COMMON Certificate Policy Change Proposal Number: 2020-02

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 and certificate profile specification
Date: August 19, 2020

Title: Consolidated update to Common Policy and associated profiles

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 1.32, April 14, 2020*

Change Advocate's Contact Information:
Organization: FPKI Policy Authority
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This is a comprehensive update to Common Policy and the associated certificate profile specification (formerly titled "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program"). High-level update summary:

- Removed Foreword
- Standardized terminology
- Realigned requirements with appropriate policy sections
- Increased use of tables to improve readability
- Aligned requirements with observed agency practices
- Clarified definitions of certificate types
- Streamlined certificate naming
- Updated certificate re-key, renewal, and modification definitions for clarity
- Removed SHA-1 references
- Updated permitted key sizes and algorithms
- Converted sections after Section 9 to appendices
- Updated format and content of certificate profiles
    - Aligned profiles with proposed updates to Common Policy
    - Added "Common PIV-I" profiles

- Split Cross Certificate profile into two profiles (Cross certificate and Intermediate CA) to help clarify requirements and reduce confusion
- Numerous worksheet updates (see Appendix C)

Background: This update consolidates CPWG policy recommendations dating back to 2018. It also cleans-up outdated references and requirements, clarifies existing requirements, aligns policy with observed agency practices (e.g., certificate naming), and improves readability.

Updates related to the following topics were discussed with CPWG members to minimize adverse impact:

- Authorization data in subscriber certificates
- Federal subscriber certificate naming
- Time to process certificate applications
- Updated CA rekey timelines
- Updated references for permissible options comparable to "digitally signed attestation under perjury" requirement (declaration of identity)
- Permitted key sizes and algorithms
- Identification and authentication requirements for routine subscriber re-key
- CA cryptographic module requirements
- Certificate profile changes

Additional detail related to update activities and milestones is included in Appendix A.

Specific Changes: Due to format changes and the number of edits, updates were highlighted to CPWG and FPKIPA members in separate, redlined versions of Common Policy.

Change Impact:

- Potential impacts resulting from the proposed updates to Common Policy are included in Appendix B.
- Potential impacts resulting from the proposed updates to the certificate profiles are included in Appendix C.

Estimated Cost: TBD

Implementation Date: September 1, 2021

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: January 14, 2020
Date change released for comment: February 17, 2020
Date comment adjudication published: August 19, 2020

APPENDIX A: UPDATE ACTIVITIES AND MILESTONES

Q3 FY 2019 (1Apr - 30Jun)

- May CPWG - Call for policy updates and clean-ups (5/28/19)
- FPKIPA Support Team began section by section review of Common Policy and Profiles

Q4 FY 2019 (1Jul - 30Sept)

- FPKIPA Support Team continued section by section review of Common Policy and Profiles
- September CPWG - Discussions related to *Authorization Data* and *Certificate Naming*
- FPKIPA Support Team began draft updates

Q1 FY 2020 (1Oct - 31Dec)

- FPKIPA Support Team continued draft updates
- November CPWG - Discussions related to *Time to Process Applications* and *Permitted Algorithms* (11/26/19)
- FPKIPA Support Team draft finalization and internal review

Q2 FY 2020 (1Jan - 31Mar)

- FPKIPA Support Team comment adjudication
- January CPWG - FPKIPA Support Team shares status update and requests additional feedback (1/28/20)
- FPKIPA Support Team shares policy artifacts for CPWG feedback (2/17/2020)
- March CPWG - Review period extended one month (4/28/20).

Q3 FY 2020 (1Apr - 30Jun)

- April CPWG - Review feedback and proposed adjudication (4/28/20)
- FPKIPA Support Team comment adjudication, incorporation of 2020-01, and distribution of Draft Release #2 (5/22/20)
- May CPWG - Summarized comment adjudication and reviewed next steps (5/28/20)
- June PA - Change proposal introduction to facilitate discussion on implementation timeline and cost (6/9/20)
- Draft Release #3 (6/18/20)
- June CPWG - Summarized recent updates and reviewed next steps (6/23/20)

Q4 FY 2020 (1Jul - 30Sept)

- Draft Release #4 (7/13/20)
- July PA - Finalized change proposal and initiated vote (7/14/20)
- August PA – Discussed agency feedback and next steps (8/11/20)
- Change proposal finalized and initiated vote (8/19/20)

APPENDIX B: IMPACT OF POLICY UPDATES

Policy Change Summary	Impact
Overall • Standardized terminology ("Human Subscriber", "Device", "must", "publicly accessible", etc.) • Clarified and streamlined language • Standardized formatting of "Practice Notes" and external references • Removed references to "legacy" agency PKIs, deprecated algorithms (e.g., SHA-1), and deprecated policies (e.g., M-04-04) • Relocated requirements to more applicable policy sections	No negative impact
Section 1 • Tabularized, re-ordered, and clarified policies covered by the CP • Updated scope of CP to remove code signing and only locally trusted CA use cases	No negative impact
Section 2 • Clarified Authority Information Access (AIA) and Subject Information Access (SIA) requirements • Added option for single DER encoded certificate file (AIA)	No negative impact
Section 3 • Reorganized certificate subject name and subject alternative name requirements into independent sub-sections • Updated naming requirements to align with observed agency practices • Removed unused name types (e.g., DC=mil) • Incorporated changes proposed in draft "Updated registration processes and biometric linkage" Change Proposal (June 12, 2019) • Included reference to FIPS 201 for the purposes of human subscriber identity proofing • Removed references to authorizations in subscriber certificates	No negative impact
Section 4 • Timeframe for certificate application process modified from 30 days to 90 days; topic discussed with CPWG • Clarified definitions of "renewal", "re-key", and "modification" • Tabularized CRL issuance frequency requirements • Defined offline CA • Incorporated OCSP requirements, moved from Section 2 • Incorporated privacy information publication restrictions, moved from Section 9	No negative impact

Section 5 • Clarified “remote workstation” practice note • Require delegated OCSP signing • Added requirement that any compromised CA must request revocation from any superior or cross certified CA	No negative impact
Section 6 • Removed references to SHA-1 • Updated cryptographic module requirements (require FIPS 140-2 Level 3 protection of CA signing keys) • Incorporated draft "Update Common Policy on use of CA signing Keys" Change Proposal submitted by Treasury • Reduce OCSP certificate validity from 3 years to 120 days • Require use of a VPN for remote workstation administration of CA	No negative impact Note: two affiliates require updates to OCSP certificate validity
Section 7 • Updated permitted key sizes (add RSA 4096 and EC P-384) and signing algorithms (sha384WithRSAEncryption, sha512WithRSAEncryption, and ecdsa-with-SHA512)	No negative impact
Section 8 • No major updates	No negative impact
Section 9 • No major updates	No negative impact

APPENDIX C: IMPACT OF CERTIFICATE PROFILE UPDATES

Profile Changes	CAs Impacted*
Authority Information Access & Certificate Revocation List Distribution Point - Require HTTP URI first	6
Authority Information Access - Allow .cer	No negative impact
DN Encoding: Allow only printableString and/or UTF8	No negative impact
Key Usage - Remove digital signature and non-repudiation bits from CA profiles • Removes ability to perform direct OCSP signing by a CA; delegated OCSP signing only	4 No CA operations currently impacted; possible future impact
Allow Subject Directory Attributes (e.g., citizenship)	No negative impact
Cross Certificate • Clarify appropriate use of requireExplicitPolicy and inhibitPolicyMapping, • Offer distinction from the Intermediate CA Certificate profile (new).	No negative impact
Intermediate Certificate (new profile) • Prohibit policy mappings • Policy constraints are optional • Subject Information Access extension is required, unless the CA certificate includes path length constraint of 0	No negative impact
OCSP Responder Certificate • EKU must be marked critical	11
Signature Certificates and Key Management Certificates • For PIV, id-kp-emailProtection must be included • rfc822Name is required if id-kp-emailProtection is asserted in Extended Key Usage	2

* based on Annual Review certificate samples