



Federal Bridge CA Certificate Policy Change Proposal
Change Number: 2003-01

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA Certificate Policy
Date: 20 September 2004

Title: Clarify FBCA requirements to facilitate cross certification with the Department of Defense

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 as amended by FBCA Change Proposals 2002-01 through 2002-05.

Change Advocates Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: (301) 975-3348
E-mail address: tim.polk@nist.gov

Name: John Cornell
Organization: GSA
Telephone number: (202) 501-1598
E-mail address: john.cornell@gsa.gov

Organization requesting change: CPWG

Change summary: The existing FBCA CP, Section 1.1.5, states that interoperability with entities outside of the federal government will require changes to the CP. In light of the pending applications of various organizations that are not elements of the executive branch of the federal government, the time to address the changes anticipated by Section 1.1.5 has arrived. The FBCA CPWG recommends the following changes to accommodate interoperability with entities outside of the federal government.

Background:

The FPKI Certificate Policy Working Group (CPWG) met on January 13, 2003, at NIST. The CPWG Co-Chair and the DoD representative to the CPWG (Francee Levene) presented the open issues identified at the December 18, 2002 DoD PKI CPMWG meeting. To facilitate the mapping of DoD and FBCA certificate policies, the FPKI CPWG has proposed modifications to address the DoD open issues.

The FPKI CPWG has requested that the DoD CPMWG review these proposed modifications. If these changes are considered sufficient, the FPKI CPWG will present a corresponding Certificate Policy Change Proposal to the FPKI Policy Authority at its February meeting.

The change proposals are ordered according to the Item number in the DoD – FBCA Certificate Policy Mapping Matrix. The proposed text changes appear as red underlined text.

Specific Changes:

Policy Mapping Matrix - Table #1

Problem: In Section 2.1.1, the FBCA Certificate Policy stated the obligations of entity CAs, but did not specify the obligations of the FBCA CAs.

Proposal: Modify the current section 2.1.1 by inserting the first sentence/paragraph.

2.1.1 CA Obligations

The FBCA is obligated to comply with the requirements of this CP, the approved CPS, and any MOAs agreed upon between the FBCA and an Entity CA.

An Entity CA that issues certificates mapped by the Federal PKI Policy Authority to the FBCA policies defined in this CP for which the Federal PKI Policy Authority has authorized the issuance of an FBCA certificate containing those mappings to the Entity’s Principal CA, shall comply with the requirements set forth in the MOA, as well as ensuring compliance with Entity CP requirements.

Policy Mapping Matrix - Table #38

Problem: The DoD CP requires that a POC be recorded for role verification. The FBCA CP did not consider role information, assuming that data was of local utility only.

Future FPKI certificates may contain role information that is interoperable within the Federal government. To ensure that data is accurate, we propose to extend the current processing and recording requirements for identity verification to any role information

included within the certificates. This is more general than the DoD CP requirement, but we believe it meets or exceeds the assurance achieved by recording the POC.

Proposal: The first paragraph in section 3.1.9 ends with a bulleted list of “process documentation and authentication requirements ... depending upon the level of assurance (as set forth below):”

Modify the list and replace current bullet 2:

- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;

With

A signed declaration by that person that he or she verified the identity of the Subscriber (including verification of any roles or authorizations that apply to that certificate) as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;

Policy Mapping Matrix - Table #59

Problem: The DoD CP section 4.4.4, bullet 3 specifies latency requirements for The FBCA CP permits certificate status distribution using on-line mechanisms (e.g., OCSP), but does not state latency requirements. The FBCA CP should explicitly state that CRL latency requirements must be achieved by any on-line certificate status distribution mechanism.

Proposal: Modify Section On-line Revocation / Status checking availability by inserting a new second sentence, extending CRL latency requirements specified earlier to on-line status checking.

In addition to CARL/CRLs, Entity CAs and Relying Party client software may optionally support on-line status checking. *The latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.4.3.1.* Client software using on-line status checking need not obtain or process CARL/CRLs. The Federal PKI Policy Authority will determine when and under what circumstances the FBCA Operational Authority will provide on-line status checking of FBCA certificates.

Policy Mapping Matrix Table #142

Problem: The FBCA CP cites FIPS 112 for password policies, but is otherwise silent. As FIPS 112 provides a framework, but no hard requirements, there is no requirement that an entity CA ever change the activation data for a password-protected cryptographic module.

Proposal: Insert text requiring that where passwords are used as activation data, at a minimum the passwords must be changed upon re-key. Insert the text as the fifth sentence in section 6.4.1, Activation data generation and installation.

insert the italicized text:

The activation data used to unlock FBCA, Entity 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 password data shall be generated in conformance with FIPS-112. *Where the FBCA or an Entity CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.* 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.

Policy Mapping Matrix – Table # 148

Problem: The DoD CP specifies that the RA equipment must be protected from malicious software. The FBCA CP is, at best, inconsistent regarding this feature.

Proposal: In section 6.6.1, “System Development Controls”, change “CA” to “CA and RA” in first sentence of bullet 6. The revised text for bullet six reads as follows:

- Proper care shall be taken to prevent malicious software from being loaded onto the CA *and RA* equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
-

Estimated Cost:

There is no financial cost associated with implementing these changes.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	13 January 2003
Date CPWG recommended approval:	30 August 2004
Date Presented to FPKI PA:	14 September 2004
Date of approval by FPKI PA:	14 September 2004