FBCA Certificate Policy Change Proposal Number: 2025-07

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Clarifications on Public Repository Requirements
Date: November 19, 2025

Title: Clarifications on Public Repository Requirements

X.509 Certificate Policy For The Federal Bridge Certification Authority [Version 3.8 August 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.

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 which impacted interoperability.

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.

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.

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