



Common Policy CP Change Proposal Number: 2011-02

To: Federal Public Key Infrastructure Policy Authority (FPKIPA)
From: See below for organizations requesting change
Subject: Proposed Modifications to the Common Policy Certificate Policy (CP)
Date: September 8, 2011
Title: Updates to the Certificate Policy to Clarify Requirements for Device Subscribers and Certificates

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework, Version 3647 – 1.15, January 24, 2011.

Submitter's Contact Information:

Name: Gladys Garcia
Organization: Department of Homeland Security PKI Management Authority
Telephone number: 202-357-1278
E-mail address: gladys.garcia@dhs.gov

Organizations requesting change: Multiple sponsors as shown below:

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

Change summary: Clarify the meaning of “device” to include hardware device and software application subscribers. Create an additional devices policy to distinguish between devices using software and hardware cryptographic modules to protect their keys. Allow automatic restart of unattended critical devices without human intervention to activate the device’s key. Address the backup of device private keys under proper controls.

Background: The Common Policy CP uses the term “device” to refer to any non-human subscriber, which includes both hardware devices and software applications. It has been observed that some readers of the Common Policy CP interpret “device” to mean hardware devices such as routers and servers, but fail to recognize that “device” includes software applications such as a financial management application. A clear statement defining “device” is needed in the Common Policy CP to avoid its misinterpretation.

Relying parties may need to distinguish between devices using hardware and software cryptographic modules. An additional policy for devices using hardware cryptographic modules, i.e., id-fpki-common-devicesHardware, needs to be added to enable this.

Automatic restart of devices in unattended operations, without requiring human intervention to reactivate their keys, is required to avoid service gaps and/or excessive staffing costs.

A separate sub-section specifically addressing backup of device private keys should be added since the sub-section structure does not address device keys that may be dual use keys, and since the sub-section needs to address the human sponsor’s responsibilities.

Specific Changes:

Specific changes are made to the Foreword and to sections 1, 1.2, 3.1.1, 3.2.3.2, 3.3.1, 4.9.2, 6.1.5, 6.2.1, 6.2.3, 6.2.4.5 (New), 6.2.8, 7.1.4, 7.1.6, and 12.

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

FOREWORD

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates seven ~~six~~ specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy....

...

The user policies apply to Federal employees, contractors, and other affiliated personnel requiring PKI credentials for access to Federal systems that have not been designated by law as national security systems. The device policies apply to hardware devices and software applications ~~deveies~~ operated by or on behalf of federal agencies. ...

...

This policy framework requires the use of FIPS 140 validated cryptographic modules by Federal employees, contractors, ~~and~~ other affiliated personnel and devices for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under this policy framework. The policies for users with hardware cryptographic modules mandate Level 2 validation.

...

1 INTRODUCTION

This certificate policy (CP) includes ~~six~~ seven distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy. In this document, the term “device” means a non-person entity, i.e., a hardware device or software application. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all ~~six~~ seven policies.

...

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CA shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
<u>id-fpki-common-devicesHardware</u>	<u>::= {2 16 840 1 101 3 2 1 3 36}</u>
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}

Additionally, this CP provides moderate assurance concerning identity of certificate subjects when the following OIDs are expressed in certificate policy extensions of certificates issued after December 31, 2010, associated with the SHA-1 Federal Root CA, and signed using SHA-1.

Table 2 - id-fpki-SHA1 Policy OIDs

SHA1 Policy	OID	Corresponding id-fpki-common policy
id-fpki-SHA1-policy	::= {2 16 840 1 101 3 2 1 3 23}	id-fpki-common-policy id-fpki-certpcy-mediumAssurance
id-fpki-SHA1-hardware	::= {2 16 840 1 101 3 2 1 3 24}	id-fpki-common-hardware id-fpki-certpcy-mediumHardware
id-fpki-SHA1-devices	::= {2 16 840 1 101 3	id-fpki-common-devices

	2 1 3 25}	id-fpki-certpcy-mediumAssurance
id-fpki-SHA1-authentication	::= {2 16 840 1 101 3 2 1 3 26}	id-fpki-common-authentication id-fpki-certpcy-mediumHardware
id-fpki-SHA1-cardAuth	::= {2 16 840 1 101 3 2 1 3 27}	id-fpki-common-cardAuth

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users, other than devices, to support digitally signed documents or key management may contain either id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. ~~Subscriber certificates issued to devices under this policy shall include id-fpki-common-devices~~ Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include either id-fpki-common-devicesHardware, id-fpki-common-devices, or both. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include id-fpki-common-devices.

...

3.1.1 Types of Names

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High ~~and id-fpki-common-devices;~~ and id-fpki-common-devicesHardware the CA shall assign X.501 distinguished names to all subscribers.

...

3.2.3.2 Authentication Devices

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications 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) service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application 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.

...

3.3.1 Identification and Authentication for Routine Re-key

...

For policies other than id-fpki-common-High, a subscriber's identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every nine years from the time of initial registration.

For device certificates, identity may be established through the use of the device's current signature key, the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

...

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The human sponsor of a device can request the revocation of the device's certificate. Other authorized agency officials may request revocation as described in the CPS.

6.1.5 Key Sizes

...

End entity certificates issued under id-fpki-common-devices and id-fpki-common-devices that expire before December 31, 2010 shall contain RSA public keys that are 1024, 2048, or 3072 bits in length or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire on or after December 31, 2010 shall contain RSA public keys that are 2048 or 3072 bits or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire after December 31, 2030 shall contain RSA public keys that are 3072 bits or elliptic curve keys that are 256 or 384 bits.

...

6.2.1 Cryptographic Module Standards and Controls

Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the authentication policies (id-fpki-common-authentication or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.3 Private Key Escrow

...

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4.5 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 Key

For certificates issued under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High, and ~~id-fpki-common-devices~~, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

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.

...

7.1.4 Name Forms

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-High, ~~and id-fpki-common-devices~~, and id-fpki-common-devicesHardware shall be populated with an X.500 distinguished name as specified in section 3.1.1.

...

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

...

12. GLOSSARY

...

Subscriber

A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.

...

Estimated Cost:

There will be implementation costs associated with issuing new CA certificates containing the new policy OID.

Risk/Impact:

Operational Risks/Impacts – None

Technical Risks/Impacts – None

Implementation Date:

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

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: September 8, 2011

Date presented to FPKIPA: September 13, 2011

Date of approval by FPKIPA: September 13, 2011