COMMON Certificate Policy Change Proposal Number: 2018-07

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Update Common Policy to remove the common-public-trusted-serverAuth certificate policy
Date: October 24, 2018

Title: Update Common Policy to remove the common-public-trusted-serverAuth certificate policy

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.30, October 4, 2018

Change Advocate's Contact Information:
Name: India Donald
Organization: FPKI Management Authority
E-mail address: india.donald@gsa.gov

Organization requesting change: FPKIMA

Change summary: Update the CP to remove the common-public-trusted-serverAuth certificate policy

Background:

In 2016, the FPKIMA introduced a change proposal (2016-01) to try to align Common Policy with the CAB Forum Baseline Requirements (BR) v1.3.4. This was to facilitate FPKI conformance to CAB Forum BRs for publicly-trusted SSL/TLS certificates, in order to help promote inclusion of the Federal Root in public trust stores and provide guidance for issuance of publicly-trusted device certificates. However, in 2017, the government decided instead to establish an independent PKI for the issuance of federally issued publicly trusted serverAuth certificates. An entirely new CP written to conform to the CAB Forum and public trust store requirements specific to certificates intended for use as publicly trusted serverAuth certificates on the Internet and limited to Domain Names ending in .gov and .mil is close to completion,

No CAs in the FPKI have been approved to issue common-public-trusted-serverAuth certificates as defined in the Common Policy CP. Therefore, we are requesting the removal of the supporting text from the Common Policy CP so as not to provide conflicting information to those who may rely on the Common Policy CP.

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 ~~eleven~~ multiple 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 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 ~~eleven~~ policies.

1.2 DOCUMENT NAME AND IDENTIFICATION

…

~~id-fpki-common-public-trusted-serverAuth~~	~~::= {2 16 840 1 101 3 2 1 3 42}~~

Certificates issued to CAs may contain 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 id-fpki-common-deviceHardware, or id-fpki-common-devices~~, or id-fpki-common-public-trusted-serverAuth~~. 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.~~

3.1.1 Types of Names

…

~~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

…

~~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.~~

~~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.

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.~~

4.9.1 Circumstances for Revocation

…

~~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:~~

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

4.9.9 On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 6960] 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~~.

…

~~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.

6.2.1 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.~~

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

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-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-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-public-trusted-serverAuth ::= {2 16 840 1 101 3 2 1 3 42}~~

Certificates that express the id-fpki-common-piv-contentSigning ~~or id-fpki-common-public-trusted-serverAuth~~ policy OID~~s~~ shall not express any other policy OIDs.

9.6.1 CA Representations and Warranties

…

~~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.~~

Estimated Cost: The only cost that may be incurred with this change is for a PKI that had updated their CPS or procedures in anticipation of issuing certificates asserting the common-public-trusted-serverAuth policy, to update their documentation to remove this option, since no CAs have been approved to issue certificates asserting this policy at the current time.

Implementation Date: Immediately upon approval and publication of the updated Common Policy CP.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	7/26/18
Date change released for comment:	7/26/18, 9/24/18, 9/26/18, 10/24/18
Date approved by PA:	12/11/2018