

Federal Bridge CA Certificate Policy Change Proposal

Change Serial Number: 2001-11

Title: Requirements for Agency CA key generation

Date: 05 November 2001

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 14 June 2001

Change Advocate Contact Information:

Name: Mike Jenkins
Organization: DoD
Telephone number:
E-mail address: mjjenki@missi.ncsc.mil

Organization requesting change: CPWG

Change summary: Adds requirements for auditable evidence that documented procedures were followed during Agency CA key generation.

Background:

The CP currently that Agency CA private keys are generated in cryptographic modules of a particular FIPS 140-1 level. However, generation of private keys on such a cryptographic module generally requires a procedure to be performed, involving key components held by several individuals. This procedure is usually described by the cryptographic module vendor in its documentation, and is specific to the module. Following this process carefully, including separation of the key components and proper storage and destruction of those components, is as important as the assurance of the cryptographic module itself.

In order for an auditor to verify in the future that the key generation process was followed, it is proposed that text be added to Section 6.1.1 to require that the process be documented (in the CA CPS), and that auditable evidence be generated. For Medium and High levels of assurance, this latter would require the presence of a third, independent party.

Specific Changes:

Existing text:

Section 6.1.1, FBCA and CA key pair generation:

Cryptographic keying material for certificates issued by the FBCA or Agency CAs shall be generated in FIPS 140 validated cryptographic modules. For the FBCA, the modules shall meet or exceed Security Level 3. For Agency CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic or Medium), or Security Level 3 (for High). Requirements for Test Assurance shall be set forth in the MOA.

Proposed revised text:

Append to the existing text in Section 6.1.1:

The FBCA and Agency CAs must document their key generation procedure in their CPSs, and generate auditable evidence that the documented procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used. For High and Medium Assurance, the process shall be validated by an independent third party.

Estimated Cost:

Assuming that the Agency CAs are already following vendor procedures for installing their hardware cryptographic modules, there should be very little cost associated with generating the auditable evidence. At the High and Medium levels, ensuring the presence of an independent third party may incur cost; however, organizational independence is recognized (e.g., an IG).

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: 05 November 2001

Date CPWG recommended approval: 05 November 2001

Date Presented to FPKI PA:

Date of approval by FPKI PA: