Archived Document	
Title:	**Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles Version 2.0**
Publication Date:	**September 1, 2020**
Archive Date:	**February 8, 2021**
Archive Notes:	**This document has been superseded**

Superseding Document	
Title:	**Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles (Version 2.1)**
Publication Date:	**February 1, 2021**
URL:	**Current and Archived Versions:** http://www.idmanagement.gov/

Additional Information	
Contact:	fpki@gsa.gov

Page Reviewed/Updated:

Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles

Federal PKI Policy Authority

Version 2.0

September 1, 2020

Revision History

Date	Version	Description
March 9, 2004	1.0	Initial version of profile
July 8, 2004	1.1	1) The dual-use certificate profile for human end users has been removed in order to align with Common Certificate Policy. 2) The section on URIs now recommends the use of a single LDAP URI that specifies multiple attributes rather than use of multiple LPAP URIs in the authorityInfoAccess and subjectInfoAccess extensions. 3) The section on URIs now indicates that the subjectInfoAccess extension may be omitted from CA certificates if the certificate subject does not issue CA certificates.
January 19, 2006	1.2	Added certificate profiles for Card Authentication Certificates and PIV Authentication Certificates as specified in FIPS 201 and aligned algorithms with NIST SP 800-78.
February 6, 2006	1.3	Modified the PIV Authentication Certificate Profile in Worksheet 9 to reflect that these certificates cannot assert id-fpki-common-hardware in the certificatePolicies extension.
March 9, 2006	1.4	Added id-pki-common-cardAuth to the list of policy OIDs that may be asserted in CA certificates (worksheets 2 and 3).
January 7, 2008	1.5	1) Modified set of elliptic curve algorithms to align with NIST SP 800-78-1. 2) Added certificate profile for OCSP responders. 3) Made subject DN in PIV Authentication certificates mandatory (Common Policy change proposal 2007-02). 4) Allow legacy Federal PKIs to include either an LDAP or an HTTP URI in the cRLDistributionPoints extension of PIV Authentication certificates, rather than requiring the inclusion of both URIs.
October 31, 2012	1.6	Incorporates changes for Common Policy Change Proposal 2011-03 – Remove Requirements for LDAP URIs.
May 5, 2015	1.7	1) Added new Common Content Signing Certificate Worksheet 10, new Common Derived PIV Authentication Worksheet 11, 2) Made changes in compliance with FIPS 201-2: added

		UUID to PIV Auth and PIV CardAuth certificates and changed Signature & Device worksheets to the piv-contentsigning EKU cannot be used after 10/31/2015 3) Incorporated changes for Common Policy Change Proposal 2015-01 (Common Derived PIV) & 2015-02 (anyEKU optional)
July 17, 2017	1.8	Align with current practice & Common Policy CP v1.27 1) Specify only minimum key size for Root CA 2) Deleted comment about discouraging the use of policy Qualifiers 3) Add Policy Constraints – non-critical exception from RFC 5280 4) Add InhibitAnyPolicy – non-critical exception from RFC 5280
May 10, 2018	1.9	2018-03 Mandate specific EKU in Common Policy subscriber certificates to align with Industry Practices
September 1, 2020	2.0	1) Enhance formatting and readability 2) Align with Common Policy CP v2.0 3) Reordered certificate profile worksheets for logical organization 4) Included an independent profile for Intermediate CA certificates 5) Add non-PIV Authentication profile 6) Add Common PIV-I associated profiles

Table of Contents

1. Introduction

This document specifies the profiles for certificates and CRLs issued under the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON] and that have a trust path to the Federal Common Policy CA operated by the Federal PKI Management Authority.

Requirements are included in five sections of this document:

- Section 2: X.509 v3 Certificates
- Section 3: X.509 v2 Certificate Revocation Lists
- Section 4: Encoding of Relative Distinguished Names
- Section 5: Use of URIs
- Section 6: Profile Worksheets

The purpose of these profiles is to maintain consistency and interoperability across the Federal PKI for cross-agency use.

2. X.509 v3 Certificates

X.509 v3 certificates contain the identity and attribute data of the certificate subject in the base certificate fields and certificate extensions. Detailed information about X.509 certificates can be found in [X.509] and [RFC 5280].

The base certificate fields identify the issuer (i.e., CA), subject, version number, subject's public key, validity period, and serial number of the certificate along with the public key algorithm used to digitally sign the certificate. Certificate extensions contain additional information about the subject or the CA.

Each of the certificate profile worksheets in Section 6 list mandatory contents of a particular class of certificates. Optional features that are supported in Federal PKI are also identified. These features may be included at the discretion of the certificate issuer.

Standard certificate extensions are defined in [X.509]. For each profile worksheet, any standard extensions that are not specified as mandatory or optional must not be included.

Certificate issuers may include additional information in non-critical private certificate extensions for local use, but should not expect clients in the Federal PKI to process this additional information. Critical certificate extensions that are not listed in these profile worksheets must not be included.

3. X.509 v2 Certificate Revocation Lists

X.509 v2 certificate revocation lists identify the issuer CA, the date the CRL was generated, the date by which the next CRL must be generated, and the list of revoked certificates.

The Certificate Revocation List worksheet in Section 6 lists mandatory contents of CRLs. Optional features that are supported in the Federal PKI are also identified. These features may be included at the discretion of the certificate issuer.

Standard CRL extensions are defined in [X.509]. For the CRL worksheet, any standard extensions that are not specified as mandatory or optional must not be included.

Certificate issuers may include additional information in non-critical private CRL extensions for local use, but should not expect clients in the Federal PKI to process this additional information. Critical CRL extensions that are not listed in the CRL worksheet must not be included in the CRLs issued.

CRLs must be stored as HTTP accessible files and may be stored as attributes in a directory.

CRLs must comply with the requirements of Section 4.9.7 of [COMMON] and must be full and complete as described in [RFC 5280], these CRLs must not be indirect CRLs, delta-CRLs, or CRLs partitioned by reason code.

CAs may optionally issue additional CRLs, such as CRLs partitioned by a value other than reason code or delta-CRLs.

If delta-CRLs are issued, then either the certificates or the full CRLs that correspond to the delta-CRLs should include a FreshestCRL extension that points to the delta-CRLs.

4. Encoding of Relative Distinguished Names

Certificates must use either PrintableString or UTF8String for all DirectoryString Relative Distinguished Names.

The issuer field of certificates and CRLs should be encoded exactly as it is encoded in the subject name of the signing CA certificate to avoid complications associated with name chaining and name constraints computation. Commonly used certificate path validation implementations may be unable to perform name comparisons when names are encoded using different character sets. CAs are strongly encouraged to use consistent encoding of identical distinguished name components within a hierarchy.

CAs should use consistent encoding of name constraints and all constrained name components within the certification path. Name constraints specified in CA certificates must be compared with the subject names in subsequent certificates in a certification path, to ensure they are applied correctly.

5. Use of URIs

Uniform Resource Identifiers (URIs) are found in three different extensions within the certificate profiles:

- cRLDistributionPoints
- authorityInfoAccess
- subjectInfoAccess

Each of these extensions must include an HTTP URI. If an LDAP URI is included, it must appear after the HTTP URI.

For all URIs:

- The scheme portion of all URIs must be either "http" or "ldap".
- The hostname must be specified as a fully qualified domain name.
- The default port for the relevant protocol (80 for HTTP and 389 for LDAP) must be used, but need not be included in the URI.

5.1. CRL Distribution Points Extension

This section includes requirements in addition to those specified in Section 2.2.1 in [COMMON].

At least one HTTP URI is required and:

- Must return a file that contains the latest DER encoded full and complete CRL, with a file extension of ".crl".
- Must include “Content-Type: application/pkix-crl” in the HTTP response headers.

If the DistributionPointName is present in the issuingDistributionPoint extension of the CRL, the value must match at least one DistributionPointName in the cRLDistributionPoints extensions in each of the certificates covered by the CRL.

An LDAP URI may be included in the cRLDistributionPoints extension. If present, the LDAP URI must include the DN of the entry containing the CRL and specify the directory attribute in which the CRL is located (certificateRevocationList, authorityRevocationList, or deltaRevocationList).

5.2. Authority Information Access Extension

This section includes requirements in addition to those specified in Section 2.2.1 in [COMMON].

The HTTP URI in the authorityInfoAccess extension must contain at least one instance of the id-ad-caIssuers access method containing a publicly accessible HTTP URI which returns a certs-only Cryptographic Message [RFC 8551]. This message:

- Must contain a binary file with an extension of ".p7c".
- Must include “Content-Type: application/pkcs7-mime” in the HTTP response headers.
- Must not contain any self-signed CA certificates.
- Must include one or more currently valid CA certificates issued to the issuer of the certificate, which may be used to verify the signature on the certificate.
- Must be an empty certs-only CMS format, if no currently valid CA certificates can be included.

Alternatively, the HTTP URI may return a single DER encoded certificate that has an extension of “.cer” [RFC 2585] and must include “Content-Type: application/pkix-cert” in the HTTP response headers. The use of this option is discouraged because it does not permit zero or multiple CA certificates, thereby reducing flexibility.

An LDAP URI may be included in the authorityInfoAccess extension, id-ad-caIssuers

access method, that specifies either or both the cACertificate and crossCertificatePair attributes. A CA may, alternatively, specify each of the attributes in a separate LDAP URI.

The authoritative OCSP [RFC 6960] service must be specified in the authorityInfoAccess extension, id-ad-ocsp access method, of each Subscriber certificate and the scheme portion of the URI must be "http". This HTTP response must include “Content-Type: application/ocsp-response” in the HTTP response headers.

5.3. Subject Information Access Extension

This section includes requirements in addition to those specified in Section 2.2.1. in [COMMON].

The subjectInfoAccess extension must appear in CA certificates, unless the CA certificate asserts a path length constraint of zero in the Basic Constraints extension.

When present, the subjectInfoAccess extension must contain at least one instance of the id-ad-caRepository access method containing a publicly accessible HTTP URI which returns a certs-only Cryptographic Message [RFC 8551]. This message:

- Must contain a binary file with an extension of ".p7c"
- Must include “Content-Type: application/pkcs7-mime” must be included in the HTTP response headers.
- Must contain all currently valid CA certificates issued by the subject of this certificate, except self-signed certificates
- Must be an empty certs-only CMS format, if no currently valid CA certificates can be included.

An LDAP URI may be included in the subjectInfoAccess extension, id-ad-caRepository access method. If present, the LDAP URI must include the DN of the entry containing the relevant certificates and specify the directory attribute in which the certificates are located.

6. Profile Worksheets

The profile worksheets identify the mandatory and optional extensions of certificates and CRLs. Unless otherwise stated, all fields and extensions listed are mandatory. Certificate extensions defined in [RFC 5280] that are not specified as mandatory or optional in the profile worksheets must not be included.

#	Profile	Description
1	Self-Signed CA Certificate	Self-Signed CA certificates issued by the Federal Common Policy CA for use as the trust anchor by PKI client applications
2	Self-Issued CA Certificate	Key rollover certificates, sometimes called link certificates

3	Cross Certificate	Issued to CAs that operate under a Certificate Policy other than the Common Certificate Policy
4	Intermediate CA Certificate	CA certificates issued to subordinate CAs operating under the Common Policy CP
5	PIV Content Signing Certificate	Content Signing certificate used to sign PIV data objects in accordance with [FIPS 201] or [SP 800-157]
6	PIV Authentication Certificate	Certificates for PIV Authentication as defined in Section 4.2.2 of FIPS 201.
7	Card Authentication Certificate	Certificates for Card Authentication as defined in Section 4.2.2 of FIPS 201.
8	Signature Certificate	Applies to signature certificates issued to Federal employees and contractors both on PIV cards and other form factors.
9	Key Management Certificate	Applies to key management certificates issued to Federal employees and contractors both on PIV cards and other form factors.
10	Derived PIV Authentication Certificate	PIV Authentication certificates issued in accordance with NIST SP 800-157.
11	Authentication Certificate	Authentication certificates not directly related to PIV.
12	Device Certificate	Certificates issue to computing or communications devices (e.g., routers, firewalls, servers, etc.) and software applications.
13	Delegated OCSP Responder Certificate	Certificates issued to OCSP responders.
14	Certificate Revocation List	CRLs issued by CAs that issue certificates under the Common Policy.
15	Common PIV-I Content Signing Certificate	Certificates for federally-issued PIV-I Content Signing as defined in Common Policy.
16	Common PIV-I Authentication Certificate	Certificates for federally-issued PIV-I Authentication as defined in Common Policy.
17	Common PIV-I Card Authentication Certificate	Certificates for federally-issued PIV-I Card Authentication as defined in Common Policy.

Worksheet 1: Self-Signed Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of this certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE keyCertSign, cRLSign
Basic Constraints	Critical = TRUE cA:TRUE Path length constraints should not be included.
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Subject Information Access	id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. See Section 5.3.

Worksheet 2: Self-Issued CA Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of this certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy. Subject DN must be encoded exactly as it is encoded in the Issuer DN of the certificates and CRLs issued by this CA.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE keyCertSign, cRLSign
Extended Key Usage *(Optional)*	Included if the CA is being restricted to the issuance of specific certificate types. This may be required for inclusion in public trust stores.
Basic Constraints	Critical = TRUE cA:TRUE The pathLenConstraint field should not appear in self-issued certificates.
Subject Key Identifier	Derived using a cryptographic hash of the public key.

Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Information Access *(Optional)*	id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. See Section 5.3.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method may be included if status information for this certificate is available via OCSP. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devices-hardware 2.16.840.1.101.3.2.1.3.39 id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 id-fpki-common-derived-pivAuth-hardware 2.16.840.1.101.3.2.1.3.45 id-fpki-common-pivi-authentication 2.16.840.1.101.3.2.1.3.46 id-fpki-common-pivi-cardAuth 2.16.840.1.101.3.2.1.3.47 id-fpki-common-pivi-contentSigning

Worksheet 3: Cross Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Distinguished name of the owner of the subject public key in the certificate. Subject DN must be encoded exactly as it is encoded in the Issuer DN of the certificates and CRLs issued by this CA.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE keyCertSign, cRLSign
Extended Key Usage *(Optional)*	Included if the CA is being restricted to the issuance of specific certificate types. This may be required for inclusion in public trust stores.
Basic Constraints	Critical = TRUE cA:TRUE If the subject CA issues only subscriber certificates, the path length constraint must be present and set to zero. In all other cases, the use of a path length constraint is optional.
Subject Key Identifier	Identical to value in the Authority Key Identifier extension of the certificates issued by this CA. Derived using a cryptographic hash of the public key.

Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Information Access	id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted. See Section 5.3.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method may be included if status information for this certificate is available via OCSP. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devices-hardware 2.16.840.1.101.3.2.1.3.39 id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 id-fpki-common-derived-pivAuth-hardware Additional applicable Federal PKI policy OIDs may be asserted.
Policy Mappings	One or more mappings from FPKI (issuer domain) certificate policies to subject domain certificate policies deemed comparable by FPKI PA.
Policy Constraints	Critical = FALSE requireExplicitPolicy with SkipCerts = 0 must be present. inhibitPolicyMapping must be included with SkipCerts = 0 when issued to an SSP. Where downstream mappings are permitted, SkipCerts is set to the minimum value required to support the expected mappings.
Inhibit Any Policy	Critical = FALSE SkipCerts = 0
Name Constraints *(Optional)*	Critical = TRUE Any combination of permitted and excluded subtrees may appear. The minimum field must be zero, and maximum field must not be present.

Worksheet 4: Intermediate CA Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy. Subject DN must be encoded exactly as it is encoded in the Issuer DN of the certificates and CRLs issued by this CA.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE keyCertSign, cRLSign
Extended Key Usage *(Optional)*	Included if the CA is being restricted to the issuance of specific certificate types. This may be required for inclusion in public trust stores.
Basic Constraints	Critical = TRUE cA:TRUE If the subject CA issues only subscriber certificates, the path length constraint must be present and set to zero. In all other cases, the use of a path length constraint is optional.
Subject Key Identifier	Identical to value in the Authority Key Identifier extension of the certificates issued by this CA. Derived using a cryptographic hash of the public key.

Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name *(Optional)*	directoryName may be included to support local requirements
Subject Information Access	id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted. See Section 5.3.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method may be included if status information for this certificate is available via OCSP. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devices-hardware 2.16.840.1.101.3.2.1.3.39 id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 id-fpki-common-derived-pivAuth-hardware 2.16.840.1.101.3.2.1.3.45 id-fpki-common-pivi-authentication 2.16.840.1.101.3.2.1.3.46 id-fpki-common-pivi-cardAuth 2.16.840.1.101.3.2.1.3.47 id-fpki-common-pivi-contentSigning Additional applicable agency specific policies may be asserted.
Policy Constraints *(Optional)*	Critical = FALSE When this extension appears, both requireExplicitPolicy and inhibitPolicyMapping must be present and assert SkipCerts = 0.
Inhibit Any Policy *(Optional)*	Critical = FALSE SkipCerts = 0
Name Constraints *(Optional)*	Critical = TRUE Any combination of permitted and excluded subtrees may appear. The minimum field must be zero, and maximum field must be absent.

Worksheet 5: PIV Content Signing Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy and must indicate the organization administering the PIV card issuance system
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	Critical = TRUE Must assert only id-PIV-content-signing keyPurposeID (2.16.840.1.101.3.6.7)
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.

Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	Must assert only 2.16.840.1.101.3.2.1.3.39 id-fpki-common-contentSigning

Worksheet 6: PIV Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive INTEGER.
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019 anyExtendedKeyUsage may be present or this extension may be absent.

Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name	Must include FASC-N and UUID. FASC-N otherName has type-id 2.16.840.1.101.3.6.6 and specifies the FASC-N of the PIV Card. UUID uniformResourceIdentifier contains the GUID data element of the CHUID of the PIV Card encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication Additional applicable agency specific policy OIDs may be asserted.
PIV NACI	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-2. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance the subject's NACI has not completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 7: Card Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use the name form specified in Section 3.1.1 of the Common Certificate Policy (must include the serialNumber Relative Distinguished Name set to the FASC-N or UUID, no other name forms may be included)
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	Critical = TRUE Must assert only id-PIV-cardAuth keyPurposeID (2.16.840.1.101.3.6.8). The id-PIV-cardAuth keyPurposeID specifies that the public key is used to authenticate the PIV Card rather than the PIV card holder.
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.

Subject Alternative Name	Must include FASC-N and UUID. No other name forms may be included. FASC-N: otherName specifies the type-id (2.16.840.1.101.3.6.6) with the FASC-N value as an OCTET STRING representing the PIV Card that contains the corresponding Card Authentication key. UUID: uniformResourceIdentifier contains the UUID from the GUID data element of the CHUID of the PIV Card encoded as a URI as specified in Section 3 of RFC 4122.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth
PIV NACI	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-2. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 8: Signature Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE digitalSignature, nonRepudiation
Extended Key Usage	One or more keyPurposeIDs consistent with digital signature must be specified. Recommended: 1.3.6.1.5.5.7.3.4 id-kp-emailProtection (required for PIV) 1.3.6.1.4.1.311.10.3.12 MSFT Document Signing Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019 anyExtendedKeyUsage may be present or this extension may be absent.
Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent

Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name *(Optional)*	rfc822Name is required if id-kp-emailProtection (1.3.6.1.5.5.7.3.4) is asserted in Extended Key Usage otherName values (e.g. Microsoft UPN) may be included to support local applications.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High Additional applicable agency specific policies may be asserted.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 9: Key Management Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE keyEncipherment for RSA Subject Public Key keyAgreement for ECC Subject Public Key
Extended Key Usage	One or more keyPurposeIds consistent with key management purposes must be included. For PIV, 1.3.6.1.5.5.7.3.4 id-kp-emailProtection must be included. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019 anyExtendedKeyUsage may be present or this extension may be absent.
Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent

Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name *(Optional)*	rfc822Name is required if id-kp-emailProtection (1.3.6.1.5.5.7.3.4) is asserted in Extended Key Usage otherName values (e.g. Microsoft UPN) may be included to support local applications.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High Additional applicable agency specific policies may be asserted.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 10: Derived PIV Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019 anyExtendedKeyUsage may be present or this extension may be absent.

Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name	Must include uniformResourceIdentifier containing the UUID encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	Must assert one of the following: 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 Id-fpki-common-derived-pivAuth-hardware Additional applicable agency specific policy OIDs may be asserted.
PIV NACI	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-2. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 11: Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication One or more additional keyPurposeIds consistent with authentication may be specified. For example; 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value.
Basic Constraints *(Optional)*	May be critical or non-critical

	cA:FALSE Path length constraint must be absent
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name *(Optional)*	One or more of the following are permitted: rfc822Name otherName values (e.g. Microsoft UPN) to support local applications directoryName to support local applications FASC-N must not be included
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High Additional applicable agency specific policies may be asserted.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 12: Device Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE nonRepudiation must not be asserted in a device certificate If a certificate is used for digital signature or authentication of ephemeral keys (e.g. TLS), digitalSignature must be asserted If a certificate is used for key management: keyEncipherment must be asserted when public key is RSA keyAgreement must be asserted when public key is elliptic curve Note: Use of a single certificate for both digital signatures and key management is deprecated, but may be used to support legacy applications that require the use of such certificates.
Extended Key Usage	May be critical or non-critical One or more key purposes consistent with the keyUsage must be specified.

	Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019 anyExtendedKeyUsage may be present or this extension may be absent.
Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name *(Optional)*	The following name types may be present: dNSName is an IA5String that contains the DNS name of the subject URI is an IA5String that contains the URI of the subject rfc822Name that contains the email address of the sponsor, administrator, or help desk otherName values may also be included to support local applications
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	Must assert one of these policy OIDs from the Common Certificate Policy. 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devicesHardware Additional applicable agency specific policy OIDs may be asserted.

Worksheet 13: Delegated OCSP Responder Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	Maximum of 45 days utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	Critical = TRUE Must assert only 1.3.6.1.5.5.7.3.9 id-kp-OCSPSigning
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.

Subject Alternative Name *(Optional)*	The following name types may be present: dNSName is an IA5String that contains the DNS name of the subject URI is an IA5String that contains the URI of the subject rfc822Name that contains the email address of the sponsor, administrator, or help desk otherName values may also be included to support local applications
Authority Information Access *(Optional)*	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must not be included. See Section 5.2.
Certificate Policies	Must assert all policy OIDs for which the OCSP server is authoritative. One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication 2.16.840.1.101.3.2.1.3.16 id-fpki-common-High 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devices-hardware 2.16.840.1.101.3.2.1.3.39 id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 id-fpki-common-derived-pivAuth-hardware Additional applicable agency specific policy OIDs may be asserted.
OCSP No Check	NULL

Worksheet 14: Certificate Revocation List

Field	Content
Version	INTEGER Value of "1" for Version 2 CRL.
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
This Update	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Next Update	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Revoked Certificates	userCertificate is the serial number of the certificate being revoked. revocationDate is the date and time of revocation. reasonCode CRL entry extension must be included for certificateHold. If the revocation reason is unspecified, this extension should be omitted. Use of this extension is optional for other reason codes. removeFromCRL must be used only in delta CRLs. Note: certificateHold must be used only for suspension of subscriber certificates. invalidityDate CRL entry extension may be included if the invalidity date precedes the revocation date.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
CRL Number	cRLNumber is a sequentially increasing number
Issuing Distribution Point *(Optional)*	Critical = TRUE This extension appears only in CRLs that do not cover all unexpired certificates in which the issuer field contains the same name as the issuer field in the CRL. For example, when a CA is rekeyed and issues separate CRLs from each key. Must conform with the requirements in section 5.2.5 of RFC 5280 with the following constraints: onlySomeReasons must not appear indirectCRL must be FALSE

Worksheet 15: Common PIV-I Content Signing Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy and must indicate the organization administering the PIV-I card issuance system
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the NIST approved curves referenced in 800-78: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	Critical = TRUE Must assert only id-fpki-pivi-content-signing keyPurposeID (2.16.840.1.101.3.8.7)
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or,

	(discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	Must assert only 2.16.840.1.101.3.2.1.3.47 id-fpki-common-pivi-contentSigning

Worksheet 16: Common PIV-I Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive INTEGER.
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the Common Certificate Policy
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the NIST approved curves referenced in 800-78: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value.
Basic Constraints *(Optional)*	May be critical or non-critical cA:FALSE Path length constraint must be absent

Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name	Must include UUID. UUID uniformResourceIdentifier contains the GUID data element of the CHUID of the PIV-I Card encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	2.16.840.1.101.3.2.1.3.45 id-fpki-common-pivi-authentication Additional applicable agency specific policy OIDs may be asserted.
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

Worksheet 17: Common PIV-I Card Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms the parameters field is NULL.
Issuer DN	Issuer DN must be encoded exactly as it is encoded in the Subject DN of the issuing CA certificate
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must use the name form specified in Section 3.1.1 of the Common Certificate Policy (must include the serialNumber Relative Distinguished Name set to the UUID, no other name forms may be included)
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public key must be encoded in uncompressed form. ECParameters is one of the NIST approved curves referenced in 800-78: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Key Usage	Critical = TRUE Must assert only digitalSignature
Extended Key Usage	Critical = TRUE Must assert only id-PIV-cardAuth keyPurposeID (2.16.840.1.101.3.6.8). The id-PIV-cardAuth keyPurposeID specifies that the public key is used to authenticate the PIV-I Card rather than the PIV-I card holder.
Subject Key Identifier	Derived using a cryptographic hash of the public key.
Authority Key Identifier	Identical to Subject Key Identifier in the issuing CA certificate. authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject Alternative Name	Must include UUID. No other name forms may be included.

	UUID: uniformResourceIdentifier contains the UUID from the GUID data element of the CHUID of the PIV Card encoded as a URI as specified in Section 3 of RFC 4122.
CRL Distribution Points	Must contain at least one HTTP URI pointing to a full and complete CRL. The reasons and cRLIssuer fields must be omitted. An LDAP URI or Directory Name may also be included, but these must appear after the HTTP URI. See Section 5.1.
Authority Information Access	Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or, (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585) The OCSP access method must be included. The access location must specify the location of the HTTP accessible OCSP server. See Section 5.2.
Certificate Policies	2.16.840.1.101.3.2.1.3.46 id-fpki-common-pivi-cardAuth
Subject Directory Attributes *(Optional)*	This extension may be included to indicate the cardholder's country or countries of citizenship, as specified in RFC 3739. countryOfCitizenship (1.3.6.1.5.5.7.9.4) will be a ISO 3166 Country Code(s) value.

7. Acronyms

AKID	Authority Key Identifier
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
RFC	Request For Comments
RSA	Rivest-Shamir-Adelman
SHA	Secure Hash Algorithm
SKID	Subject Key Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universally Unique IDentifier

8. References

ABADSG	Digital Signature Guidelines, 1996-08-01. http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines
APL	Approved Products List (APL) http://www.idmanagement.gov/approved-products-list-apl
AUDIT	FPKI Annual Review Requirements https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-annual-review-requirements.pdf
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-ssp.pdf
COMMON	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf
Executive Order 12968	Executive Order 12968 - Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. https://csrc.nist.gov/publications/detail/fips/140/2/final
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013. https://csrc.nist.gov/publications/detail/fips/201/2/final
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. https://govinfo.library.unt.edu/npr/library/misc/itref.html
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/TIG_SCEPACS_v2.3.pdf

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 Profile	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-x509-cert-profiles-pivi.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS #12: Personal Information Exchange Syntax v1.1 July 2014. https://tools.ietf.org/html/rfc7292
RFC 2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP, Russel Housley and Paul Hoffman, May 1999. https://www.ietf.org/rfc/rfc2585.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt
RFC 5322	Internet Message Format http://www.ietf.org/rfc/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. https://tools.ietf.org/html/rfc6960
RFC 8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification, J. Schaad, B. Ramsdell, S. Turner, April 2019. https://tools.ietf.org/rfc/rfc8551.txt
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special

Publication 800-37, Revision 2, December2018.
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A
https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

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

SP 800-76-2 Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 2013.
https://csrc.nist.gov/publications/detail/sp/800-76/2/final

SP 800-78-4 Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78-4, May 2015.
https://csrc.nist.gov/publications/detail/sp/800-78/4/final

SP 800-79-2 Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST Special Publication 800-79
https://csrc.nist.gov/publications/detail/sp/800-79/2/final

SP 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89
https://csrc.nist.gov/publications/detail/sp/800-89/final

SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157.
https://csrc.nist.gov/publications/detail/sp/800-157/final

X.509 ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.