



FBCA Certificate Policy Change Proposal Number: 2009-02

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modification to the FBCA CP
Date: 5 March 2009

Title: Change to the FBCA CP to align key length requirements with SP 800-57

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for Federal Bridge Certificate Authority (FBCA), Version 2.12, February 11, 2009

Change Advocates Contact Information:

David Cooper, NIST
david.cooper@nist.gov

Organization requesting change: NIST

Background: Part 1 of NIST Special Publication 800-57, Recommendation for Key Management, imposes stronger cryptographic requirements than are currently required by the FBCA CP for keys with lifetimes that extend beyond 2030. This change proposal aligns the FBCA CP with SP 800-57.

Change summary: This change proposal imposes stronger cryptographic requirements for key pairs that may be used after December 31, 2030.

Specific Changes: Specific changes are made to Section 6.1.5, as shown below. Text with ~~strikethrough~~ will be removed. Underlined text will be added.

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. Public keys in all self-signed certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA, or at least 256 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. 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. All certificates, except self-signed certificates, that expire after 12/31/2030 shall be signed with keys of at least 3072 bits for RSA or at least 256 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. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

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 expire after 12/31/2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.
- 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 end-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit 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, other than self-signed certificates, that expire after 12/31/2030 are signed with keys of at least 3072 bits for RSA or at least 256 bits for ECDSA.
- 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. 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 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

Estimated Cost:

There is no financial cost associated with implementing this change.

Risk/Impact:

Low risk – the impact of this change is to strengthen the cryptographic requirements in the FBCA CP. Since Section 6.3.2 of the FBCA CP does not permit any keys to be used for more than 20 years, this change will have no impact on any existing CAs until 01/01/2011 at the earliest.

Implementation Date:

This change will be implemented 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: October 20, 2009

Date presented to FPKI PA: November 10, 2009

Date of approval by FPKI PA: December 8, 2009