COMMON Certificate Policy Change Proposal Number: 2025-04

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Clarifications on Delegated Digital Signature Certificate naming, KRA authentication, and PKI Sponsor definition
Date: July 9, 2025

Title: Clarify Delegated Digital Signature Certificate naming, KRA authentication and PKI Sponsor definition

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.11 May 5, 2025

Change Advocate's Contact Information: fpki@gsa.gov

Organization requesting change: CPWG

Change summary:

Clarify naming conventions for Delegated Digital Signature certificates by logically separating role-based certificate common names schemas and examples from specific Delegated Digital Signature common name schemas and examples. These updates are also be reflected in Worksheet 18 of the Common Certificate and CRL profiles.

Clarify KRA and KRO authentication requirements which are confusing, use novel terminology and originated in the legacy Key Recovery Policy (KRP).

Additionally, update the definition of PKI sponsor to also include group certificate sponsors since the adoption of v2.11 of Common.

Background:

The CPWG was made aware of some potential discrepancies with regards to naming conventions used in support of Delegated Digital Signature certificates. The consolidation of role-based and delegated digital signature common name examples in Section 3.1.1.1 may generate unnecessary confusion with potential implementers.

Additionally the CPWG received comments about potentially confusing terminology regarding KRA and KRO authentication requirements which were the result of the effort to consolidate the older FPKI Key Recovery Policy (KRP) contents into both Common and FBCA certificate policies. This change intends to clarify those potentially confusing requirements.

Additionally, the most recent update to Common (v2.11) included an allowance for issuance of group encryption certificates. While these group certificates have been an existing capability within Bridge for some time, the definition of PKI sponsor in both policies has been limited to device sponsorship. This change aims to update that definition to ensure that like device sponsors, group certificate sponsors are responsible for the private key security of the associated certificate.

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**~~**.**

3.1.1.1 Subject Names

…

Role-based signature certificates must assert a common name as follows:

- CN=role [, department/agency]

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.

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").~~ Examples of role-based certificate common names may include:

- CN=Secretary of Commerce
- CN=On behalf of the Secretary of Commerce
- CN=Office of the Secretary of Commerce

Role-based signature certificates that support delegated digital signature uses, must be issued under id-fpki-common-hardware (see Section 1.3.6). For these delegated digital signature ~~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 parenthetical purpose for the certificate must be included ~~(e.g., (OFR), (delegated), (acting agent), etc.)~~ to identify the certificate as a delegated digital signature certificate and ~~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, and (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").~~ Examples of delegated digital signature certificate common names may include:

- CN=Secretary of the Treasury, Alexander Hamilton (OFR)[1]
- CN=Secretary of the Treasury, Alexander Hamilton (delegated)
- CN=On behalf of the Secretary of the Treasury, Alexander Hamilton (acting agent)

Practice Note: Common Name (CN) fields are limited to 64 characters.

… [page footnote]

[1] - The parenthetical purpose "(OFR)" is only for certificates used to digitally sign official documents submitted to the Office of the Federal Register and should not be used for any other purpose.

3.5.3 KRA Authentication

The KRA must authenticate to the KED or DDS directly or using a public key certificate issued by the ~~associated PKI~~ governing organization. When a public key certificate is used, it must be on a FIPS 140 level 2 or higher validated hardware cryptographic module. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered ~~and must meet the requirements of an RA credential~~.

3.5.4 KRO Authentication

The KRO must authenticate to the KRA using a public key certificate issued by the ~~associated PKI~~ governing organization. The assurance level of the certificate must be the same as or greater

than that of the certificate whose corresponding private key is being recovered ~~and must meet the requirements of an RA credential~~.

Appendix D: Glossary

…

PKI Sponsor	~~Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.~~ An individual who represents a device or group in all certificate life-cycle activities. A PKI Sponsor asserts that the certificate and associated private key are being used in accordance with the subscriber and certificate specific obligations in this CP.

Worksheet 18: Delegated Digital Signature Certificate

Field	Content
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. CN=role ~~[~~,department/agency~~]~~~~[~~,firstname lastname (purpose)~~]~~ Middlename or initials of the role holder may also be included in the CN of delegated digital signature certificates. ~~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 common name must specify the role, the department or agency associated with that role, the name of the individual role holder, and a general purpose for the certificate. The order of appearance of role, department, ~~and~~ name, and (purpose) in the CN is determined by the issuing authority.

Estimated Cost: No additional direct costs are expected to be incurred by any other parties as a result of this change proposal.

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	April 27, 2025
Date change released for comment:	May 15, 2025 and June 16, 2025
Date comment adjudication published:	June 26, 2025