FPKIPA
Federal Public Key Infrastructure Policy Authority

FBCA 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 FBCA Certificate Policy
Date: November 4, 2013

Title: Move SHA-1 policies from Common Policy to FBCA and remove 12/31/2013 restriction on all SHA-1 policies

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.26, April 26, 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: Move SHA-1 policy definitions from Common Policy CP to the FBCA CP and remove the 12/31/2013 restriction on the use of all SHA-1 policies.

Background: The SHA-1 certificate policies were added to the Common Policy and FBCA CPs as a transition mechanism to allow more time for federal agencies and other FPKI affiliates to fully transition off the SHA-1 algorithm. These policies were only to be used by those that were not able to meet the NIST guidelines for transitioning to SHA-2 by 12/31/2010.

Some affiliates will rely on SHA-1 beyond the 12/31/2013 deadline. In order to support the FPKI mandate to enable interoperability across the FPKI ecosystem, the FPKIPA has authorized continued operation of the SHA1 FRCA to support continued interoperability. SHA-1 is no longer permitted in support of Personal Identify Verification (PIV) cards and the Federal Common Policy under any circumstance. All mention of SHA-1 certificate policies will be moved to the Federal Bridge CP and only permitted via a mapped relationship with the FPKI.

Specific Changes:

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

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

1. INTRODUCTION

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011 according to NIST SP 800-131. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore, a ~~new~~ parallel SHA-1 FPKI ~~shall be~~ was created to facilitate the interoperability for those unable to transition to SHA-256 by January 1, 2011. Accordingly, this CP additionally defines ~~two~~ five certificate policies for use by the SHA-1 Federal Root Certification Authority (SHA1 Federal Root CA) ~~and allows mapping to additional SHA-1 certificate policies defined in the X.509 U.S. Federal PKI Common Policy Framework Certificate Policy~~ to facilitate interoperability between Federal agencies and other Entity PKI domains that require the use of SHA-1 after December 31, 2010. Use of certificates asserting certificate policy OIDs that identify the use of SHA-1 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 and will only be asserted within the parallel SHA-1 FPKI. CAs that issue SHA-1 end entity certificates after December 31, 2010 shall not also issue SHA-256 certificates, asserting non-SHA-1 policies.

1.2 DOCUMENT IDENTIFICATION

In addition, there are ~~two~~ five certificate policies specified at two different levels of assurance associated with the SHA-1 Federal Root CA. Each level of assurance has an OID to be asserted in certificates issued by the SHA-1 Federal Root CA. Entity Principal CAs may assert these OIDs in policyMappings extensions of certificates issued to the SHA-1 Federal Root CA. The id-fpki-SHA1 policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

Table 1 - Certificate Policy OIDs Identifying the Use of SHA-1

id-fpki-SHA1-medium-CBP	::= { fbca-policies 21 }
id-fpki-SHA1-mediumHW-CBP	::= { fbca-policies 22 }
id-fpki-SHA1-medium	::= { fbca-policies 23 }
id-fpki-SHA1-hardware	::= { fbca-policies 24 }
id-fpki-SHA1-devices	::= { fbca-policies 25 }

…

The requirements associated with id-fpki-SHA1-medium policy are identical to those defined for the FBCA medium policy, except that the certificates asserting id-fpki-SHA1-medium are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.

The requirements associated with id-fpki-SHA1-hardware policy are identical to those defined for the FBCA medium-hardware policy, except that the certificates asserting id-fpki-SHA1-hardware are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.

The requirements associated with id-fpki-SHA1-medium-CBP (commercial best practice) policy are identical to those defined for the FBCA medium-CBP policy, except that the certificates asserting id-fpki-SHA1-medium-CBP 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~~.

The requirements associated with id-fpki-SHA1-mediumHW-CBP (commercial best practice) policy are identical to those defined for the FBCA mediumHW-CBP policy, except that the certificates asserting id-fpki-SHA1-mediumHW-CBP 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~~.

The requirements associated with id-fpki-SHA1-device policy are identical to those defined for the FBCA device policy, except that the certificates asserting id-fpki-SHA1-device are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses.

~~The SHA-1 Federal Root CA also includes the following policy OIDs defined in the X.509 U.S. Federal PKI Common Policy Framework and compatible with the FBCA as follows:~~

~~Table 3 - id-fpki-SHA1 Policy OIDs~~

~~**SHA1 Policy**~~	~~**OID**~~	~~**Corresponding id-fpki-common policy**~~
~~id-fpki-SHA1-policy~~	~~::= { fbca-policies 23 }~~	~~id-fpki-common-policy id-fpki-certpcy-mediumAssurance~~
~~id-fpki-SHA1-hardware~~	~~::= { fbca-policies 24 }~~	~~id-fpki-common-hardware id-fpki-certpcy-mediumHardware~~
~~id-fpki-SHA1-devices~~	~~::= { fbca-policies 25 }~~	~~id-fpki-common-devices id-fpki-certpcy-mediumAssurance~~
~~id-fpki-SHA1-authentication~~	~~::= { fbca-policies 26 }~~	~~id-fpki-common-authentication id-fpki-certpcy-mediumHardware~~
~~id-fpki-SHA1-cardAuth~~	~~::= { fbca-policies 27}~~	~~id-fpki-common-cardAuth~~

1.3.1.3 FPKI Management Authority (FPKIMA)

The FPKIMA is the organization that operates and maintains the FBCA and the SHA1 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 FBCA except that the SHA1 Federal Root CA and entity CAs cross certified with the SHA1 Federal Root CA 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

Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium, Medium CBP. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-medium, id-fpki-SHA1-medium-CBP, and id-fpki-SHA1-devices, level of assurance should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.
PIV-I Card Authentication	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: Medium Hardware, Medium Hardware CBP, PIV-I Hardware, and PIV-I Content Signing. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-hardware, id-fpki-SHA1-mediumHW-CBP level of assurance should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.
High	This level is reserved for cross-certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

6.1.5 Key Sizes

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. For Rudimentary and Basic Assurance, signatures on certificates and CRLs that are issued after

12/31/2013 shall be generated using, at a minimum, SHA-224. For Medium and High Assurance, signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs ~~that are issued~~ ~~on or after January 1, 2012, but before January 1, 2014~~ that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256. For Medium assurance, signatures on certificates and CRLs asserting certificate policy OIDs that identify the use of SHA-1 may be generated using SHA-1 ~~until December 31, 2013~~. CAs that issue end entity certificates that assert non-SHA1 policies ~~generated using, at a minimum, SHA-224~~ after December 31, 2010 must not also issue end entity certificates signed with SHA-1.

Certificates issued to OCSP responders that only include SHA-1 certificates may be signed using SHA-1 ~~until December 31, 2013~~.

Delta Mapping: < need to update mapping tables>

Estimated Cost:

There is no cost expected to implement this change, since Affiliates requiring SHA-1 CAs are already operating these CAs.

Implementation Date: After FPKIPA Approval

Prerequisites for Adoption:

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

Plan to Meet Prerequisites:

Common CP change proposal submitted at the same time.

Approval and Coordination Dates:

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