

Federal Bridge CA Certificate Policy Change Proposal

Change Serial Number: 2002-05

Title: Clarify FBCA requirements to facilitate cross certification with nonfederal entities

Date: 12 July 2002

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 11 February 2002 as amended by FBCA Change Proposals 2002-01 through 2002-04.

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 CP at ¶ 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 ¶ 1.1.5 has arrived. The FBCA CPWG recommends the following changes to accommodate interoperability with entities outside of the federal government.

Background:

The FBCA CPWG met on 28 June 2002 to review the detailed mapping comparison of the FBCA CP (Medium Assurance Level) and USDA NFC CP. At that meeting, the CPWG determined that it was time to make the changes anticipated in ¶ 1.1.5 to accommodate interoperability with entities outside of the federal government. The CPWG began the first iteration of this review at this meeting, and completed the task for the 12 July 2002 CPWG meeting. This action necessitated nine significant changes to various portions of the CP and a general change of “entity” in place of “agency” in most places.

The following conventions are used to depict specific changes: language deleted appears as ~~strikethrough~~; language inserted appears as underlined.

Specific Changes:

Item 1, ¶ 1 Introduction

This Certificate Policy (CP) defines five certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate ~~Agency CA~~ interoperability ~~with~~ between the FBCA and ~~with other Agency~~ Entity PKI domains. The five policies represent four different assurance levels (Rudimentary, Basic, Medium, and High) for public key digital certificates, plus one assurance level used strictly for testing purposes (Test). The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task.

The FBCA supports interoperability among ~~Federal Agency~~ Entity PKI domains in a peer to peer fashion. The FBCA ~~will~~ issues certificates only to those ~~Agency~~ Entity CAs ~~determined~~ designated by the owning ~~Agency~~ Entity (called “Principal CAs”). The FBCA, or a CA that interoperates with the FBCA, may also issue certificates to individuals who operate the FBCA. The FBCA certificates issued to ~~Agency~~ Principal CAs act as a conduit of trust. The FBCA does not add to and should not subtract from trust relationships existing between the transacting parties as established through the Federal PKI Policy Authority.

At their discretion, ~~agencies~~ entities may elect to interoperate among themselves without using the FBCA. Those ~~agencies~~ entities that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP. ~~However, FBCA CP object identifiers (OIDs) may be used only by agencies that interoperate with the FBCA.~~ Any use of or reference to this FBCA CP outside the purview of the Federal PKI Policy Authority is completely at the using party’s risk. ~~Further, unless specifically approved by the Federal PKI Policy Authority, a~~ An ~~Agency~~ Entity shall not assert the FBCA CP OIDs in any certificates the ~~Agency~~ Entity CA issues, except in the *policyMappings* extension establishing an equivalency between an FBCA OID and an OID in the ~~Agency~~ Entity CA’s CP. When used in the *policyMappings* extension, the ~~Agency~~ Entity may employ the OIDs only after a policy mapping determination is made by the Federal PKI Policy Authority allowing their use.

This FBCA CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

The terms and provisions of this FBCA CP shall be interpreted under and governed by applicable Federal law.

The terms and provisions of this FBCA CP shall be interpreted under and governed by applicable Federal law. ~~The United States Government disclaims any liability that may arise from the use of this FBCA CP.~~

Item 2, ¶ 1.1.4 Scope

~~The current version of this CP provides for interoperability through the FBCA between federal agency PKI domains only. The FBCA exists to facilitate trusted electronic business transactions for federal organizations. To facilitate the missions of these organizations, interoperability is offered to non-federal entities. The generic term “entity” applies equally to federal organizations and other organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an organization’s PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.~~

Item 3, ¶ 1.1.5 Interaction with PKIs External to the Federal Government

~~The FBCA will extend interoperability with non-federal entities only when it is beneficial to the federal government. Interoperability with entities outside the Federal government will be established when directed by the Federal PKI Policy Authority and will require changes to this CP to address issues associated with liability and other matters. Nonetheless, it is the ultimate intent of the Federal PKI Policy Authority to make the FBCA available to support interoperability between Federal and non-Federal entities. Moreover, interoperability with entities external to the Federal government for purposes of technical testing may be performed when directed by, and in a fashion determined by, the Federal PKI Policy Authority, employing the “Test” level of assurance.~~

Item 4, ¶ 1.2 Identification

First paragraph:

There are five levels of assurance in this Certificate Policy which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FBCA ~~and Agency Principal CAs responsible for Agency PKI domains which comply with the policy stipulations herein.~~ The OIDs are registered under the id-infosec arc as follows:

Item 5, ¶ 1.3.1.2 Federal PKI Policy Authority

Final paragraph:

The Federal PKI Policy Authority will enter into a Memorandum of Agreement (MOA) with an ~~Agency~~ Entity setting forth the respective responsibilities and obligations of both

parties, and the mappings between the certificate levels of assurance contained in this CP and those in the Agency Entity CP. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph. When the entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.

Item 6, ¶ 1.3.4 Applicability

First two ¶¶:

The sensitivity of the information processed or protected using certificates issued by FBCA or an Agency Entity CA will vary significantly. Agencies Entities must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Agency Entity for each application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at four increasing, qualitative levels of assurance: Rudimentary, Basic, Medium and High. ~~It also defines an assurance level for testing purposes.~~ It is assumed that the FBCA will issue at least one High assurance certificate, so the FBCA will be operated at that level. The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

This CP also defines the Test level of assurance, which is used by the FBCA prototype bridge and CAs when conducting interoperability testing. The FBCA does not issue certificates with the Test level of assurance.

Item 7, ¶ 2.6.3 Access Controls

The FBCA Operational Authority shall protect any repository information not intended for public dissemination or modification. Public keys and certificate status information in the FBCA repository shall be publicly available through the Internet. Access to information in Agency Entity CA repositories shall be determined by the Agency Entity pursuant to ~~its authorizing and controlling statutes~~ the rules and statutes that apply to that entity.

Item 8, ¶ 2.7.5 Actions taken as a result of deficiency

second bullet:

- The compliance auditor shall notify the Agency Entity of the discrepancy. ~~If the discrepancy is judged by the Agency to be severe in nature (that is, it is determined to be a “material discrepancy” relative to the applicable requirements),~~ tThe Agency Entity shall notify the Federal PKI Policy Authority promptly;

Item 9, ¶ 4.6.2 Retention period for archive

The minimum retention periods for archive data are identified below. Executive branch agencies must follow either the General Records Schedule established by the The National Archives and Records Administration must give authority either in a General Records Schedule or an agency specific records disposition schedule or an agency specific schedule as applicable. All other entities shall comply with their respective records retention policy in accordance with whatever law applies to that entity.

Item 10, ¶ Glossary

two modified definitions; one new definition (remainder of glossary omitted)

Agency ~~Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government. For purposes of this CP only, agency is defined as any instrumentality of the federal government, executive, legislative, or judicial branch.~~

Entity ~~For purposes of this CP, Entity is any person, organization, corporation or government (state, local, federal or foreign) operating, or directing the operation of, one or more CAs~~

Agency Entity CA ~~A CA that acts on behalf of an Agency Entity, and is under the operational control of an Agency Entity.~~

Item 11, throughout

“Entity” replaced “Agency” where applicable. “Principal CA” replaced “Agency Principal CA” throughout.

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: 2002

Date CPWG recommended approval: 9 May 2002 and 10 May 2002

Date Presented to FPKI PA: 10 September 2002

Date of approval by FPKI PA: 10 September 2002