FBCA Policy Change Proposal Number: 2008-01

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Federal Bridge Certificate Policy

Date: January 11, 2008

Title: Alignment of Cryptographic Algorithm Requirements with NIST Special Publication 800-57

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.7, September 26, 2007

Change Advocate's Contact Information:

Name: Morris Hymes
Organization: DoD
Telephone number**:** 410-854-4900
E-mail address**:** mahyme1@missi.ncsc.mil

Organization requesting change: Department of Defense

Change summary: In order to ease the migration path for legacy PKIs, the language of this section has been modified to conform to NIST Special Publication 800-57. The final deadline for the implementation of stronger algorithms to be used operationally has not changed. The method of transiting to stronger algorithms is not specified to allow a greater flexibility for legacy PKIs to use in order to meet this requirement. There is the assurance of meeting the final end date of 12/31/2010 through the use of the cross-certificate.

Background: NIST Special Publication 800-57 allows for the continued use of SHA-1 and 1024 bit RSA subscriber keys beyond the period currently allowed by the FBCA CP. NIST Special Publication 800-57 permits this extra time in order to address concerns that legacy PKIs 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 NIST Special Publication 800-57.

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. Those CAs that distribute self-signed certificates and whose key pairs were generated before September 13, 2005 may be 1024 bits for RSA.

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.~~ Beginning 01/01/2011, all valid certificates shall be signed with keys of at least 2048 bits for RSA 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 12/31/2010 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 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.

- Beginning 01/01/2011, all valid e~~E~~nd-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, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

The FBCA shall not issue a cross-certificate with a validity period extending beyond 12/31/2010 to any Entity Principal CA unless all of the following conditions apply:

- Certificates that expire after 12/31/2010 are signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA.

- End-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

- End-entity certificates that do not include a keyUsage extension that expire on or after 12/31/2010 contain public keys that are at least 2048 bits for RSA, DSA, 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:

Certificate caching, CRL caching, and latency times of legacy PKIs may extend the use of certificate and CRLs until the cache is refreshed. These times are typically in the range of hours to days. Implementing the stronger algorithms before the required date and the maximum caching and latency times would minimize the additional risk of applications not using the most recent certificate.

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: 15 January 2008
Date Presented to FPKI PA: 12 February 2008
Date of approval by FPKI PA: 12 February 2008