Common Policy Change Proposal

Change Number: 2005-02

To: Federal PKI Policy Authority

From: FIPS 201 Development Team

Subject: Proposed modifications to the Common Certificate Policy

Date: 21 March 2005

Title: Common Policy Modifications to Support FIPS 201

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Common Policy Framework Version 2.1, 9 February 2005.

Change Advocates Contact Information:

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

Organization requesting change: FIPS 201 Development Team

Change summary: The FIPS 201 Development Team is proposing changes in the Common Policy to support deployment of FIPS 201 compliant identity credentials.

Background: this issue was identified by several reviewers during the FIPS 201 Public Comment Period.

Issue

Elliptic Curve Cryptography (ECC) is particularly attractive when implemented on devices with limited power and computing capability. Agencies have indicated a desire to use ECC to satisfy the requirements defined in FIPS Pub 201 to meet HSPD #12. While ECC algorithms are FIPS Approved, the Common Policy currently is limited to the RSA cryptographic algorithm. By adding policy OIDs for ECC keys and ECDSA signatures, the Common Policy can meet this agency identified requirement. To promote interoperability, the Common Policy should limit the EC parameters associated with the subject public keys to the NIST-approved curves with key sizes up to 283 bits.

Specific Changes:

Specific changes are made to the foreword, section 6.1.5, and section 7.1.3. Insertions are in *italics*, deletions are in ~~strikethrough~~.

FOREWORD

Modify paragraph 5 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* and the SHA-256 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, 2008. CAs are required to use *SHA-224 or* SHA-256 when signing certificates and CRLs issued on or after January 1, 2009. All subscriber 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*.

6.1.5 Key Sizes and Signature Algorithms

This CP requires use of RSA PKCS#1 *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 January 1, 2009 shall be generated with at least 2048 bit keys *for RSA and 224 bit keys for elliptic curve algorithms*.

CAs that generate certificates and CRLs under this policy shall use *the* SHA-1, *SHA-224,* or SHA-256 hash algorithm when generating digital signatures. *RSA PKCS #1 s*ignatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1. *RSA PKCS #1* signatures on certificates and CRLs that are issued on or after January 1, 2009 shall be generated using SHA-256. *ECDSA signatures on certificates and CRLs shall be generated using the appropriate hash algorithm for the key length*.

End entity certificates that expire before January 1, 2009 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 that expire on or after January 1, 2009 shall contain RSA public keys that are at least 2048 bits *or elliptic curve keys that are at least 224 bits.*

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 163 bit elliptic curve keys* ~~or equivalent for the asymmetric keys~~ through 12/31/08. 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 224 bit elliptic curve keys* ~~equivalent for the asymmetric keys~~ after 12/31/08.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA1	*{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1}*
ecdsa-with-SHA224	*{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}*
ecdsa-with-SH256	*{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}*

Certificates issued under this CP shall use the following OID to identify the algorithm associated with the subject key:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	*{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(1) 1}*

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	*{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }*
ansit163k1	*{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }*
ansit163r2	*{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }*
ansip224r1	*{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }*
ansit233k1	*{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }*
ansit233r1	*{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }*
ansip256r1	*{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }*
ansit283k1	*{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }*

Specific Changes: Modified sections are reproduced below in their entirety; *insertions are in italics*. No text was deleted in these changes.

Estimated Cost:

No cost.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to FIPS 201 Development Team:	23 December 2004
Date FIPS 201 Team recommended approval:	10 January 2005
Date presented to CPWG:	1 March 2005
Date Presented to FPKI PA:	8 March 2005
Date of approval by FPKI PA:	8 March 2005