X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program

Federal PKI Policy Authority
Shared Service Provider Working Group

January 7, 2008

Revision History Table

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

1. Introduction

This document specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for certificates and CRLs issued under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [1]. The profiles serve to identify unique parameter settings for certificates and CRLs issued under this policy.

In the interest of establishing commonality and interoperability among PKI communities outside the Federal government, it was decided that this profile should be based on a "standard PKI profile" but still contain the unique parameter settings for Federal systems. The only widely accepted PKI profile currently on track to become a standard is 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 under the Common Certificate Policy. 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. 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
FASC-N	Federal Agency Smart Credential Number
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
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
RFC	Request For Comments
RSA	Rivest-Shamir-Adelman
SHA	Secure Hash Algorithm
SKID	Subject Key Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.3. References

[1] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

[2] Russel Housley and Paul Hoffman. Internet X.509 Public Key Infrastructure: *Operational Protocols: FTP and HTTP*, RFC 2585, May 1999.

[3] Russel Housley, Tim Polk, Warwick Ford, and David Solo. Internet Public Key Infrastructure: *X.509 Certificate and Certificate Revocation List (CRL) Profile*, RFC 3280, April 2002.

[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 800-78-1, August 2007.

[9] Blake Ramsdell. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*, RFC 3851, July 2004.

[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.

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 3280.

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.

All certification paths start from a trust anchor. A trust anchor is a CA that a user trusts to issue certificates based on out-of-band knowledge. The public key of a trust anchor is distributed to certificate users in the form of a "trust anchor certificate." A trust anchor certificate:

- is self-signed, that is, signed with the private key corresponding to the public key contained in the subject public key field of the certificate;[1]

[1] NOTE: While in most cases, the public key of a CA that is to act as a trust anchor is distributed using

- contains any needed parameters in the subject public key info field, where the digital signature algorithm used in the certificate requires the use of parameters;
- contains few or no extensions;
- is kept in protected memory or otherwise protected from alteration by an intruder;
- is transferred to the application or certificate using system in an authenticated manner. The signature on the trust anchor certificate cannot authenticate the certificate.

There is no single trust anchor for the entire Federal Government. The trust anchor used by a certificate using application may be the CA that issued it a certificate or may be a CA that is at the top of a hierarchy of CAs. Which trust anchors may be used by agency certificate using systems to start certification paths is a matter of agency security policy.

Agencies will designate the CAs that may be used as trust anchors by certificate using systems within the agency, and will establish the approved mechanisms for obtaining the trust anchors' public keys in a secure, authenticated manner. The FBCA will make the self-signed certificate of the Common Certificate Policy Root CA available for use as a trust anchor, and it is expected that this CA will be used as the trust anchor for most users who are issued certificates under the Common Certificate Policy.

V3 certificates provide a mechanism for CAs to append additional information about the subject's public key, issuer's public key, and issuer's CRLs. Standard certificate extensions are defined for X.509 v3 certificates. These extensions provide methods of increasing the amount of information the X.509 certificate conveys to facilitate automated certificate processing.

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 4.4.3 of the Common Certificate Policy [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 4.4.3 of the Common Certificate Policy. CAs that issue segmented CRLs are strongly encouraged to also issue full CRLs in order to accommodate third parties that use CRLs to generate

self-signed certificates, this is not strictly necessary. Relying parties may obtain the public key of a trust anchor by other means.

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 under the Common Certificate Policy, attributes of type DirectoryString in the issuer fields of certificates and CRLs and the distributionPoint fields of cRLDistributionPoints and issuingDistributionPoint extensions shall be encoded in PrintableString. In the subject field of end entity certificates, all attributes of type DirectoryString, except the common name attribute type, shall be encoded in PrintableString. The common name attribute type in the subject field of end entity

certificates shall be encoded in PrintableString if it is possible to encode the certificate subject's name using that encoding. If the certificate subject's name can not be encoded using PrintableString, then UTF8String shall be used. The subject name in CA certificates shall be encoded exactly as it is encoded in the issuer field of certificates and CRLs signed by the subject of the CA certificate.

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

Uniform Resource Identifiers (URIs) are used in five different extensions within the certificate and CRL profiles in this document: cRLDistributionPoints, FreshestCRL, issuingDistributionPoint, authorityInfoAccess, and subjectInfoAccess. 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, all URIs must have a prefix of "ldap" or "http" 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 URI must have a prefix of "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 and FreshestCRL extensions, 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, FreshestCRL, or issuingDistributionPoint extension are:

ldap://smime2.nist.gov/cn=Good%20CA,o=Test%20Certificates,c=US?certificateRevocationList

ldap://129.6.20.71/cn=onlyContainsCACerts%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary

http://fictitious.nist.gov/fictitiousCRLdirectory/fictitiousCRL1.crl

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 3851). 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 under the Common Certificate Policy must include an authorityInfoAccess extension that contains (at least) two instances of the id-ad-caIssuers access method. The access locations for these instances must be (1) an HTTP URI and (2) an LDAP URI that specifies both the cACertificate and crossCertificatePair attributes (a CA may, alternatively, specify each of the attributes in a separate LDAP 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:

ldap://smime2.nist.gov/cn=Good%20CA,o=Test%20Certificates,c=US?cACertificate,crossCertificatePair

ldap://129.6.20.71/cn=Good%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary

http://fictitious.nist.gov/fictitiousCertsOnlyCMSdirectory/certsIssuedToGoodCA.p7c

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 have a prefix of "https" 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 3851). 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 issued under the Common Certificate Policy should include a subjectInfoAccess extension that contains (at least) two instances of the id-ad-caRepository access method. The access locations for these instances should be (1) an HTTP URI and (2) an LDAP URI that specifies both the cACertificate and

crossCertificatePair attributes (a CA may, alternatively, specify each of the attributes in a separate LDAP URI). If the subject of the certificate only issues end entity certificates, then the subjectInfoAccess extension may be excluded. If the subject of the certificate issues self-issued certificates (e.g., key rollover certificates), but does not issue certificates to other CAs, then the LDAP URI in the subjectInfoAccess extension only needs to specify the cACertificate attribute.

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:

ldap://smime2.nist.gov/cn=Good%20CA,o=Test%20Certificates,c=US?cACertificate,crossCertificatePair

ldap://129.6.20.71/cn=Good%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary

http://fictitious.nist.gov/fictitiousCertsOnlyCMSdirectory/CAcertsIssuedByGoodCA.p7c

6. PIV Certificates

The certificate profiles for the PIV Authentication and Card Authentication certificates 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 FIPS 201 [11]. 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 Authentication certificates and Card Authentication certificates and the authorityInfoAccess extension in these certificates must include an access method of type id-ad-ocsp where the access location has a prefix of "http".
- PIV Authentication certificates must assert the id-fpki-common-authentication policy OID.
- Card Authentication certificates must assert the id-fpki-common-cardAuth policy OID and must include a critical extended key usage extension that asserts id-PIV-cardAuth.
- The inclusion of a non-NULL subject name in Card Authentication certificates is optional.
- Both PIV Authentication certificates and Card Authentication certificates must include a subjectAltName extension that includes the FASC-N from the PIV card that holds the certificates. The subjectAltName extension in the Card Authentication certificates must not include any name forms other than the FASC-N, but the subjectAltName extension in PIV Authentication certificates may contain any name forms in addition to the FASC-N that are required by the various applications with which the certificate will be used.
- The nonRepudiation key usage bit must not be set in either PIV Authentication certificates or Card Authentication certificates.

- Both PIV Authentication certificates and Card Authentication certificates must include a piv-interim extension that indicates whether the certificate subject's NACI had been completed and successfully adjudicated at the time of certificate issuance.

FIPS 201 also requires that certificates that can be used to verify signatures on the CHUID or biometric data on PIV cards include an extended key usage extension that asserts id-PIV-content-signing.

7. Worksheet Contents

The certificate and CRL profiles consist of ten 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 under the Common Certificate Policy.

The nine worksheets are:

1. The *Self-Signed Certificates* worksheet defines the mandatory and optional contents of self-signed CA certificates issued by CAs for use by PKI client systems when establishing trust anchors.
2. The *Self-Issued CA Certificates* worksheet defines the mandatory and optional contents of key rollover certificates.
3. The *Cross-Certificates* worksheet defines the mandatory and optional contents of certificates issued by CAs under the Common Certificate Policy where the subject is another CA and the public key will be used to verify the signature on certificates and CRLs.
4. The *CRL* worksheet table defines the mandatory and optional contents of CRLs issued by CAs that issue certificates under the Common Certificate Policy.
5. The *End Entity Signature Certificates* worksheet defines the mandatory and optional contents of certificates issued by CAs to Federal employees and contractors where the public key will be used to verify the signatures.
6. The *Key Management Certificates* worksheet defines the mandatory and optional contents of certificates issued by CAs to Federal employees and contractors where the public key will be used to perform key management operations.
7. The *Certificates for Computing and Communications Devices* worksheet defines the mandatory and optional contents of certificates issued by CAs to computing or communications devices (e.g., routers, firewalls, servers, etc.).

8. The *Card Authentication Certificates* worksheet defines the mandatory and optional contents of certificates that correspond to the Card Authentication Key defined in section 4.3 of FIPS 201.
9. The *PIV Authentication Certificates* worksheet defines the mandatory and optional contents of certificates that correspond to the PIV Authentication Key defined in section 4.3 of FIPS 201.
10. The *Delegated OCSP Responders* worksheet defines the mandatory and optional contents of certificates issued to OCSP responders.

Worksheet 1: Self-Signed Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique Positive Integer
signature			
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
		1.2.840.113549.1.1.10	id-RSASSA-PSS (RSA with PSS padding; 800-78-1 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
issuer			
Name			Will match the subject DN.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			Will match the issuer DN.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.

Field	Criticality Flag	Value	Comments
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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, modulus must be 2048, 3072, or 4096 bits
required extensions			
subjectKeyIdentifier	FALSE		This extension is required to assist in path development.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectInfoAccess	FALSE		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 (1.3.6.1.5.5.7.48.5)	Each self-signed certificate must include at least two instances of this access method: one that includes the URI name form to specify the location of an LDAP accessible directory server and one that includes a URI name form to specify an HTTP accessible Web server. Each URI must 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.
basicConstraints	TRUE		The contents of this extension are not used in the X.509 path validation algorithm. Path length constraints should not be included since they will not be enforced.
cA		TRUE	

Field	Criticality Flag	Value	Comments
keyUsage	TRUE		The contents of this extension are not used in the X.509 path validation algorithm. 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	
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
optional extensions			
issuerAltName	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
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 2: Self-Issued CA Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			Subject name should be encoded exactly as it is encoded in the issuer field of this certificate.

Field	Criticality Flag	Value	Comments
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
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
subjectPublicKeyInfo			
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 800-78-1:	
		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 that expire before December 31, 2010 shall have a modulus of 1024, 2048, 3072, or 4096 bits; certificates that expire on or after December 31, 2010 shall have a modulus of 2048, 3072, or 4096 bits. (No sunset date for specified elliptic curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
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	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	

Field	Criticality Flag	Value	Comments
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			The following five OIDs are defined in the Common Certificate Policy. CA certificates may assert one or more of the following OIDs. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy
		2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware
		2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices
		2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication
		2.16.840.1.101.3.2.1.3.16	id-fpki-common-High
		2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth
basicConstraints	TRUE		This extension must appear in all CA certificates. The pathLenConstraint field should not appear in self-issued certificates.
cA		TRUE	
cRLDistributionPoints	FALSE		This extension is required in all CA certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.

Field	Criticality Flag	Value	Comments
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
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.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
subjectInfoAccess	FALSE		CA Certificates issued under the Common Certificate Policy must 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 (1.3.6.1.5.5.7.48.5)	Each CA certificate must include at least two instances of this access method: one that includes the URI name form to specify the location of an LDAP accessible directory server and one that includes a URI name form to specify an HTTP accessible Web server. Each 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.
optional extensions			
issuerAltName	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
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 3: Cross Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
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.

Field	Criticality Flag	Value	Comments
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
subjectPublicKeyInfo			
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 800-78-1:	
		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 that expire before December 31, 2010 shall have a modulus of 1024, 2048, 3072, or 4096 bits; certificates that expire on or after December 31, 2010 shall have a modulus of 2048, 3072, or 4096 bits. (No sunset date for specified elliptic curves.)
required extensions			
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	
dataEncipherment		0	
keyAgreement		0	

Field	Criticality Flag	Value	Comments
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			The following five OIDs are defined in the Common Certificate Policy. CA certificates may assert one or more of the following OIDs. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy
		2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware
		2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices
		2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication
		2.16.840.1.101.3.2.1.3.16	id-fpki-common-High
		2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth
basicConstraints	TRUE		This extension must appear in all CA certificates.
cA		TRUE	
pathLenConstraint		INTEGER	The use of a path length constraint is optional.
cRLDistributionPoints	FALSE		This extension is required in all CA certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.

Field	Criticality Flag	Value	Comments
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
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.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
subjectInfoAccess	FALSE		CA Certificates issued under the Common Certificate Policy must 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 (1.3.6.1.5.5.7.48.5)	Each CA certificate must include at least two instances of this access method: one that includes the URI name form to specify the location of an LDAP accessible directory server and one that includes a URI name form to specify an HTTP accessible Web server. Each 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.
optional extensions			
issuerAltName	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

Field	Criticality Flag	Value	Comments
policyMappings	FALSE		This extension may be included in cross-certificates if the subject CA issues certificates under a policy other than the Common Certificate Policy and the subject CA's policy is deemed by the FPKI PA to map to the Common Certificate Policy.
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.
nameConstraints	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			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.

Field	Criticality Flag	Value	Comments
minimum		0	minimum is always zero, maximum is never present.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 4: CRL Profile

Field	Criticality Flag	Value	Comments
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
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; 800-78-1 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
issuer			
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.
thisUpdate			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
nextUpdate			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
revokedCertificates			
userCertificate		INTEGER	serial number of certificate being revoked
revocationDate			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.

Field	Criticality Flag	Value	Comments
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
crlEntryExtensions			
Extensions			
reasonCode	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. The certificateHold reason code may only be used for end entity certificates.
invalidtyDate	FALSE		This extension may be included if the invalidity date precedes the revocation date.
GeneralizedTime		YYYYMMDDHHMMSSZ	use this format for all dates.
crlExtensions			
Extensions			
authorityKeyIdentifier	FALSE		Must be included in all CRLs.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
cRLNumber	FALSE	INTEGER	Monotonically increasing sequential number. Must be included in all CRLs.
issuingDistributionPoint	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 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			

Field	Criticality Flag	Value	Comments
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	
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 5: End Entity Signature Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in

Field	Criticality Flag	Value	Comments
			section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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 that expire before December 31, 2008 shall have a modulus of 1024 or 2048 bits; certificates that expire on or after December 31, 2008 shall have a modulus of 2048 bits. (No sunset date for specified elliptic curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	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	
certificatePolicies	FALSE		

Field	Criticality Flag	Value	Comments
PolicyInformation			Three policy OIDs are defined for digital signature certificates issued to human subscribers under the Common Certificate Policy. End Entity certificates should assert one of the three policies. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy
		2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware
		2.16.840.1.101.3.2.1.3.16	id-fpki-common-High
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
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.
accessLocation			
GeneralName			

Field	Criticality Flag	Value	Comments
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
optional extensions			
extKeyUsage	BOOLEAN		This extension need not appear. If included in a certificate that is specifically designated for use in a single application (e.g., code signing or signing content on PIV cards), the extension may be marked either critical or non-critical. If included in any other certificate (to support specific applications), the extension must include the anyExtendedKeyUsage value and must be marked non-critical. Additional key purposes may be specified.
keyPurposeID		2.16.840.1.101.3.6.7	The id-PIV-content-signing keyPurposeID specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.
issuerAltName	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
subjectAltName	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.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 6: Key Management Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			X.500 Distinguished name of the owner of the certificate.

Field	Criticality Flag	Value	Comments
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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 that expire before December 31, 2008 shall have a modulus of 1024 or 2048 bits; certificates that expire on or after December 31, 2008 shall have a modulus of 2048 bits. (No sunset date for specified elliptic curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	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.
certificatePolicies	FALSE		

Field	Criticality Flag	Value	Comments
PolicyInformation			Three policy OIDs are defined for key management certificates issued to human subscribers under the Common Certificate Policy. End Entity certificates should assert one of the three policies. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy
		2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware
		2.16.840.1.101.3.2.1.3.16	id-fpki-common-High
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
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.
accessLocation			

Field	Criticality Flag	Value	Comments
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
optional extensions			
issuerAltName	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
subjectAltName	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.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 7: Certificate Profile for Computing and Communications Devices

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			X.500 Distinguished name of the owner of the certificate.

Field	Criticality Flag	Value	Comments
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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 that expire before December 31, 2010 shall have a modulus of at least 1024 bits; certificates that expire on or after December 31, 2010 shall have a modulus of at least 2048 bits. (No sunset date for specified elliptic curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	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		1	May be asserted when public key is RSA.
dataEncipherment		0	
keyAgreement		1	May be asserted when public key is elliptic curve.
keyCertSign		0	
cRLSign		0	
encipherOnly		0	

Field	Criticality Flag	Value	Comments
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			Other policy OIDs may be asserted in addition to the OID from the Common Certificate Policy.
policyIdentifier		2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
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.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.

Field	Criticality Flag	Value	Comments
optional extensions			
extKeyUsage	BOOLEAN		This extension may be included as either a critical or non-critical extension if its inclusion is required by the application(s) for which the certificate will be used. If the inclusion of this extension is not intended to limit acceptable uses of the subject public key, then the extension should be marked non-critical and the anyExtendedKeyUsage value should be included. Additional key purposes may be specified.
KeyPurposeID		2.16.840.1.101.3.6.7	The id-PIV-content-signing keyPurposeID specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.
issuerAltName	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
subjectAltName	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.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 8: Card Authentication Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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 card expiration date.
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			This field may include a NULL DN.

Field	Criticality Flag	Value	Comments
RDNSequence			If DN is not NULL (i.e., an empty sequence), must use the name form specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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 curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
extKeyUsage	TRUE		This extension shall assert only the id-PIV-cardAuth keyPurposeID.

Field	Criticality Flag	Value	Comments
keyPurposeID		2.16.840.1.101.3.6.8	The id-PIV-cardAuth keyPurposeID specifies that the public key is used to authenticate the PIV card rather than the PIV card holder.
certificatePolicies	FALSE		
PolicyInformation			One policy OID is specified for Card Authentication certificates. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth (private key computations can be performed with the Card authentication key without user participation).
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method must also be included since Common Certificate Policy 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.

Field	Criticality Flag	Value	Comments
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (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.
subjectAltName	See comment		If the subject name contains a DN, set criticality to FALSE. Otherwise set criticality to TRUE.
GeneralNames			Must only include FASC-N name form.
GeneralName			
otherName			This field contains the FASC-N
type-id		2.16.840.1.101.3.6.6	pivFASC-N
value		OCTET STRING	This field specifies the FASC-N of the PIV Card that contains the corresponding Card Authentication key.
piv-interim (2.16.840.1.101.3.6.9.1)	FALSE		The PIV interim indicator extension is defined in appendix D.2 of FIPS 201-1.
interim_indicator		BOOLEAN	The value of this extension is asserted as follows: • TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. • FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
optional extensions			
issuerAltName	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
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 9: PIV Authentication Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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 card expiration date.
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			X.500 Distinguished name of the owner of the certificate.

Field	Criticality Flag	Value	Comments
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		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 curves.)
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			One policy OID is specified for PIV Authentication certificates. Other policy OIDs may be asserted as

Field	Criticality Flag	Value	Comments
			well.
policyIdentifier		2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication (must be asserted in PIV Authentication Certificates).
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP[2]. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	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 under the Common Certificate Policy must include an authorityInfoAccess extension with at least two instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method must also be included since FIPS 201 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.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.

[2] For legacy Federal PKIs only, the cRLDistributionPoints extension may include a single URI, either LDAP or HTTP.

Field	Criticality Flag	Value	Comments
accessMethod		id-ad-ocsp (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.
subjectAltName	See comment		If the subject name contains a DN, set criticality to FALSE. Otherwise set criticality to TRUE.
GeneralNames			This extension MUST include the FASC-N 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			
otherName			This field MUST be present and MUST contain the FASC-N
type-id		2.16.840.1.101.3.6.6	pivFASC-N
value		OCTET STRING	This field specifies the FASC-N of the PIV Card that contains the corresponding PIV Authentication key.
otherName			Where supporting Microsoft *Smart Card Logon*, this name must be present
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			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
piv-interim (2.16.840.1.101.3.6.9.1)	FALSE		The PIV interim indicator extension is defined in appendix D.2 of FIPS 201-1.
interim_indicator		BOOLEAN	The value of this extension is asserted as follows: • TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. • FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
optional extensions			
issuerAltName	FALSE		Any name types may be present; only the most common are specified here.

Field	Criticality Flag	Value	Comments
GeneralNames			
GeneralName			
rfc822Name		IA5String	Electronic mail address of the PKI administration
extKeyUsage	FALSE		This extension need not appear. If included to support specific applications, the extension MUST include the anyExtendedKeyUsage value. Additional key purposes may be specified.
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
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Worksheet 10: Certificate Profile for Delegated OCSP Responders

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
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; 800-78-1 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
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
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
subject			
Name			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in

Field	Criticality Flag	Value	Comments
			section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
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 800-78-1:	
		1.2.840.10045.3.1.7	Curve P-256
		1.3.132.0.34	Curve P-384
subjectPublicKey		BIT STRING	As per section 6.1.5 of [1], the subject public key shall be type (RSA or elliptic curve) and key size as used by the issuing CA to sign CRLs.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
id-pkix-ocsp-nocheck	FALSE	NULL	
extKeyUsage	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

Field	Criticality Flag	Value	Comments
optional extensions			
certificatePolicies	FALSE		
PolicyInformation			Other policy OIDs may be asserted in addition to, or in place of, the OID from the Common Certificate Policy.
policyIdentifier		2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices
authorityInfoAccess	FALSE		
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.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
issuerAltName	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
subjectAltName	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.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			