FBCA Certificate Policy Change Proposal Number: 2025-05

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

Title: Clarify KRA authentication and PKI Sponsor definition

X.509 Certificate Policy For The Federal Bridge Certification Authority Version 3.7 May 5, 2025

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

Organization requesting change: CPWG

Change summary:

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 in alignment with recent changes to Common.

Background:

The CPWG was made aware of some 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**~~**.**

3.5.1 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~~e~~ 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~~.

3.5.2 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 F - 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.

Estimated Cost: No costs are expected to be incurred by any 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, June 16, 2025
Date comment adjudication published:	June 26, 2025