FPKIPA
Federal Public Key Infrastructure Policy Authority

Common Policy Change Proposal Number: 2008-02

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the Common Certificate Policy
Date: 2 October 2008

Title: Changes to Federal PKI Common Policy Framework 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 U.S. Federal PKI Common Policy Framework, Version 1.4, August 13, 2008.

Change Advocates Contact Information:

Name: Timothy Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: wpolk@nist.gov

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

Organization requesting change: Office of Management and Budget

---

Background: Federal organizations publish public-release documents on the web. Currently, the individuals responsible for these publications have personal identity verification (PIV) cards that contain digital signature credentials in the individual holder’s name. However, the need is for the document to be published in a way that identifies the government position <job title> held, rather than the individual applying the signature.

Currently, the U.S. Federal PKI Common Policy Framework, 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 Common Policy Framework 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. Use of the individual's PIV card for storage of this role-based credential may be an option, but for immediate implementation, it is expected deploying agencies will issue a second card for the sole purpose of storage and protection of the role-based credential.

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

Specific Changes: There are three specific changes listed below. New text is underlined.

Section 1.3.4 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. For this policy, subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

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 "Secretary of Commerce" 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 are held by a unique individual within an organization (e.g. *Chief Information Officer, GSA* is a unique individual whereas *Program Analyst, GSA* is not).

> Practice Note: When determining whether a role-based certificate is authorized, 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*."

Section 1.3.5 Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name (or role) of a federal employee, contractor, or other affiliated personnel.

Section 3.1.1 Types of Names

. . .The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between lastname and "(affiliate)".

Signature certificates issued under id-fpki-common-hardware or id-fpki-common-High may be issued with a common name that specifies an organizational role, such as the head of an agency, as follows:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*role [, department/agency]*

- dc=gov,dc=…., [ou=*structural_container*], cn=*role [, department/agency]*

The combination of organizational role and agency must unambiguously identify a single person. (That is, widely held roles such as *Computer Scientist* or *Procurement Specialist* cannot be included since they do not identify a particular person. *Chief Information Officer*, *AgencyX* could be included as it specifies a role held by a single person.)

Where the *[department/agency]* is implicit in the role (e.g., Secretary of Commerce), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name must match that in the organizational unit attributes.

> Practice Note: In the case of "Chief Information Officer", use of department/agency in the common name is redundant but is included for usability purposes. Display of the common name is widely supported in applications. Other attributes may or may not be presented to users.

Devices that are the subject of certificates issued under this policy shall be assigned either a geo-political name or an Internet domain component name. Device names shall take one of the following forms: . . .

Section 3.1.3 Anonymity or Pseudonymity of Subscribers

The CA shall not issue anonymous certificates. Pseudonymous certificates may be issued by the CA to support internal operations. CAs may also issue pseudonymous certificates that identify subjects by their organizational roles, as described in section 3.1.1. CA certificates issued by the CA shall not contain anonymous or pseudonymous identities.

Section 3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. 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: Examples of signature certificates that assert organizational authority are code signing certificates and FIPS 201 id-PIV-content-signing certificates.

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 Common Policy Framework CP.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:
Date presented to CPWG: 7 May 2008
Date CPWG recommended approval: 21 October 2008
Date presented to FPKIPA: 12 November 2008
Date of approval by FPKI PA: 12 November 2008