FBCA Certificate Policy Change Proposal Number: 2017-01

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

Title: Align FBCA Certificate Policy with certificate profile operational practice

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)
Version 2.30, October 5, 2016

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.

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

Specific Changes:

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

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 *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, May 5, 2015* and the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Version 1.1, May 5, 2015.*

Add the following lines to Worksheet 3 in the FPKI profiles and Worksheet 2 in the PIV-I profiles:

Worksheet n: 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 FBCA 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