

Federal Bridge CA Certificate Policy Change Proposal

Change Serial Number: 2001-01

Title: Preventing unauthorized access attempts

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: mjenki@missi.ncsc.mil

Organization requesting change: CPWG

Change summary: see Background

Background:

The CP currently requires a facility to temporarily lock an account following a predetermined number of login attempts. The requirement should be based on failed login attempts. Additionally, the Entrust product does not provide the required lock out. Instead, it terminates the application and requires that the application be restarted. The failed logins are audited. In light of FBCA audit review procedures, this is deemed sufficient to forestall repeated unauthorized access attempts.

Specific Changes:

Existing text:

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account after a predetermined number of login attempts as set forth in the respective CP or CPS.

Proposed revised text:

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, *or terminate the application*, after a predetermined number of *failed* login attempts as set forth in the respective CP or CPS.

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: