FBCA Policy Change Proposal Number: 2008-06

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Federal Bridge Certificate Policy

Date: July 15, 2008

Title: Change to CA Key Usage Period for CAs issuing end user certificates and clarification of organizational responsibilities concerning device certificates.

Version and Date of Certificate Policy Requested to be changed:
X.509 Certificate Policy for the Federal Bridge Certification Authority Version 2.10, October 16, 2008.

Change Advocate's Contact Information:

Name: Morris Hymes
Organization: DoD
Telephone number**:** 410-854-4900
E-mail address**:** mahyme1@missi.ncsc.mil

Organization requesting change: Department of Defense

Change summary: DoD is requesting an increase in the key usage period for CAs issuing end user certificates from four (4) years to six (6) years. In addition, some clarifying language concerning the control of Device certificates is also recommended.

Background: The DoD is issuing certificates for devices for which they will be implementing an automatic credential renewal process. In order to minimize costs for the migration and maintenance of device certificates, whose anticipated useful life is generally six years, they are requesting an extension to the key usage period for end user certificate issuing CAs of two years, bringing it to 6 years, which coincides with the lifecycle of the device. This change was originally conceived to affect CAs issuing device certificates, but it was determined that allowing CAs that issue human end-user certificates the same key usage period would prevent further complication of the requirements and not add any perceived risk to the process. During the discussion, it was determined that some clarification on the responsibilities of organizations and their human sponsors concerning device certificates was warranted, and this language was subsequently included in this change proposal.

Specific Changes: Specific changes are made to the following sections: 3.2.3.3, 6.3.2

Insertions are underlined, deletions are in ~~strikethrough~~:

3.2.3.3 Authentication of Devices
Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

These certificates shall be issued only to devices under the issuing entity's control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued). In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The Registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

6.3.2 Certificate Operational Periods/Key Usage Periods
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~~ six 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.

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

Practice Note: Subscriber key usage periods (and key modulus as noted in Section 6.1.5) shall be appropriate to the security requirements of the intended use.

CAs must not issue subscriber certificates that extend beyond the expiration date of their own certificates and public keys.

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in section 3.3.1.

Practice Note. The actual CA signing key usage must be determined in the context of the length of the validity periods of the certificates issued to and by the CA.

Estimated Cost:
No cost to the Federal Bridge CA.

Risk/Impact:
Extending the lifetime of the signing key usage period for CAs issuing end user certificates slightly increases the possibility of that CA's key being compromised.

Implementation Date:
This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Bridge 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: 15 July 2008
Date presented to FPKIPA: 12 November 2008
Date of approval by FPKIPA: 12 November 2008