**COMMON Certificate Policy Change Proposal Number: 2024-06**

**To:** Federal PKI Policy Authority (FPKIPA)
**From:** USAccess
**Subject:** Role-Based Certificate Clarifications for Delegated Signatures
**Date:** October 2, 2024

---

**Title:** Modify role-based certificate requirements for delegated digital signature uses

**X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.8 May 8, 2024**

**Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles Version 2.2 September 30, 2022**

**Change Advocate's Contact Information:**

Name: Darlene Gore
Organization: GSA
Telephone number: 703-517-0805
E-mail address: darlene.gore@gsa.gov

**Organization requesting change**: USAccess

**Change summary**: Add requirements around role-based certificates that can be used to support delegated digital signatures that convey the authority of a given role to specific delegates.

**Background**:

Federal Agencies submit records to the Office of the Federal Registry (OFR) for a variety of reasons to include proposed modifications to the Code of Federal Regulations. The OFR only accepts these digitally signed records from federal employees assigned or appointed to roles that have been granted this submission authority. When that assigned or appointed individual is not available to digitally sign these records, they may need to delegate the role's signatory authority to another individual in order to continue business operations. USAccess has been requested to work with the OFR to develop an efficient, secure way to support this type of delegation of authority to digitally sign documents for submission to the Federal Registry.

**Specific Changes:**

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

### 1.3.6 Subscribers

…

There is a subset of Human Subscribers who will be issued role-based certificates. These certificates identify a specific role on behalf of which the Subscriber or "private key holder" is authorized to act rather than the Subscriber's name. These certificates 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~~ role-based certificates will be issued in addition to ~~an~~ individual Subscriber certificates. A specific role may be identified in certificates issued to multiple Subscribers; however, the key pairs will be unique to each individual role-based certificate. For example, there may be four individuals with a certificate issued in the role of "General Counsel, DHS ~~Secretary of Commerce~~." However, each of the four certificates will have unique keys and certificate serial numbers. A specific example of a role-based certificate may be a delegated digital signature certificate that is issued to private key holder(s) who have been delegated the authority to sign documents on behalf of a "role holder" who is another individual assigned or appointed to a role that has unique authorization (e.g., "Secretary of Commerce," who has the authority to provide official submissions to the Office of the Federal Register). ~~Roles~~ Delegated digital signature certificates, ~~for which role-based certificates may be issued,~~ are limited to those roles 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: In many cases a Role-Based certificate may be authorized for the individual(s) assigned to that role, in which case the role holder and the private key holder(s) are the same person. Delegated digital signature certificates are the only instance where an authorized private key holder is a different individual than the role holder named in the subjectDN. In these instances, private key holder traceability is maintained via unique identifiers asserted in the Subject Alternative Name extension. |

### 1.4.2 Prohibited Certificate Uses

Certificates that assert id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth must only be used to authenticate the hardware token containing the associated private key and must not be interpreted as authenticating the presenter or holder of the token.

Delegated digital signature certificates must not assert authentication OIDs in a certificate Extended Key Usage (EKU) extension.

Certificates intended for code signing are not permitted under this policy.

### 3.1.1.1 Subject Names

Role-based signature certificates, to include those that support delegated digital signatures, ~~may~~ must be issued under id-fpki-common-hardware ~~or id-fpki-common-high~~ (see Section 1.3.~~4~~6). For these certificates, the common name must specifi~~es~~y the role, and may optionally specify the department or agency associated with that role, the name of the individual role holder, and a general purpose for the certificate, as follows:

- CN=role [, department/agency] [,firstname lastname (purpose)]

Where the [department/agency] is implicit in the role (e.g., Secretary of Commerce), it ~~should~~ may 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~~ correspond to that in the organizational unit attributes. When the role holder's name is included in the CN, a purpose for the certificate must be included (e.g., (OFR), (delegated), (acting agent), etc.) in order to more readily convey to relying parties that the private key holder is not the named role holder. The order of appearance of role, department, and name (purpose) in the CN is determined by the issuing authority. Additional descriptors that indicate role-based certificates may be included before the role or role holder's name if acceptable for relying party use (e.g. "Office of the Secretary of Commerce," or "On behalf of the Secretary of Commerce").

| |
|---|
| Practice Note: In the case of "Chief Information Officer", use of department/agency in the common name is redundant to the RDN 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. |

### 3.1.1.2 Subject Alternative Names

…
Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

Role-based certificates including those that support delegated digital signatures, must include at least one subject alternative name extension that uniquely identifies the individual subscriber that controls the private signature key (e.g., rfc822Name or otherName like Microsoft User Principal Name). Another example of a compliant identifier is the full Distinguished Name from the PIV Authentication certificate of the individual who is to be issued the role-based certificate (e.g., the private key holder) that may be included as a directoryName.

### 3.2.3.3 Authentication for Role-Based Certificates

Prior to issuance of a delegated digital signature certificate, authentication of both the role holder and the private key holder is required. This authentication can be performed either through the same procedures for authentication of individual identity (see Section 3.2.3.1), or through the use of a private key associated with a current certificate, having same or higher assurance, that identifies the individual.

| |
|---|
| Practice Note: The RA or CA can leverage a digital signature from supporting auditable artifacts (e.g., authorization form or subscriber agreement) to fulfill authentication requirements for role-based certificates. |

### 3.2.5 Validation of Authority

The CA must validate the requestor's authority to act in the name of the organization before issuing organizational certificates, such as CA certificates, role-based certificates, or content signing certificates.

For example, before issuing role-based certificates, the CA must validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role or person appointed to the role. Before requesting a role-based certificate for delegated digital signature, the RA must receive signed authorization that the individual role holder named in the certificate has authorized the delegation of signing authority to the individual private key holder(s) who will receive the tokens containing the delegated digital signature certificate(s) and private signature key(s).

…

### 5.4.1. Types of Events Recorded

…

The CA and KRS must record all events identified in the list below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented with physical logs as necessary.

…

- CERTIFICATE REGISTRATION:
    - All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process. This includes records associated with authentication and authorization of role-based delegated digital signature certificates.

### 5.5.1. Types of Events Archived

CA archive records must be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data must be recorded for archive:

…

- All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process. This includes records associated with authentication and authorization of role-based certificates.

…

- Subscriber Agreements, including agreements signed by subscribers who are recipients of role-based certificates and keys.

**Estimated Cost:**
Cost will vary, depending on how a CA or CMS implements certificate profiles or templates and the need to update the CPS and documented procedures and train appropriate personnel.

Additional costs may be incurred by the agency in developing the processes and procedures to make use of a role-based delegated digital signature certificates, but it is assumed this cost will be recovered over time through the efficiencies enabled by the use of these certificates.

**Implementation Date:** Immediate upon publication

**Prerequisites for Adoption:** None

**Plan to Meet Prerequisites:** Not applicable

**Approval and Coordination Dates:**

| | |
|---|---|
| Date presented to CPWG: | August 27, 2024 |
| Date change released for comment: | August 26, 2024 |
| Date comment adjudication published: | September 5, 2024 |

**Worksheet 18: Delegated Digital Signature Certificate**

| Field | Content |
|---|---|
| **Version** | Integer Value of 2 for Version 3 certificate |
| **Serial Number** | Unique positive integer |
| **Signature Algorithm** | Choice of the following algorithms:<br>id-RSASSA-PSS (1.2.840.113549.1.1.10)<br>sha256WithRSAEncryption (1.2.840.113549.1.1.11)<br>sha384WithRSAEncryption (1.2.840.113549.1.1.12)<br>sha512WithRSAEncryption (1.2.840.113549.1.1.13)<br>ecdsa-with-Sha256 (1.2.840.10045.4.3.2)<br>ecdsa-with-Sha384 (1.2.840.10045.4.3.3)<br>ecdsa-with-Sha512 (1.2.840.10045.4.3.4)<br><br>For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL. |
| **Issuer DN** | Must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate |
| **Validity Period** | utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049<br>generalTime (YYYYMMDDHHMMSSZ) for dates after 2049 |
| **Subject DN** | Must use one of the name forms for delegated digital signature certificate in Section 3.1.1.1 of the Common Certificate Policy.<br><br>CN=role [,department/agency] [,firstname lastname (purpose)]<br><br>Middlename or initials of the role holder may also be included in the CN of delegated digital signature certificates.<br><br>Bracketed items [] are optional attributes; however, if the optional role holder's name is asserted in the CN, a parenthetical certificate purpose must also be included. The order of appearance of role, department, and name(purpose) in the CN is determined by the issuing authority. |
| **Subject Public Key** | Must be either RSA or elliptic curve:<br>RSA Encryption (1.2.840.113549.1.1.1)<br>Elliptic Curve (1.2.840.10045.2.1)<br><br>For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves:<br>Curve P-256 (1.2.840.10045.3.1.7)<br>Curve P-384 (1.3.132.0.34) |
| **Key Usage** | Critical = TRUE<br>digitalSignature, nonRepudiation |

| | |
|---|---|
| **Extended Key Usage** | One or more keyPurposeIDs consistent with digital signature must be specified.<br>Recommended:<br>1.3.6.1.5.5.7.3.36 id-kp-documentSigning<br>1.3.6.1.4.1.311.10.3.12 MSFT Document Signing<br><br>Must not include any keyPurposeIDs associated with authentication uses (e.g., TLS client authentication, Microsoft Smart Card Logon, KPClientAuth, secureShellClient, etc.) |
| **Basic Constraints** *(Optional)* | May be critical or non-critical<br>cA:FALSE<br>Path length constraint must be absent |
| **Subject Key Identifier** | Derived using a cryptographic hash of the public key. |
| **Authority Key Identifier** | Identical to Subject Key Identifier in the issuing CA certificate.<br>authorityCertIssuer and authorityCertSerialNumber must not be populated. |
| **Subject Alternative Name** | At least one subject alternative name is required, which identifies the individual who is to be issued the role-based certificate (e.g., private key holder), as described in Section 3.1.1.2 of the Common Certificate Policy. An example of a compliant identifier is the full Distinguished Name from the PIV Authentication certificate of the individual who is to be issued the delegated signature certificate (e.g., private key holder) that may be included as a directoryName.<br><br>Name forms associated with any individual other than the private key holder are not permitted. |
| **CRL Distribution Points** | Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1. |
| **Authority Information Access** | Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585)<br><br>The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.*2.* |
| **Certificate Policies** | The following policy must be asserted:<br>2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware |