FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2023-06

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Updates to account for certificate Modification and Restoration
Date: September 26, 2023

Title: Certificate Modifications and Restorations

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.5 July 2023

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

Organization requesting change: CPWG

Change summary: Clarify the requirements around certificate modifications, define requirements for certificate restoration, align audit and archive terminology for certificate status changes, and to generalize two document references.

Background: Recent review of policy showed some confusion around the different requirements between a certificate rekey and a certificate modification.

Additionally, the current policy requires entities document their suspension requirements specifically who can request suspensions and the minimum requirements for the suspension process; however, it is currently silent on policy requirements for restoring certificates (e.g., removal from suspension). This change seeks to provide parity with the suspension requirements to include who can request restoration, how they must be authenticated to support that request and what actions need to take place upon restoration.

Finally, Common Policy currently references specific revisions of FIPS 140 and FIPS 201 (specifically FIPS 140-2, and FIPS 201-2). Both of these reference standards have since been updated and this change generalizes the references and updates the links to the most recent publications.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

4.8.1. Circumstance for Certificate Modification

CA certificates and Delegated OCSP responder certificates whose characteristics have changed (e.g., assert new policy OID) may be modified. ~~The new certificate may have the same or a different subject public key.~~

A certificate associated with a Subscriber whose characteristics have changed (e.g., name change due to marriage) may be modified. ~~The new certificate must have a different subject public key~~.

4.8.3. Processing Certificate Modification Requests

A modified certificate may use the same or a different subject public key as the original certificate, depending on issuance constraints. However, if the same key is used, certificate operational periods and key lifetimes as defined in Section 6.3.2 continue to apply.

…

4.9.13. Circumstances for Suspension and Restoration

For CA certificates and device certificates, suspension is not permitted.

CAs may support certificate suspension and restoration for Subscriber certificates. If suspension and restoration are supported by the CA, the CPS must describe under what circumstances and provide details as specified in Sections 4.9.14, 4.9.15 and 4.9.16 ~~for the corresponding sections below~~.

Practice Note: Certificate suspension should only be used in circumstances where there is a reasonable possibility that the certificate will need to be restored (e.g., suspension while background investigation outcome is appealed). It is not recommended to use certificate suspension as a mechanism to enforce access controls on a temporary basis or to circumvent account deprovisioning. Additionally, a certificate must be permanently revoked if it meets the circumstances stated in Section 4.9.1.

4.9.14. Who Can Request Suspension and Restoration

For CAs that support suspension and restoration, those personnel authorized to request suspension and restoration of a certificate must be identified.

4.9.15. Procedure for Suspension and Restoration Requests

For CAs that support suspension and restoration, all suspended certificate serial numbers must be populated on a full CRL within a timeframe specified in Section 4.9.7. The reason code CRL entry extension shall be populated with “certificateHold.” Restored certificate serial numbers must not be present on the next full CRL published by the CA.

Practice Note: A certificate is considered restored only if its status at the time of CRL generation is neither suspended nor revoked.

~~For CAs that support suspension, a~~ A request to suspend or restore a certificate must include:

- authentication of the requestor,
- identification of the certificate to be suspended or restored, and
- explanation of the reason for suspension or restoration.

If a CA or CMS product conducts certificate suspensions and restorations in an automated fashion (e.g., without a formal request outlined above), the circumstances or parameters associated with those automated suspensions and restorations must be documented in a CPS.

If a subscriber is requesting restoration of their suspended certificate, the identity of the subscriber must be re-established before restoring the certificate. The subscriber’s identity may be re-established using processes defined in Section 3.2.3.1, through the use of biometrics on file through the chain of trust defined in [FIPS 201], or by the use of another private signature key of equivalent or greater assurance level issued to the subscriber.

The private key associated with any suspended certificate must not be used to authenticate the identity of the certificate subject.

5.4.1. Types of Events Recorded

- ~~CERTIFICATE REVOCATION:~~
    - ~~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 CHANGES ~~APPROVAL~~:
    - All records including request authorization, approval and execution related to certificate status changes (e.g., revocation, suspension or restoration) ~~including request authorization, approval and execution~~ whether generated directly on the CA or generated by a related external system or process

5.5.1. Types of Events Archived

…

- All records related to certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated as part of a related external system or process

Appendix B: References

FIPS 140~~-2~~	Security Requirements for Cryptographic Modules, FIPS 140-3~~2, May 25, 2001.~~ https://csrc.nist.gov/publications/detail/fips/140/3~~2~~/final
FIPS 201~~-2~~	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-3~~2, August 2013.~~ https://csrc.nist.gov/publications/detail/fips/201/3~~2~~/final

Estimated Cost: None

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	5/23/2023
Date change released for comment:	9/8/2023
Date comment adjudication published:	9/26/2023