**COMMON Certificate Policy Change Proposal Number: 2025-01**

**To:** Federal PKI Policy Authority (FPKIPA)
**From:** Department of Veterans Affairs
**Subject:** Accommodations for group/shared encryption certificates
**Date:** January 31, 2025

---

**Title:** Allowance for the issuance of group encryption certificates in Common

**X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.9 October 25, 2024**

**Change Advocate's Contact Information:**

Name: Gerald Singh
Organization: Department of Veterans Affairs
Telephone number: (304) 266-0947
E-mail address: Gerald.Singh@va.gov

**Organization requesting change**: Department of Veterans Affairs

**Change summary**: Expanding Common policy to allow for the issuance of group encryption certificates in support of valid group email encryption use cases.

**Background**:
Federal Agencies, including the Department of Veterans Affairs, maintain a valid use case for facilitating email transactions containing sensitive information that must be encrypted (e.g., PII, PHI, or other information of a legal or investigatory nature) for mailboxes that have multiple users. To support that use case, this change proposal establishes allowances for shared private key management keys and associated certificates, to be included in Common policy, where applicable, to facilitate these encryption transactions in the most efficient manner possible.

**Specific Changes:**

Insertions are underlined, deletions are in ~~strikethrough~~, and moves to a location are **bolded red** (where they are moved from are ~~**bolded red strikethrough**~~)

### 1.1.3 Scope

The scope of this U.S. Federal PKI Common Policy Framework CP includes the Certification Authorities used for issuing and managing certificates that are valid to the Federal Common Policy CA on behalf of federal executive branch agencies. This CP applies to certificates issued to CAs, devices, and federal employees, contractors and other affiliated personnel. ~~This CP does not include certificates issued to groups or intended to be shared.~~

Federal Government departments and agencies operate CAs that are intended to issue certificates for only locally trusted purposes. These CAs do not have a certification path to the Federal Common Policy CA and should not assert the policy OIDs defined in this CP.

### 1.3.6 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. For this CP and all certificates issued, Subscribers are limited to federal employees, contractors, affiliated personnel, and devices operated by or on behalf of federal agencies. 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. A Subscriber may be referred to as an "Applicant" after applying for a certificate, but before the certificate issuance procedure is completed.

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, role-based certificates will be issued in addition to individual Subscriber certificates. A specific role may be identified in signing certificates issued to multiple Subscribers; however, the key pairs will be unique to each individual role-based signing certificate. For example, there may be four individuals with a certificate issued in the role of "General Counsel, DHS" However, each of the four certificates will have unique keys and certificate serial numbers. A specific example of a role-based signature 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). Delegated digital signature certificates 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 subject DN. In these instances, private key holder traceability is maintained via unique identifiers asserted in the Subject Alternative Name extension.

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"

Another category of subscriber certificates includes group key management keys and certificates, also known as group encryption certificates. These private encryption keys and certificates facilitate scenarios where multiple individuals, using a shared private key, have the ability to decrypt information that was encrypted using one public key (e.g., group email address).

### 3.1.1.1 Subject Names

…

Role-based signature certificates~~, to include those~~ that support delegated digital signature~~s~~ uses, must be issued under id-fpki-common-hardware (see Section 1.3.6). For ~~these~~ all role-based signature certificates, the common name must specify 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 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 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.

Group encryption certificate distinguished names must take the following form:

- Base DN, CN=group name

where the group name is descriptive for the group, to include group email names (e.g., OMBmax Support Email). The group encryption certificate must not imply that a subject is a single individual (e.g., by asserting a human subscriber name form in any field of the certificate).

Device Subscriber distinguished names must take the following form:

- Base DN, CN=device name

where device name is a descriptive name for the device.

### 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 an rfc822Name.

Role-based signature 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.

### 3.2.3.4 Authentication of Human Subscribers for Group Certificates

Normally, a certificate is issued to a single Subscriber. However, for cases where there are several individuals acting in one capacity to decrypt data, an encryption certificate may be issued to a group composed of multiple Subscribers. Each group certificate shall have a sponsor who is responsible for ensuring that only authorized individuals have access to the corresponding private key. Prior to group encryption certificate issuance, CAs and/or RAs must authenticate the group sponsor using a current signature key of equal or greater assurance than the group certificate itself, or follow the authentication process identified in Section 3.2.3.1. In addition to the authentication of the group sponsor, the following applies to group encryption certificates:

- The group sponsor assigns the subject DN and SAN of the group encryption certificate, must ensure that each group member has signed an individual Shared Key Usage Agreement and must maintain a list of subscribers with access to the shared private key at all times. This list must be provided to an authorized representative of the CA, RA, or an auditor upon request or at certificate revocation or expiration (see Section 9.6.3.2); and

- The procedures for issuing hardware tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations)

### 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:

- Documentation of receipt and acceptance of certificates
- Subscriber Agreements, including agreements signed by subscribers who are recipients of role-based certificates and keys.
- All shared key access lists and shared key user agreements supporting group encryption certificates provided by the group sponsor to the CA or RA upon certificate revocation or expiration
- Documentation of receipt of tokens

**9.6.3.2 Group Encryption Certificate Sponsor and User Representations and Warranties**

Sponsors of group encryption certificates must:

- Assign the subject DN and Subject Alternate Name (SAN) of the group encryption certificate, ensuring they reflect the correct group and do not identify nor imply a single individual,
- Maintain a list of individuals having access to the group encryption certificate and its associated private key,
- Maintain a record of the dates and times individual group members have access to a centrally managed hardware group encryption certificate and its associated private key,
- Maintain a Shared Key Usage Agreement for each group member,
- Coordinate revocation requests or key recovery requests with the CA or RA,
- Provide the group member list and Shared Key Usage Agreements to the CA, RA or an auditor upon request or once the group encryption certificate expires or is revoked.

An individual with access to a shared key corresponding to a group encryption certificate must:

- Accurately represent themselves in all communications with the PKI authorities and the group sponsor.
- Protect the shared private key(s) at all times, in accordance with this policy and locally defined processes and procedures.
- Promptly notify the group sponsor, or other designated individual, upon suspicion of loss, compromise, or inappropriate use of the shared private key(s). Such notification must 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 the shared private key(s) and certificate(s).

**9.6.3.~~2~~3. Data Decryption Server Representations and Warranties**

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

Accommodation of the shared key/group certificate use case may reduce alternative technology spending for implementing organizations.

**Implementation Date:** Immediate upon publication

**Prerequisites for Adoption:** None

**Plan to Meet Prerequisites:** Not applicable

**Approval and Coordination Dates:**

| | |
|---|---|
| Date presented to CPWG: | January 14 and January 28, 2025 |
| Date change released for comment: | December 23, 2024 |
| Date comment adjudication published: | January 28, 2025 |