COMMON Certificate Policy Change Proposal Number: 2018-06

To: Federal PKI Policy Authority (FPKIPA)

From: PKI Certificate Policy Working Group (CPWG)
Subject: Incorporate "supervised remote identity proofing and other new guidance as defined in NIST SP 800-63-3
Date: April 23, 2018

Title: Add *supervised remote identity proofing* and other guidance as defined by NIST SP800-63-3

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.28, 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 Federal Common Policy CP to incorporate supervised remote identity proofing and other requirements 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**.**

Specific Changes:

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

3.2.3.1 Authentication of Human Subscribers

. . .

The RA shall ensure that the applicant's identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance.

At id-fpki-common-High, id-fpki-common-derived-pivAuth-hardware and id-fpki-common-authentication, the applicant shall appear at the RA in person or via supervised remote[1]. For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent ~~to support identity proofing of remote applicants~~, assuming agency identity badging requirements are otherwise satisfied. Authentication by a trusted agent does not relieve the RA of its responsibility to verify required procedures were followed as described below. ~~perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), below~~.

At a minimum, authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by agency management.
2) Verify Applicant's employment through use of official agency records.
3) Establish applicant's identity by in-person or supervised remote proofing before the registration authority or trusted agent, as follows: ~~based on either of the following processes~~:

~~a) Process #1:~~

~~i)~~a) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license), as proof of identity, and

[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. In addition, the supervised remote process must have the capability of capturing an approved biometric.

~~ii)~~b) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

~~iii)~~ c) The credential presented in step 3) a)~~ i)~~ above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

~~b) Process #2:~~

~~i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and~~

~~ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and~~

~~iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).~~

~~Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.~~

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative).

2) Verify sponsoring agency employee's identity and employment as follows: ~~through either one of the following methods~~:

   a) A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by an agency CA, may be accepted as proof of both employment and identity,

b) Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or

c) In-person or supervised remote identity proofing of the sponsoring agency employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official agency records.

3) Establish applicant's identity by in-person or supervised remote proofing before the registration authority or trusted agent, as follows: ~~based on either of the following processes:~~

~~a) Process #1~~

~~i)~~ a) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license), as proof of identity, and

~~ii)~~ b) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

~~iii)~~ c) The credential presented in step 3) a) ~~i)~~ above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying official records maintained by the organization that issued the credential.

~~b) Process #2~~

~~i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and~~

~~ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and~~

~~iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3)~~

~~Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.~~

~~b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).~~

4) Record and maintain a biometric of the applicant (e.g., ~~a photograph or~~ fingerprint) by the RA or CA. (Handwritten signatures and other behavioral

characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

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.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature 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).

~~FIPS 201 imposes the strict requirement of in-person registration. The following text only applies to the issuance of non-FIPS 201 credentials:~~

~~For all certificate policies except id-fpki-common-High, where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The trusted agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the trusted agent. The trusted agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the trusted agent satisfy this requirement; other secure methods are also acceptable.~~

3.2.3.2 Authentication of Devices

. . .

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or

- 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.

3.2.3.3 Authentication for Derived PIV Credentials

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, identity shall be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. The RA or CA shall:

1) Verify that the request for certificate issuance to the applicant was submitted by an authorized agency employee.
2) Use the PKI-AUTH authentication mechanism from Section 6 of FIPS 201 to verify that the PIV Authentication certificate on the applicant's PIV Card is valid and that the applicant is in possession of the corresponding private key.
3) Maintain a copy of the applicant's PIV Authentication certificate.

Seven days after issuing the Derived credential, the issuer should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV Card to obtain a derived credential

For certificates issued under id-fpki-common-derived-pivAuth-hardware, the applicant shall appear ~~at the RA~~ in person or via supervised remote to present the PIV Card and perform the PKI-AUTH authentication mechanism. The RA shall perform a one-to-one comparison of the applicant against biometric data stored on the PIV Card, in accordance with [SP 800-76], and shall record and maintain the biometric sample used to validate the applicant. In cases where a 1:1 biometric match against the biometrics available on the PIV Card or in the chain-of-trust, as defined in [FIPS201] is not possible:

1) The applicant shall present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV Card, and
2) The RA shall examine the presented credentials for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of the applicant), and
3) The process documentation for the issuance of the certificate shall include the identity of the person performing the verification of the second (non-PIV) form of identification, a signed declaration by that person that he or she verified the identity of the applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the applicant, and the date and time of the verification.

3.3.1 Identification and Authentication for Routine Re-key

. . .

For policies other than id-fpki-common-High, a subscriber's identity may be established through use of current signature key, except that identity shall be re-established through

an in-person or supervised remote registration process at least once every nine years from the time of initial registration.

. . .

6.2.8 Method of Activating Private Keys

For certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, 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).

. . .

9.4.1 Privacy Plan

The FPKIMA or Agency PMA shall conduct a Privacy Impact Assessment. If deemed necessary, the FPKIMA or Agency PMA shall have a Privacy Plan to protect personally identifying information (PII) from unauthorized disclosure. For the Common Policy Root CA, the FPKIPA shall approve the Privacy Plan. Privacy plans will be implemented in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2 Information Treated as Private

Federal entities acquiring services under this policy shall protect all subscriber ~~personally identifying information~~ PII from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as required by law.

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.

9.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2. However, certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).

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 Agency PMA terminates 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

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

~~SP 800-63 Electronic Authentication Guideline, NIST Special Publication 800-63-2, August 2013.~~
~~http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf~~

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.

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

Implementation Date: Entity CAs will have 180 days to update their CPSes to incorporate this change and communicate the new requirements related to protection of PII and applicant redress to their issuing organizations. Implementation of supervised remote identity proofing capabilities is optional for issuing organizations.

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