Common Policy Change Proposal Number: 2007-01

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the Common 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 U.S. Federal PKI Common Policy Framework, Version 3647 – 1.0, May 8, 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: To bring the Common Policy CP into alignment with the newly-issued NIST SP 800-78-1, the FPKIPA is requesting the following changes: 1) allow the use of SHA-1 to sign certificates and CRLs that are issued on or before December 31, 2010 rather than precluding use of SHA-1 to sign certificates and CRLs that expire after December 31, 2010; 2) extend the period of time for which subscriber RSA authentication keys may be 1024 bits until December 31, 2013. This change proposal also adds a sentence to section 1.2 clarifying that id-fpki-common-authentication and id-fpki-common-cardAuth may only be asserted in certificates that are issued in accordance with FIPS 201.

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 Common Policy. 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 customers of Shared Service Providers to take advantage of the extra time allowed by SP 800-78-1 while still maintaining conformance to the Common Policy.

Specific Changes: Specific changes are made to the following sections: foreword, 1.2, 6.1.5

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

FOREWORD

Modify the fifth paragraph of the Foreword as follows:

This policy framework requires the use of either 2048 bit RSA keys or 224 bit elliptic curve keys along with the SHA-224, SHA-256, and SHA-384 hash algorithms. CAs are required to use 2048 bit RSA keys or 224 bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2010. CAs are required to use SHA-224, SHA-256, or SHA-384 when signing certificates and CRLs that ~~expire on or~~ are issued after December 31, 2010. All subscriber signature keys in certificates that expire on or after December 31, 2008 must be at least 2048 bit RSA keys or 224 bit elliptic curve keys. Subscriber authentication keys in certificates that expire on or after December 31, 201~~0~~3 must be at least 2048 bit RSA keys or ~~224~~256 bit elliptic curve keys.

1.2 DOCUMENT NAME AND IDENTIFICATION

Modify the final paragraph of section 1.2 as follows:

This document includes two policies specific to the FIPS 201 Personal Identity Verification Card. Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth.

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 shall contain subject public keys of at least 2048 bits for RSA or 224 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 bits for RSA and 163 bits for elliptic curve algorithms. Certificates that expire on or after December 31, 2010 shall be generated with at least 2048 bit keys for RSA and at least 224 bit keys for elliptic curve algorithms.

> Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, CAs shall use signature keys of at least 2048 bits for RSA and 256 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.

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-224, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that ~~expire on or~~ 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-224, 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-authentication, id-fpki-common-cardAuth, and~~ id-fpki-common-devices that expire before December 31, 2010 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under ~~id-fpki-common-authentication, id-fpki-common-cardAuth, and~~ id-fpki-common-devices that expire on or after December 31, 2010 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 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 at least 1024 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 at least 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 163 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 bits or elliptic curve keys that are at least 224 bits.

Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, implementations are limited to SHA-256 and SHA-384 for ECDSA.

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 12/31/2010 and AES for the symmetric key after 12/31/2010 and (2) at least 1024 bit RSA or 163 bit elliptic curve keys through 12/31/2008 and at least 2048 bit RSA or 224 bit elliptic curve keys after 12/31/2008.

Estimated Cost:

No cost to the Common Policy Root 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 Common 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: 14 August 2007