E-Governance CA Certificate Policy Change Proposal Number: 2007-01

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the E-Governance CA 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 E-Governance Certification Authorities, Version 1.3, November 9, 2005.

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: This change proposal allows for the continued use of SHA-1 to sign certificates and CRLs for an additional two years and allows for the continued use of 1024 bit RSA subject public keys for an additional two years. This change proposal also aligns the requirements for the use of TLS with the requirements in the Common Policy by allowing for the use of triple-DES for an additional two years.

Background: 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 allow the e-Governance CAs to take advantage of this additional flexibility.

Specific Changes: Specific changes are made to the following sections:

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

6.1.5 Key Sizes and Signature Algorithms

This CP requires use of RSA PKCS#1 signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys. [Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.]

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bit keys.

CAs that generate certificates and CRLs under this policy shall use SHA-1, or SHA-256 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued before January 1, 20~~09~~11 shall be generated using SHA-1 or SHA-256. Signatures on certificates and CRLs that are issued on or after January 1, 20~~09~~11 shall be generated using SHA-256.

End entity certificates that expire before January 1, 2011~~09~~ shall contain RSA public keys that are at least 1024 bits in length. End entity certificates that expire on or after January 1, 2011~~09~~ shall contain RSA public keys that are at least 2048 bits.

Use of TLS or another protocol providing similar security to accomplish certificate issuance or 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. ~~at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. 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 equivalent for the asymmetric keys after 12/31/08.~~

Estimated Cost:

No cost to the E-Governance CAs.

Risk/Impact:

This change proposal extends the period of use for SHA-1 when signing certificates and CRLs, and the use of Triple-DES in certificate management protocols. 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, Triple-DES, 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 E-Governance CA 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