FPKIPA
Federal Public Key Infrastructure Policy Authority

FBCA Certificate Policy Change Proposal Number: 2018-06

To: Federal PKI Policy Authority (FPKIPA)

From: Federal PKI Policy Authority Chair

Subject: Incorporate “supervised remote identity proofing” and other new guidance as defined in NIST SP 800-63-3

Date: April 23, 2018

Title: Add requirements to include *supervised remote identity proofing* and other guidance as defined by NIST SP 800-63-3

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.32 April 4, 2018

Change Advocate’s Contact Information:
Name: LaChelle LeVan
Organization: FPKI Policy Authority
Telephone number:

E-mail address: Lachelle.levan@gsa.gov

Organization requesting change: FPKI Policy Authority

Change summary: Update the CP to incorporate supervised remote identity proofing and other guidance as defined in NIST SP 800-63-3

Background:

In June 2017, NIST released Special Publication 800-63-3 Digital Identity Guidelines and three related documents:

- SP 800-63A *Digital Identity Guidelines: Enrollment and Identity Proofing*
- SP 800-63B *Digital Identity Guidelines: Authentication and Lifecycle Management*
- SP 800-63C *Digital Identity Guidelines: Federation and Assertions*

This suite of documents replaces the previously existing SP 800-63-2 *Electronic Authentication Guideline*. This new document recognizes the applicability of a supervised remote identity proofing capability as equivalent to in-person proofing. In addition, it provides guidance on protecting PII and other private information, minimum requirements for pass phrases and PINs, and requires a process of appeal and redress.

It is of interest to the FPKI community to align with SP 800-63-3 and incorporate these new definitions and requirements. Incorporation of supervised remote identity proofing capabilities by organizations cross certified with the bridge is optional; however, the protection of PII and applicant redress must be addressed**.**

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

3.2.3.1 Authentication of Human Subscribers

. . .

The FPKIMA, Entity CAs and/or RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- If in-person or supervised remote[1] identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

. . .

For All Levels except PIV-I: If an applicant is unable to perform face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both

[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, Section 5.3.3.

himself/herself and the applicant whom the trusted person is representing.

. . .

The table below summarizes the identification requirements for each level of assurance.

. . .

Assurance Level	**Identification Requirements**
Medium (all policies)	Identity shall be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID, or two Non Federal Government I.D.s, one of which shall be a photo I.D. ~~.(e.g. Non REAL ID Act compliant Drivers Llicense).~~ Any credentials presented must be unexpired. Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the *FBCA Supplementary Antecedent, In-Person Definition* document. For PIV-I, required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form 1-9 OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g. Drivers License).

In the event an applicant is denied a credential based on the results of the identity proofing process, the Entity shall provide a mechanism for appeal or redress of the decision.

3.2.3.4 Authentication of Devices

. . .

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued with the medium Device and mediumDeviceHardware policies, registration information shall be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

6.2.8 Method of Activating Private Keys

. . .

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. When pass-phrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

. . .

9.4.2 Information Treated as Private

The FBCA shall protect all subscriber personally identifying information (PII) from unauthorized disclosure. The FBCA shall also protect personally identifying information for Entity personnel collected to support cross-certification and MOA requirements from unauthorized disclosure. The contents of the archives maintained by the FPKIMA shall not be released except as required by law.

For Entity CAs, ~~no stipulation.~~ collection of PII shall be limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA shall provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes shall not be used for any other purpose.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely and may be released only in accordance with other stipulations in Section 9.4.

All information collected as part of the identity proofing process shall be protected to ensure confidentiality and integrity. In the event the Entity terminated PKI activities, it shall be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

10. Bibliography

NIST SP 800-63-3	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final

12 Glossary

Supervised Remote Identity Proofing

A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.

Estimated Cost: The change in procedures for protecting PII and providing redress may incur some expense for the Entity PKI.

Implementation Date: Entity CAs will have 180 days to update their CPs to incorporate this change and communicate the new requirements to issuing organizations. Incorporation of the supervised remote identity proofing capabilities is optional.

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	December 19, 2018
Date change released for comment:	April 26, 2018
Date approved by FPKIPA:	August 28, 2018