

# Federal Bridge CA Certificate Policy Change Proposal

**Change Serial Number:** 2001-02

**Title:** Clarifying applicability of FIPS 112 requirement

**Date:** 31 May 2001

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

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 1.1.5

**Change Advocate Contact Information:**

Name: Mike Jenkins

Organization: DoD

Telephone number:

E-mail address: mjjenki@missi.ncsc.mil

**Organization requesting change:** CPWG

**Change summary:** Make FIPS 112 refer only to passwords.

**Background:**

The CP currently requires activation data to be generated in conformance with FIPS 112. The Chryalis Luna3 cryptomodule does not use passwords as activation data; rather, it uses CIK (black plastic keys containing cryptographic information). Therefore, this requirement must be changed to allow the (stronger) mechanism, but cannot be removed since it will still be a requirement for Agencies who do use passwords as activation data.

**Specific Changes:**

**Existing text:**

## **6.4.1 Activation data generation and installation**

The activation data used to unlock FBCA, Agency CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. For Rudimentary, Basic, and Medium assurance levels, activation data may be user selected. For the High assurance level, it shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. Activation data shall be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

**Proposed revised text:**

## **6.4.1 Activation data generation and installation**

The activation data used to unlock FBCA, Agency CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. For Rudimentary, Basic, and Medium assurance levels, activation data may be user selected. For the High assurance level, it shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. *Where passwords are used as activation data, the passwords shall be generated in conformance with FIPS-112.* If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

**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: 31 May 2001

Date CPMWG recommended approval: 31 May 2001

Date Presented to FPKI PA:

Date of approval by FPKI PA: