FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Profiles Change Proposal Number: 2022-05

To: Federal PKI Policy Authority (FPKIPA)
From: Federal PKI Certificate Policy Working Group (CPWG)
Subject: Multiple updates to the Common Policy Certificate and CRL Profiles
Date: September 16, 2022

Title: Consolidated changes to the Common Policy Certificate and CRL Profiles

Version and Date of Certificate Policy Requested to be changed:

- *Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles Version 2.1, February 1, 2021*

Change Advocate's Contact Information:
Organization: Department of Treasury PKI Policy Management Authority (PMA)
E-mail address: Daniel.Wood@Treasury.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This proposal incorporates multiple change to the Common Policy Certificate and CRL Profiles, to include the following worksheets and Sections:

- *Worksheet 3: Cross Certificate and Worksheet 4: Intermediate CA Certificate* – currently the Policy Constraints and Inhibit Any Policy fields require a criticality flag be FALSE (or excluded), this Criticality statement can be removed as it is not aligned with RFC 8520 or current FPKIMA practice, the update provides additional flexibility for affiliate partners
- *Worksheet 6: PIV Authentication Certificate Worksheet 7: Card Authentication Certificate, and Worksheet 10: Derived PIV Authentication Certificate* – Currently the PIV NACI indicator is a mandatory element of these certificates; this field is made optional as FIPS 201-3 no longer mandates the extension in these certificates
- *Worksheet 11: Authentication Certificate* – currently there is a requirement not to assert a FASC-N in the SAN field of this certificate; due to relying party directory configurations this restriction is removed for additional relying party flexibility
- *Worksheet 12: Device Certificate* – currently iPaddress is not included as a potential value in the SAN of a device certificate, some relying parties require it to authenticate specific devices on their networks; the intent of this change is to meet operational needs during times of routine operations and incident recovery

    - The Department of Homeland Security (DHS) has identified Cisco appliances in their environment that specifically require IP Address in the SAN to properly function, and DNS name is not an option
    - The Department of the Treasury, Internal Revenue Service (IRS) relies on IP Address in the SAN for continuity of operations during a degradation of DNS being unavailable; further, the ability to continue to function securely via TLS during a potential DNS degradation is particularly concerning when considering the disablement of the "HTTPS warning page bypass" as recommended
- *Worksheet 13: Delegated OCSP Responder Certificate* – add the basic constraints field as optional to allow flexibility and align with current practices of affiliate partners
- *Section 8: References* – the table that includes all references is removed and a link to Common Policy Appendix D is included in its place as all references are incorporated in the base policy

The CPWG also recommended that all end-entity certificates remove the critical or non-critical specification on the Basic Constraints Field as it was deemed unnecessary. Additionally, the end entity certificate policies field should specifically be marked as non-critical in alignment with Common Policy Section 7 and to prevent relying party applications from rejecting certificates due to inclusion of the required extension.

The purpose of these requested changes is multi-faceted and includes alignment to RFC 5280, FIPS 201-3, increased interoperability, and to account for known and acceptable certificate practices.

Specific Changes:

Insertions are <u>underlined</u>; deletions are in ~~strikethrough~~.

Worksheet 3: Cross-Certificate

Policy Constraints	~~Critical = FALSE~~ requireExplicitPolicy with SkipCerts = 0 must be present. inhibitPolicyMapping must be included with SkipCerts = 0 when issued to an SSP. Where downstream mappings are permitted, SkipCerts is set to the minimum value required to support the expected mappings.
Inhibit Any Policy	~~Critical = FALSE~~ SkipCerts = 0

Worksheet 4: Intermediate Certificate

Policy Constraints	~~Critical = FALSE~~ When this extension appears, both requireExplicitPolicy and inhibitPolicyMapping must be present and assert SkipCerts = 0
Inhibit Any Policy	~~Critical = FALSE~~ SkipCerts = 0

Worksheet 6: PIV Authentication Certificate, Worksheet 7: Card Authentication Certificate, and Worksheet 10: Derived PIV Authentication Certificate

PIV NACI *(Optional)*	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-~~2~~3. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed, and (2) a ~~NACI~~ background investigation has been initiated but has not completed. FALSE if, at the time of credential issuance, the subject's ~~NACI~~ background investigation has been completed and successfully adjudicated.

Worksheet 11: General Authentication Certificate

Subject Alternative Name *(Optional)*	One or more of the following are permitted: rfc822Name otherName values (e.g., Microsoft UPN) to support local applications directoryName to support local applications ~~FASC-N must not be included~~

Worksheet 12: Device Certificate

Subject Alternative Name *(Optional)*	The following name types may be present: dNSName is an IA5String that contains the DNS name of the subject URI is an IA5String that contains the URI of the subject rfc822Name that contains the email address of the sponsor, administrator, or help desk iPAddress is an octet string that contains the Internet Protocol address of the subject otherName values may also be included to support local applications

Worksheet 13: Delegated OCSP Responder Certificate

Basic Constraints *(Optional)*	cA:FALSE Path length constraint must be absent

All End-Entity Certificate Worksheets 5-12 and 15-17

Basic Constraints *(Optional)*	~~May be critical or non-critical~~ cA:FALSE Path length constraint must be absent
Certificate Policies	Critical = FALSE … [Certificate Policies assertions vary by worksheet]

8. References

Please see X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Appendix D for references.

~~[Reference Name]~~	~~[Reference Title, date and link]~~

Change Impacts: No impacts anticipated. All of the recommended profile updates are meant to ease restrictions compared to the current profiles and should not require changes to certificate templates unless implementers wish to incorporate optional elements.

Additionally, the elimination of a separate list of references in the profiles document will ensure the authoritative list of references is maintained in Common Policy, limiting duplication of effort when updates are required.

Estimated Cost: No cost anticipated.

Implementation Date: Immediate

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: August 23, 2022
Date change released for comment: August 23, 2022
Date comment adjudication published: September 13, 2022