



FBCA Certificate Policy Change Proposal Number: 2010-07

To: Federal PKI Policy Authority
From: CPWG
Subject: Proposed modifications to the Federal Bridge Certificate Policy
Date: November 5, 2010
Title: Legacy use of SHA-1 during the transition period January 1, 2011 to December 31, 2013

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 2.19, dated 10/15/2010.

Organization requesting change: CPWG

Change summary: This change proposal permits the continued use of SHA-1 to generate signatures on CRLs and OCSP responses that provide status information for certificates whose signatures were generated using SHA-1. It also permits the continued use of SHA-1 at the Rudimentary and Basic Assurance levels and introduces new certificate policy OIDs for certificates signed with SHA-1 at the Medium and Medium Hardware levels of assurance after January 1, 2011

Background: The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information that was signed using SHA-256. This change proposal makes it possible for such applications to accept certificates that were signed before December 31, 2010, using SHA-1 by permitting the certificate status information for such certificates to also be signed using SHA-1.

In addition, certificates issued between January 1, 2011 and December 31, 2014 can be signed using SHA-1 if they use certificate policy OIDs that identify the use of SHA-1.

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.

Specific Changes: Specific changes are made to the following sections:

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

1. INTRODUCTION

Add a new paragraph after the first paragraph in the introduction:

This Certificate Policy (CP) defines ten certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent six different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

The use of SHA-1 to create digital signatures is 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, a new parallel SHA-1 FPKI shall be created to facilitate the interoperability for those unable to transition to SHA-256 by January 1, 2011. Accordingly, this CP additionally defines two 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 may not also issue SHA-256 certificates.

1.2 DOCUMENT IDENTIFICATION

Modify the first paragraph of 1.2 and add a new table, captions to both tables and 2 additional paragraphs at the end:

There are ten policies specified at six different levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FBCA. Entity Principal CAs may assert these OIDs in policyMappings extensions of certificates issued to the FBCA. The FBCA policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

Table 1 FBCA Certificate Policies

csor-certpolicy OBJECT IDENTIFIER	::= { 2 16 840 1 101 3 2 1 }
fbca-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
id-fpki-certpcy-rudimentaryAssurance	::= { fbca-policies 1 }
id-fpki-certpcy-basicAssurance	::= { fbca-policies 2 }
id-fpki-certpcy-mediumAssurance	::= { fbca-policies 3 }
id-fpki-certpcy-mediumHardware	::= { fbca-policies 12 }

id-fpki-certpcy-medium-CBP	::={ fbca-policies 14 }
id-fpki-certpcy-mediumHW-CBP	::={ fbca-policies 15 }
id-fpki-certpcy-highAssurance	::= { fbca-policies 4 }
id-fpki-certpcy-pivi-hardware	::= { fbca-policies 18 }
id-fpki-certpcy-pivi-cardAuth	::= { fbca-policies 19 }
id-fpki-certpcy-pivi-contentSigning	::= { fbca-policies 20 }

In addition, there are two 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

<u>id-fpki-SHA1-medium-CBP</u>	<u>::= {TBD}</u>
<u>id-fpki-SHA1-mediumHW-CBP</u>	<u>::= {TBD}</u>

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 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

<u>SHA1 Policy</u>	<u>OID</u>	<u>Corresponding id-fpki-common policy</u>
<u>id-fpki-SHA1-policy</u>	<u>::= {TBD}</u>	id-fpki-common-policy id-fpki-certpcy-mediumAssurance
<u>id-fpki-SHA1-hardware</u>	<u>::= {TBD}</u>	id-fpki-common-hardware id-fpki-certpcy-mediumHardware

<u>id-fpki-SHA1-devices</u>	::= {TBD}	id-fpki-common-devices id-fpki-certpcy-mediumAssurance
<u>id-fpki-SHA1-authentication</u>	::= {TBD}	id-fpki-common-authentication id-fpki-certpcy-mediumHardware
<u>id-fpki-SHA1-cardAuth</u>	::= {TBD}	id-fpki-common-cardAuth

1.3.1.3 FPKI Management Authority (FPKI MA)

Modify 1.3.1.3 as follows:

The FPKI Management Authority is the organization that operates and maintains the FBCA and 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

Modify the table in Section 1.4.1 as follows:

Medium	<p>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.</p> <p><u>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-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.</u></p>
Medium Hardware	<p>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.</p> <p><u>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-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</u></p>

acceptable.

6.1.5 Key Sizes

Modify the fourth and fifth paragraphs of Section 6.1.5 and add an additional paragraph as follows:

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 generated using, at a minimum, SHA 224 after December 31, 2010 must not issue end entity certificates signed with SHA 1.

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

Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, for Medium and High Assurance, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).

7.1.6 Certificate Policy Object Identifier

Modify 7.1.6 as follows:

All certificates issued by the FBCA or SHA 1 Federal Root CA shall include a certificate policies extension asserting the OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs.

~~For Entity CAs, no stipulation.~~

Entity CAs that do not meet the SHA-2 requirements may assert a certificate policy OID that maps to the appropriate SHA-1 Federal Root CA SHA-1 OID for all certificates generated using SHA-1 after December 31, 2010. When an Entity CA subsequently meets the SHA-2 requirements, the Entity CA shall assert OIDs that can be differentiated from the SHA-1 issued OIDs and map to the appropriate FBCA OID.

Estimated Cost:

The FPKI MA will incur the costs for establishing the new parallel SHA1 Federal Root CA.

Federal Agencies unable to transition to SHA-256 by January 1, 2011 may incur the costs for establishing one or more new SHA-1 parallel CAs.

Risk/Impact:

The use of SHA-1 to create digital signatures will be deprecated beginning on January 1, 2011, due to the risk of collision attacks. While this is a significant concern for certificates, where the applicant, who may be untrusted, may provide some of the information that will be placed in a certificate, this is less of a concern when all of the information to be signed is created by a trusted entity without input from any untrusted source. For this reason the risk of collision attacks against CRLs are considered to be less significant than for certificates. OCSP responders may either generate a fresh response for each OCSP request or may pre-produce signed responses and only provide these cached responses in response to OCSP requests. If the OCSP responder creates a fresh response for each request that is tailored to the request, then there is a risk that the untrusted client may have crafted the request in such a way as to create a collision in the response. If the OCSP responder only provides pre-produced signed responses, then this possibility is eliminated since the client's request cannot influence the contents of the signed response.

At the Rudimentary Assurance level, the risk of malicious activity is considered to be low. Similarly, at the Basic Assurance level, the risks and consequences of data compromised are not considered to be of major significance. Therefore, at these assurance levels, the risks associated with using a deprecated cryptographic algorithm are considered to be acceptable.

Federal agencies and other members of the FPKI community have identified critical applications that are unable to support the use of PKI objects generated with SHA-256 signatures by January 1, 2011. These organizations may determine the risk of continued use of the deprecated SHA-1 is outweighed by the known risk of disruption of services which will be caused by transitioning to SHA-256 at this time.

Implementation Date:

This change will be effective immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	November 5, 2010
Date presented to FPKIPA:	November 9, 2010
Date of approval by FPKIPA:	TBD