Common Policy CP Change Proposal Number: 2012-03

To: Federal Public Key Infrastructure Policy Authority (FPKIPA)

From: Department of Homeland Security

Subject: Proposed Modification to the Common Policy Certificate Policy (CP)

Date: May 17, 2012

Title: Delegation of Certain Device Sponsor Responsibilities

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 – 1.17, December 9, 2011.

Submitter's Contact Information:

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

Change summary: A human device sponsor is responsible for protecting the device's private key and ensuring that the device's certificate is only used for authorized purposes. This proposed change will allow a human device sponsor, who is not physically located near the sponsored device, and/or who does not have sufficient administrative privileges on the sponsored device to fulfill these responsibilities, to delegate them to an authorized administrator of the device. The delegation must be documented in writing and signed by both parties. Accountability remains with the human device sponsor.

Background: A human device sponsor is responsible for protecting the device's private key and ensuring that the device's certificate is only used for authorized purposes. In order to effectively execute these responsibilities, a device's human sponsor must be physically located near the device and have appropriate administrative privileges on the device, i.e., must be an authorized administrator for the device.

In many organizations, the persons authorized to sponsor devices, i.e., request the issuance, re-key, modification and revocation of certificates for devices are managers, are not local device administrators. Furthermore, these managers may sponsor multiple devices. In these cases it

makes sense to allow these managers (device sponsors) to delegate their responsibilities, for protecting the device's private key and ensuring that the device's certificate is only used for authorized purposes, to a local authorized administrator for each sponsored device. This will ensure the required control of each device's private key and certificate use. The delegations should be documented so that an auditor can determine if the required control is being maintained. Delegation of the responsibilities should not relieve the device sponsor of his or her accountability for these responsibilities.

The Common Policy CP needs to be modified to allow delegation of these responsibilities, when appropriate.

Specific Changes:

Specific changes are made to section 9.6.3.

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

3.2.3.2 Authentication of Devices

….

- Contact information to enable the CA or RA to communicate with the sponsor when required.

These certificates shall be issued only to authorized devices under the subscribing organization's control. 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. See section 9.6.3 for subscriber responsibilities.

9.6.3 Subscriber Representations and Warranties

A subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. Wherever possible, subscriber documents must be digitally signed.

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.

Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

Delta Mapping:

None

Estimated Cost:

None

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: June 21, 2012, July 17, 2012
Date presented to FPKIPA: August 14, 2012
Date of approval by FPKIPA: TBD