

Federal Bridge CA Certificate Policy Change Proposal

Change Serial Number: 2001-04

Title: Remove auditing requirements for storage and export of secret (symmetric) keys

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 imposes audit requirements for the storage and export of secret (symmetric) keys. The CP imposes no requirements for secret keys elsewhere, so it is unreasonable to impose audit requirements on the FBCA or Agency CAs.

Specific Changes:

Existing text:

Table from Section 4.5.1 that includes the following entries:

SECRET KEY STORAGE				
The manual entry of secret keys used for authentication			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X

Proposed revised text:

Replace cited entries with the following rows (note deleted text):

PRIVATE KEY EXPORT				
The export of private keys (keys used for a single session or message are excluded)	X	X	X	X

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: