



## Federal Bridge CA Certificate Policy Change Proposal Change Number: 2004-02

**To:** Federal PKI Policy Authority  
**From:** FPKI Certificate Policy Working Group  
**Subject:** Proposed modifications to the FBCA CP  
**Date:** 24 September 2004

---

**Title:** Various editorial changes from CPWG meetings for the HEBCA CP mapping and the DoD ECA CP mapping.

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

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 10 September 2002.

### **Change Advocates Contact Information:**

Name: <b>Tim Polk</b>	Name: <b>John Cornell</b>
Organization: <b>NIST</b>	Organization: <b>GSA</b>
Telephone number: <b>(301) 975-3348</b>	Telephone number: <b>(202) 501-1598</b>
E-mail address: <b>tim.polk@nist.gov</b>	E-mail address: <b>john.cornell@gsa.gov</b>

**Organization requesting change:** NOAA (Gene McDowell) and CPWG.

---

### **Change summary:**

The FBCA CPWG recommends the following changes for clarity in various areas of the FBCA CP.

**Background:** This change proposal is a collection of CPWG approved modifications to the FBCA CP from the 26 April 2004 CPWG meeting for the HEBCA CP mapping and the 22 March 2004 CPWG meeting for the DoD ECA CP mapping.

### **Specific Changes:**

1) Make the following changes in Section 1.3.1.6 (Entity Principal Certification Authority (Principal CA)):

The Principal CA is a CA within a PKI that has been designated to interoperate directly with the FBCA (e.g., through the exchange of cross-certificates), and which issues either end-entity certificates, or cross-certificates (or other means of interoperation) to other Entity or external party CAs, or both. It should be noted that an Entity may request that the FBCA interoperate with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are "subordinate" to the Principal CA. The use of this term shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether the Entity employs a hierarchical or other PKI architecture.

2) In Section 4.2.1 (Delivery of Subscriber's private key to Subscriber) add the 2<sup>nd</sup> bullet below:

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:

- An Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time;
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

3) Replace the original text of Section 4.6.5 (Requirements for time-stamping of records):

No stipulation.

With the following text:

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

---

**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:	<b>04 June 2004</b>
Date CPWG recommended approval:	<b>30 August 2004</b>
Date Presented to FPKI PA:	<b>14 September 2004</b>
Date of approval by FPKI PA:	<b>24 September 2004</b>