Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile

Version 2.0

October 18, 2022

Document History

Status	Release	Date	Comment	Audience
Approved		10/12/2005		FPKI Community
Draft		10/31/2012	Incorporates changes for FBCA Change Proposal 2011-6 – Remove Requirements for LDAP URIs. Updated references, RFC 5289 in place of 3280, added RFC 4055, 5758, 2560, 3279, RFC 2616 replaced 1738, RFC 4516 in place of 2255, RFC 5751 replaced 3851, RFC 4514 replaced 2253,	FPKI Community
Approved		5/5/2015	Incorporate changes for FBCA Change Proposal 2015-1 – make anyEKU optional when EKU is asserted in digital signature certificates.	FPKI Community
Approved	1.8	7/17/2017	Align with current practice and FBCA CP v2.31 No longer allow IP in URIs used in certificates • Specify only minimum key size for Root CA • Deleted comment about discouraging the use of policy Qualifiers • Include Policy Constraints – non-critical – exception from RFC 5280 • Include InhibitAnyPolicy – non-critical – exception from RFC 5280	FPKI Community
Approved	1.9	5/10/2018	2018-03 Mandate specific EKU in Common Policy subscriber certificates to align with Industry Practices	FPKI Community
Approved	2.0	10/19/2022	Update worksheet formats. Consolidation of PIV-I profiles within FBCA Profiles. Expansion of worksheets to include general authentication and device certificates.	FPKI Community

Table of Contents

1. INTRODUCTION

This document specifies the profiles for X.509 certificates and certificate revocation lists (CRLs) associated with CAs cross-certified with the Federal Bridge Certification Authority (FBCA). Entities cross-certified with the FBCA must utilize certificate profiles that demonstrate interoperability with the corresponding profiles in this document. Federal Entities must adhere to these profiles, commercial Entities must be interoperable. Certificate profiles for digital certificates whose policy OIDs cross-certify to a FBCA PIV-I policy OID must adhere to the PIV-I profiles in this document without exception.

Requirements are detailed 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 trust community.

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].

Self-signed CA certificates must contain a non-null distinguished name in the Issuer DN that identifies the CA in a meaningful way. The Subject DN must be encoded exactly as it is encoded in the Issuer DN.

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

The **Signature Algorithm** field must be populated with one of the following:

- 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), SHA-384 hash algorithm (2.16.840.1.101.3.4.2.2), or SHA-512 hash algorithm (2.16.840.1.101.3.4.2.3) as a parameter. For all other RSA algorithms, the parameters field is NULL.

The **Subject Public Key** must be one of the following:

- RSA Encryption (1.2.840.113549.1.1.1)
  For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL.
- Elliptic Curve (1.2.840.10045.2.1)
  For EC, the 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)

Each of the certificate profile worksheets in Section 6 lists 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 private certificate extensions for local use but should not expect clients in the Federal PKI to process this additional information. When used in Subscriber certificates, critical private extensions must be interoperable in their intended community of use.

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.

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 [FBCA CP]. At least one CRL must be full and complete as described in [RFC 5280], and must not be indirect CRLs, delta-CRLs, or CRLs partitioned by reason code.

In addition to the full and complete CRL, CAs may issue additional CRLs, such as CRLs partitioned by a value other than reason code.

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 should 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 should 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 should be specified as a fully qualified domain name.
- The default port for the relevant protocol (80 for HTTP and 389 for LDAP) should be used, but need not be included in the URI.

5.1. CRL Distribution Points Extension

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.

At least one HTTP URI is required which:

- 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 header.

If the DistributionPointName is present in the issuingDistributionPoint extension of the CRL, the value must match at least one DistributionPointName in the cRLDistributionPoints extension 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). If used, the LDAP URI must appear after the HTTP URI.

5.2. Authority Information Access Extension

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)
If the OCSP access method is included, the access location must specify the location of the HTTP accessible OCSP server.

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] (preferred) or a single DER encoded certificate [RFC 2585] (discouraged)*. This message:

- 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).

In addition, the certs-only Cryptographic Message:

- Must contain a binary file with an extension of ".p7c".
- Must include “Content-Type: application/pkcs7-mime” in the HTTP response headers.

If used, the single DER encoded certificate:

- Must have an extension of ".cer".
- Must include “Content-Type: application/pkix-cert” in the HTTP response headers.

*The use of the single DER encoded certificate 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. If present, the LDAP URI must appear after the HTTP URI.

If implemented, 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

The subjectInfoAccess extension must appear in CA certificates issued after December 31, 2022, 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” in the HTTP response headers.
- Must contain all currently valid CA certificates, with the exception of self-signed certificates, issued by the subject of this certificate (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. If present, the LDAP URI must appear after the HTTP URI.

6. PROFILE WORKSHEETS

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

Worksheet #	Profile	Description
1	Self-Signed CA Certificate	Self-signed certificate issued by CAs primarily for establishing a trust anchor.
2	Self-Issued CA Certificate	Key rollover certificate, sometimes called a link certificate, that is self-issued by a CA but not self-signed.
3	Cross Certificate	Issued by a CA in one PKI domain to a CA in another PKI domain to enable interoperability through certificate policy mapping.
4	Intermediate/Signing CA Certificate	CA certificate issued to a subordinate CA
5	Signature Certificate	Subscriber certificate used to verify signatures.
6	Key Management Certificate	Subscriber certificate used to perform key management operations (e.g., key transport using RSA or Diffie-Hellman key agreement).
7	Authentication Certificate (non-PIV-I)	Subscriber certificate, not associated with a PIV-I credential, used to authenticate identity.
8	Device Certificate	Certificate issued to a computing or communications device (e.g., router, firewall, server) or software application.
9	PIV-I Authentication Certificate	Subscriber certificate, on a PIV-I credential, used to authenticate identity. This certificate type corresponds to the PIV-I implementation of the PIV Authentication Key defined in Section 4.3 of [FIPS 201-3].
10	PIV-I Card Authentication Certificate	Subscriber certificate on a PIV-I credential, used to authenticate the PIV-I card. This certificate type corresponds to the PIV-I implementation of the Card Authentication Key defined in Section 4.3 of [FIPS 201-3].
11	PIV-I Content Signing Certificate	Certificate issued to a Card Management System for use in signing data objects on the PIV-I card.
12	Certificate Revocation List	List of revoked certificate serial numbers signed by the CA.
13	Delegated OCSP Responder Certificate	Certificate issued to an OCSP responder.

Worksheet 1: Self-Signed CA Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
Issuer DN	Non-null Unique DN as specified in the associated CP that identifies the CA in a meaningful way (see Section 4 for preferred encoding).
Validity Period	utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Must be encoded exactly as it is encoded in the Issuer DN of this certificate.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
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 (*Optional for non-Federal entities)*	Must include the 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 If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.

Worksheet 2: Self-Issued CA Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Subject DN must be encoded exactly as it is encoded in the Issuer DN of certificates and CRLs issued by this CA.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE keyCertSign, cRLSign
Basic Constraints	Critical = TRUE cA:TRUE Path length constraints 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	Must include the 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 If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points	See Section 5.1
Authority Information Access	See Section 5.2.
Certificate Policies	Must assert at least one certificate policy OID as specified in Section 1.2 of the Entity CP.

Worksheet 3: Cross Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name of the Subject CA as provided in the certificate request from the Subject CA. Subject DN must be encoded exactly as it is encoded in the Issuer DN of the certificates and CRLs issued by the Subject CA.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE keyCertSign, cRLSign
Extended Key Usage *(Optional)*	Not recommended. May be 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 subscriber certificates only, 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 the Subject CA. Derived using a cryptographic hash of the Subject CA's 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	Must include the 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. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2.
Certificate Policies	Must assert at least one certificate policy OID as specified in Section 1.2 of the Issuing CA's CP.
Policy Mappings	One or more mappings from Issuing CA certificate policies to Subject CA certificate policies.as determined by the Issuing domain.
Policy Constraints	Critical = TRUE requireExplicitPolicy with SkipCerts = 0 must be present. inhibitPolicyMapping must be included with SkipCerts = 0 when issued to a CA that is not a Bridge CA. inhibitPolicyMapping must be included with SkipCerts = 1 (or more). When issued to a Bridge CA SkipCerts is set to the minimum value required to support the expected mappings, usually 1.
Inhibit Any Policy	Critical = TRUE 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	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name of the Subject CA as provided in the certificate request from the Subject CA. Subject DN must be encoded exactly as it is encoded in the Issuer DN of the certificates and CRLs issued by the Subject CA.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE keyCertSign, cRLSign
Extended Key Usage *(Optional)*	Not recommended. May be 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 subscriber certificates only, 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 the Subject CA. Derived using a cryptographic hash of the Subject CA's 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	Must include the 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. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2.
Certificate Policies	Must assert at least one certificate policy OID as specified in Section 1.2 of the Issuing CA's CP.
Policy Constraints *(Optional)*	Critical = TRUE When this extension appears, both requireExplicitPolicy and inhibitPolicyMapping must be present and assert SkipCerts = 0.
Inhibit Any Policy *(Optional)*	Critical = TRUE 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 5: Signature Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name of the owner of the subject public key in the certificate. For requirements related to specific certificate types (e.g. PIV-I, Role-based), see [FBCACP] Section 3.1.1.1.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
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-I*) 1.3.6.1.4.1.311.10.3.12 MSFT Document Signing 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)*	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	See Section 5.1.
Authority Information Access	See Section 5.2 *Both the caIssuers and OCSP access method must be included for certificates associated with a PIV-I Card.*
Certificate Policies	Must assert at least one certificate policy OID contained in the Certificate Policies extension of the Issuing CA.
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 an ISO 3166 Country Code(s) value.

Worksheet 6: Key Management Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name of the owner of the subject public key in the certificate For requirements related to specific certificate types (e.g. PIV-I, Role-based), see [FBCACP] Section 3.1.1.1.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
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. Recommended: 1.3.6.1.5.5.7.3.4 id-kp-emailProtection *(required for PIV-I)* 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)*	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	See Section 5.1.
Authority Information Access	See Section 5.2. *Both the caIssuers and OCSP access method must be included for certificates associated with a PIV-I Card.*
Certificate Policies	Must assert at least one certificate policy OID contained in the Certificate Policies extension of the Issuing CA..
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: Authentication Certificate (Non-PIV-I)

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name of the owner of the subject public key in the certificate For requirements related to specific certificate types (e.g. Role-based), see [FBCACP] Section 3.1.1.1:
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE Must assert digitalSignature only
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 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
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2
Certificate Policies	Must assert at least one certificate policy OID contained in the Certificate Policies extension of the Issuing CA.
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: Device Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	Unique Distinguished Name that contains the name of the device in the CN.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE nonRepudiation must not be asserted If the certificate is used for digital signature or authentication of ephemeral keys (e.g. TLS), digitalSignature must be asserted If the 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.
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: an IA5String that contains the DNS name of the subject URI: 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	See Section 5.1.
Authority Information Access	See Section 5.2.
Certificate Policies	Must assert at least one certificate policy OID designated for devices contained in the Certificate Policies extension of the Issuing CA. Device certificates should not contain policy OIDs intended for human subscribers.

Worksheet 9: PIV-I Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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 The notAfter time must be on or before the PIV-I card expiration date.
Subject DN	Must include the CN of the subscriber using one of the name forms for PIV-I Hardware specified in [FBCACP] Section 3.1.1.1 For certificates with an Affiliated Organization: cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN} For certificates with no Affiliated Organization: cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN} For Enterprise CAs that issue PIV-I certificates only within their own organizations, the Affiliation ou may be absent provided the organization's name appears in the {Base DN}.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE digitalSignature
Extended Key Usage	The following keyPurposeId values must be included: 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon 1.3.6.1.5.5.7.3.2 TLS client authentication One or more additional keyPurposeIds consistent with keyUsage 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 the UUID (GUID data element) from the CHUID of the PIV-I card, encoded as a URI as specified in Section 3 of RFC 4122. In addition, one or more of the following are permitted: rfc822Name otherName values (e.g. Microsoft UPN) to support local applications directoryName to support local applications
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2. *Both the caIssuers and OCSP access method must be included*.
Certificate Policies	Contains one certificate policy used only for PIV-I authentication certificates and mapped to 2.16.840.1.101.3.2.1.18. May contain additional certificate policies.
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 an ISO 3166 Country Code(s) value.

Worksheet 10: PIV-I Card Authentication Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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 The notAfter time must not be after the PIV-I card expiration date.
Subject DN	Must include the serialNumber Relative Distinguished Name set to UUID, no other name forms may be included. For certificates with an Affiliated Organization: serialNumber=UUID, ou=Affiliated Organization Name, {Base DN} For certificates with no Affiliated Organization: serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name, {Base DN} For Enterprise CAs that issue PIV-I certificates only within their own organizations, the Affiliation ou may be absent provided the organization's name appears in the {Base DN}.
Subject Public Key	Must be either RSA or elliptic curve. See Section 2.
Key Usage	Critical = TRUE Must assert digitalSignature only
Extended Key Usage	Critical = TRUE Must assert only the id-PIV-cardAuth keypurposeID (2.16.840.1.101.3.6.8)
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 the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122. No other name forms are permitted.
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2 *Both the caIssuers and OCSP access method must be included*.
Certificate Policies	Contains a single certificate policy used only for card authentication certificates and mapped to 2.16.840.1.101.3.2.1.19
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: PIV-I Content Signing Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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 indicating the organization administering the PIV-I card issuance system
Subject Public Key	Must be either RSA or elliptic curve. See Section 2
Key Usage	Critical = TRUE digitalSignature
Extended Key Usage	Critical = TRUE Must assert only the id-fpki-pivi-content-signing keypurposeID (2.16.840.1.101.3.8.7)
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)*	otherName values (e.g. Microsoft UPN) may be included to support local applications.
CRL Distribution Points	See Section 5.1.
Authority Information Access	See Section 5.2 *Both the calssuers and OCSP access method must be included.*
Certificate Policies	Contains a single certificate policy used only for content signing certificates and mapped to 2.16.840.1.101.3.2.1.20

Worksheet 12: Certificate Revocation List

Field	Content
Version	INTEGER Value of "1" for Version 2 CRL.
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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	The following values are included: userCertificate - the serial number of the certificate being revoked. revocationDate - the date and time of revocation. reasonCode CRL entry extension of certificateHold must be included for suspended certificates* - Use of this extension is optional for reason codes other than certificateHold. - If the revocation reason is unspecified, the reasonCode CRL entry extension should be omitted. removeFromCRL must be used only in delta CRLs. invalidityDate CRL entry extension may be included if the invalidity date precedes the revocation date. *Note: certificateHold must be used for suspension of subscriber certificates only.
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 for which the issuer field contains the same name as the issuer field in the CRL. For example, when a CA is rekeyed and the old and new keys are used to issue separate CRLs. 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 13: Delegated OCSP Responder Certificate

Field	Content
Version	Integer Value of 2 for Version 3 certificate
Serial Number	Unique positive integer
Signature Algorithm	Must include one of the signature algorithms identified in Section 2.
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 120 days utcTime (YYMMDDHHMMSSZ) for dates up to and including 2049 generalTime (YYYYMMDDHHMMSSZ) for dates after 2049
Subject DN	Unique Distinguished name assigned to the OCSP Responder
Subject Public Key	Must be either RSA or elliptic curve. See Section 2
Key Usage	Critical = TRUE Must assert digitalSignature May assert nonRepudiation
Extended Key Usage	Critical = TRUE Must assert only 1.3.6.1.5.5.7.3.9 id-kp-OCSPSigning
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: an IA5String that contains the DNS name of the subject URI: an IA5String that contains the URI of the subject rfc822Name that contains the email address of the sponsor, administrator, or help desk
Authority Information Access *(Optional)*	See Section 5.2. *The OCSP access method must not be included.*
Certificate Policies	Must assert all policy OIDs for which the OCSP server is authoritative.
OCSP No Check	NULL

7. ACRONYMS

AKID Authority Key Identifier

CA Certification Authority

CMS Cryptographic Message Syntax

CN Common Name

CRL Certificate Revocation List

DER Distinguished Encoding Rules

DN Distinguished Name

FBCA Federal Bridge Certification Authority

FIPS Federal Information Processing Standards

FPKI Federal Public Key Infrastructure

GUID Global Unique Identifier

HTTP Hypertext Transfer Protocol

LDAP Lightweight Directory Access Protocol

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

UUID Universal Unique Identifier

UPN User Principal Name

URI Uniform Resource Identifier

URL Uniform Resource Locator

URN Uniform Resource Name

8. REFERENCES

Please see FBCA Certificate Policy Appendix D for references.