DRAFT

Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile

April 30, 2002

Prepared By:

BOOZ•ALLEN & HAMILTON INC.
900 Elkridge Landing Road
Linthicum, Maryland 21090

Updated By:

National Institute of Standards and Technology
100 Bureau Dr.
Gaithersburg, MD 20899-8930

1 Introduction

This document specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for Federal public key infrastructure (FPKI) systems. The profiles serve to identify unique parameter settings for Federal public key infrastructure systems.

In the interest of establishing commonality and interoperability among PKI communities outside the Federal government, it was decided that the FPKI 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. The profile can be found at http://www.ietf.org/rfc/rfc3280.txt. The PKIX profile, Internet X.509 Public Key Infrastructure Certificate and CRL 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 http://www.ietf.org/rfc/rfc3279.txt.

This FPKI profile complements the current PKIX profile. If a specific program needs to implement a subset of the FPKI certificate and/or CRL profile, the program should tailor their X.509 certificate and/or CRL using the parameters stipulated in this document together with the parameters stipulated in PKIX. Parameters stipulated in this document should take precedence. Any program deciding to tailor their FPKI-compliant X.509 certificate and/or CRLs to meet their specific needs must document the intended subset profile (referencing FPKI profile as a basis) so that the certificate generation element will know how to populate the program-specific certificates.

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 FPKI profile. 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 provides an overview of each of the certificate and CRL profiles included in the worksheets corresponding to this document.

1.2 Acronyms

CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
EE	End Entity
FBCA	Federal Bridge Certification Authority
FPKI	Federal Public Key Infrastructure
OID	Object Identifier

PKIX	Public Key Infrastructure (X.509)
RFC	Request For Comments
SDN	Secure Data Network
v2	version 2
v3	version 3

1.3 References

[1] SDN.706, *X.509 Certificate and Certificate Revocation List Profiles and Certificate Path Processing Rules for the Multilevel Information Systems Security Initiative*, Revision D, 12 May 1999.

[2] SDN.801, *Access Control Concepts and Mechanisms*, Revision C, 12 May 1999.

[3] Internet Public Key Infrastructure: *X.509 Certificate and Certificate Revocation List (CRL) Profile*, RFC 3280, April 2002.

[4] Internet Public Key Infrastructure: *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3279, April 2002.

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.

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.

In the FPKI, 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;
- 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.

The CAs in the FPKI may be cross-certified with each other. In order to facilitate secure intra-agency communication, CAs within the FPKI may either cross-certify with each other directly or may cross-certify with the Federal Bridge Certification Authority (FBCA). In general, cross-certification with the FBCA is the preferable option since it maximizes intra-agency connectivity while minimizing the number of cross-certifications that any given CA needs to maintain.

Any certificate using system in the FPKI can view any CA in the FPKI as the trust anchor for starting certification paths, provided:

1. the certificate using system has an authenticated copy of the trust anchor's self-signed certificate; and,
2. local agency security policy allows the use of that CA as a trust anchor.

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 should not be used as a trust anchor.

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.

CAs may optionally supplement the CRL based revocation mechanisms with on-line revocation mechanisms.

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 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. To ensure support for non-English names, the IETF requires encoding

of names in certificates using UTF8String after December 31, 2003. 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, so names in current certificates can theoretically be changed to UTF8String in 2004 without loss of information.

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 PrintableString, 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.

Subject names in end entity certificates do not figure in name chaining, but are used to validate name constraints. In order to ensure that name constraints can be computed correctly, attribute values that are shared between an end entity and its certificate issuer should be encoded identically. Attribute values in end entity names that are unique to the end entity (e.g., the common name) may be encoded in UTF8String without concern for name comparison issues.

New CAs established after December 31, 2003, should use UTF8String encodings exclusively for attributes of type DirectoryString. As products that compare names encoded in different character sets become available, CAs should transition to UTF8String encodings when they roll over to new key pairs.

5 Use of URIs in Distribution Points and AuthorityInfoAccess Extensions

Uniform Resource Identifiers (URIs) are used in four different extensions within the certificate and CRL profiles in this document: cRLDistributionPoints, 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 1738 and RFC 2255.

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

In the cRLDistributionPoints extension, the URI is a pointer to a current CRL that provides status information about the certificate. If the CRL is located in the CRL issuer's directory entry, then the URI may omit the DN. Otherwise, the URI must include the DN of the entry containing

the CRL. The URI may, optionally, specify the directory attribute in which the CRL is located. When a URI is used as the DistributionPointName in the issuingDistributionPoint extension in a CRL, the value should match the URI in the corresponding distribution points in cRLDistributionPoints extensions in certificates.

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. Since the certificates should always be located in the certificate issuer's directory entry, in attributes as specified in X.509, it is not necessary to include the DN or attributes in the URI.

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 certificates issued by the subject of the certificate may be found. CA certificates issued by the subject should be located in the subject's directory entry. End entity certificates issued by the subject will not be located in the subject's directory entry, but will only be located in the end entities' entries. Since there is no single directory entry containing all certificates issued by the certificate subject, the URI should not specify a DN or attributes.

6 Worksheet Contents

This document consists 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 used in the Federal PKI.

The nine worksheets are:

1. The *Preamble* worksheet contains this Word document with overview and introductory information.
2. The *BCA-Issued Certificates* worksheet defines the mandatory and optional contents of CA certificates issued by the Bridge CA. (Note that end entity certificates issued by the BCA for local operational purposes are out of scope for this specification.)
3. The *BCA-Issued CRL* worksheet defines the mandatory and optional contents of CRLs issued by the Bridge CA.
4. The *CRL Issuer* worksheet defines the mandatory and optional contents of certificates issued by CAs in the Federal PKI where the subject public key will be used to verify the signature on CRLs but not certificates. (Note that the subject may function solely as a CRL issuer, or may sign certificates under a different key pair.)

5. The *CA Certificates* worksheet defines the mandatory and optional contents of certificates issued by CAs in the Federal PKI where the subject is a CA and the public key will be used to verify the signature on certificates. One optional feature in this worksheet is the use of the public key to verify the signature on CRLs.
6. The *End Entity Signature Certs* worksheet defines the mandatory and optional contents of certificates issued by CAs in the Federal PKI where the subject is an end entity and the public key will be used to verify the signatures.
7. The *Key Management Certificates* worksheet defines the mandatory and optional contents of certificates issued by CAs in the Federal PKI where the subject is a CA and the public key will be used to perform key management operations (e.g., key transport using RSA or Diffie-Hellman key agreement).
8. The *Self-Signed Certificates* worksheet defines the mandatory and optional contents of self-signed CA certificates issued by CAs in the Federal PKI for use by PKI client systems when establishing trust anchors. Note that self-issued CA certificates (e.g., key rollover certificates) are covered by the CA certificate worksheet.
9. The *CRL* worksheet table defines the mandatory and optional contents of CRLs issued by CRL issuers in the Federal PKI other then the BCA itself.

Note that the Federal PKI does not absolutely prohibit the use of dual-use end entity certificates, where an RSA or elliptic curve key is used for both digital signatures and key management. However, dual-use certificates are generally discouraged. As such, a worksheet for dual-use certificates is not supplied with this profile. CAs in the Federal PKI that issue dual-use certificates may use the End Entity Signature Certs profile and assert the additional key usage bits as appropriate (i.e., key encipherment for RSA keys or key agreement for elliptic curve keys).

Bridge CA 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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; and CN= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	use PrintableString for all attributes. (For rationale, see preamble.)
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			C= ; O= ; OU= ; CN=; and DC= are recommended.
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 used.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters.
subjectPublicKey		BIT STRING	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Match the authority key identifier included in certificates and CRLs signed by the subject with this public key.
keyUsage	TRUE		Any combination of the indicated values is acceptable.
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	Always asserted in BCA certificates.
cRLSign		1	Asserted if this key is also used to sign CRLs.
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			
policyIdentifier		OID	
policyQualifiers			Use of policy qualifiers is optional, but limited to qualifier types identified below.
PolicyQualifierInfo			*Approved qualifier #1*
policyQualifierId		id-qt-cps	CPS

qualifier		cPSuri	URI for publishing CPS. Use IA5String.
PolicyQualifierInfo			*Approved qualifier #2*
policyQualifierId		id-qt-unotice	
qualifier			
UserNotice		See comment.	UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
noticeRef			
NoticeReference			
organization			
DisplayText		See comment.	visableString, bmpString or utf8String
noticeNumbers			
explicitText			
DisplayText		See comment.	visableString, bmpString or utf8String
policyMappings	FALSE		This extension does not necessarily appear in all cross certificates.
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 (above).
basicConstraints	TRUE		
cA		TRUE	
pathLenConstraint		INTEGER	The use of a path length constraint is optional.
nameConstraints	TRUE	See comment.	This extension appears in most, but not all, BCA 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.
GeneralSubtree			
base			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
excludedSubtrees			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.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
policyConstraints	TRUE		This extension is optional. If it appears, at least one of requireExplicitPolicy and inhibitPolicyMapping must be present.
requireExplicitPolicy			
SkipCerts		0	
inhibitPolicyMapping			
SkipCerts		INTEGER	
cRLDistributionPoints	FALSE		This extension appears in every certificate issued by the BCA. The BCA does not segment CRLs based on reasons, so reason code does not appear
DistributionPoint			
distributionPoint			
DistributionPointName			BCA uses this field to differentiate between CRLs issued by different BCA nodes
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			

RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
cRLIssuer			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
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.
AccessDescription			Access Method #1
accessMethod		id-ad-caIssuers	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 where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
AccessDescription			Access Method #2
accessMethod		id-ad-ocsp	For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectInfoAccess	FALSE		subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is defined for use in CA certificates.
AccessDescription			
accessMethod		id-ad-caRepository	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 where certificates issued by the subject of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

Bridge CA 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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; and CN= are recommended
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.
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. If the revocation reason is unspecified, then the reasonCode extension should not be included.
invalidtyDate	FALSE		This extension may be included if the invalidity date precedes the revocation date.
GeneralizedTime		YYYYMMDDHHMMSSZ	use this format for all dates.
certificateIssuer	TRUE		This extension MUST appear if this certificate was issued by a different issuer than the previous certificate in the list, or the certificate is the first on an indirect CRL. If the first certificate in the list was issued by the CRL issuer, this extension may be omitted from that entry.
GeneralNames			
GeneralName			
directoryName			for this profile, only the distinguished name form is supported.
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
crlExtensions			
Extensions			
cRLNumber	FALSE	INTEGER	Monotonically increasing sequential number.
issuingDistributionPoint	TRUE		BCA does not segment CRLs based on reasons, so onlySomeReasons does not appear.
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			

RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
uniformResourceIdentifier		IA5String	matches the URI in the crl distribution points extension of certificates covered by this CRL.
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		BOOLEAN	If set to true, this CRL covers certificates that were not issued by the issuer of this CRL.

CRL Issuer Certificate Profile

This profile is used for certificates that contain subject public keys used to sign CRLs but not certificates. CRL issuers should not use CRL signing keys for general applications.

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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			C= ; O= ; OU= ; CN=; and DC= are recommended
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 used.
algorithm			Choice of following three algorithms.
		1:2:840:113549:1:1:1	RSA Encryption
		1:2:840:10040:4:1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	
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		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		1	Always asserted; indicates this key is used to sign CRLs.
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		A CRL issuer certificate should not include policy qualifiers.
PolicyInformation			
policyIdentifier		OID	

subjectAltName	FALSE		This extension is optional. 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 CRL issuer
dNSName		IA5String	This field contains the DNS name of the CRL issuer.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
issuerAltName	FALSE		This extension is optional. 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 issuing CA
dNSName		IA5String	This field contains the dns name of the issuing CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
cRLDistributionPoints	FALSE		This extension appears in all CRL issuer certificates.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
reasons			if present, this field indicates which reasons are covered by this distribution point. If omitted all reasons are covered.
ReasonFlags			Any combination of reasons may be asserted.
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	
certificateHold		1	
privilegeWithdrawn		1	
aACompromise		1	
cRLIssuer			If present, this field indicates that the distribution point is an indirect CRL.
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.

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.
AccessDescription			Access Method #1
accessMethod		id-ad-caIssuers	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 where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
AccessDescription			Access Method #2
accessMethod		id-ad-ocsp	For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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.
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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 used.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Match the authority key identifier included in certificates and CRLs signed by the subject with this public key.
keyUsage	TRUE		Any combination of the indicated values is acceptable.
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	Always asserted in CA certificates.
cRLSign		1	Asserted if this key is also used to sign CRLs.
encipherOnly		0	
decipherOnly		0	
certificatePolicies	See comment.		Set as critical if policy is designed to restrict usage of the certificate (e.g., "only use for access to www.agency.gov"); otherwise set as non-critical.
PolicyInformation			

policyIdentifier		OID	
policyQualifiers			Use of policy qualifiers is optional, but limited to qualifier types identified below.
PolicyQualifierInfo			defined policy qualifier #1
policyQualifierId		id-qt-cps	CPS
qualifier		cPSuri	URI for publishing CPS. Use IA5String.
PolicyQualifierInfo			defined policy qualifier #2
policyQualifierId		id-qt-unotice	
qualifier			
UserNotice			UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
noticeRef			
NoticeReference			
organization			
DisplayText		See comment.	visableString, bmpString or utf8String
noticeNumbers			
explicitText			
DisplayText		See comment.	visableString, bmpString or utf8String
policyMappings	See comment.		This extension may appear in a CA certificate. This extension may be set to noncritical to support legacy applications that cannot process policy mapping.
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 (above).
subjectAltName	FALSE		In general, this extension will not appear in CA certificates.
GeneralNames			
GeneralName			
rfc822Name		IA5String	This field contains the electronic mail address of the subject CA
dNSName		IA5String	This field contains the dns name of the subject CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
issuerAltName	FALSE		In general, this extension will not appear in certificates.
GeneralNames			
GeneralName			
rfc822Name		IA5String	This field contains the electronic mail address of the issuing CA
dNSName		IA5String	This field contains the dns name of the issuing CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
basicConstraints	TRUE		This extension must appear in all CA certificates.
cA		TRUE	
pathLenConstraint		INTEGER	The use of a path length constraint is optional.
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.
GeneralSubtree			
base			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
excludedSubtrees			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.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
policyConstraints	TRUE		This extension is optional, if present should be critical.
requireExplicitPolicy			Should be asserted if certificate policies extension is critical
SkipCerts		INTEGER	
inhibitPolicyMapping			Should be asserted if local policy prohibits policy mapping
SkipCerts		INTEGER	
cRLDistributionPoints	FALSE		This extension is required in all CA certificates.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
reasons			if present, this field indicates which reasons are covered by this distribution point. If omitted all reasons are covered.
ReasonFlags			Any combination of reasons may be asserted.
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	
certificateHold		1	
privilegeWithdrawn		1	
aACompromise		1	
cRLIssuer			If present, this field indicates that the distribution point is an indirect CRL.
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
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.
AccessDescription			Access Method #1
accessMethod		id-ad-calssuers	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 where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.

AccessDescription			Access Method #2
accessMethod		id-ad-ocsp	For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectInfoAccess	FALSE		subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is defined for use in CA certificates.
AccessDescription			
accessMethod		id-ad-caRepository	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 where certificates issued by the subject of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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			C= ; O= ; OU= ; CN= ; and DC= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	
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		Any combination of the indicated values is acceptable. At least one value must be asserted.
digitalSignature		1	may be asserted.
nonRepudiation		1	may be asserted.
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	See comment.		Set as critical if policy is designed to restrict usage of the certificate (e.g., "only use for access to www.agency.gov"); otherwise set as non-critical.
PolicyInformation			
policyIdentifier		OID	
policyQualifiers			Use of policy qualifiers is optional, but limited to qualifier types identified below.
PolicyQualifierInfo			defined policy qualifier #1

policyQualifierId		id-qt-cps	CPS
qualifier		cPSuri	URI for publishing CPS. Use IA5String.
PolicyQualifierInfo			defined policy qualifier #2
policyQualifierId		id-qt-unotice	
qualifier			
UserNotice			UserNotice should only appear in EE certs issued to other organizations to prevent multiple duplicate displays.
noticeRef			
NoticeReference			
organization			
DisplayText		See comment.	visibleString, bmpString or utf8String
noticeNumbers			
explicitText			
DisplayText		See comment.	visableString, bmpString or utf8String
subjectAltName	FALSE		This extension is optional. 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
dNSName		IA5String	For devices, this field contains the dns name of the subject
iPAddress		IA5String	For devices, this field contains the IP address of the subject
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
issuerAltName	FALSE		This extension is optional. 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 issuing CA
dNSName		IA5String	This field contains the dns name of the issuing CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
cRLDistributionPoints	FALSE		This extension is required.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
reasons			If the CRL distribution point covers all reasons, this field is omitted. If present, this distribution point covers only the specified reasons.
ReasonFlags			Any combination of reasons may be asserted.
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	

certificateHold		1	
privilegeWithdrawn		1	
aACompromise		1	
cRLIssuer			If present, this field indicates that the distribution point is an indirect CRL.
GeneralNames			
GeneralName			matches the DN in the issuer field of the corresponding CRL
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
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.
AccessDescription			Access Method #1
accessMethod		id-ad-caIssuers	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 where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
AccessDescription			Access Method #2
accessMethod		id-ad-ocsp	For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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			C= ; O= ; OU= ; CN= ; and DC= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10046.2.1	Diffie- Hellman
		1.2.840.10045.2.1	Elliptic Curve Diffie-Hellman
parameters		See comment	For Diffie-Hellman, always include parameters. For RSA include NULL; for ECDH include parameters unless inherited from issuer. If elliptic curve parameters are inherited, include NULL.
subjectPublicKey		BIT STRING	
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		As specifiefd below according to algorithm. (Assumes RSA key is not also used for signatures)
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		1	Used when subject public key is RSA
dataEncipherment		0	
keyAgreement		1	Used when subject public key is DH or ECDH
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	See comment.		Set as critical if policy is designed to restrict usage of the certificate (e.g., "only use for access to www.agency.gov"); otherwise set as non-critical.
PolicyInformation			
policyIdentifier		OID	
policyQualifiers			Use of policy qualifiers is optional, but limited to qualifier types identified below.

PolicyQualifierInfo			defined policy qualifier #1
policyQualifierId		id-qt-cps	CPS
qualifier		cPSuri	URI for publishing CPS. Use IA5String.
PolicyQualifierInfo			defined policy qualifier #2
policyQualifierId		id-qt-unotice	
qualifier			
UserNotice			UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
noticeRef			
NoticeReference			
organization			
DisplayText		See comment.	visableString, bmpString or utf8String
noticeNumbers			
explicitText			
DisplayText		See comment.	visableString, bmpString or utf8String
subjectAltName	FALSE		This extension is optional. 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
dNSName		IA5String	For devices, this field contains the dns name of the subject
iPAddress		IA5String	For devices, this field contains the IP address of the subject
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
issuerAltName	FALSE		This extension does not necessarily appear in all certificates.
GeneralNames			
GeneralName			
rfc822Name		IA5String	This field contains the electronic mail address of the issuing CA
dNSName		IA5String	This field contains the dns name of the issuing CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
cRLDistributionPoints	FALSE		This extension is required.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://…	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
reasons			If the CRL distribution point covers all reasons, this field is omitted. If present, this distribution point covers only the specified reasons.
ReasonFlags			Any combination of reasons may be asserted.
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	

certificateHold		1	
privilegeWithdrawn		1	
aACompromise		1	
cRLIssuer			If present, this field indicates that the distribution point is an indirect CRL.
GeneralNames			
GeneralName			matches the DN in the issuer field of the corresponding CRL
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
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.
AccessDescription			Access Method #1
accessMethod		id-ad-caIssuers	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 where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://...	See preamble text on URIs.
AccessDescription			Access Method #2
accessMethod		id-ad-ocsp	For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://...	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			Will match the subject DN.
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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			C= ; O= ; OU= ; CN= ; and DC= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm			Choice of following two algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters.
subjectPublicKey		BIT STRING	
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.
basicConstraints	FALSE		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	
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			

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.
algorithm			Choice of following three algorithms.
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1WithRSAEncryption
issuer			
Name			
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are recommended
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.
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, removeFromCRL. 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 and the use certificateHold is deprecated.
invalidtyDate	FALSE		This extension may be included if the invalidity date precedes the revocation date.
GeneralizedTime		YYYYMMDDHHMMSSZ	use this format for all dates.
certificateIssuer	TRUE		This extension MUST appear if this certificate was issued by a different issuer than the previous certificate in the list, or the certificate is the first on an indirect CRL. If the first certificate in the list was issued by the CRL issuer, this extension may be omitted from that entry.
GeneralNames			
GeneralName			
directoryName			for this profile, only the distinguished name form is supported.
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
crlExtensions			
Extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
issuerAltName	FALSE		This extension is optional. 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 CRL issuer
dNSName		IA5String	This field contains the DNS name of the CRL issuer.
directoryName			

Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
cRLNumber	FALSE	INTEGER	Monotonically increasing sequential number.
issuingDistributionPoint	TRUE		This extension appears in segmented CRLs and indirect CRLs.
distributionPoint			
DistributionPointName			If the issuer generates segmented or indirect CRLs, this field must be present.
fullName			matches the distinguished name or name relative to issuer In the crl distribution points extension of certificates covered by this CRL.
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
uniformResourceIdentifier		IA5String	matches the URI in the crl distribution points extension of certificates covered by this CRL.
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.
onlySomeReasons			This field describes the revocation reasons within the scope of this CRL. Any combination of reasons may be asserted. If the CRL covers all reasons, this field is omitted.
ReasonFlags			
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	
certificateHold		1	
privilegeWithdrawn		1	
aACompromise		1	
indirectCRL		BOOLEAN	If set to true, this CRL covers certificates that were not issued by the issuer of this CRL.
deltaCRLIndicator	TRUE		This extension is included if and only if the CRL is a delta CRL.
BaseCRLNumber		INTEGER	This value shall be identical to the value in the cRLNumber extension of the base certificate.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton			