Common Policy Framework Certificate Policy Change Proposal Number: 2016-01

To: Federal PKI Policy Authority (FPKIPA)

From: FPKI Management Authority (FPKIMA)

Subject: Proposed modifications to the Common Policy Framework Certificate Policy

Date: April 26, 2016

Title: CAB Forum Baseline Requirements Alignment

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.24, May 7, 2015

Change Advocate's Contact Information: FPKIMA

Organization requesting change: FPKI Management Authority

Change summary: Implementation of this change proposal will harmonize Common Policy Requirements with CAB Forum Baseline Requirements (BR) v1.3.4

Background:

M-15-13 (Policy to Require Secure Connections across Federal Websites and Web Services) states HTTPS certificates should be used to secure federal web sites. A certificate has to have a certificate path to a publicly trusted root certificate for public web browsers to recognize it as trusted. Currently the FCPCA root certificate is not distributed in all web browser trust stores. This makes it difficult for federal agencies to use FPKI issued SSL/TLS certificates on public facing websites.

Although the current FPKI root certificate (FCPCA) is distributed in the Microsoft Trust Store for multiple purposes, industry best practice is moving toward separate issuing CA's for people (end-entity) and non-people (devices). For instance, a CA that issues Server Authentication certificates (SSL/TLS certificate) would not issue Client Authentication certificates for human users. While the FPKIMA has been successful in adding the FCPCA to multiple public trust stores, Mozilla has been reluctant to approve the FCPCA root certificate in the Mozilla Network Security Service (NSS) Trust Store because of the wide use of cross-certificates in the FPKI and the lack of detail in the FPKI CP around the requirements for issuing server certificates that web browsers consider important. One of the current roadblocks for Mozilla is the inability for the FPKI to claim conformance to the CAB Forum BRs for publicly trusted SSL/TLS certificates.

Guidance for issuance of device certificates have not been very specific within the FCPCA CP,

aligning FCPCA CP requirements with industry best practice, as defined in the CAB Forum BRs will help promote the inclusion of the Federal Root in public trust stores and provides guidance for issuance of publically trusted device certificates. This change proposal is a first step toward harmonizing FPKI device certificate policies with CAB Forum BRs.

Specific Changes:

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

FOREWORD

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates ~~ten~~ eleven specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices that sign Personal Identity Verification (PIV) data objects, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a policy for publicly trusted Server Authentication certificates, a high assurance user policy, three user authentication policies, and a card authentication policy. There is one Certification Authority (CA) associated with the Common Policy Framework: The Federal Common Policy Root CA.

1. INTRODUCTION

This certificate policy (CP) includes ~~ten~~ many distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a policy for devices that sign PIV data objects, a policy for publicly trusted Server Authentication certificates, a high assurance user policy, three user authentication policies, and a card authentication policy. In this document, the term “device” means a non-person entity, i.e., a hardware device or software application. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all ~~ten~~ eleven policies.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CAs shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-devicesHardware	::= {2 16 840 1 101 3 2 1 3 36}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}

id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}
id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}
id-fpki-common-public-trusted-serverAuth	::= {2 16 840 1 101 3 2 1 3 tbd}

Certificates issued to CAs may contain ~~any or all~~ a subset of these OIDs. Certificates issued to users, other than devices, to support digitally signed documents or key management may contain either id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include one or more of~~either~~ id-fpki-common-deviceHardware, id-fpki-common-devices, or id-fpki-common-public-trusted-serverAuth~~both~~. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include id-fpki-common-devices or id-fpki-common-public-trusted-serverAuth.

CAs that issue id-fpki-common-public-trusted-serverAuth certificates shall only issue certificates asserting serverAuth in the EKU. CAs that issue publicly trusted Code Signing certificates shall only issue certificates asserting codeSigning in the EKU.

1.3.1.3 FPKI Management Authority (FPKIMA)

The FPKIMA is the organization that operates and maintains the Federal Common Policy Root CAs on behalf of the U.S. Government, subject to the direction of the FPKIPA.

1.3.1.4 FPKI Management Authority Program Manager

The Program Manager is the individual within the FPKIMA who has principal responsibility for overseeing the proper operation of the Federal Common Policy Root CAs, including the required ~~Common Policy Root CA~~ repository, and selecting the FPKIMA staff. The Program Manager is selected by the FPKIMA and reports to the FPKIPA. The FPKIMA Program Manager must hold a Top Secret security clearance.

2.2.2 Publication of CA Information

The Common Policy CP shall be publicly available on the FPKIPA website (see ~~http://www.idmanagement.gov/fpkipa~~ http://www.idmanagement.gov/). ~~The CPS for the Common Policy Root CA will not be published; a~~ A redacted version of ~~this~~ the CPS for the Federal Common Policy Root CAs and the annual PKI Compliance Audit Letter will be publicly available from the FPKIMA website (See ~~http://www.idmanagement.gov/fpkima~~ http://www.idmanagement.gov/). Other CAs operating under this policy shall make available a redacted CPS and annual PKI Compliance Audit Letter in their organization's public repository.

~~Practice Note: There is no requirement for the publication of CPSs of other CAs that issue certificates under this policy.~~

3.1.1 Types of Names

Devices that are the subject of certificates issued under this policy shall be assigned either a geo-political name or an Internet domain component name. Device names shall take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*
- dc=gov, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]
- dc=mil, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

In addition, id-fpki-common-public-trusted-serverAuth certificates shall conform to the following:

- The extendedKeyUsage extension shall assert the serverAuthentication value:
- The *SubjectAltName* field shall contain a *dNSName* containing a Fully Qualified Domain Name (FQDN) of a server;
- Internet Protocol (IP) Addresses shall not be included in the *SubjectAltName* field;

For certificates that assert serverAuth in the EKU:

- Wildcard Domain Names are permitted if all sub-domains covered by the wildcard fall within the same application, cloud service, or system accreditation boundary within the scope of the sponsoring Agency.
- Wildcards shall not be used in subdomains that host more than one distinct application platform. The use of third-level Agency wildcards, (e.g., *.[agency].gov), shall be prohibited to reduce the likelihood that a certificate will overlap multiple systems or services. Third level wildcards are permitted for DNS names dedicated to a specific application (e.g., *.[application_name].gov).
- Before issuing a publicly trusted serverAuth certificate containing a wildcard, the CA shall ensure the sponsoring agency has a documented procedure for determining that the scope of the certificate does not now and will not infringe on other agency applications.

3.2.3.2 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications will be named as certificate subjects. In such cases, the device must have a human sponsor who is affiliated with the agency under which the certificate is being issued. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys

- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

These certificates shall be issued only to authorized devices under the subscribing organization's control. In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained. See section 9.6.3 for subscriber responsibilities.

For each Fully-Qualified Domain Name listed in an id-fpki-common-public-trusted-serverAuth certificate, the CA shall confirm and maintain documented evidence that, as of the date the Certificate was issued, the Sponsor's agency has control over the FQDN and the sponsor is authorized to request the certificate.

Each agency shall have a naming policy for devices that receive an id-fpki-common-public-trusted-serverAuth certificate that specifies unique meaningful FQDN names and the CPS shall document how the CA ensures compliance with the sponsoring agency's policy.

Note: FQDNs shall be listed in id-fpki-common-public-trusted-serverAuth Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA shall establish and follow a documented procedure to ensure that the wildcard does not fall immediately to the left of an agency or organization name, but is qualified down to a unique application, server, or server farm under control of the sponsor's organization. The device sponsor shall demonstrate that the domain name requested is entirely within the name space to be covered by the wildcard certificate.

All requests for device certificates shall be digitally signed by the sponsor

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

In accordance with section 3.2.3.2, all requests for device certificates in the name of an organization, shall be digitally signed by the sponsor. In addition, the CPS shall specify a

process by which an organization identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of the organization's authorized certificate requesters upon the Applicant's verified written request.

4.1.1.4 Code Signing Certificates

A code signing certificate has an Extended Key Usage (EKU) containing a value of id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }(1.3.6.1.5.5.7.3.3) - See [CCP-PROF] for appropriate EKU bit settings.

An application for a code signing certificate shall be submitted by an authorized representative of the organization. The representative shall assert that the organization has access to a Time Stamp Authority (TSA) prior to issuance of the code signing certificate. CAs subordinate to the publicly trusted Federal Common Policy Root CAs for device certificates that issue publicly trusted Code Signing certificates shall not issue other types of certificates from the same CA that issues code signing certificates.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP. The PKI Authority must identify the components of the PKI Authority (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case. For CAs that issue id-fpki-common-public-trusted-serverAuth certificates and subordinate to a publicly trusted Federal Common Policy Root CA, the CPS shall state whether the CA reviews Certification Authority Authorization (CAA) DNS Resource Records, and if so, the CA's practice on processing CAA records for fully Qualified Domain Names.

4.2.2 Approval or Rejection of Certificate Applications

For the Common Policy Root CAs, the FPKIPA may approve or reject a certificate application. For CAs operating under this policy, approval or rejection of certificate applications is at the discretion of the Agency PMA or its designee.
For Device certificates, the CA shall reject a certificate request if the requested Public Key has a known weak Private Key.

Public key parameters generation and quality checking, shall be conducted in accordance with NIST SP 800-89. Key validity shall be confirmed in accordance with NIST SP 800-56A.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—

- Identifying information or affiliation components of any names in the certificate becomes invalid. This would include evidence that a wild card certificate has been issued with a name where PKI Sponsor does not exercise control of the entire name space associated with the wild card certificate.
- Privilege attributes asserted in the subscriber's certificate are reduced.

- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
- The failure of a CA to adequately adhere to the requirements of this CP or the approved CPS. E.G., there is strong evidence that the CA has failed to comply with the requirements of Section 6.7 of the CP.

In addition, for id-fpki-common-public-trusted-serverAuth certificates, a certificate shall be revoked when:

- The CA obtains evidence that the issuing CA (or Subordinate CA) no longer complies with the requirements of section 6.7. In this case, all certificates under an issuing CA or subordinate CA shall be revoked.
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name

Whenever any of the above circumstances are reported, the appropriate authority shall review the circumstances and make a revocation decision. The revocation decision shall be made based on appropriate criteria, to include:

- 1. The nature of the alleged problem;
- 2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber; and
- 3. Relevant legislation

If it is determined that revocation is required, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The human sponsor of a device can request the revocation of the device's certificate. Other authorized agency officials may request revocation as described in the CPS.

The CA shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall publicly disclose the instructions through a readily accessible online means.

4.9.9 On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-

derived-pivAuth, ~~and~~ id-fpki-common-cardAuth, id-fpki-common-public-trusted-serverAuth, and all publicly trusted device certificates.

Where on-line status checking is supported, status information must be updated and available to relying parties within 18 hours of certificate revocation.

Where on-line status checking is supported and a certificate issued under id-fpki-common-High is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours.

For publicly trusted server authentication and code signing certificates, CAs shall support an OCSP capability using the GET method for Certificates issued in accordance with this CP.

For the status of Subscriber Certificates:

> The CA shall update information provided via an Online Certificate Status Protocol at least every 18 hours. OCSP responses from this service shall have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

> The CA shall update information provided via an Online Certificate Status Protocol whenever CRLs are generated and at least within 18 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder should not respond with a "good" status. The CA should monitor the responder for such requests as part of its security response procedures.

The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

In addition, for id-fpki-common-public-trusted-serverAuth certificates, OCSP responses must be signed either:

> 1. by the CA that issued the certificates whose revocation status is being checked, or
>
> 2. by a delegated OCSP Responder using a certificate signed by the CA that issued the certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate shall contain an extension of type id-pkix-ocsp-

nocheck, as defined by RFC2560.

Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

6.1.5 Key Sizes

Trusted Certificates that expire before January 1, 2031 shall contain subject public keys of 2048 or 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key. Trusted Certificates that expire on or after January 1, 2031 shall contain subject public keys of at least 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key

6.2.1 Cryptographic Module Standards and Controls

…

CSSes that provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CSSes that do not provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

For CAs that issue id-fpki-common-public-trusted-serverAuth device certificates, The CA shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

9.6.1 CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy….

- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

This CP will be reviewed and updated as appropriate when Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org are updated.

10. BIBLIOGRAPHY

…

SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89 http://csrc.nist.gov/publications/nistpubs/
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A

http://csrc.nist.gov/publications/nistpubs/

Estimated Cost:

TBD

Implementation Date:

This change will be effective 6 months from the date of approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	2/4/2016, 4/19/16, 5/24/16, 8/16/16
Date presented to FPKIPA:	9/15/2016
Date of approval by FPKIPA:	9/22/16