive information, must be included in the CPS/KRPS.

6.2.5. Private Key Archival

CA private signature keys and Subscriber private signature keys must not be archived.

CAs that retain Subscriber private encryption keys for business continuity purposes ~~must archive such~~may require an archive of escrowed Subscriber private keys, so that they can be recovered for as long as the business continuity purposes require. Archives of escrowed private keys must be protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2.1~~ 5.5~~.

6.3.1. Public Key Archival

~~The ~~P~~p~~ublic key ~~is archived~~archival must be ~~as part of the certificate archival~~in accordance with Section 5.5.

APPENDIX B: REFERENCES

APL	Approved Products List (APL) ~~http://www.idmanagement.gov/approved-products-list-apl~~ https://www.idmanagement.gov/buy/#products/
AUDIT	FPKI Annual Review Requirements ~~https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-annual-review-requirements.pdf~~ https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles ~~https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-ssp.pdf~~ https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf
NARA GRS	National Archives and Records Administration, General Records Schedules https://www.archives.gov/records-mgmt/grs.html
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. ~~https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/TIG_SCEPACS_v2.3.pdf~~ https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf
PIV-I Issuers	Personal Identity Verification Interoperability for Issuers ~~https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-i-for-issuers.pdf~~ https://www.idmanagement.gov/docs/fpki-pivi-for-issuers.pdf
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/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profiles-pivi.pdf~~ https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-pivi.pdf

APPENDIX C: ACRONYMS AND ABBREVIATIONS

CMS	Card Management System
IDMS	Identity Management System

APPENDIX D: GLOSSARY

Archive	~~Long-term, physically separate storage.~~A collection of documents created or gathered by the CA and selected for long-term preservation as evidence of their activities.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit ~~Data~~Record	~~Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]~~An individual entry in an audit log related to an audited event.