COMMON Certificate Policy Change Proposal Number: 2025-06

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Clarification on Public Repository Requirements and Changes to Authentication/Authorization for Delegated Digital Signature Certificates
Date: November 19, 2025

Title: Clarification on Public Repository Requirements and Changes to Authentication and Authorization for Delegated Digital Signature Certificates

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.12 August 4, 2025

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

Organization requesting change: CPWG

Change summary:

This change seeks to:

- Clarify that AIA and SIA materials in public repositories are encoded in binary (DER) format in alignment with established FPKI certificate profile documents.
- Define acceptable alternatives for authentication and authorization artifacts supporting issuance of a Delegated Digital Signature certificate in the event a role-holder is not available

Background:

Both Common and FBCA profiles include a requirement for AIA and SIA .p7c files to be published in DER (digital) encoding format with appropriate http response header information. This change incorporates file encoding and repository response details into the body of the policy for consistency with similar information contained in the certificate profiles due to recent operational issues where PEM encoding was used, impacting interoperability.

Additionally, the CPWG was made aware by recent implementers of Delegated Digital Signature certificates that the role-holder authentication and private key holder authorizations could be modified to account for established agency processes. These processes leverage established organizational policies that authorize specific positions for Delegated Digital Signature certificates and also remove the requirement for direct role holder authentication in favor of authenticating an "authorizing sponsor" who can act on behalf of the role holder for direct appointment of private key holders.

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**~~**.**

2.2.1 Publication of Certificates and Certificate Status

…

With the exception of self-signed certificates, all CA certificates must be published by the Subject CA in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by the Subject CA. The ~~file~~ repository must ~~be~~:

- contain a binary (DER encoded) certs-only Cryptographic Message Syntax file that has an extension of .p7c and a http response content type header of 'application/pkcs7-mime', or
- contain a single binary (DER encoded) certificate that has an extension of .cer and a http response content type header of 'application/pkix-cert'.

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

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 and an authorizing sponsor is required. Th~~is~~ese authentications can be performed using 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 that

has~~ving~~ the same or higher assurance than the certificate being requested and~~, that~~ identifies the individual.

Practice Note: In the context of a delegated digital signature certificate, an "authorizing sponsor" is an individual other than the private key holder who can attest to the need to issue the certificate under the authority of the role holder in support of a documented business practice. For example, an "authorizing sponsor" can either be the role holder themselves or a Chief of Staff, Deputy, legal counsel, or similar position relative to the role holder

Practice Note: The RA or CA can leverage a digital signature from supporting auditable artifacts (e.g., authorization form, official appointment letter, 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~~ Prior to issuing role-based certificates, the CA or RA must validate that the individual role-based certificate applicant either holds that role or, in support of delegated digital signature certificates, has been appropriately delegated the authority to sign official documents on behalf of the role or the role holder ~~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).~~

Practice Note: Some organizations may have established policies that indicate which positions are authorized to receive delegated digital signature certificates. While these policies may not individually name the private key holders, other supporting documents; such as official appointment letters provided by an authorizing sponsor, can indicate the individual private key holders to whom delegated digital signature certificates can be issued.

Estimated Cost:

- There are no costs associated with the reiteration of public repository requirements from the certificate profiles document to the body of the policy.
- There are no costs associated with expanding authentications in support of delegated digital signatures to other authorizing sponsors outside of role holders. Costs associated with authentication and authorization process redesign for delegated digital signatures may be reduced for agencies.

Implementation Date: Upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	August 26, 2025 and September 23, 2025
Date change released for comment:	August 22, 2025 and September 16, 2025
Date comment adjudication published:	September 23, 2025