COMMON Certificate Policy Change Proposal Number: 2013-02

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the COMMON Certificate Policy
Date: November 4, 2013

Title: Remove SHA-1 policies from Common Policy

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.21, December 18, 2012

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

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Remove SHA-1 policies from Common Policy CP.

Background: The SHA-1 certificate policies were added to the Common Policy CP as a transition mechanism to allow more time for federal agencies to fully transition off the SHA-1 algorithm. These policies were only to be used by agencies that were not able to meet the NIST guidelines for transitioning to SHA-2 by 12/31/2013.

Although some agencies may still rely on SHA-1 beyond the 12/31/2013 deadline, in order to be very clear that SHA-1 is no longer permitted in support of Personal Identify Verification (PIV) cards and the Federal Common Policy, all mention of SHA-1 certificate policies will be move to the Federal Bridge CP and only permitted via a mapped relationship with the FPKI.

Specific Changes:

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

Forward, 1 Introduction, 2 Document Name and Identification, 1.3.1.3 FPKI Management Authority (FPKIMA), 1.4.1 Appropriate Certificate Uses, 7.1.6 Certificate Policy Object Identifier, and 7.2 CRL Profile

FOREWARD:
… There ~~are two~~ is one Certification Authorit~~ies~~y associated with the Common Policy Framework: The Federal Common Policy Root CA ~~and the SHA-1 Federal Root CA~~.
…

~~For entities associated with the SHA-1 Federal Root CA, subscriber certificates may assert a certificate policy OID that indicates the use of SHA-1, if issued before December 31, 2013. CAs that issue SHA-1 certificates after December 31, 2013 may not also issue SHA-256 certificates.~~

1. INTRODUCTION

The use of SHA-1 to create digital signatures is not allowed under Common Policy after 12/31/2013. ~~deprecated beginning January 1, 2011. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore this CP also includes five additional distinct certificate policies which indicate the use of the deprecated SHA-1 after December 31, 2010. These id-fpki-sha1 policies adhere to all the requirements of the associated id-common policy with the exception that the certificate is generated with a SHA-1 signature and the issuing CA may use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013. It should be noted that certificates issued on or after January 1, 2011 are not FIPS 201 compliant, and therefore do not meet the requirements of HSPD-12. CAs that issue SHA-1 certificates after December 31, 2010 may not also issue FIPS 201 compliant certificates.~~

1.2 DOCUMENT NAME AND IDENTIFICATION

~~Additionally, this CP provides moderate assurance concerning identity of certificate subjects when the following OIDs are expressed in certificate policy extensions of certificates issued after December 31, 2010, associated with the SHA-1 Federal Root CA, and signed using SHA-1.~~

~~*Table 2 – id-fpki-SHA1 Policy OIDs* SHA1 Policy~~	~~OID~~	~~Corresponding id-fpki-common policy~~
~~id-fpki-SHA1-policy~~	~~::= {2 16 840 1 101 3 2 1 3 23}~~	~~id-fpki-common-policy id-fpki-certpcy-mediumAssurance~~
~~id-fpki-SHA1-hardware~~	~~::= {2 16 840 1 101 3 2 1 3 24}~~	~~id-fpki-common-hardware id-fpki-certpcy-mediumHardware~~
~~id-fpki-SHA1-devices~~	~~::= {2 16 840 1 101 3 2 1 3 25}~~	~~id-fpki-common-devices id-fpki-certpcy-mediumAssurance~~
~~id-fpki-SHA1-authentication~~	~~::= {2 16 840 1 101 3 2 1 3 26}~~	~~id-fpki-common-authentication id-fpki-certpcy-mediumHardware~~
~~id-fpki-SHA1-cardAuth~~	~~::= {2 16 840 1 101 3 2 1 3 27}~~	~~id-fpki-common-cardAuth~~

~~The requirements associated with a id-fpki-SHA1 policy are identical to those defined for the corresponding id-fpki-common policy, except that the certificates asserting id-fpki-SHA1-policies are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013.~~

1.3.1.3 FPKI Management Authority (FPKIMA)

The FPKIMA is the organization that operates and maintains the Common Policy Root CA ~~and the SHA-1 Federal Root CA~~ on behalf of the U.S. Government, subject to the direction of the FPKIPA. ~~All of the requirements for the SHA1 Federal Root CA are identical to the Common Policy Root CA except that the SHA-1 Federal Root CA asserts id-fpki-sha1 policies and shall use SHA-1 for generation of PKI objects such as certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses after December 31, 2010 and before December 31, 2013.~~

1.4.1 Appropriate Certificate Uses

~~The digital signatures on certificates issued under this policy may be generated using SHA-1 only when one or more of the id-fpki-SHA1 policy OIDs is used. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of SHA-1 certificates issued under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.~~

7.1.6 Certificate Policy Object Identifier

~~Certificates generated with SHA-1 after December 31, 2010 shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:~~

~~id-fpki-SHA1-policy ::= {2 16 840 1 101 3 2 1 3 23}~~
~~id-fpki-SHA1-hardware ::= {2 16 840 1 101 3 2 1 3 24}~~
~~id-fpki-SHA1-devices ::= {2 16 840 1 101 3 2 1 3 25}~~
~~id-fpki-SHA1-authentication ::= {2 16 840 1 101 3 2 1 3 26}~~
~~id-fpki-SHA1-cardAuth ::= {2 16 840 1 101 3 2 1 3 27}~~

7.2 CRL PROFILE

CRLs issued by a CA under this CP ~~the id-fpki-SHA1-authentication, id-fpki-SHA1-cardAuth, or id-fpki-SHA1-hardware policy~~ shall conform to the CRL profile specified in [CCP-PROF] ~~except that SHA-1WithRSAEncryption may be used as the signature algorithm in CRLs that are issued before January 1, 2014~~.

Delta Mapping: Not Applicable

Estimated Cost:

There is no cost expected to implement this change, since all federal agencies operating strictly under Common Policy should already have transitioned off SHA-1.

Implementation Date: After FPKIPA Approval

Prerequisites for Adoption:

Modification to the FBCA CP to move all required SHA-1 policy definitions to the FBCA CP.

Plan to Meet Prerequisites:

FBCA CP change proposal submitted at the same time.

Approval and Coordination Dates:

Date presented to CPWG:	11/7/2013
Date presented to FPKIPA:	11/17/13
Date of approval by FPKIPA:	12/2/13