FBCA Policy Change Proposal Number: 2007-05

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the Federal Bridge Certificate Policy
Date:	July 17, 2007
Title:	Alignment of Cryptographic Algorithm Requirements with SP 800-78-1

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.6, August 16, 2007.

Change Advocate's Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: tim.polk@nist.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: In order to maintain alignment between the Common Policy and the FBCA CP and in order to allow members of the Federal PKI other than Shared Service Providers to take advantage of the additional flexibility allowed by SP 800-78-1, the FPKIPA is requesting the following changes: 1) allow for the use of SHA-1 to sign certificates and CRLs for an additional two years and 2) allow digital signature certificates that are only used for authentication to include 1024 bit RSA subject public keys for an additional three years.

Background: SP 800-78-1 allows for the continued use of SHA-1 and 1024 bit RSA subscriber keys beyond the period currently allowed by the FBCA CP. SP 800-78-1 permits this extra time in order to address concerns that several Federal agencies have about moving to SHA-256 and 2048 bit RSA keys too soon. The changes in this change proposal are required in order to allow members of the Federal PKI other than Shared Service Providers to take advantage of the extra time allowed by SP 800-78-1.

Specific Changes: Specific changes are made to the following section: 6.1.5

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

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/2010 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA.

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. Signatures on certificates and CRLs that are issued after ~~12/31/08 and expire after~~ 12/31/2010 shall be generated using, at a minimum, SHA-224.

Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates ~~that expire before 12/31/10~~ shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.
- End-entity certificates that do not include a keyUsage extension or that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit that expire on or after 12/31/2010 shall contain public keys that are at least 2048 bits for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010.

Estimated Cost:

No cost to the Federal Bridge CA.

Risk/Impact:

This change proposal extends the period of use for SHA-1 when signing certificates and CRLs. This change proposal also extends the period of use for 1024 bit RSA for end users. NIST and other cryptographic experts have determined that the additional risk imposed by extending the period of use for SHA-1 and RSA 1024 is minimal, and is outweighed by the positive impact on interoperability.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Bridge Certificate Policy.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 17 July 2007
Date Presented to FPKI PA 14 August 2007
Date of approval by FPKI PA: 25 September 2007