FPKIPA
Federal Public Key Infrastructure Policy Authority

Common Policy Change Proposal Number: 2007-03

To: **Federal PKI Policy Authority**

From: Certificate Policy Working Group

Subject: Proposed modifications to the Common Certificate Policy

Date: October 16, 2007

Title: Accommodating legacy PKIs for PIV Authentication

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 – 1.2, October 4, 2007.

Change Advocate's Contact Information:

Name: Judith Spencer
Organization: GSA
Telephone number: 202-208-6576
E-mail address: judith.spencer@gsa.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: This change proposal incorporates provisions specifically to ensure legacy PKIs can issue PIV Authentication certificates beyond January 1, 2008. In addition, this change proposal eliminates certain options that are not available to Shared Service Providers or to other CAs issuing certificates under FIPS 201.

Background: FIPS 201 section 5.4.4 specifically requires legacy PKIs to begin asserting id-fpki-common-authentication in PIV Authentication certificates beginning January 1, 2008. NIST is preparing a change to FIPS 201 that may delete this requirement, however, such change will not become effective prior to January 1, 2008. Therefore, provision must be made to ensure that legacy PKIs can continue to issue PIV Authentication credentials without falling afoul of FIPS 201.

Specific Changes: Specific changes are made to the following sections: Foreword, 3.1.1, 4.9.7, 4.9.9, 4.9.12, 6.1.5, 7.1, 7.1.2, 7.1.3, 10

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~~256 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~~256 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 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~~256 bit elliptic curve keys. Subscriber authentication keys in certificates that expire on or after December 31, 2013 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys.

3.1.1 Types of Names

Modify the second and third paragraphs of section 3.1.1 as follows:

All geo-political distinguished names assigned to federal employees shall be in ~~one of~~ the following directory information tree~~s~~:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]
- ~~C=US, [o=*department*], [ou=*agency*], [ou=*structural container*]~~

~~New implementations shall assign names in the following directory tree:~~

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]~~

Delete the ninth paragraph of section 3.1.1 as follows:

~~Legacy implementations that predate this policy may use the directory tree:~~

- ~~C=US, [o=*department*], [ou=*agency*], [ou=*structural container*]~~

Modify the second to last paragraph of section 3.1.1 as follows:

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is mandatory. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, ~~D~~distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201-1]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

CAs operating as part of the Shared Service Providers program that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). For legacy Federal PKIs only, CAs that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 31 days, and the *nextUpdate* time in the CRL may be no later than 32 days after issuance time (i.e., the *thisUpdate* time).

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every ~~24~~18 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.9 On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

Where on-line status checking is supported, status information must be updated and available to relying parties within ~~24~~18 hours of certificate revocation.

Where on-line status checking is supported and a certificate issued under id-fpki-common-High is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours.

Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

4.9.12 Special Requirements Related To Key Compromise

When a CA certificate is revoked ~~or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key,~~ a CRL must be issued within 18 hours of notification.

When a CA certificate issued under id-fpki-common-High is revoked or subscriber certificate issued under id-fpki-common-High is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.

5.1.8 Off-Site Backup

Full system backups sufficient to recover from system failure shall be made on a periodic schedule, and described in a CA’s CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

For legacy Federal PKIs operating an offline CA, the full system backup shall be performed each time the system is turned on or once a week, whichever is less frequent.

Requirements for CA private key backup are specified in section 6.2.4.1.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a CA’s private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

The CA’s signing key shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA’s certificate that it has been changed. ~~CAs~~ When a CA that distributes self-signed certificates updates its private signature key, the CA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

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~~256 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~~256 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~~256 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 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-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~~256 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 bits or elliptic curve keys that are at least ~~224~~256 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 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 ~~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~~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 bits or elliptic curve keys that are at least ~~224~~256 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 12/31/10 and AES for the symmetric key after 12/31/10 and (2) at least 1024 bit RSA or 163 bit elliptic curve keys through 12/31/08 and at least 2048 bit RSA or 224 bit elliptic curve keys after 12/31/08.

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to ~~either the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile [FPKI-PROF] or~~ the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF].~~ Certificates issued under this policy by a CA operating as part of the Shared Service Providers program shall conform to [CCP-PROF].~~

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [CCP-PROF]~~ and [FPKI-PROF]~~.

7.1.3 Algorithm Object Identifiers

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

sha-1WithRSAEncryption	{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}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
~~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-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045)

	signatures(4) ecdsa-with-SHA2(3) 3}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID shall be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs 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(2) 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}~~
~~ansit283r1~~	~~{iso(1) identified-organization(3) certicom(132) curve(0) 17}~~
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

10. Bibliography

Delete the following bibliography entry:

~~FPKI-PROF~~ ~~Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.~~
http://www.cio.gov/fpkipa/documents/fpki_certificate_profile.pdf

12. Glossary

Add the following Glossary entry:

Legacy Federal PKI A PKI Implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005.

Estimated Cost:

No cost to the Common Policy Root CA.

Risk/Impact:

This change would not lower the assurance level of any certificates issued under the Common Policy.

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:	October 16, 2007
Date presented to FPKI PA:	December 11, 2007
Date of approval by FPKI PA:	December 11, 2007