



The attached document has been archived and is provided solely for historical purposes.

It may have been superseded by another document (indicated below).

### Archived Document

|                          |  |
|--------------------------|--|
| <b>Title:</b>            | <b>X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards Version 1.3</b> |
| <b>Publication Date:</b> | <b>May 10, 2018</b>  |
| <b>Archive Date:</b>     | <b>November 4, 2022</b>  |
| <b>Archive Notes:</b>    | <b>This document has been superseded.</b>  |

### Superseding Document

|                          |  |
|--------------------------|--|
| <b>Title:</b>            | <b>Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile Version 3.0</b>  |
| <b>Publication Date:</b> | <b>October 19, 2022</b>  |
| <b>URL:</b>              | <b>Current Version:</b><br><a href="https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf">https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf</a> |

### Additional Information

|                 |  |
|-----------------|--|
| <b>Contact:</b> | <a href="mailto:fpki@gsa.gov">fpki@gsa.gov</a> |
|-----------------|--|

**Page Reviewed/Updated: November 4, 2022**



# **X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards**

**Federal PKI Policy Authority**

**May 10, 2018**

**Revision History Table**

| <b>Date</b>    | <b>Version</b> | <b>Description</b>   |
|----------------|----------------|--|
| April 23, 2010 | 1.0            | Initial version of profile   |
| May 5, 2015    | 1.1            | Make anyEKU optional   |
| July 17, 2017  | 1.2            | Align with current practice & FBCA v2.31 <ul style="list-style-type: none"><li>• Specify only minimum key size for Root CA</li><li>• Deleted comment about discouraging the use of policy Qualifiers</li><li>• Include Policy Constraints – non-critical – exception from RFC 5280</li><li>• Include InhibitAnyPolicy – non-critical – exception from RFC 5280</li></ul> |
| May 10, 2018   | 1.3            | 2018-03 Mandate specific EKU in subscriber certificates to align with Industry Practices   |

## **1. Introduction**

This document specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for certificates and CRLs issued for use with Personal Identity Verification Interoperable (PIV-I) cards. The profiles serve to identify unique parameter settings for certificates and CRLs issued for use with these cards.

This profile is based the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [13], which is based on the Internet Engineering Task Force (IETF) Public Key Infrastructure (PKIX) profile developed by the PKIX working group [3]. The PKIX profile identifies the format and semantics of certificates and CRLs for the Internet PKI. Procedures are described for processing and validating certification paths in the Internet environment. Encoding rules are provided for all fields and extensions profiled in both the X.509 v3 certificate and v2 CRL. Encoding rules for cryptographic algorithms specified in this profile are specified in [7] and [10].

### **1.1. Structure**

This document is divided into six sections. Section 1 includes this introduction. Sections 2 and 3 describe the v3 certificate and v2 CRL respectively. These sections specifically describe the differences in generation and processing requirements between the PKIX profile and the profile for certificates and CRLs issued for PIV-I. Unless otherwise noted in this profile, the reader should follow the PKIX generation and processing requirements for a particular field. Section 4 specifies rules for choosing character encoding sets for attribute values of type DirectoryString in distinguished names. Section 5 profiles the use of uniform resource identifiers (URIs) in certificates. Section 6 highlights certificate contents that are particular to PIV-I. Section 7 provides an overview of each of the certificate and CRL profiles included in the worksheets corresponding to this document.

### **1.2. Acronyms**

|       |  |
|-------|--|
| AKID  | Authority Key Identifier                   |
| CA    | Certification Authority                    |
| CMS   | Cryptographic Message Syntax               |
| CRL   | Certificate Revocation List                |
| DER   | Distinguished Encoding Rules               |
| DN    | Distinguished Name                         |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FBCA  | Federal Bridge Certification Authority     |
| FBI   | Federal Bureau of Investigation            |
| FIPS  | Federal Information Processing Standards   |
| FPKI  | Federal Public Key Infrastructure          |
| FTP   | File Transfer Protocol                     |
| HTTP  | Hypertext Transfer Protocol                |
| IETF  | Internet Engineering Task Force            |
| IP    | Internet Protocol                          |

|        |  |
|--------|--|
| LDAP   | Lightweight Directory Access Protocol          |
| NIST   | National Institute of Standards and Technology |
| OCSP   | Online Certificate Status Protocol             |
| OID    | Object Identifier                              |
| PIV-I  | Personal Identity Verification Interoperable   |
| PKI    | Public Key Infrastructure                      |
| PKIX   | Public Key Infrastructure (X.509)              |
| PSS    | Probabilistic Signature Scheme                 |
| RFC    | Request For Comments                           |
| RSA    | Rivest-Shamir-Adelman                          |
| SHA    | Secure Hash Algorithm                          |
| SKID   | Subject Key Identifier                         |
| S/MIME | Secure/Multipurpose Internet Mail Extensions   |
| TLS    | Transport Layer Security                       |
| UPN    | User Principal Name                            |
| URI    | Uniform Resource Identifier                    |
| URL    | Uniform Resource Locator                       |
| URN    | Uniform Resource Name                          |
| UUID   | Universally Unique IDentifier                  |

### **1.3. References**

- [1] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA).
- [2] Russel Housley and Paul Hoffman. Internet X.509 Public Key Infrastructure: *Operational Protocols: FTP and HTTP*, RFC 2585, May 1999.
- [3] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russel Housley, and Tim Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280, May 2008.
- [4] Mark Smith and Tim Howes. *Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator*, RFC 4516, June 2006.
- [5] Roy T. Fielding, James Gettys, Jeffrey C. Mogul, Henrik Frystyk Nielsen, Larry Masinter, Paul J. Leach, and Tim Berners-Lee. *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, June 1999.
- [6] Steve Lloyd. *AKID/SKID Implementation Guideline*, September 2002.
- [7] Tim Polk, Russel Housley, and Larry Bassham. Internet Public Key Infrastructure: *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3279, April 2002.
- [8] W. Timothy Polk, Donna F. Dodson, and William E. Burr. *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST Special Publication 800-78-2, February 2010.
- [9] Blake Ramsdell and Sean Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*, RFC 5751, January 2010.

- [10] Jim Schaad, Burt Kaliski, and Russell Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 4055, June 2005.
- [11] Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1, March 2006.
- [12] Paul J. Leach, Michael Mealling, and Rich Salz. *A Universally Unique Identifier (UUID) URN Namespace*, RFC 4122, July 2005.
- [13] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program.

## **2. X.509 v3 Certificates**

X.509 v3 certificates contain the identity and attribute data of a subject using the base certificate with applicable extensions. The base certificate contains such information as the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the validity period of the certificate, the distinguished name of the subject, and information about the subject's public key. To this base certificate are appended numerous certificate extensions. More detailed information about X.509 certificates can be found in Recommendation X.509 and RFC 5280.

CAs create certificates for user authentication procedures that require one user to obtain another user's public key. So that users trust the public key, the CA employs a digital signature to cryptographically sign the certificate in order to provide assurance that the information within the certificate is correct. The fields in a certificate identify the issuer (i.e., CA), subject (i.e., user), version number, subject's public key, validity period, and serial number of the certificate along with the public key algorithm used to certify the certificate. A CA may also add certificate extensions containing additional information about the user or the CA, depending on the implementation.

## **3. X.509 v2 Certificate Revocation Lists**

CAs use CRLs to publicize the revocation of a subject's certificate. The CRLs are stored in the directory as attributes and are checked by relying parties to verify that a user's certificate has not been revoked. The fields in a CRL identify the issuer, the date the current CRL was generated, the date by which the next CRL will be generated, and the revoked users' certificates.

The CRLs issued to comply with the requirements of Section 4.9.7 of the FBCA [1] must be complete for scope: they may not be indirect CRLs, delta-CRLs, or CRLs segmented by reason code. CAs may optionally issue additional CRLs, such as delta-CRLs, so long as complete for scope CRLs are also made available and are issued with sufficient frequency to meet the requirements specified in Section 4.9.7 of the FBCA. CAs that issue segmented CRLs are strongly encouraged to also issue full CRLs in order to accommodate third parties that use CRLs to generate OCSP responses. CAs may optionally supplement the CRL based revocation mechanisms with on-line revocation mechanisms.

If delta-CRLs are issued, then either the certificates or the complete CRLs that correspond to the delta-CRLs should include a FreshestCRL extension that points to the delta-CRLs. If an OCSP server is available that provides status information about a certificate, then the authorityInfoAccess extension for that certificate should include a pointer to the OCSP server.

#### **4. Encoding Distinguished Names with Attributes of type DirectoryString**

X.509 certificates and CRLs include distinguished names to identify issuers (of certificates and CRLs), subjects of certificates, and to specify CRL distribution points. Many of the attributes in distinguished names use the DirectoryString syntax. DirectoryString permits encoding of names in a choice of character sets: PrintableString, TeletexString, BMPString, UniversalString, and UTF8String.

PrintableString is currently the most widely used encoding for attribute values in distinguished names. PrintableString is a subset of ASCII; it does not include characters required for most international languages. UTF8String is an encoding that supports all recognized written languages, including some ancient languages (e.g., Runic). Any name that can be represented in PrintableString can also be encoded using UTF8String.

Name comparison is an important step in X.509 path validation, particularly for name chaining and name constraints computation. Many legacy implementations are unable to perform name comparisons when names are encoded using different character sets. To simplify correct operation of path validation, CAs are strongly encouraged to honor the subject's chosen character set when issuing CA certificates or populating extensions. That is, if a subject CA encodes its own name in the issuer field of certificates and CRLs it generates using TeletexString, the cross certificate should use the same character set to specify that CA's name.

Name constraints are specified in CA certificates. The names specified in name constraints must be compared with the subject names in subsequent certificates in a certification path. To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates. In general, it may be assumed that subject names are encoded in the same way as the issuer field in the certificates issued by the subject of the certificate containing the name constraints extension.

For certificates and CRLs issued for PIV-I, attributes of type DirectoryString shall be encoded in either PrintableString or UTF8String. Attribute values should be encoded in PrintableString whenever possible.

#### **5. Use of URIs in Distribution Points, AuthorityInfoAccess, and subjectInfoAccess Extensions**

Uniform Resource Identifiers (URIs) are used in four different extensions within the certificate and CRL profiles in this document: authorityInfoAccess, subjectInfoAccess, cRLDistributionPoints, and issuingDistributionPoint. Two different protocols are used in this document: LDAP and HTTP. The specifications for URIs for these protocols may be found in RFC 4516 and RFC 2616, respectively.

Except for the id-ad-ocsp access method of the authorityInfoAccess extension, the scheme portion of all URIs must be either "http" or "ldap" to indicate that the relevant information is located in an LDAP accessible directory or via HTTP. For the id-ad-ocsp access method of the authorityInfoAccess, the scheme portion of the URI must be "http" to indicate that the transport protocol for the OCSP request/response messages is HTTP. The hostname of every URI must be specified as either a fully qualified domain name or an IP address. The information must be made available via the default port number for the relevant protocol (80 for HTTP and 389 for LDAP) and so does not need to be specified in the URI.

In the cRLDistributionPoints extension, the URI is a pointer to a current CRL that provides status information about the certificate. If LDAP is used, the 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 the directory in which the CRL is stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI. If HTTP is used, the URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL (see RFC 2585). When a URI is used as the DistributionPointName in the issuingDistributionPoint extension in a CRL, the value must match the URI in the corresponding distribution points in the cRLDistributionPoints extensions in certificates covered by the CRL.

Some examples of URIs that may appear in a cRLDistributionPoints or issuingDistributionPoint extension are:

`http://www.example.com/fictitiousCRLdirectory/fictitiousCRL1.crl`

`ldap://ldap.example.com/cn=Good%20CA,c=US?certificateRevocationList;binary`

The authorityInfoAccess extension uses URIs for two purposes. When the id-ad-caIssuers access method is used, the access location specifies where certificates issued to the issuer of the certificate may be found. If LDAP is used, the URI must include the DN of the entry containing the relevant certificates and specify the directory attribute in which the certificates are located. If the directory in which the certificates are stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI. If HTTP is used, the URI must point to a file that has an extension of ".p7c" that contains a certs-only CMS message (see RFC 5751). The CMS message should include all certificates issued to the issuer of this certificate, but must at least contain all certificates issued to the issuer of this certificate in which the subject public key may be used to verify the signature on this certificate.

Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI.

For a certificate issued by "Good CA", some examples of URIs that may appear as the access location in an authorityInfoAccess extension when the id-ad-caIssuers access method is used are:

`http://www.example.com/fictitiousCertsOnlyCMSdirectory/certsIssuedToGoodCA.p7c`

`ldap://ldap.example.com/cn=Good%20CA,o=Test%20Certificates,c=US?cACertificate,crossCertificatePair;binary`



When the id-ad-ocsp access method is used, the access location specifies the location of an OCSP server that provides status information about the certificate. The URI may include a path. Where privacy is a requirement, the URI may specify the "https" scheme to indicate that the transport protocol for OCSP requests/responses is HTTP over SSL/TLS. In this case, the default port number is 443, and the URI must include the server's port number if this default port number is not used.

The id-ad-caRepository access method for the subjectInfoAccess extension uses URIs to specify the location where CA certificates issued by the subject of the certificate may be found. If LDAP is used, the URI must include the DN of the entry containing the relevant certificates and specify the directory attribute in which the certificates are located. If the directory in which the certificates are stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI. If HTTP is used, the URI must point to a file that has an extension of ".p7c" that contain a certs-only CMS message (see RFC 5751). The CMS message should include all CA certificates issued by the subject of this certificate, but must at least contain all CA certificates issued by the subject of this certificate in which the signature on the certificate may be verified using the subject public key in this certificate.

CA certificates for PIV-I should include a subjectInfoAccess extension that contains at least one instance of the id-ad-caRepository access method. The access location for this instance should be an HTTP URI. If the subject of the certificate only issues end entity certificates, then the subjectInfoAccess extension may be excluded.

For a certificate issued to "Good CA", some examples of URIs that may appear as the access location in an subjectInfoAccess extension when the id-ad-caRepository access method is used are:

`http://www.example.com/fictitiousCertsOnlyCMSdirectory/CAcertsIssuedByGoodCA.p7c`  
`ldap://ldap.example.com/cn=Good%20CA,c=US?cACertificate,crossCertificatePair;binary`

## **6. PIV-I Certificates**

The certificate profiles for PIV-I are based on the profile for End Entity Signature Certificates, but these profiles differ in a number of ways based on requirements that are specified in the FBCA [1]. The main differences in these profiles are as follows:

- There must be an OCSP server that responds on port 80 that provides certificate status information for PIV-I certificates and the authorityInfoAccess extension in these certificates must include an access method of type id-ad-ocsp where the access location is a URI with a scheme of "http".
- PIV-I Card Authentication certificates must include a critical extended key usage extension that asserts id-PIV-cardAuth.
- Authentication certificates and PIV-I Card Authentication certificates must include a subjectAltName extension that includes the UUID from the PIV-I card that holds the certificates.
- The subjectAltName extension in the PIV-I Card Authentication certificates must not include any name forms other than the UUID.
- The nonRepudiation key usage bit must not be set in either PIV-I Authentication

or PIV-I Card Authentication certificates.

- PIV-I Content Signing certificates that are used to verify signatures on the CHUID or biometric data on PIV-I cards include an extended key usage extension that asserts id-fpki-pivi-content-signing.

## **1. Worksheet Contents**

The certificate and CRL profiles consist of nine worksheets. Each worksheet lists mandatory contents of a particular class of certificates or CRLs. Optional features that will be widely supported in the Federal PKI are also identified. These features MAY be included at the issuer's option. Certificate and CRL issuers may include additional information in non-critical extensions for local use, but should not expect clients in the Federal PKI to process this additional information. Critical extensions that are not listed in these worksheets MUST NOT be included in certificates or CRLs issued for PIV-I.

The nine worksheets are:

1. The *Self-Issued CA Certificate Profile* worksheet defines the mandatory and optional contents of key rollover certificates.
2. The *Cross Certificate Profile* worksheet defines the mandatory and optional contents of certificates issued by CAs for PIV-I where the subject is another CA and the public key will be used to verify the signature on certificates and CRLs.
3. The *CRL Profile* worksheet table defines the mandatory and optional contents of CRLs issued by CAs that issue certificates for PIV-I.
4. The *PIV-I Card Authentication Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the Card Authentication Key defined in Section 4.3 of FIPS 201.
5. The *PIV-I Authentication Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the PIV Authentication Key defined in Section 4.3 of FIPS 201.
6. The *PIV-I Digital Signature Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the Digital Signature Key defined in Section 4.3 of FIPS 201.
7. The *PIV-I Key Management Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the Key Management Key defined in Section 4.3 of FIPS 201.
8. The *PIV-I Content Signing Certificate Profile* worksheet defines the mandatory and optional contents of certificates issued by CAs to Card Management Systems for use in signing data objects on the PIV-I card.
9. The *Delegated OCSP Responder Certificate Profile* worksheet defines the mandatory and optional contents of certificates issued to OCSP responders that are delegated to provide certificate revocation status.

**Worksheet 1: Self-Issued CA Certificate Profile**

| Field                     | Criticality Flag | Value                           | Comments   |
|---------------------------|------------------|---------------------------------|--|
| Certificate               |                  |                                 |  |
| tbsCertificate            |                  |                                 | Fields to be signed.   |
| <b>version</b>            |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>          |                  |                                 |  |
| AlgorithmIdentifier       |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  | Choice of following algorithms: |  |
|                           |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2             | ecdsa-with-Sha256  |
|                           |                  | 1.2.840.10045.4.3.3             | ecdsa-with-Sha384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                                 |  |
| Name                      |                  |                                 |  |
| RDNSequence               |                  |                                 |  |
| RelativeDistinguishedName |                  |                                 |  |
| AttributeTypeAndValue     |                  |                                 |  |
| AttributeType             |                  | OID                             |  |
| AttributeValue            |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>           |                  |                                 |  |
| notBefore                 |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                  |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>            |                  |                                 |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

| Field                         | Criticality Flag | Value  | Comments   |
|-------------------------------|------------------|--|--|
| Name                          |                  |  | Subject name should be encoded exactly as it is encoded in the issuer field of this certificate.   |
| RDNSequence                   |                  |  |  |
| RelativeDistinguishedName     |                  |  |  |
| AttributeTypeAndValue         |                  |  |  |
| AttributeType                 |                  | OID  |  |
| AttributeValue                |                  | see comment  | Encoding of name must use the encoding of the issuer field in certificates and CRLs issued by this subject CA  |
| <b>subjectPublicKeyInfo</b>   |                  |  |  |
| algorithm                     |                  |  |  |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key. May be either RSA or elliptic curve.  |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption   |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key   |
| parameters                    |                  |  | Format and meaning dependent upon algorithm  |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.  |
| EcpkParameters                |                  |  |  |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |  |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256  |
|                               |                  | 1.3.132.0.34   | Curve P-384  |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys certificates shall have a modulus of 2048, 3072, or 4096 bits.   |
| <b>required extensions</b>    |                  |  |  |
| <b>authorityKeyIdentifier</b> | FALSE            |  |  |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.  |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |  |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.  |
| <b>keyUsage</b>               | TRUE             |  | If the subject public key may be used for purposes other than certificate and CRL signing (e.g., signing OCSP responses), then the digitalSignature and/or nonRepudiation bits may be set as well. |
| digitalSignature              |                  | 0  |  |
| nonRepudiation                |                  | 0  |  |
| keyEncipherment               |                  | 0  |  |
| dataEncipherment              |                  | 0  |  |
| keyAgreement                  |                  | 0  |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                    | Comments   |
|------------------------------|------------------|--------------------------|--|
| keyCertSign                  |                  | 1                        |  |
| cRLSign                      |                  | 1                        |  |
| encipherOnly                 |                  | 0                        |  |
| decipherOnly                 |                  | 0                        |  |
| <b>certificatePolicies</b>   | FALSE            |                          |  |
| PolicyInformation            |                  |                          |  |
| policyIdentifier             |                  |                          |  |
| <b>basicConstraints</b>      | TRUE             |                          | This extension must appear in all CA certificates. The pathLenConstraint field should not appear in self-issued certificates.  |
| cA                           |                  | TRUE                     |  |
| <b>cRLDistributionPoints</b> | FALSE            |                          | This extension is required in all CA certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.  |
| DistributionPoint            |                  |                          |  |
| distributionPoint            |                  |                          |  |
| DistributionPointName        |                  |                          |  |
| fullName                     |                  |                          |  |
| GeneralNames                 |                  |                          |  |
| GeneralName                  |                  |                          |  |
| directoryName                |                  |                          |  |
| Name                         |                  |                          |  |
| RDNSSequence                 |                  |                          |  |
| RelativeDistinguishedName    |                  |                          |  |
| AttributeTypeAndValue        |                  |                          |  |
| AttributeType                |                  | OID                      |  |
| AttributeValue               |                  | see comment              | See preamble text on naming.   |
| uniformResourceIdentifier    |                  | ldap://... or http://... | See preamble text on URIs.   |
| <b>authorityInfoAccess</b>   | FALSE            |                          | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP. |
| AccessDescription            |                  |                          |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                                      | Comments   |
|----------------------------|------------------|--|--|
| accessMethod               |                  | id-ad-caIssuers<br>(1.3.6.1.5.5.7.48.2)    | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.             |
| accessLocation             |                  |  |  |
| GeneralName                |                  |  |  |
| uniformResourceIdentifier  |                  | ldap://... or http://...                   | See preamble text on URIs.   |
| <b>optional extensions</b> |                  |  |  |
| <b>subjectInfoAccess</b>   | FALSE            |  | CA Certificates issued for PIV-I may include a subjectInfoAccess extension. subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access method is defined for use in CA certificates.   |
| AccessDescription          |                  |  |  |
| accessMethod               |                  | id-ad-caRepository<br>(1.3.6.1.5.5.7.48.5) | Each CA certificate should include at least one instance of this access method that includes a URI name form to specify an HTTP accessible Web server. The URI should point to a location where certificates issued by the subject of this certificate may be found. |
| accessLocation             |                  |  |  |
| GeneralName                |                  |  |  |
| uniformResourceIdentifier  |                  | ldap://... or http://...                   | See preamble text on URIs.   |
| <b>issuerAltName</b>       | FALSE            |  | Any name types may be present; only the most common are specified here.  |
| GeneralNames               |                  |  |  |
| GeneralName                |                  |  |  |
| rfc822Name                 |                  | IA5String                                  | Electronic mail address of the PKI administration  |

**Worksheet 2: Cross Certificate Profile**

| Field                     | Criticality Flag | Value                           | Comments   |
|---------------------------|------------------|---------------------------------|--|
| Certificate               |                  |                                 |  |
| tbsCertificate            |                  |                                 | Fields to be signed.   |
| <b>version</b>            |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>          |                  |                                 |  |
| AlgorithmIdentifier       |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  | Choice of following algorithms: |  |
|                           |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2             | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3             | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                                 |  |
| Name                      |                  |                                 |  |
| RDNSequence               |                  |                                 |  |
| RelativeDistinguishedName |                  |                                 |  |
| AttributeTypeAndValue     |                  |                                 |  |
| AttributeType             |                  | OID                             |  |
| AttributeValue            |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>           |                  |                                 |  |
| notBefore                 |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                  |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>            |                  |                                 |  |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

| Field                       | Criticality Flag | Value                | Comments  |
|-----------------------------|------------------|----------------------|---|
| Name                        |                  |                      | X.500 Distinguished name of the owner of the subject public key in the certificate. Subject name should be encoded exactly as it is encoded in the issuer field of certificates issued by the subject.  |
| RDNSequence                 |                  |                      |   |
| RelativeDistinguishedName   |                  |                      |   |
| AttributeTypeAndValue       |                  |                      |   |
| AttributeType               |                  | OID                  |   |
| AttributeValue              |                  | see comment          | Encoding of name must use the encoding of the issuer field in certificates and CRLs issued by this subject CA   |
| <b>subjectPublicKeyInfo</b> |                  |                      |   |
| algorithm                   |                  |                      |   |
| AlgorithmIdentifier         |                  |                      | Public key algorithm associated with the public key. May be either RSA or elliptic curve.   |
| algorithm                   |                  | 1.2.840.113549.1.1.1 | RSA Encryption  |
|                             |                  | 1.2.840.10045.2.1    | Elliptic curve key  |
| parameters                  |                  |                      | Format and meaning dependent upon algorithm   |
| RSAParameters               |                  | NULL                 | For RSA, parameters field is populated with NULL.   |
| EcpkParameters              |                  |                      |   |
| namedCurve                  |                  |                      | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2:  |
|                             |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
|                             |                  | 1.3.132.0.34         | Curve P-384   |
| subjectPublicKey            |                  | BIT STRING           | For RSA public keys certificates shall have a modulus of 2048, 3072, or 4096 bits.  |
| <b>required extensions</b>  |                  |                      |   |
| authorityKeyIdentifier      | FALSE            |                      |   |
| keyIdentifier               |                  | OCTET STRING         | Derived using the SHA-1 hash of the public key.   |
| subjectKeyIdentifier        | FALSE            |                      |   |
| keyIdentifier               |                  | OCTET STRING         | The value in this field must be the same as the value that the subject CA uses in the authority key identifier extension of the certificates and CRLs that it signs with the private key that corresponds to the subject public key included in this certificate. |
| keyUsage                    | TRUE             |                      | If the subject public key may be used for purposes other than certificate and CRL signing (e.g., signing OCSP responses), then the digitalSignature and/or nonRepudiation bits may be set as well.  |
| digitalSignature            |                  | 0                    |   |
| nonRepudiation              |                  | 0                    |   |
| keyEncipherment             |                  | 0                    |   |



**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                    | Comments   |
|------------------------------|------------------|--------------------------|--|
| dataEncipherment             |                  | 0                        |  |
| keyAgreement                 |                  | 0                        |  |
| keyCertSign                  |                  | 1                        |  |
| cRLSign                      |                  | 1                        |  |
| encipherOnly                 |                  | 0                        |  |
| decipherOnly                 |                  | 0                        |  |
| <b>certificatePolicies</b>   | FALSE            |                          |  |
| PolicyInformation            |                  |                          |  |
| policyIdentifier             |                  |                          |  |
| <b>basicConstraints</b>      | TRUE             |                          | This extension must appear in all CA certificates.   |
| cA                           |                  | TRUE                     |  |
| pathLenConstraint            |                  | INTEGER                  | The use of a path length constraint is optional.   |
| <b>cRLDistributionPoints</b> | FALSE            |                          | This extension is required in all CA certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.  |
| DistributionPoint            |                  |                          |  |
| distributionPoint            |                  |                          |  |
| DistributionPointName        |                  |                          |  |
| fullName                     |                  |                          |  |
| GeneralNames                 |                  |                          |  |
| GeneralName                  |                  |                          |  |
| directoryName                |                  |                          |  |
| Name                         |                  |                          |  |
| RDNSSequence                 |                  |                          |  |
| RelativeDistinguishedName    |                  |                          |  |
| AttributeTypeAndValue        |                  |                          |  |
| AttributeType                |                  | OID                      |  |
| AttributeValue               |                  | see comment              | See preamble text on naming.   |
| uniformResourceIdentifier    |                  | ldap://... or http://... | See preamble text on URIs.   |
| <b>authorityInfoAccess</b>   | FALSE            |                          | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP. |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                                      | Comments  |
|----------------------------|------------------|--|---|
| AccessDescription          |                  |  |   |
| accessMethod               |                  | id-ad-calssuers<br>(1.3.6.1.5.5.7.48.2)    | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.  |
| accessLocation             |                  |  |   |
| GeneralName                |                  |  |   |
| uniformResourceIdentifier  |                  | ldap://... or http://...                   | See preamble text on URIs.  |
| PolicyConstraints          | FALSE            |  | When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension should be marked as noncritical*, to support legacy applications that cannot process policyConstraints   |
| requireExplicitPolicy      |                  |  |   |
| SkipCerts                  |                  | INTEGER                                    |   |
| inhibitPolicyMapping       |                  |  | Should be included if local policy prohibits policy mapping.  |
| SkipCerts                  |                  | INTEGER                                    | 1 in certs issued to a cross-certified PKI, 0 when issued to an SSP, 2 within the infrastructure to a CA which may issue a cross-certificate to a Bridge  |
| InhibitAnyPolicy           | FALSE            |  | This extension should be marked as noncritical*, to support legacy applications that cannot process InhibitAnyPolicy.   |
| SkipCerts                  |                  | INTEGER                                    | 0 – specific policies are required in the FPKI  |
| <b>optional extensions</b> |                  |  |   |
| <b>subjectInfoAccess</b>   | FALSE            |  | CA Certificates issued for PIV-I may include a subjectInfoAccess extension (unless the certificate subject does not issue any CA certificates, as specified in Section 8). subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access method is defined for use in CA certificates. |
| AccessDescription          |                  |  |   |
| accessMethod               |                  | id-ad-caRepository<br>(1.3.6.1.5.5.7.48.5) | Each CA certificate should include at least one instance of this access method that includes a URI name form to specify an HTTP accessible Web server. The URI should point to a location where certificates issued by the subject of this certificate may be found.  |
| accessLocation             |                  |  |   |
| GeneralName                |                  |  |   |
| uniformResourceIdentifier  |                  | ldap://... or http://...                   | See preamble text on URIs.  |
| <b>issuerAltName</b>       | FALSE            |  | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |  |   |
| GeneralName                |                  |  |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                     | Criticality Flag | Value       | Comments   |
|---------------------------|------------------|-------------|--|
| rfc822Name                |                  | IA5String   | Electronic mail address of the PKI administration  |
| <b>policyMappings</b>     | FALSE            |             | This extension may be included in cross-certificates if the subject CA issues certificates under a different set of policies than the issuing CA and the subject CA's policies are deemed by the issuer to map to the issuer's policies. |
| issuerDomainPolicy        |                  | OID         | OID of policy from the issuing CA domain that maps to the equivalent policy in the subject CA's domain.  |
| subjectDomainPolicy       |                  | OID         | OID of policy in the subject CA's domain that may be accepted in lieu of the issuing domain policy.  |
| <b>nameConstraints</b>    | TRUE             |             | This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees overlap, the excluded subtree takes precedence.                             |
| permittedSubtrees         |                  |             | minimum is always zero, maximum is never present.  |
| GeneralSubtrees           |                  |             |  |
| GeneralSubtree            |                  |             |  |
| base                      |                  |             |  |
| GeneralName               |                  |             |  |
| directoryName             |                  |             |  |
| Name                      |                  |             |  |
| RDNSequence               |                  |             |  |
| RelativeDistinguishedName |                  |             |  |
| AttributeTypeAndValue     |                  |             |  |
| AttributeType             |                  | OID         |  |
| AttributeValue            |                  | see comment | See preamble text on naming.   |
| minimum                   |                  | 0           | minimum is always zero, maximum is never present.  |
| excludedSubtrees          |                  |             |  |
| GeneralSubtrees           |                  |             |  |
| GeneralSubtree            |                  |             |  |
| base                      |                  |             |  |
| GeneralName               |                  |             |  |
| directoryName             |                  |             |  |
| Name                      |                  |             |  |
| RDNSequence               |                  |             |  |
| RelativeDistinguishedName |                  |             |  |
| AttributeTypeAndValue     |                  |             |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field          | Criticality Flag | Value       | Comments  |
|----------------|------------------|-------------|---|
| AttributeType  |                  | OID         |   |
| AttributeValue |                  | see comment | See preamble text on naming.                      |
| minimum        |                  | 0           | minimum is always zero, maximum is never present. |

\*Note: The recommended criticality setting is different from RFC 5280.

**Worksheet 3: CRL Profile**

| Field                     | Criticality Flag | Value                  | Comments   |
|---------------------------|------------------|------------------------|--|
| CertificateList           |                  |                        |  |
| tbsCertList               |                  |                        | Fields to be signed.   |
| <b>version</b>            |                  | 1                      | Integer Value of "1" for Version 2 CRL.  |
| <b>signature</b>          |                  |                        |  |
| AlgorithmIdentifier       |                  |                        | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  |                        | Choice of following algorithms:  |
|                           |                  | 1.2.840.113549.1.1.5   | Sha1WithRSAEncryption (may only be used in CRLs issued before January 1, 2011)   |
|                           |                  | 1.2.840.113549.1.1.10  | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11  | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2    | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3    | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1 | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                   | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                        |  |
| Name                      |                  |                        | Issuer name should be encoded exactly as it is encoded in the issuer fields of the certificates that are covered by this CRL.  |
| RDNSequence               |                  |                        |  |
| RelativeDistinguishedName |                  |                        |  |
| AttributeTypeAndValue     |                  |                        |  |
| AttributeType             |                  | OID                    |  |
| AttributeValue            |                  | See Comment.           | See preamble text on naming.   |
| <b>thisUpdate</b>         |                  |                        |  |
| Time                      |                  |                        |  |
| utcTime                   |                  | YYMMDDHHMMSSZ          | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ        | Use for dates after 2049   |
| <b>nextUpdate</b>         |                  |                        |  |
| Time                      |                  |                        |  |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

---

| Field                           | Criticality Flag | Value           | Comments   |
|---------------------------------|------------------|-----------------|--|
| utcTime                         |                  | YYMMDDHHMMSSZ   | Use for dates up to and including 2049.  |
| generalTime                     |                  | YYYYMMDDHHMMSSZ | Use for dates after 2049   |
| <b>revokedCertificates</b>      |                  |                 |  |
| userCertificate                 |                  | INTEGER         | serial number of certificate being revoked   |
| revocationDate                  |                  |                 |  |
| Time                            |                  |                 |  |
| utcTime                         |                  | YYMMDDHHMMSSZ   | Use for dates up to and including 2049.  |
| generalTime                     |                  | YYYYMMDDHHMMSSZ | Use for dates after 2049   |
| crEntryExtensions               |                  |                 |  |
| Extensions                      |                  |                 |  |
| <b>reasonCode</b>               | FALSE            |                 |  |
| CRLReason                       |                  |                 | Any one of these CRL reasons may be asserted: keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold. If the revocation reason is unspecified, then the reasonCode extension should not be included. The removeFromCRL reason code may only be used in delta CRLs.   |
| <b>invalidityDate</b>           | FALSE            |                 | This extension may be included if the invalidity date precedes the revocation date.  |
| GeneralizedTime                 |                  | YYYYMMDDHHMMSSZ | use this format for all dates.   |
| <b>crExtensions</b>             |                  |                 |  |
| Extensions                      |                  |                 |  |
| <b>authorityKeyIdentifier</b>   | FALSE            |                 | Must be included in all CRLs.  |
| keyIdentifier                   |                  | OCTET STRING    | Derived using the SHA-1 hash of the public key.  |
| <b>cRLNumber</b>                | FALSE            | INTEGER         | Monotonically increasing sequential number. Must be included in all CRLs.  |
| <b>issuingDistributionPoint</b> | TRUE             |                 | This extension appears in segmented CRLs. If the CRL covers all unexpired certificates issued by the CRL issuer (i.e., all unexpired certificates in which the issuer field contains the same name as the issuer field of the CRL), then this extension does not need to be included. CRLs must cover all reason codes and may not be indirect. Thus, the onlySomeReasons field must be absent and the indirectCRL flag must be false. |
| distributionPoint               |                  |                 |  |
| DistributionPointName           |                  |                 | If the issuer generates segmented CRLs (i.e., CRLs that do not cover all unexpired certificates in which the issuer field contains the same name as  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                     | Criticality Flag | Value        | Comments  |
|---------------------------|------------------|--------------|---|
|                           |                  |              | the issuer field in the CRL), this field must be present and must specify the same names as are specified in the distributionPoint field of the cRLDistributionPoints extensions of certificates covered by this CRL. |
| fullName                  |                  |              |   |
| GeneralNames              |                  |              |   |
| GeneralName               |                  |              |   |
| directoryName             |                  |              |   |
| Name                      |                  |              |   |
| RDNSequence               |                  |              |   |
| RelativeDistinguishedName |                  |              |   |
| AttributeTypeAndValue     |                  |              |   |
| AttributeType             |                  | OID          |   |
| AttributeValue            |                  | See comment. |   |
| uniformResourceIdentifier |                  | IA5String    |   |
| onlyContainsUserCerts     |                  | BOOLEAN      | If set to TRUE, this CRL only covers end entity certificates  |
| onlyContainsCACerts       |                  | BOOLEAN      | If set to TRUE, this CRL only covers CA certificates. If onlyContainsUserCerts is TRUE, this field must be FALSE.   |
| IndirectCRL               |                  | FALSE        |   |

**Worksheet 4: PIV-I Card Authentication Certificate Profile**

| Field                     | Criticality Flag | Value                  | Comments   |
|---------------------------|------------------|------------------------|--|
| Certificate               |                  |                        |  |
| tbsCertificate            |                  |                        | Fields to be signed.   |
| <b>version</b>            |                  | 2                      | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                | Unique positive integer.   |
| <b>signature</b>          |                  |                        |  |
| AlgorithmIdentifier       |                  |                        | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  |                        | Choice of following algorithms:  |
|                           |                  | 1.2.840.113549.1.1.5   | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10  | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11  | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2    | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3    | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1 | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                   | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                        |  |
| Name                      |                  |                        |  |
| RDNSSequence              |                  |                        |  |
| RelativeDistinguishedName |                  |                        |  |
| AttributeTypeAndValue     |                  |                        |  |
| AttributeType             |                  | OID                    |  |
| AttributeValue            |                  | see comment            | See preamble text on naming.   |
| <b>validity</b>           |                  |                        |  |
| notBefore                 |                  |                        |  |
| Time                      |                  |                        |  |
| utcTime                   |                  | YYMMDDHHMMSSZ          | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ        | Use for dates after 2049   |
| notAfter                  |                  |                        | The notAfter time MUST not be after the PIV-I card expiration date.  |
| Time                      |                  |                        |  |
| utcTime                   |                  | YYMMDDHHMMSSZ          | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ        | Use for dates after 2049   |



**Federal PKI Policy Authority  
PIV-I Tiger Team**

| Field                         | Criticality Flag | Value  | Comments  |
|-------------------------------|------------------|--|---|
| <b>subject</b>                |                  |  |   |
| Name                          |                  |  | MUST include a Non-NULL Subject DN<br>see naming requirements in [1]  |
| RDNSequence                   |                  |  |   |
| RelativeDistinguishedName     |                  |  |   |
| AttributeTypeAndValue         |                  |  |   |
| AttributeType                 |                  | OID  |   |
| AttributeValue                |                  | see comment  | See preamble text on naming.  |
| <b>subjectPublicKeyInfo</b>   |                  |  |   |
| algorithm                     |                  |  |   |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key.<br>May be either RSA or elliptic curve.  |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption  |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key  |
| parameters                    |                  |  | Format and meaning dependent upon algorithm   |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.   |
| EcpkParameters                |                  |  |   |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |   |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys: certificates that expire before January 1, 2014 shall have a modulus of 1024 or 2048 bits; certificates that expire on or after January 1, 2014 shall have a modulus of 2048 bits.<br>(No sunset date for specified elliptic curve.) |
| <b>required extensions</b>    |                  |  |   |
| <b>authorityKeyIdentifier</b> | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>keyUsage</b>               | TRUE             |  | Only digitalSignature shall be set.   |
| digitalSignature              |                  | 1  |   |
| nonRepudiation                |                  | 0  |   |
| keyEncipherment               |                  | 0  |   |
| dataEncipherment              |                  | 0  |   |
| keyAgreement                  |                  | 0  |   |
| keyCertSign                   |                  | 0  |   |
| cRLSign                       |                  | 0  |   |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                                | Comments  |
|------------------------------|------------------|--------------------------------------|---|
| encipherOnly                 |                  | 0                                    |   |
| decipherOnly                 |                  | 0                                    |   |
| <b>extKeyUsage</b>           | TRUE             |                                      | This extension shall assert only the id-PIV-cardAuth keyPurposeID.  |
| 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.  |
| <b>certificatePolicies</b>   | FALSE            |                                      |   |
| PolicyInformation            |                  |                                      |   |
| policyIdentifier             |                  |                                      |   |
| <b>cRLDistributionPoints</b> | FALSE            |                                      | This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.   |
| DistributionPoint            |                  |                                      |   |
| distributionPoint            |                  |                                      |   |
| DistributionPointName        |                  |                                      |   |
| fullName                     |                  |                                      |   |
| GeneralNames                 |                  |                                      |   |
| GeneralName                  |                  |                                      |   |
| directoryName                |                  |                                      |   |
| Name                         |                  |                                      |   |
| RDNSSequence                 |                  |                                      |   |
| RelativeDistinguishedName    |                  |                                      |   |
| AttributeTypeAndValue        |                  |                                      |   |
| AttributeType                |                  | OID                                  |   |
| AttributeValue               |                  | see comment                          | See preamble text on naming.  |
| uniformResourceIdentifier    |                  | ldap://... or http://...             | See preamble text on URIs.  |
| <b>authorityInfoAccess</b>   | FALSE            |                                      | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| AccessDescription            |                  |                                      |   |
| accessMethod                 |                  | id-ad-calssuers (1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                              | Comments  |
|----------------------------|------------------|------------------------------------|---|
|                            |                  |                                    | certificates issued to the issuer of this certificate may be found.   |
| accessLocation             |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | ldap://... or http://...           | See preamble text on URIs.  |
| accessMethod               |                  | id-ad-ocsp<br>(1.3.6.1.5.5.7.48.1) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. |
| accessLocation             |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | http://...                         | See preamble text on URIs.  |
| <b>subjectAltName</b>      | FALSE            |                                    |   |
| GeneralNames               |                  |                                    | Must only include UUID name form.   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | UUID                               | This field contains the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122.   |
| <b>optional extensions</b> |                  |                                    |   |
| <b>issuerAltName</b>       | FALSE            |                                    | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| rfc822Name                 |                  | IA5String                          | Electronic mail address of the PKI administration   |

**Worksheet 5: PIV-I Authentication Certificate Profile**

| Field                     | Criticality Flag | Value                  | Comments   |
|---------------------------|------------------|------------------------|--|
| Certificate               |                  |                        |  |
| tbsCertificate            |                  |                        | Fields to be signed.   |
| <b>version</b>            |                  | 2                      | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                | Unique positive integer.   |
| <b>signature</b>          |                  |                        |  |
| AlgorithmIdentifier       |                  |                        | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  |                        | Choice of following algorithms:  |
|                           |                  | 1.2.840.113549.1.1.5   | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10  | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11  | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2    | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3    | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1 | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                   | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                        |  |
| Name                      |                  |                        |  |
| RDNSequene                |                  |                        |  |
| RelativeDistinguishedName |                  |                        |  |
| AttributeTypeAndValue     |                  |                        |  |
| AttributeType             |                  | OID                    |  |
| AttributeValue            |                  | see comment            | See preamble text on naming.   |
| <b>validity</b>           |                  |                        |  |
| notBefore                 |                  |                        |  |
| Time                      |                  |                        |  |
| utcTime                   |                  | YYMMDDHHMMSSZ          | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ        | Use for dates after 2049   |
| notAfter                  |                  |                        | The notAfter time MUST not be after the PIV-I card expiration date.  |
| Time                      |                  |                        |  |
| utcTime                   |                  | YYMMDDHHMMSSZ          | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ        | Use for dates after 2049   |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

| Field                         | Criticality Flag | Value  | Comments   |
|-------------------------------|------------------|--|--|
| <b>subject</b>                |                  |  |  |
| Name                          |                  |  | X.500 Distinguished name of the owner of the certificate. See naming requirements in [1].  |
| RDNSequence                   |                  |  |  |
| RelativeDistinguishedName     |                  |  |  |
| AttributeTypeAndValue         |                  |  |  |
| AttributeType                 |                  | OID  |  |
| AttributeValue                |                  | see comment  | See preamble text on naming.   |
| <b>subjectPublicKeyInfo</b>   |                  |  |  |
| algorithm                     |                  |  |  |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key. May be either RSA or elliptic curve.  |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption   |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key   |
| parameters                    |                  |  | Format and meaning dependent upon algorithm  |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.  |
| EcpkParameters<br>namedCurve  |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |  |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256  |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys: certificates that expire before January 1, 2014 shall have a modulus of 1024 or 2048 bits; certificates that expire on or after January 1, 2014 shall have a modulus of 2048 bits. (No sunset date for specified elliptic curve.) |
| <b>required extensions</b>    |                  |  |  |
| <b>authorityKeyIdentifier</b> | FALSE            |  |  |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.  |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |  |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.  |
| <b>keyUsage</b>               | TRUE             |  | Only digitalSignature shall be set.  |
| digitalSignature              |                  | 1  |  |
| nonRepudiation                |                  | 0  |  |
| keyEncipherment               |                  | 0  |  |
| dataEncipherment              |                  | 0  |  |
| keyAgreement                  |                  | 0  |  |
| keyCertSign                   |                  | 0  |  |
| cRLSign                       |                  | 0  |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                                   | Comments  |
|------------------------------|------------------|---|---|
| encipherOnly                 |                  | 0                                       |   |
| decipherOnly                 |                  | 0                                       |   |
| <b>certificatePolicies</b>   | FALSE            |   |   |
| PolicyInformation            |                  |   |   |
| policyIdentifier             |                  |   |   |
| <b>cRLDistributionPoints</b> | FALSE            |   | This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.   |
| DistributionPoint            |                  |   |   |
| distributionPoint            |                  |   |   |
| DistributionPointName        |                  |   |   |
| fullName                     |                  |   |   |
| GeneralNames                 |                  |   |   |
| GeneralName                  |                  |   |   |
| directoryName                |                  |   |   |
| Name                         |                  |   |   |
| RDNSSequence                 |                  |   |   |
| RelativeDistinguishedName    |                  |   |   |
| AttributeTypeAndValue        |                  |   |   |
| AttributeType                |                  | OID                                     |   |
| AttributeValue               |                  | see comment                             | See preamble text on naming.  |
| uniformResourceIdentifier    |                  | ldap://... or http://...                | See preamble text on URIs.  |
| <b>authorityInfoAccess</b>   | FALSE            |   | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| AccessDescription            |                  |   |   |
| accessMethod                 |                  | id-ad-calssuers<br>(1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found.   |
| accessLocation               |                  |   |   |
| GeneralName                  |                  |   |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                     | Criticality Flag | Value                              | Comments   |
|---------------------------|------------------|------------------------------------|--|
| uniformResourceIdentifier |                  | ldap://... or http://...           | See preamble text on URIs.   |
| accessMethod              |                  | id-ad-ocsp<br>(1.3.6.1.5.5.7.48.1) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.  |
| accessLocation            |                  |                                    |  |
| GeneralName               |                  |                                    |  |
| uniformResourceIdentifier |                  | http://...                         | See preamble text on URIs.   |
| <b>subjectAltName</b>     | FALSE            |                                    |  |
| GeneralNames              |                  |                                    | This extension MUST include the UUID as specified below. Any additional name types may be present; only the most common are specified here. Other names may be included to support local applications.   |
| GeneralName               |                  |                                    |  |
| uniformResourceIdentifier |                  | UUID                               | This field contains the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122.  |
| otherName                 |                  |                                    |  |
| type-id                   |                  | 1.3.6.1.4.1.311.20.2.3             | UPN OtherName OID  |
| value                     |                  | UTF8String                         | This field specifies Microsoft user principal name for use with Microsoft Windows logon.   |
| directoryName             |                  |                                    |  |
| Name                      |                  |                                    |  |
| RDNSSequence              |                  |                                    |  |
| RelativeDistinguishedName |                  |                                    |  |
| AttributeTypeAndValue     |                  |                                    |  |
| AttributeType             |                  | OID                                |  |
| AttributeValue            |                  | see comment                        | See preamble text on naming.   |
| <b>extKeyUsage</b>        | BOOLEAN          |                                    | <p>This extension MUST appear in certificates issued after June 30, 2018. The extension should be non-critical and shall not include the anyExtendedKeyUsage value.</p> <p>The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs consistent with authentication purposes may be specified.</p> <p>Note: for certificates issued prior to June 30, 2018 anyExtendedKeyUsage may be present or the entire extension may be absent</p> |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                  | Comments  |
|----------------------------|------------------|------------------------|---|
| keyPurposeID               |                  | 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   |
|                            |                  | 1.3.6.1.5.2.3.4        | id-pkinit-KPClientAuth  |
|                            |                  | 1.3.6.1.5.5.7.3.21     | id-kp-secureShellClient<br>This key purpose value may be implemented as needed by the Subscriber, eg. may only be required for administrators |
| <b>optional extensions</b> |                  |                        |   |
| <b>issuerAltName</b>       | FALSE            |                        | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |                        |   |
| GeneralName                |                  |                        |   |
| rfc822Name                 |                  | IA5String              | Electronic mail address of the PKI administration   |



**Worksheet 6: PIV-I Digital Signature Certificate Profile**

| Field                       | Criticality Flag | Value                           | Comments   |
|-----------------------------|------------------|---------------------------------|--|
| Certificate                 |                  |                                 |  |
| tbsCertificate              |                  |                                 | Fields to be signed.   |
| <b>version</b>              |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>         |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>            |                  |                                 |  |
| AlgorithmIdentifier         |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                   |                  | Choice of following algorithms: |  |
|                             |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                             |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                             |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                             |                  | 1.2.840.10045.4.3.2             | ecdsa-with-SHA256  |
|                             |                  | 1.2.840.10045.4.3.3             | ecdsa-with-SHA384  |
| parameters                  |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                             |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>               |                  |                                 |  |
| Name                        |                  |                                 |  |
| RDNSequence                 |                  |                                 |  |
| RelativeDistinguishedName   |                  |                                 |  |
| AttributeTypeAndValue       |                  |                                 |  |
| AttributeType               |                  | OID                             |  |
| AttributeValue              |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>             |                  |                                 |  |
| notBefore                   |                  |                                 |  |
| Time                        |                  |                                 |  |
| utcTime                     |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime                 |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                    |                  |                                 |  |
| Time                        |                  |                                 |  |
| utcTime                     |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime                 |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>              |                  |                                 |  |
| Name                        |                  |                                 | X.500 Distinguished name of the owner of the certificate.  |
| RDNSequence                 |                  |                                 |  |
| RelativeDistinguishedName   |                  |                                 |  |
| AttributeTypeAndValue       |                  |                                 |  |
| AttributeType               |                  | OID                             |  |
| AttributeValue              |                  | see comment                     | See preamble text on naming.   |
| <b>subjectPublicKeyInfo</b> |                  |                                 |  |
| algorithm                   |                  |                                 |  |
| AlgorithmIdentifier         |                  |                                 | Public key algorithm associated with the public key.   |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

| Field                         | Criticality Flag | Value  | Comments  |
|-------------------------------|------------------|--|---|
|                               |                  |  | May be either RSA or elliptic curve.  |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption  |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key  |
| parameters                    |                  |  | Format and meaning dependent upon algorithm   |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.   |
| EcpkParameters                |                  |  |   |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |   |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
|                               |                  | 1.3.132.0.34   | Curve P-384   |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys: certificates shall have a modulus of 2048 bits.  |
| <b>required extensions</b>    |                  |  |   |
| <b>authorityKeyIdentifier</b> | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>keyUsage</b>               | TRUE             |  | Both digitalSignature and nonRepudiation shall be set.  |
| digitalSignature              |                  | 1  |   |
| nonRepudiation                |                  | 1  |   |
| keyEncipherment               |                  | 0  |   |
| dataEncipherment              |                  | 0  |   |
| keyAgreement                  |                  | 0  |   |
| keyCertSign                   |                  | 0  |   |
| cRLSign                       |                  | 0  |   |
| encipherOnly                  |                  | 0  |   |
| decipherOnly                  |                  | 0  |   |
| <b>certificatePolicies</b>    | FALSE            |  |   |
| PolicyInformation             |                  |  |   |
| policyIdentifier              |                  |  |   |
| <b>cRLDistributionPoints</b>  | FALSE            |  | This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted. |
| DistributionPoint             |                  |  |   |
| distributionPoint             |                  |  |   |
| DistributionPointName         |                  |  |   |
| fullName                      |                  |  |   |
| GeneralNames                  |                  |  |   |
| GeneralName                   |                  |  |   |
| directoryName                 |                  |  |   |
| Name                          |                  |  |   |
| RDNSequence                   |                  |  |   |
| RelativeDistinguishedName     |                  |  |   |
| AttributeTypeAndValue         |                  |  |   |
| AttributeType                 |                  | OID  |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

| Field                      | Criticality Flag | Value                                   | Comments  |
|----------------------------|------------------|---|---|
| AttributeValue             |                  | see comment                             | See preamble text on naming.  |
| uniformResourceIdentifier  |                  | ldap://... or http://...                | See preamble text on URIs.  |
| <b>authorityInfoAccess</b> | FALSE            |   | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| AccessDescription          |                  |   |   |
| accessMethod               |                  | id-ad-calssuers<br>(1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.  |
| accessLocation             |                  |   |   |
| GeneralName                |                  |   |   |
| uniformResourceIdentifier  |                  | ldap://... or http://...                | See preamble text on URIs.  |
| accessMethod               |                  | id-ad-ocsp<br>(1.3.6.1.5.5.7.48.1)      | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.   |
| accessLocation             |                  |   |   |
| GeneralName                |                  |   |   |
| uniformResourceIdentifier  |                  | http://...                              | See preamble text on URIs.  |
| <b>extKeyUsage</b>         | BOOLEAN          |   | This extension MUST appear in certificates issued after June 30, 2019. The extension should be non-critical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with signing purposes, may be specified.<br><br>Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.   |
| keyPurposeID               |                  | 1.3.6.1.5.5.7.3.4                       | id-kp-emailProtection   |
|                            |                  | 1.3.6.1.4.1.311.10.3.12                 | MSFT Document Signing   |
|                            |                  | 1.2.840.113583.1.1.5                    | Adobe Certified Document Signing<br>Note: this value has been deprecated by Adobe   |
| <b>optional extensions</b> |                  |   |   |
| <b>issuerAltName</b>       | FALSE            |   | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |   |   |
| GeneralName                |                  |   |   |
| rfc822Name                 |                  | IA5String                               | Electronic mail address of the PKI administration   |
| <b>subjectAltName</b>      | FALSE            |   | Any name types may be present; only the most common are specified here. Other names may be included to support local applications.  |
| GeneralNames               |                  |   |   |
| GeneralName                |                  |   |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                     | Criticality Flag | Value       | Comments  |
|---------------------------|------------------|-------------|---|
| rfc822Name                |                  | IA5String   | This field contains the electronic mail address of the subject. |
| directoryName             |                  |             |   |
| Name                      |                  |             |   |
| RDNSSequence              |                  |             |   |
| RelativeDistinguishedName |                  |             |   |
| AttributeTypeAndValue     |                  |             |   |
| AttributeType             |                  | OID         |   |
| AttributeValue            |                  | see comment | See preamble text on naming.                                    |

**Worksheet 7: PIV-I Key Management Certificate Profile**

| Field                     | Criticality Flag | Value                           | Comments   |
|---------------------------|------------------|---------------------------------|--|
| Certificate               |                  |                                 |  |
| tbsCertificate            |                  |                                 | Fields to be signed.   |
| <b>version</b>            |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>          |                  |                                 |  |
| AlgorithmIdentifier       |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  | Choice of following algorithms: |  |
|                           |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2             | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3             | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                                 |  |
| Name                      |                  |                                 |  |
| RDNSSequence              |                  |                                 |  |
| RelativeDistinguishedName |                  |                                 |  |
| AttributeTypeAndValue     |                  |                                 |  |
| AttributeType             |                  | OID                             |  |
| AttributeValue            |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>           |                  |                                 |  |
| notBefore                 |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                  |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>            |                  |                                 |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                         | Criticality Flag | Value  | Comments  |
|-------------------------------|------------------|--|---|
| Name                          |                  |  | X.500 Distinguished name of the owner of the certificate.                                 |
| RDNSequence                   |                  |  |   |
| RelativeDistinguishedName     |                  |  |   |
| AttributeTypeAndValue         |                  |  |   |
| AttributeType                 |                  | OID  |   |
| AttributeValue                |                  | see comment  | See preamble text on naming.  |
| <b>subjectPublicKeyInfo</b>   |                  |  |   |
| algorithm                     |                  |  |   |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key. May be either RSA or elliptic curve. |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption  |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key  |
| parameters                    |                  |  | Format and meaning dependent upon algorithm   |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.   |
| EcpkParameters                |                  |  |   |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |   |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
|                               |                  | 1.3.132.0.34   | Curve P-384   |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys certificates shall have a modulus of 2048 bits.                       |
| <b>required extensions</b>    |                  |  |   |
| <b>authorityKeyIdentifier</b> | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>keyUsage</b>               | TRUE             |  |   |
| digitalSignature              |                  | 0  |   |
| nonRepudiation                |                  | 0  |   |
| keyEncipherment               |                  | 1  | Asserted when public key is RSA.  |
| dataEncipherment              |                  | 0  |   |
| keyAgreement                  |                  | 1  | Asserted when public key is elliptic curve.   |
| keyCertSign                   |                  | 0  |   |
| cRLSign                       |                  | 0  |   |
| encipherOnly                  |                  | 0  | There is no requirement to support this key usage.  |
| decipherOnly                  |                  | 0  | There is no requirement to support this key usage.  |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                                   | Comments  |
|------------------------------|------------------|---|---|
| <b>certificatePolicies</b>   | FALSE            |   |   |
| PolicyInformation            |                  |   |   |
| policyIdentifier             |                  |   |   |
| <b>cRLDistributionPoints</b> | FALSE            |   | This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.   |
| DistributionPoint            |                  |   |   |
| distributionPoint            |                  |   |   |
| DistributionPointName        |                  |   |   |
| fullName                     |                  |   |   |
| GeneralNames                 |                  |   |   |
| GeneralName                  |                  |   |   |
| directoryName                |                  |   |   |
| Name                         |                  |   |   |
| RDNSSequence                 |                  |   |   |
| RelativeDistinguishedName    |                  |   |   |
| AttributeTypeAndValue        |                  |   |   |
| AttributeType                |                  | OID                                     |   |
| AttributeValue               |                  | see comment                             | See preamble text on naming.  |
| uniformResourceIdentifier    |                  | ldap://... or http://...                | See preamble text on URIs.  |
| <b>authorityInfoAccess</b>   | FALSE            |   | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| AccessDescription            |                  |   |   |
| accessMethod                 |                  | id-ad-calssuers<br>(1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.  |
| accessLocation               |                  |   |   |
| GeneralName                  |                  |   |   |
| uniformResourceIdentifier    |                  | ldap://... or http://...                | See preamble text on URIs.  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                              | Comments  |
|----------------------------|------------------|------------------------------------|---|
| accessMethod               |                  | id-ad-ocsp<br>(1.3.6.1.5.5.7.48.1) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.   |
| accessLocation             |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | http://...                         | See preamble text on URIs.  |
| <b>extKeyUsage</b>         | BOOLEAN          |                                    | This extension <b>MUST</b> appear in certificates issued after June 30, 2019. The extension should be non-critical and shall not include the anyExtendedKeyUsage value. The value listed below for keyPurposeID is recommended for inclusion. Additional keyPurposeIDs, consistent with key management purposes, may be specified.<br><br>Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent. |
| keyPurposeID               |                  | 1.3.6.1.5.5.7.3.4                  | id-kp-emailProtection   |
| <b>optional extensions</b> |                  |                                    |   |
| <b>issuerAltName</b>       | FALSE            |                                    | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| rfc822Name                 |                  | IA5String                          | Electronic mail address of the PKI administration   |
| <b>subjectAltName</b>      | FALSE            |                                    | Any name types may be present; only the most common are specified here. Other names may be included to support local applications.  |
| GeneralNames               |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| rfc822Name                 |                  | IA5String                          | This field contains the electronic mail address of the subject.   |
| directoryName              |                  |                                    |   |
| Name                       |                  |                                    |   |
| RDNSequence                |                  |                                    |   |
| RelativeDistinguishedName  |                  |                                    |   |
| AttributeTypeAndValue      |                  |                                    |   |
| AttributeType              |                  | OID                                |   |
| AttributeValue             |                  | see comment                        | See preamble text on naming.  |



**Worksheet 8: PIV-I Content Signing Certificate Profile**

| Field                     | Criticality Flag | Value                           | Comments   |
|---------------------------|------------------|---------------------------------|--|
| Certificate               |                  |                                 |  |
| tbsCertificate            |                  |                                 | Fields to be signed.   |
| <b>version</b>            |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>          |                  |                                 |  |
| AlgorithmIdentifier       |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  | Choice of following algorithms: |  |
|                           |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2             | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3             | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                                 |  |
| Name                      |                  |                                 |  |
| RDNSSequence              |                  |                                 |  |
| RelativeDistinguishedName |                  |                                 |  |
| AttributeTypeAndValue     |                  |                                 |  |
| AttributeType             |                  | OID                             |  |
| AttributeValue            |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>           |                  |                                 |  |
| notBefore                 |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                  |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>            |                  |                                 |  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                         | Criticality Flag | Value  | Comments  |
|-------------------------------|------------------|--|---|
| Name                          |                  |  | X.500 Distinguished name of the owner of the certificate.   |
| RDNSequence                   |                  |  |   |
| RelativeDistinguishedName     |                  |  |   |
| AttributeTypeAndValue         |                  |  |   |
| AttributeType                 |                  | OID  |   |
| AttributeValue                |                  | see comment  | See preamble text on naming.  |
| <b>subjectPublicKeyInfo</b>   |                  |  |   |
| algorithm                     |                  |  |   |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key. May be either RSA or elliptic curve.   |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption  |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key  |
| parameters                    |                  |  | Format and meaning dependent upon algorithm   |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.   |
| EcpkParameters                |                  |  |   |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |   |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
|                               |                  | 1.3.132.0.34   | Curve P-384   |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys certificates shall have a modulus of 2048 or 3072 bits.   |
| <b>required extensions</b>    |                  |  |   |
| <b>authorityKeyIdentifier</b> | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>keyUsage</b>               | TRUE             |  | 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. |
| digitalSignature              |                  | 1  | may be asserted.  |
| nonRepudiation                |                  | 0  | Must not be asserted in certificates issued to computing or communications devices.   |
| keyEncipherment               |                  | 0  |   |
| dataEncipherment              |                  | 0  |   |
| keyAgreement                  |                  | 0  |   |
| keyCertSign                   |                  | 0  |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                        | Criticality Flag | Value                                | Comments  |
|------------------------------|------------------|--------------------------------------|---|
| cRLSign                      |                  | 0                                    |   |
| encipherOnly                 |                  | 0                                    |   |
| decipherOnly                 |                  | 0                                    |   |
| <b>extKeyUsage</b>           | YES              |                                      |   |
| KeyPurposeID                 |                  | 2.16.840.1.101.3.8.7                 | id-fpki-pivi-content-signing  |
| <b>certificatePolicies</b>   | FALSE            |                                      |   |
| PolicyInformation            |                  |                                      |   |
| policyIdentifier             |                  |                                      |   |
| <b>cRLDistributionPoints</b> | FALSE            |                                      | This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.   |
| DistributionPoint            |                  |                                      |   |
| distributionPoint            |                  |                                      |   |
| DistributionPointName        |                  |                                      |   |
| fullName                     |                  |                                      |   |
| GeneralNames                 |                  |                                      |   |
| GeneralName                  |                  |                                      |   |
| directoryName                |                  |                                      |   |
| Name                         |                  |                                      |   |
| RDNSSequence                 |                  |                                      |   |
| RelativeDistinguishedName    |                  |                                      |   |
| AttributeTypeAndValue        |                  |                                      |   |
| AttributeType                |                  | OID                                  |   |
| AttributeValue               |                  | see comment                          | See preamble text on naming.  |
| uniformResourceIdentifier    |                  | ldap://... or http://...             | See preamble text on URIs.  |
| <b>authorityInfoAccess</b>   | FALSE            |                                      | authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| AccessDescription            |                  |                                      |   |
| accessMethod                 |                  | id-ad-caIssuers (1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.  |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                      | Criticality Flag | Value                              | Comments  |
|----------------------------|------------------|------------------------------------|---|
| accessLocation             |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | ldap://... or http://...           | See preamble text on URIs.  |
| accessMethod               |                  | id-ad-ocsp<br>(1.3.6.1.5.5.7.48.1) | When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. |
| accessLocation             |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| uniformResourceIdentifier  |                  | http://...                         | See preamble text on URIs.  |
| <b>optional extensions</b> |                  |                                    |   |
|                            |                  |                                    |   |
|                            |                  |                                    |   |
| <b>issuerAltName</b>       | FALSE            |                                    | Any name types may be present; only the most common are specified here.   |
| GeneralNames               |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| rfc822Name                 |                  | IA5String                          | Electronic mail address of the PKI administration   |
| <b>subjectAltName</b>      | FALSE            |                                    | Any name types may be present; only the most common are specified here. Other names may be included to support local applications.  |
| GeneralNames               |                  |                                    |   |
| GeneralName                |                  |                                    |   |
| dnsName                    |                  | IA5String                          | This field contains the DNS name of the subject   |
| iPAddress                  |                  | IA5String                          | This field contains the IP address of the subject   |
| directoryName              |                  |                                    |   |
| Name                       |                  |                                    |   |
| RDNSequence                |                  |                                    |   |
| RelativeDistinguishedName  |                  |                                    |   |
| AttributeTypeAndValue      |                  |                                    |   |
| AttributeType              |                  | OID                                |   |
| AttributeValue             |                  | see comment                        | See preamble text on naming.  |

**Worksheet 9: Delegated OCSP Responder Certificate Profile**

| Field                     | Criticality Flag | Value                           | Comments   |
|---------------------------|------------------|---------------------------------|--|
| Certificate               |                  |                                 |  |
| tbsCertificate            |                  |                                 | Fields to be signed.   |
| <b>version</b>            |                  | 2                               | Integer Value of "2" for Version 3 certificate.  |
| <b>serialNumber</b>       |                  | INTEGER                         | Unique positive integer.   |
| <b>signature</b>          |                  |                                 |  |
| AlgorithmIdentifier       |                  |                                 | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm                 |                  | Choice of following algorithms: |  |
|                           |                  | 1.2.840.113549.1.1.5            | Sha1WithRSAEncryption (Use is limited to certificates that are issued before 1/1/2011)   |
|                           |                  | 1.2.840.113549.1.1.10           | id-RSASSA-PSS (RSA with PSS padding; 800-78-2 requires use with SHA-256 hash algorithm)  |
|                           |                  | 1.2.840.113549.1.1.11           | Sha256WithRSAEncryption  |
|                           |                  | 1.2.840.10045.4.3.2             | ecdsa-with-SHA256  |
|                           |                  | 1.2.840.10045.4.3.3             | ecdsa-with-SHA384  |
| parameters                |                  | 2.16.840.1.101.3.4.2.1          | For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter  |
|                           |                  | NULL                            | For all RSA algorithms except id-RSASSA-PSS  |
| <b>issuer</b>             |                  |                                 |  |
| Name                      |                  |                                 |  |
| RDNSSequence              |                  |                                 |  |
| RelativeDistinguishedName |                  |                                 |  |
| AttributeTypeAndValue     |                  |                                 |  |
| AttributeType             |                  | OID                             |  |
| AttributeValue            |                  | see comment                     | See preamble text on naming.   |
| <b>validity</b>           |                  |                                 |  |
| notBefore                 |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| notAfter                  |                  |                                 |  |
| Time                      |                  |                                 |  |
| utcTime                   |                  | YYMMDDHHMMSSZ                   | Use for dates up to and including 2049.  |
| generalTime               |                  | YYYYMMDDHHMMSSZ                 | Use for dates after 2049   |
| <b>subject</b>            |                  |                                 |  |

**Federal PKI Policy Authority  
PIV-I Tiger Team**

| Field                         | Criticality Flag | Value  | Comments  |
|-------------------------------|------------------|--|---|
| Name                          |                  |  | X.500 Distinguished name of the owner of the certificate.                                 |
| RDNSequence                   |                  |  |   |
| RelativeDistinguishedName     |                  |  |   |
| AttributeTypeAndValue         |                  |  |   |
| AttributeType                 |                  | OID  |   |
| AttributeValue                |                  | see comment  | See preamble text on naming.  |
| <b>subjectPublicKeyInfo</b>   |                  |  |   |
| algorithm                     |                  |  |   |
| AlgorithmIdentifier           |                  |  | Public key algorithm associated with the public key. May be either RSA or elliptic curve. |
| algorithm                     |                  | 1.2.840.113549.1.1.1   | RSA Encryption  |
|                               |                  | 1.2.840.10045.2.1  | Elliptic curve key  |
| parameters                    |                  |  | Format and meaning dependent upon algorithm   |
| RSAParameters                 |                  | NULL   | For RSA, parameters field is populated with NULL.   |
| EcpkParameters                |                  |  |   |
| namedCurve                    |                  | Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-2: |   |
|                               |                  | 1.2.840.10045.3.1.7  | Curve P-256   |
|                               |                  | 1.3.132.0.34   | Curve P-384   |
| subjectPublicKey              |                  | BIT STRING   | For RSA public keys certificates shall have a modulus of 2048 or 3072 bits.               |
| <b>required extensions</b>    |                  |  |   |
| <b>authorityKeyIdentifier</b> | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>subjectKeyIdentifier</b>   | FALSE            |  |   |
| keyIdentifier                 |                  | OCTET STRING   | Derived using the SHA-1 hash of the public key.   |
| <b>keyUsage</b>               | TRUE             |  |   |
| digitalSignature              |                  | 1  |   |
| nonRepudiation                |                  | 0  |   |
| keyEncipherment               |                  | 0  |   |
| dataEncipherment              |                  | 0  |   |
| keyAgreement                  |                  | 0  |   |
| keyCertSign                   |                  | 0  |   |
| cRLSign                       |                  | 0  |   |
| encipherOnly                  |                  | 0  |   |
| decipherOnly                  |                  | 0  |   |

**Federal PKI Policy Authority**  
**PIV-I Tiger Team**

---

| Field                       | Criticality Flag | Value                                   | Comments   |
|-----------------------------|------------------|---|--|
| <b>id-pkix-ocsp-nocheck</b> | FALSE            | NULL                                    |  |
| <b>extKeyUsage</b>          | BOOLEAN          |   | This extension may be included as either a critical or non-critical extension.   |
| KeyPurposeID                |                  | 1.3.6.1.5.5.7.3.9                       | id-kp-OCSPSigning  |
| <b>optional extensions</b>  |                  |   |  |
| <b>certificatePolicies</b>  | FALSE            |   |  |
| PolicyInformation           |                  |   |  |
| policyIdentifier            |                  |   |  |
| <b>authorityInfoAccess</b>  | FALSE            |   |  |
| AccessDescription           |                  |   |  |
| accessMethod                |                  | id-ad-calssuers<br>(1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found. |
| accessLocation              |                  |   |  |
| GeneralName                 |                  |   |  |
| uniformResourceIdentifier   |                  | ldap://... or http://...                | See preamble text on URIs.   |
| <b>issuerAltName</b>        | FALSE            |   | Any name types may be present; only the most common are specified here.  |
| GeneralNames                |                  |   |  |
| GeneralName                 |                  |   |  |
| rfc822Name                  |                  | IA5String                               | Electronic mail address of the PKI administration  |
| <b>subjectAltName</b>       | FALSE            |   | Any name types may be present; only the most common are specified here.  |
| GeneralNames                |                  |   |  |
| GeneralName                 |                  |   |  |
| dNSName                     |                  | IA5String                               | This field contains the DNS name of the subject  |
| iPAddress                   |                  | IA5String                               | This field contains the IP address of the subject  |
| directoryName               |                  |   |  |
| Name                        |                  |   |  |
| RDNSequence                 |                  |   |  |
| RelativeDistinguishedName   |                  |   |  |
| AttributeTypeAndValue       |                  |   |  |
| AttributeType               |                  | OID                                     |  |
| AttributeValue              |                  | see comment                             | See preamble text on naming.   |