**E-Governance CA Certificate Policy Change Proposal**

**Change Number:** 2005-02

**To:** Federal PKI Policy Authority  
**From:** FPKI Certificate Policy Working Group  
**Subject:** Proposed modifications to the E-Governance CA CP  
**Date:** 20 September 2005

---

**Title:** Modify the E-Governance CA CP to permit centrally generated key pairs for agency application servers.

**Version and Date of Certificate Policy Requested to be changed:**  

**Change Advocates Contact Information:**  
**Name:** Tim Polk  
**Organization:** NIST  
**Telephone number:** (301) 975-3348  
**E-mail address:** tim.polk@nist.gov

**Name:** John Cornell  
**Organization:** GSA  
**Telephone number:** (202) 501-1598  
**E-mail address:** john.cornell@gsa.gov

**Organization requesting change:** CPWG

---

**Change summary:**
To allow the E-Governance CA to generate keys on behalf of the agency applications.

**Background:** The FPKI OA requested this change proposal to accommodate agencies whose application servers cannot generate acceptable certificate requests.

**Specific Change:**
Make the following changes in Section 6.1.2 and 6.1.2. Insert text is shown in *italics*; deleted text is shown with *strikethrough*.

### 6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation is performed by the subscriber.
Where the subscriber is an agency application server, either the subscriber or an e-Governance CA shall generate the subscriber key pair. In all other cases, the subscriber shall perform their own key pair generation.

Key generation shall be performed using a FIPS approved method.

### 6.1.2 Private Key Delivery to Subscriber

Subscribers generate their own key pairs; there is no need to deliver private keys, and this section does not apply.

*If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.*

*Where the Subscriber is an agency application server and an e-Governance CA generates the key pair, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. The e-Governance CA shall not retain any copy of the key after delivery of the private key to the Subscriber. The Subscriber shall acknowledge receipt of the private key(s).*

**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: **20 September 2005**
- Date CPWG recommended approval: **20 September 2005**
- Date Presented to FPKI PA: **21 September 2005**
- Date of approval by FPKI PA: **23 September 2005**