NOTE: THIS DOCUMENT CAPTURES THE CHANGES THAT NEED TO BE MADE TO THE FBCA CP MAPPING MATRICES. IMPACT AND RECOMMENDED CHANGES ARE IN RED TEXT

FBCA Certificate Policy Change Proposal

Change Number: *2006-02*

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the FBCA Certificate Policy

Date: 7 September 2006

Title: Omnibus Policy Issues Raised During the CertiPath Mapping and e-Auth Business Rules Review

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certification Authority Version 2.1, 12 January 2006.

Change Advocates Contact Information:

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

Organization requesting change: National Institute of Standards and Technology

Change summary: This change proposal resolves issues raised during (1) CertiPath's mapping of the FBCA Certificate Policy to the CertiPath CP and (2) the FPKIPA's comparison of the FBCA Certificate Policy with the e-Auth business rules. Most are clarifications of current practices with the FPKI. This change proposal also includes editorial corrections for alignment with the current version of the Common Policy.

Specific Changes:

Specific changes are made to the sections: forward, 1.1.3, 1.3.1.7 (new section), 1.5.4, 2.2.1, 3.1.5, 3.2.3.1, 4.3.2, 4.6.2, 4.7.2, 4.7.3, 4.9.1, 4.9.4, 5.1.3, 5.2.4, 5.4.2, 5.4.6, 5.6, 6.1.5, 6.2.10, and 8.1. A new appendix is also added.

Inserted text is in *italics*, deleted text in ~~strikethrough~~.

Section 1.1.3

The FPKI Policy Authority maps Entity CP(s) to one or more of the ~~five~~ levels of assurance in the FBCA CP. The relationship between these CPs and the FBCA is asserted in CA certificates issued by the FBCA in the *policyMappings* extension.

NO IMPACT – NO SHALL STATEMENTS

Section 1.3.1

Insert a new section 1.3.1.7

1.3.1.7 Certificate Status Servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. In particular, PKIs may include OCSP responders to provide online status information. Such an authority is termed a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

NO IMPACT – NO SHALL STATEMENTS

Section 1.5.4 CPS Approval Procedures

The FPKI Operational Authority shall submit the FBCA CPS and the results of a compliance *audit* ~~analysis study~~ to the FPKI PA for approval. The FPKI PA shall vote to accept or reject the CPS ~~and accompanying analysis~~. If rejected, the FPKI Operational Authority shall resolve the identified discrepancies and resubmit to the FPKI PA. *The FBCA is required to meet all facets of the policy. The FPKI PA will not issue waivers.*

Entity CAs shall submit their CPS and the results of their compliance audit to the appropriate authority (See Section 1.5.3) for approval. An Entity CA's CPS shall be required to meet all facets of its policy. Waivers, while discouraged, may be permitted in order to meet urgent unforeseen operational requirements. Any waivers issued by Entity CAs are considered changes to the corresponding CP, and may result in revocation of the cross-certificate by the FPKI PA.

NO APPARENT IMPACT, SINCE THIS LANGUAGE DOES NOT BELONG IN THE MAPPING MATRICES (EVEN THOUGH THERE IS A SHALL STATEMENT)

Section 2.2.1

Append the following:

For the FBCA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

Entity CAs being considered for cross certification shall be designed to comply with this requirement.

Practice Note: The FBCA will impose this requirement on existing cross-certified Entity CAs one year from the effective date of this change.

Practice Note: Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component. Availability targets exclude network outages.

NEW TABLE IN GENERAL MATRIX REQUIRED

Section 3.1.5

The Federal PKI Policy Authority is responsible for ensuring name uniqueness in certificates issued by the FBCA. *Entity CAs shall identify the authority that is responsible for ensuring name uniqueness in certificates issued by the entity CA.*

NEW TABLE IN GENERAL MATRIX REQUIRED

Section 3.2.3.1 insert the following at the end of the first paragraph:

For Medium and High Assurance, identity shall be established no more than 30 days before initial certificate issuance Entity CAs being considered for cross certification must comply with this requirement.

Practice Note: The FBCA will impose this requirement on existing cross- certified Entity CAs one year from the effective date of this change

NEW TABLE IN MEDIUM AND HIGH MATRICES REQUIRED

Section 4.3.2

Insert the following practice note:

Practice Note: Where notification is not an integral component of the issuance process, CAs should proactively notify subscribers that certificates have been generated.

MODIFY Current TABLE #?? IN GENERAL MATRIX REQUIRED

Section 4.6.2

For Entity CAs that support renewal, such requests shall only be accepted from certificate subjects, PKI sponsors or RAs. Additionally, a CA may perform renewal of its subscriber certificates without a corresponding request, such as when the CA re-keys.

NEW TABLE IN GENERAL MATRIX REQUIRED

Section 4.7.2

For Entity CAs that support re-key, such requests shall only be accepted from the subject of the certificate or PKI sponsors. Additionally, CAs and RAs may initiate re-key of a subscriber's certificates without a corresponding request.

NEW TABLE IN GENERAL MATRIX REQUIRED

Section 4.7.3

For Entity CAs, ~~no stipulation~~ *see Sections 3.2 and 3.3.*

NO IMPACT

Section 4.9.1

Insert new first sentence:

For the FBCA and Entity CAs, a certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid.

NEW TABLE IN GENERAL MATRIX REQUIRED (OR modify current table #??)

Entity CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity. ~~Other circumstances for certificate revocation may be supported by Entity CAs.~~

NO IMPACT – DELETED TEXT DOES NOT APPEAR IN CURRENT TABLES

Section 4.9.4

~~For Entity CAs, no stipulation.~~
For Entity CAs, see Section 9.6.3.

No Impact.

Section 5.1.3

In addition, the FBCA directories (containing FBCA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. *Entity CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.*

No impact.

Section 5.2.4, table

Replace the content associated with the Basic, Medium, and High policies with the following text from the Common Policy (RFC 3647 format):

Basic:

Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.

UPDATE TO TABLE XX IN GENERAL (NEED TO VERIFY THIS BELONGS IN GENERAL MATRIX) MATRIX REQUIRED

Medium:
Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

UPDATE TO TABLE XX IN MEDIUM MATRIX REQUIRED

High:
Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator and Auditor roles. Individuals designated as Officer or Administrator may also assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one identity.

UPDATE TO TABLE XX IN HIGH MATRIX REQUIRED

Section 5.4.2

Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. *Examples of irregularities include discontinuities in the logs and loss of audit data.* Actions taken as a result of these reviews shall be documented.

NO IMPACT

Section 5.4.6

Insert parentheses into the following sentence [text is unchanged.]

Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown.

REVISE TABLE 63 IN GENERAL MATRIX

Section 6.1.5

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures.

Signatures on certificates and CRLs that are issued after 12/31/08 shall be generated using, at a minimum, *SHA-224*~~SHA-256~~.

REVISE TABLE 85 IN GENERAL MATRIX

Section 6.2.10

6.2.10 Method of Destroying ~~Subscriber~~ Private ~~Signature~~ Keys~~s~~

Individuals in trusted roles shall destroy CA, RA and status server (e.g., OCSP server) private signature keys when they are no longer needed. Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware *is* ~~should~~ not ~~be~~ required.

REVISE TABLE 101 IN GENERAL MATRIX OR ADD NEW TABLE

Section 6.3.2 Certificate Operational Periods/Key Usage Periods

Replace the first paragraph with the following:

The FBCA shall limit the use of its private keys to a maximum of three years for certificate signing and six years for CRL signing. CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of four years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.

Insert Practice Note: Signatures generated with these keys may be validated after expiration of the certificate.

FIVE NEW TABLES IN GENERAL MATRIX REQUIRED (Each sentence, except the first and the practice note, corresponds to a new table.)

Section 8.1

Amend first paragraph as follows:

The FBCA, Entity Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, and Medium Assurance, and at least once every two years for Basic Assurance. *Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.*

REVISE RELEVANT TABLES (SECTION 8.1) IN MEDIUM AND HIGH MATRICES

Estimated Cost:

No cost. All requirements imposed by this change proposal are already in place at the FBCA and Agency PKIs.

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	June 1, 2006
Date Presented to FPKI PA:	June 13, 2006
Date of approval by FPKI PA:	September 12, 2006