

# Federal Bridge CA Certificate Policy Change Proposal

**Change Serial Number:** 2001-14

**Title:** Remove confusing prohibition against escrow of FBCA private signing key.

**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:** See background.

**Background:**

Section 6.2.3.1 of the CP currently indicates that that no information shall be encrypted in the FBCA public key. This is consistent with the prohibition to use the FBCA signing key as an encryption key, but it is confusing in this section that deals with escrow of Agency CA encryption keys. The prohibition over using the FBCA keys for other than signing certificates and CRLs and verifying signatures on objects so signed is adequately covered elsewhere in the CP. Therefore, it is proposed that the confusing text be deleted.

**Specific Changes:**

**Existing text:**

Section 6.2.3.1, Escrow of Agency CA encryption keys:

The FBCA shall not perform any encryption key recovery functions involving encryption keys issued to Agency CAs, and shall not store any information encrypted in the FBCA public key that may require key recovery capabilities. However, if encryption key pairs need to be issued by the FBCA covering repository system access or for other purposes, the Federal PKI Policy Authority shall publish applicable requirements for that purpose.

**Proposed revised text:**

Delete first sentence from first comma to the end of the first sentence:

The FBCA shall not perform any encryption key recovery functions involving encryption keys issued to Agency CAs. However, if encryption key pairs need to be issued by the FBCA covering repository system access or for other purposes, the Federal PKI Policy Authority shall publish applicable requirements for that purpose.

**Estimated Cost:**

No cost is associated with 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: 05 November 2001

Date CPWG recommended approval: 05 November 2001

Date Presented to FPKI PA:

Date of approval by FPKI PA: