FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2020-01

To:	Federal PKI Policy Authority (FPKIPA)
From:	Federal PKI Certificate Policy Working Group (CPWG) PIV-I Work Team
Subject:	Add support for PIV-I credentials issued under Common
Date:	March 10, 2020

Title: Support for Personal Identity Verification-Interoperable (PIV-I) credentials issued under Common

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 1.31, February 8, 2019*

Change Advocate's Contact Information:
Organization: FPKI Policy Authority
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group - PIV-Interoperable (PIV-I) Issuers Work Team

Change summary: Update the CP to support federally issued and managed PIV-I smart cards issued to non-PIV users under Common

Background: Federal agencies have identified use cases not addressed under the current Common Policy to include issuance of smart cards to non-NACI users managed by the executive branch agencies. A work team was formed to discuss options and identified new policy OIDs under Common as an approach to be considered. This change proposal adds new common-PIV-Interoperable OIDs to Common Policy to support these use cases. Though temporary credential use cases were included in earlier versions of the change proposal, agency participants determined requirements could be fully satisfied by the common-PIV-Interoperable policies.

Specific Changes:

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

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CA shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-devicesHardware	::= {2 16 840 1 101 3 2 1 3 36}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}
id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}
id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}
id-fpki-common-pivi-authentication	::= {2 16 840 1 101 3 2 1 3 xx}
id-fpki-common-pivi-cardAuth	::= {2 16 840 1 101 3 2 1 3 xx}
id-fpki-common-pivi-contentSigning	::= {2 16 840 1 101 3 2 1 3 xx}

...

This document includes five policies specific to FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors. Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV Card, may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key is stored on a PIV Card and can be used without user authentication may contain id-fpki-common-cardAuth. Certificates issued to users, in accordance with NIST SP 800-157, supporting authentication, but not digital signature, where the corresponding private key is not stored on a PIV Card, may contain either id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth as appropriate. The id-fpki-common-piv-contentSigning policy shall only be asserted in certificates issued to devices that sign PIV data objects in accordance with [FIPS 201] or [SP 800-157].

Certificates issued to users supporting authentication where the private key is stored on a Common PIV-I credential and requires user authentication shall contain id-fpki-common-pivi-authentication. Certificates issued to users supporting authentication where the private key is stored on a Common PIV-I credential and can be used without user authentication shall contain id-fpki-common-pivi-cardAuth. The id-fpki-common-pivi-contentSigning policy shall only be asserted in certificates issued to devices that sign Common PIV-I credential data objects.

The requirements associated with id-fpki-common-pivi-authentication and id-fpki-common-pivi-cardAuth are identical to id-fpki-common-authentication and id-fpki-common-cardAuth, respectively, with the exception of the need for a NACI and associated favorable adjudication. For additional comparisons, see Appendix [A].

The requirements associated with id-fpki-common-piv-contentSigning and id-fpki-common-pivi-contentSigning are identical to id-fpki-common-devicesHardware, except where specifically noted in the text.

1.4.1 Appropriate Certificate Uses

...

This CP is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this CP may also be used for key establishment. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations.

Credentials issued under the id-fpki-common-policy and id-fpki-common-derived-pivAuth policies are intended to meet the requirements for Level 3 authentication, as defined by the OMB E Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

Credentials issued under the id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning policy are intended to meet the requirements in FIPS 201 and SP 800-157 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV data objects.

In addition, this policy may support signature and confidentiality requirements for Federal government processes.

1.4.2 Prohibited Certificate Uses

Certificates that assert id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth shall only be used to authenticate the hardware token containing the associated private key and shall not be interpreted as authenticating the presenter or holder of the token.

3.1.1 Types of Names

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-devices and id-fpki-common-devicesHardware the CA shall assign X.501 distinguished names to all subscribers. These distinguished names may be in either of two forms: a geo-political name or an Internet domain component name.

…

For certificates issued under id-fpki-common-authentication or id-fpki-common-pivi-authentication, assignment of X.500 distinguished names is mandatory. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions. Certificates issued under id-fpki-common-authentication or id-fpki-common-pivi-authentication shall include a subject alternative name. ~~At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.~~

For certificates asserting id-fpki-common-authentication, at a minimum, the subject alternative name extension shall include:

1) the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card
2) The UUID [RFC 4122]

For certificates asserting id-fpki-common-pivi-authentication, at a minimum, the subject alternative name extension shall include:

1) The UUID [RFC 4122]

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth ~~may~~ shall also include a UUID [RFC 4122] in the subject alternative name extension, ~~if the UUID is included~~ as specified in Section 3.3 of [SP 800-73-3(1)]. Certificates issued under id-fpki-common-pivi-cardAuth shall only include a UUID [RFC 4122] in the subject alternative name extension. Certificates issued under id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

PIV Examples:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*FASC-N*
- dc=gov, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*
- dc=mil, dc=*org0*, [*dc=org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*

PIV or PIV-I Examples:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*UUID*
- dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*
- dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*

3.2.3.1 Authentication of Human Subscribers

Procedures used by agencies to issue identification to their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the agency procedures for authentication of personnel shall apply in addition to the guidance in this section.

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, and id-fpki-common-pivi-authentication, the applicant shall appear at the RA in person or via supervised remote. For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent, 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.

...

4.9.9 On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 6960] for end entity certificates issued under id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-cardAuth and id-fpki-common-pivi-cardAuth.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For the id fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-pivi-cardAuth and id-fpki-common-cardAuth policies, subscriber key pairs shall be generated in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both. User certificates that assert id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, ~~or~~ id-fpki-common-cardAuth, or id-fpki-common-pivi-cardAuth shall only assert the *digitalSignature* bit. Other user certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

…

Signing certificates issued under the policy for id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning shall include an extended key usage of *id-PIV-content-signing* (see [CCP-PROF]).

6.2.1 Cryptographic Module Standards and Controls

…

RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

PIV Cards are PKI tokens that have private keys associated with certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth. PIV Cards shall only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL).

PIV-I cards have private keys associated with certificates asserting id-fpki-common-pivi-authentication or id-fpki-common-pivi-cardAuth. PIV-I cards issued by federal executive branch agencies and the certification authorities operating under this policy shall only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL).

Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. ~~PIV cards~~ Smart cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA. On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV and/or PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the authentication policies (id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, ~~or~~ id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

...

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, or id-fpki-common-High policy shall not be backed up or copied.

6.2.8 Method of Activating Private Key

For certificates issued under id-fpki-common-authentication, id-fpki-common-pivi-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 passphrases 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).

For certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. For certificates issued under id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning, the PIV card issuance system or device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

For certificates issued under id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth, subscriber authentication is not required to use the associated private key.

6.3.2 Certificate Operational Periods and Key Usage Periods

...

Subscriber public keys in certificates that assert the id-PIV-content-signing or id-fpki-common-pivi-contentSigning OID in the extended key usage extension have a maximum usage period of nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning certificate shall be later than the expiration of the credential's id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, or id-fpki-common-derived-pivAuth certificates.

7.1.4 Name Forms

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-High, id-fpki-common-devices, id-fpki-common-devicesHardware, ~~and~~ id-fpki-common-piv-contentSigning, and id-fpki-common-pivi-contentSigning shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

The subject alternative name extension shall be present and include a UUID, encoded as a URI, in certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-derived-pivAuth-hardware ~~and~~ id-fpki-common-derived-pivAuth, id-fpki-common-pivi-authentication, and id-fpki-common-pivi-cardAuth.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-derived-pivAuth ::= {2 16 840 1 101 3 2 1 3 40}

id-fpki-common-derived-pivAuth-hardware ::= {2 16 840 1 101 3 2 1 3 41}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

id-fpki-common-piv-contentSigning ::= {2 16 840 1 101 3 2 1 3 39}

id-fpki-common-pivi-authentication ::= {2 16 840 1 101 3 2 1 3 XX}

id-fpki-common-pivi-cardAuth ::= {2 16 840 1 101 3 2 1 3 XX}

id-fpki-common-pivi-contentSigning ::= {2 16 840 1 101 3 2 1 3 XX}

Certificates that express the id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning policy OID shall not express any other policy OIDs.

10. Bibliography

The following documents were used in part to develop this CP:

PIV-I Issuers	Personal Identity Verification Interoperability for Issuers https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-i-for-issuers.pdf
PIV-I Profiles	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-pivi-cert-profiles.pdf

APPENDIX [A] – PIV AND COMMON PIV INTEROPERABLE (COMMON PIV-I) COMPARISON

	Technical Requirements	PIV	PIV-I
Trust	Suitability Assurance: Favorably adjudicated National Agency Check with Inquiries (minimum) or other Tier 1 investigation	x	
	PIV policy object identifier on PIV Authentication Certificates	x	
	PIV-I equivalent policy object identifier on PIV-I Authentication Certificates		x
	PIV Content Signing object signing certificate	x	
	PIV-I Content Signing equivalent object signing certificate		x
	PIV Card Authentication Certificate	x	
	PIV-I Card Authentication Certificate		x
	Card shall not be valid for more than 6 years and card expiration shall not exceed the expiration date of object signing certificate	x	x
Credential Edge	Card stock certified by FIPS 201 Evaluation Program	x	x
	Command edge and NIST SP 800-85 conformant	x	x
	NIST SP 800-73 conformant data model and PIV Application Identifier (AID)	x	x
	NIST SP 800-73 conformant to include GUID present in the CHUID	x	x
	RFC 4122 conformant UUID required in the GUID data element of the CHUID	x	x
	RFC 4122 conformant UUID present in the Authentication Certificates	x	x

Topography	FIPS 201 compliant topography	x	
	Minimally contains facial image, cardholder name, issuing organization, and expiration, but does not replicate FIPS 201 topography requirements		x
Card Management System	Card Management Master Key maintained in a FIPS 140-2 Level 2 Cryptographic Module and conforms to [NIST SP 800-78] requirements; activation of the Card Management Master Key requires commensurate authentication of Trusted Roles	x	x

Estimated Cost: The change would only apply to agencies wanting to support smart cards for non-PIV users and would require CA updates and the issuance of new policy OIDS to the issuing CAs. CAs supporting the new policies would require updated CPS and approval by the FPKIPA.

Implementation Date: Immediately approval upon approval and publication of the updated Common Policy

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG: January 28, 2020
Date change released for comment: March 10, 2020
Date approved by FPKIPA: March 27, 2020