E-Governance CA Certificate Policy Change Proposal

Change Number: *2005-01*

To: Federal PKI Policy Authority (FPKIPA)
From: FPKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the E-Governance CA CP
Date: 22 June 2005

Title: Change in Certificate Profile specified for Self-Signed Certificates

Version and Date of Certificate Policy Requested to be changed:
X.509 Certificate Policy For The E-Governance Certification Authorities, 29 September 2004.

Change Advocates Contact Information:
Name: **David Cooper**
Organization: **NIST**
Telephone number: **(301) 975-3194**
E-mail address: **david.cooper@nist.gov**

Organization requesting change: Federal PKI Architecture Operational Authority (FPKIA OA)

Change summary: The CPWG proposes changes to the E-Governance CAs Certificate Policy (CP) to specify that self-signed certificates be generated in conformance with the Self-Signed Certificate Profile in [CCP-PROF] rather than the Self-Issued CA Certificate Profile.

Background: The E-Governance CAs Certificate Policy (CP) states that CA certificates should be issued in conformance with the Self-Issued CA Certificate Profile from the *X.509 Certificate and CRL Extensions Profile for the Common Policy* [CCP-PROF], however this profile should only be used for key rollover certificates, not the self-signed certificates that will be issued to enable the distribution of trust anchor information.

Specific Changes:
Specific recommended changes are to the Section 7.1. Deleted text is shown with strikethrough; inserted text is underlined:

7.1 CERTIFICATE PROFILE

Certificates issued by a CA under this policy shall conform to the Common CP Certificate Profile [CCP-PROF], except as specified below. ~~with the exception of the~~

~~policy OIDs. Policy OIDs for certificates issued under this policy are specified below in Section 7.1.6.~~ Subscriber certificates shall conform to the Certificate Profile for Computing and Communication Devices in [CCP-PROF], except that the certificatePolicies extension shall assert one of the policies specified in Section 7.1.6 instead of id-fpki-common-devices and the LDAP URI in the authorityInfoAccess extension does not need to specify the crossCertificatePair attribute. Self-Signed certificates shall conform to the Self-Signed Certificate Profile in [CCP-PROF], except that the subjectInfoAccess extension does not need to be included. CA certificates that are not self-signed shall conform to the Self-Issued CA Certificate Profile in [CCP-PROF], except that the certificatePolicies extension shall assert one of the policies specified in Section 7.1.6 instead of the OIDs from the Common Certificate Policy and the authorityInfoAccess and subjectInfoAccess extensions do not need to be included.

Estimated Cost:
There is no financial cost associated with implementing this change.

Implementation Date:
This change will be implemented immediately.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	**28 July 2005**
Date CPWG recommended approval:	**28 July 2005**
Date Presented to FPKI PA:	**13 September 2005**
Date of approval by FPKI PA:	**13 September 2005**