COMMON Certificate Policy Change Proposal Number: 2017-01

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Align COMMON Certificate Policy with certificate profile operational practice
Date: April 14, 2017

Title: Align COMMON Certificate Policy with certificate profile operational practice

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework
Version 1.26, February 2, 2017

Change Advocate's Contact Information:
Name: Darlene Gore
Organization: FPKI Management Authority
Telephone number: 703-306-6109
E-mail address: darlene.gore@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Update the CP and Certificate Profiles to align with current practice for CA certificates

Background:

The FPKIMA has been including PolicyConstraints and InhibitAnyPolicy extensions in CA certificates issued from the Federal Common Policy CA and Federal Bridge CA since 2011, in order to technically constrain CAs in the FPKI eco-system. Due to feedback that not all commonly used relying party applications support these extensions, it was recommended by two of the authors of RFC 5280 that these be marked non-critical rather than following the RFC 5280 recommendation to make them critical.

Additionally, Common Policy only allowed a 3072 bit RSA key for CA certificates that expire after 2030. However, NSA recently recommended that PKIs not yet transitioning to ECC to consider staying with RSA until Quantum Computing resistant algorithms are approved. Some CAs have decided to go with 4096 bit RSA keys for root CAs that had to rekey before the new algorithms are available.

This change proposal documents the current practice in the CP and associated certificate profiles.

Specific Changes:

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

6.1.5 Key Sizes

…

CAs that generate certificates and CRLs under this policy shall use signature keys of 1024, 2048, ~~or~~ 3072, or 4096 bits for RSA and 256 or 384 bits for elliptic curve algorithms. Certificates that expire on or after December 31, 2010 shall be generated with 2048 or 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms. Certificates that expire after December 31, 2030 shall be generated with at least 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms

Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, CAs shall use signature keys of 2048 or 3072 or 4096 bits for RSA and 256 or 384 bits for elliptic curve algorithms to sign certificates issued on or after January 1, 2008. ~~CAs may continue to use 1024 bit RSA keys to sign CRLs that only cover certificates that were signed using 1024 bit RSA keys. CAs may also use 1024 bit RSA keys to sign OCSP responder certificates that expire before December 31, 2010.~~

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension should be marked as noncritical*, to support legacy applications that cannot process policyConstraints. For Subordinate CA certificates inhibitPolicyMappings, skip certs will be set to 0. For cross-certificates inhibitPolicyMappings, skip certs will be set to 1, or 2 for the Federal Bridge CA. When requireExplicitPolicy is included skip certs will be set to 0.

7.1.10 Inhibit Any Policy Extension

The CAs may assert InhibitAnyPolicy in CA certificates. When present, this extension should be marked as noncritical*, to support legacy applications that cannot process InhibitAnyPolicy. Skip Certs shall be set to 0, since certificate policies are required in the Federal PKI.

*Note: The recommended criticality setting is different from RFC 5280.

Modify the associated worksheets in the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program Version 1.7, May 5, 2015* as follows:

Modify the following line in Worksheet 1: Self-Signed Certificate Profile, Worksheet 2: Self-Issued CA Certificate Profile, and Worksheet 3: Cross Certificate Profile

subjectPublicKey		BIT STRING	For RSA public keys, modulus must be 2048, ~~or~~ 3072, or 4096 bits. For elliptic curve public keys, public key must be encoded in uncompressed form.

Add the following lines to Worksheet 3: Cross Certificate Profile

PolicyConstraints	FALSE		When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension should be marked as noncritical*, to support legacy applications that cannot process policyConstraints.
requireExplicitPolicy			
SkipCerts		INTEGER	
inhibitPolicyMapping			Should be included if local policy prohibits policy mapping.
SkipCerts		INTEGER	0 when issued to an SSP, 1 in certs issued to a cross-certified PKI, 2 within the infrastructure to a CA which may issue a cross-certificate to a Bridge
InhibitAnyPolicy	FALSE		This extension should be marked as noncritical*, to support legacy applications that cannot process InhibitAnyPolicy
SkipCerts		INTEGER	0 – specific policies are required in the FPKI

*Note: The recommended criticality setting is different from RFC 5280.

Delta Mapping: Not applicable

Estimated Cost: There should not be a cost associated with this change since this is already how CA Certificates are being issued.

Implementation Date: This change is a clarification and is effective upon approval by the FPKIPA and incorporation into the Common Policy CP.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG: April 14, 2017
Date change released for comment: May 17, 2017
Date comment adjudication published: June 1, 2017