FBCA Certificate Policy Change Proposal Number: 2010-04

To: Federal PKI Policy Authority

From: CPWG

Subject: Proposed modifications to the Federal Bridge Certificate Policy

Date: May 26, 2010

Title: Specify String Format for UUID in serialNumber RDN

Version and Date of Certificate Policy Requested to be changed:


Change Advocate’s Contact Information:

Name: Terry McBride (CPWG Co-Chair)
Organization: Protiviti Government Services (on behalf of GSA)
Telephone number: 703-299-3444
E-mail address: terry.mcbride@pgs.protiviti.com

Organization requesting change: CPWG

Change summary: The FBCA policy requires a serialNumber attribute in the subject DN of the PIV-I Card Authentication certificate. The value of the serialNumber must be the UUID associated with the PIV-I Card. However, the FBCA does not currently indicate the format of the UUID. This change declares the format of the UUID to be the string format as specified in RFC 4122.

Background: PIV-I cards include a UUID that is used consistently throughout security objects and certificates on the card. The FBCA CP requires UUID to be in the subject-alternative-name of both the PIV-I Authentication Certificate and the PIV-I Card Authentication Certificate in URI format. In addition, the CP requires the UUID to be in the serialNumber attribute of the PIV-I Card Authentication certificate subject DN. However, the FBCA CP does not specify a format for the UUID in the serialNumber attribute. The Common Policy recommends a string format. To help ensure interoperability, it has been recommended that the FPKI PA declare the string format to be policy for PIV-I through the FBCA CP.

Specific Changes: Specific changes are made to the following sections:

Insertions are underlined, deletions are in strikethrough:
3.1.1 Types of Names

[...]

PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

\[ \text{serialNumber}=\text{UUID}, \text{ou}=\text{Affiliated Organization Name}, \{\text{Base DN}\} \]

For certificates with no Affiliated Organization:

\[ \text{serialNumber}=\text{UUID}, \text{ou}=\text{Unaffiliated}, \text{ou}=\text{Entity CA's Name}, \{\text{Base DN}\} \]

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

**Estimated Cost:**
There is no cost expected for Federal Agencies as the changes apply to a new policy under which no issuers have yet mapped.

**Implementation Date:**
This change will be effective 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: June 3, 2010
Date presented to FPKIPA: June 8, 2010
Date of approval by FPKIPA: June 8, 2010