



Federal Common Policy Change Proposal Number: 2010-01

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modification to the FCPF CP
Date: 4 December 2009

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

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FCPF), Version 3647 1.7, April 15, 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 FCPF CP for keys with lifetimes that extend beyond 2030. This change proposal aligns the FCPF CP with SP 800-57. This change proposal also aligns the FCPF CP with FIPS 186-3, which specifies only three choices for modulus lengths for RSA: 1024, 2048, and 3072.

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

This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.
--

Trusted Certificates that expire before January 1, 2031 shall contain subject public keys of at least 2048 or 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key. Trusted Certificates that expire on or after January 1, 2031 shall contain subject public keys of 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024, 2048, or 3072 bits for RSA and 256 or 384 bits for elliptic curve algorithms. Certificates that expire on or after December 31, 2010 shall be generated with at least 2048 or 3072 bit keys for RSA and at least 256 or 384 bit keys for elliptic curve algorithms. Certificates that expire after December 31, 2030 shall be generated with 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms.

Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, CAs shall use signature keys of <u>at least 2048 or 3072 bits for RSA and 256 or 384 bits for elliptic curve algorithms to sign certificates issued on or after January 1, 2008. CAs may continue to use 1024 bit RSA keys to sign CRLs that only cover certificates that were signed using 1024 bit RSA keys. CAs may also use 1024 bit RSA keys to sign OCSP responder certificates that expire before December 31, 2010.</u>
--

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that are issued after December 31, 2010 shall be generated using SHA-256. ECDSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-256 or SHA-384, as appropriate for the key length.

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

End entity certificates issued under id-fpki-common-devices that expire before December 31, 2010 shall contain RSA public keys that are at least 1024, 2048, or 3072 bits in length or elliptic curve keys that are at least 256 or 384 bits. End entity certificates issued under id-fpki-common-devices that expire on or after December 31, 2010 shall contain RSA public keys that are at least 2048 or 3072 bits or elliptic curve keys that are at least 256 or 384 bits. End entity certificates issued under id-fpki-common-devices that expire after December 31, 2030 shall contain RSA public keys that are 3072 bits or elliptic curve keys that are 256 or 384 bits.

End entity certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth that expire before January 1, 2014 shall contain RSA public keys that are 1024 or 2048 bits in length or elliptic curve keys that are 256 bits. End entity certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth that expire on or after January 1, 2014 shall contain RSA public keys that are 2048 bits in length or elliptic curve keys that are 256 bits.

~~End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire before December 31, 2008 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 256 bits. End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire on or after December 31, 2008 shall contain RSA public keys that are at least 2048 or 3072 bits or elliptic curve keys that are at least 256 or 384 bits.~~

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require (1) triple-DES or AES for the symmetric key through December 31, 2010 and AES for the symmetric key after December 31, 2010 and (2) at least 1024 bit RSA or 163 bit elliptic curve keys through December 31, 2008, ~~and~~ at least 2048 bit RSA or 224 bit elliptic curve keys after December 31, 2008, and 3072 bit RSA or at least 256 bit elliptic curve keys after December 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 FCPF CP. Since Section 6.3.2 of the FCPF CP limits the Common Policy Root CA key pair to 20 years, this change will have no impact on the Common Policy Root CA until 01/01/2011 at the earliest. Since Section 6.3.2 of the FCPF CP limits all other key pairs to lifetimes of 10 years or less, this change will have no impact any other CA other than the Common Policy Root CA until 01/01/2021 at the earliest.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FCPF CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: December 14, 2009

Date presented to FPKI PA: January 12, 2010

Date of approval by FPKI PA: January 12, 2010