



FBCA Certificate Policy Change Proposal Number: 2011-05

To: Federal PKI Policy Authority
From: See below for organizations requesting change
Subject: Proposed modifications to the Federal Bridge Certificate Policy
Date: September 8, 2011
Title: Updates to Certificate Policy to add a New Device Specific Policy

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy, Version 2.24, February 25, 2011

Submitter's Contact Information:

Name: Debbie Mitchell
Organization: Department of Defense
Telephone number: 410-854-4900
E-mail address: dmmite3@missi.ncsc.mil

Organizations requesting change: Multiple sponsors as shown below:

Organization	Name / Title	Phone Number / Email Address
Department of Defense	Denise Holmes Director, DoD PKI PMO	410-854-4900 dsholm2@missi.ncsc.mil
Department of Homeland Security	Gladys Garcia DHS PKI Program Manager	202-357-1278 gladys.garcia@dhs.gov

Change summary: This change implements the addition of the Common Device policy to the FBCA to distinguish certificates issued to devices from certificates issued to human users. In addition, this change implements a new hardware device policy at the Medium Assurance level to distinguish between devices using software and hardware cryptographic modules to protect their keys. This new hardware device policy is the same as the one being proposed by DHS to be added to Common.

Background: Device to device authentication is becoming a regular use of PKI. However, because devices have inherent differences in the way identity proofing is performed, the cost of hardware security modules for devices, and the desire to allow automatic system or device restart in lights-out operations, certificates issued to devices are often lower assurance than those issued to human counterparts. This change proposal provides a new Device Policy at the Medium Assurance level that allows member PKIs to distinguish certificates issued to devices from those issued to human users.

Issue

FPKI CPs are evolutionary documents that continue to grow and change as new understanding and insight is gained by the Federal sector. As a result of the need to identify certificates issued to devices, the Federal Bridge CP should be changed to add a new Medium Assurance Device Policy.

Specific Changes:

Specific changes are made to sections 1, 1.2, 1.3.4, 3.2.3.4, 3.3.1, 6.2.3.4, 6.2.4.6 (new), and 6.2.8.

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

1. INTRODUCTION

This Certificate Policy (CP) defines ten certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent six different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High) for public key certificates. In addition two device certificate policies at the Medium Assurance level are defined to facilitate server to server authentication between FBCA and other PKI domains.

1.2 DOCUMENT IDENTIFICATION

[Add the following paragraph after Table 1 - FBCA Certificate Policies]

...

In addition to the ten policies specified in Table 1, the following two device policies are added to the FBCA and may be used to be asserted in certificates issued to devices. These policies are defined in the Common Policy Framework Certificate Policy:

Table 2

<u>id-fpki-common-devices</u>	<u>::= {2 16 840 1 101 3 2 1 3 8}</u>
<u>id-fpki-common-devicesHardware</u>	<u>::= {2 16 840 1 101 3 2 1 3 36}</u>

The requirements associated with the id-fpki-common-devices and id-fpki-common-devicesHardware policies are identical to those defined for the Medium and Medium Hardware policies with the exception of identity proofing, re-key, and activation data. In this document, the term “device” is defined as a non-person entity, i.e., a hardware device or software application. The use of the id-fpki-common-devices and id-fpki-common-devicesHardware policies are restricted to devices and systems. However, this does not restrict certificates issued to non-person entities from asserting one or more other policies if all requirements for those policies are met.

Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules may include either the id-fpki-common-devices or the id-fpki-common-devicesHardware, or both. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include id-fpki-common-devices.

1.3.4 Subscribers

A Subscriber is the user or device to whom or to which a certificate is issued. FBCA Subscribers include only FPKI Management Authority personnel and, when determined by the Federal PKI Policy Authority, network or hardware devices. Where certificates are issued to devices, the entity must have a human sponsor who is responsible for carrying out Subscriber duties. Note that CAs are sometimes technically considered “subscribers” in a PKI. However, the term “Subscriber” as used in this document does not refer to CAs.

3.2.3.4 Authentication of Devices

...

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued at the id-fpki-common-devices policy and id-fpki-common-devicesHardware policy, registration information shall be verified commensurate with the Medium assurance level. 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.

3.3.1 Identification and Authentication for Routine Re-key

...

Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in table below.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration. <u>For device certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the</u>

	<u>certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.</u>
--	--

6.2.3.4 Escrow of Subscriber private encryption and dual use keys

Subscriber private dual use keys shall not be escrowed. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4.6 Backup of Device Private Keys

Device private keys may be backed up or copied, but must be held under the control of the device’s human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device’s cryptographic module.

6.2.8 Method of Activating Private Keys

...

For PIV-I Card Authentication, user activation of the private key is not required.

For certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device’s environment, and shall protect the device’s hardware, software, and the cryptographic token and its activation data from compromise.

Estimated Cost:

No cost.

Implementation Date:

This change will be implemented 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: July 7, 2011
- Date Presented to FPKIPA: September 13, 2011
- Date of approval by FPKIPA: September 13, 2011