Federal Bridge CA Certificate Policy
Change Proposal

Change Serial Number: 2001-06

Title: Clarify cryptographic module standard requirement

Date: 23 October 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: See Background

Background:
The CP currently requires cryptographic modules to be validated to the "latest version of FIPS 140 series". This creates a moving requirement, and one that is impossible to achieve.

Revisions of FIPS 140 do not "grandfather" older validations to the new standard (that is, a cryptomodule recently validated to the -1 version is not considered validated to the -2 version). Even when the new version of the FIPS has been published, validations cannot commence until supporting documentation is available, such as the *Derived Test Requirements*.The validations themselves take time, on the order of months. Thus, the current wording would invalidate all PKIs based on this CP as soon as a new version of FIPS 140 is published, and no valid PKI could be installed until valid cryptomodules became available. Only the specific version of FIPS 140 for which validated cryptomodules are available should be referenced. This is currently FIPS 140-1 (in spite of the fact that -2 has been published).

While it would be prudent to put a sunset clause on when new PKIs could be installed using the old FIPS 140 version, our ability to predict the availability of cryptomodules that will have been validated to the new version is poor. Therefore, it is proposed that no future date be given for use of the the new

version, but that a new change proposal be submitted when sufficient cryptomodules have been validated to the new version to make such a requirement possible to meet.

Specific Changes:

Existing text:

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Federal PKI Policy Authority. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level identified in this section, or validated, certified, or verified to requirements published by the Federal PKI Policy Authority. Additionally, the FEDERAL PKI Policy Authority reserves the right to review technical documentation associated with any cryptomodules under consideration for use by the FBCA.

Proposed revised text:

The relevant standard for cryptographic modules is FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*. The Federal PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Federal PKI Policy Authority. Cryptographic modules shall be validated to the FIPS 140-1 level identified in this section, or validated, certified, or verified to requirements published by the Federal PKI Policy Authority. Additionally, the FEDERAL PKI Policy Authority reserves the right to review technical documentation associated with any cryptomodules under consideration for use by the FBCA.

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: 30 October 2001
Date CPWG recommended approval: 30 October 2001
Date Presented to FPKI PA:
Date of approval by FPKI PA: