FBCA Policy Change Proposal Number: 2008-05

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the Federal Bridge Certificate Policy
Date: 26 August 2008

Title: Changes to Federal Bridge Certification Authority CP to include a provision for a role-based signature certificate.

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 Advocates Contact Information:

Name: Judith Spencer
Organization: GSA
Telephone number: 202-208-6576
E-mail address: judith.spencer@gsa.gov

Organization requesting change: General Services Administration, Office of Governmentwide Policy

---

Background: Organizations publish documents on the web. In many cases, these documents will be signed by individuals identified as human subscribers. However, the need exists for the document to be published in a way that identifies the role held, rather than the individual applying the signature.

Currently, the U.S. Federal Bridge Policy, the authority under which digital signature credentials are issued, does not recognize a 'role-based' signature credential for use in the manner described here.

This proposed change modifies the Federal Bridge policy to accommodate the issuance of role-based signature credentials. In this scenario, multiple certificates may be issued with a single role identified; however, for internal accountability purposes, each will be unique to the individual to whom it was issued.

Change summary: Add language to the Federal Bridge Policy to include issuance of role-based digital signature certificates in order to allow entities to publish signed electronic documents where the signatures are associated with a role rather than an individual

Specific Changes: For this purpose, a new section is proposed, and a renumbering of subsequent sections. New text is underlined.

3.2.3.2 Authentication of Human Subscribers For Role-based Certificates

There is a subset of human subscribers who will be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Chief Information Officer;" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific individual within an organization (e.g. *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). Role-based certificates shall not be shared, but shall be issued to individual subscribers and protected in the same manner as individual certificates.

The FPKI Management Authority and/or Entity CAs shall record the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based certificate.

The procedures for issuing role-based tokens must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

> Practice Note: When determining whether a role-based certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Watch Commander, Task Force 1.*"

3.2.3.3 Authentication of Human Subscribers For Group Certificates

[Text omitted for expedience]

3.2.3.4 Authentication of Devices

[Text omitted for expedience]

Estimated Cost:

There is no financial cost associated with implementing this change.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Bridge Certification Authority CP.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:
Date presented to CPWG: 4 September 2008
Date CPWG recommended approval: 21 October 2008
Date presented to FPKIPA: 12 November 2008
Date of approval by FPKIPA: 12 November 2008