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

May 31, 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 <u>http://www.ietf.org/rfc/rfc3280.txt</u>. 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

April 30, 2002

DRAFT

PKIXPublic Key Infrastructure (X.509)RFCRequest For CommentsSDNSecure Data Networkv2version 2v3version 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 intraagency 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, crosscertification 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

April 30, 2002

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 five different extensions within the certificate and CRL profiles in this document: cRLDistributionPoints, issuingDistributionPoint, FreshestCRL, 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 and FreshestCRL extensions, 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

April 30, 2002

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		HOLE	
Name			
RDNSequence			
RelativeDistinguishedName			
	-		
AttributeTupe		OID	
Attribute / ype		OID See comment	use PrintableString for all attributes (For rationale see preamble)
validity		dee comment.	use r finableoting for all attributes. (For fationale, see preamble.)
notBefore			
Time	1		
		YYMMDDHHMMSS7	Use for dates up to and including 2049
generalTime			Lice for dates of to and molecular 2040.
general line	-		USE IOI dates alter 2049
Time			
		\0/4/4/DDUU0007	Use for deter up to and including 0040
		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
general lime		YYYYMMDDHHMM55Z	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
subjectPublicKevInfo			
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
parametere		See comment	Enclude NULL : for DSA and ECDSA include parameters
parameters			T OF NOA Include NOLE, IOF DOA and EODOA Include parameters.
subjectPublicKey		BITSTRING	
extensions	EALOE		
authoritykeyidentiller	FALSE		Derived using the SUA 1 hash of the public loss
	FALOF	OCTET STRING	Derived using the SFIA-T hash of the public key.
subjectiveyidentiller	FALSE	ļ	Match the authority key identifier included in certificates and CPLs signed
keyldentifier		OCTET STRING	by the subject with this public key.
keyUsage	TRUE		Any combination of the indicated values is acceptable.
digitalSignature		0	
nonRepudiation		0	
kevEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
kevCertSign		- 1	Always asserted in BCA certificates.
cRLSign	1	1	Asserted if this key is also used to sign CRLs
encipherOnly	1	0	
decipherOnly	<u> </u>		
accipiter Only	EALOF	U	1
PolicyInformation	FALSE		
FolloyInformation		015	
policyldentifier		UID	Lies of policy qualifiers is optional, but limited to qualifier types identified
policyQualifiers			below.
PolicyQualifierInfo	1		Approved qualifier #1
policyQualifierId		id-qt-cps	CPS

qualifier		oPSuri	LIPI for publiching CPS Lipo IAEString
qualifier		CF Sull	OKI IDI publishing CF3. Ose IASSung.
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
noticoBof			organizatione to provont matchie adplicate alopidyo.
noileertei			
NoticeReference			
organization			
DisplayText		See comment.	visableString, bmpString or utf8String
noticeNumbers			
explicitText			
DisplayTast		Coo commont	visable String Imm String or utf0 String
DisplayText		See comment.	visablestning, bripstning of utostning
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	1		
kees			
Dase			
GeneralName			
directoryName			
Name			
RDNSequence			
KDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
avaluate d Cubira e a		0	minimum is always may mayimum is naver present
excludedSubtrees			minimum is always zero, maximum is never present.
GeneralSubtrees			
GeneralSubtree			
base			
GeneralName			
Generalivanie			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
Attribute I ypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
rfc822Name		IA5String	
dNSName		IA5String	
minimum		0	
Il O t in t-	TRUE		This extension is optional. If it appears, at least one of requireExplicitPolicv
policyConstraints	IRUE		and inhibitPolicyMapping must be present.
requireExplicitPolicy			
SkipCerts	İ	0	
inhihitBolioyMonning	1	Ť	
	<u> </u>		
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
fullName	ł	1	
CanaralNamaa			
Generalivames			
GeneralName			
directoryName			
Name	1		
RDNSequence	l		
Nonoequence	I	1	

RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	See preamble text on naming.
uniformResourceIdentifier		Idap://	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-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		Idon://	See proomble text on LIPIc
AccessDescription		iuap.//	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		1	• • • • • • • •
uniformResourceIdentifier		http://	See preamble text on URIs.
subjectInfoAccess	FALSE		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		Idap://	See preamble text on LIPIs
Designed by Robert Moskowitz (ICSA) and modified by	Booz Allen & Hamilton	iuap.//	Gee preamble text on onts.
seeignee sy nobert mosilowite (rooky and mounted by			

Bridge CA CRL Profile

Field	Criticality Flag	Value	Comments
Certificatel ist	jj		
theCartlist			Fields to be signed
LOSCERLIST Version		1	Interes Volue of #1# for Version 2 CDI
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			
BDNSeguenee			
RDINSequence			C=, O=, OO=, and CN= are recommended
RelativeDistinguishedName			
Attribute I ypeAndValue			
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		YYMMDDHHMMSS7	Use for dates up to and including 2049
gonoralTimo			Lice for dates of to and molecular 2040.
general i line			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		
	THEOE		Any one of these CRL reasons may be asserted: keyCompromise
CRLReason			cAcompromise, affiliationChanged, superseded, cesationOfOperation. 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
GeneralizedTime		YYYYMMDDHHMMSS7	use this format for all dates
Conordaneod rinno			
certificatelssuer	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			
BDNSoguence			
RDNSequence			
RelativeDistinguishediname			
Attribute I ypeAndValue			
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	ł		···
DistributionPointName	1		
fullName	ł		1
GeneralNames			
GeneralName	Į		
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.

Field	Criticality Flag
ate	
rtificate	

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. **Comments**

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
iceuar		11022	
Name			
PDNSequence			C - : O - : O I - : CN - : and DC - are recommended
RelativeDictinguichedName			
AttributeTuneAndVolue			
AttributeType		OID	
Attribute/ ype		CID see comment	See preamble text on paming
validity		see comment	Gee preamble text on haming.
notBefore			
Time			
utcTime		YYMMDDHHMMSS7	Use for dates up to and including 2049
generalTime		YYYYMMDDHHMMSSZ	Lise for dates after 2049
notAfter			036 101 04163 4161 2043
Time			
utaTimo			Lice for dates up to and including 2040
dic i ille generalTime			Lice for dates of to and including 2049.
general inte			Use for dates after 2049
subject			V 500 Distinguished as a state surger of the serificate
Name			A.Soo Distinguished harne of the owner of the certificate.
RDNSequence			C=, $O=$, $OO=$, $CN=$, and $DC=$ are recommended
RelativeDistinguisnediname			
Attribute i ypeAndvalue		010	
Attribute i ype		UD	oncoding of name must use the encoding of the issuer field in
AttributeValue		see comment	certificates and CRLs issued by this subject CA
subjectPublicKeyInfo			
algorithm			
Algorithmldentifier			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 i subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	
extensions			
authorityKeyldentifier	FALSE		
keyldentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyldentifier	FALSE		
keyldentifier		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	l	A CRL issuer certificate should not include policy qualifiers.
PolicyInformation			
policyIdentifier	1	UID	1

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	l		
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 issuerAltName	FALSE	see comment	See preamble text on naming 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			ļ
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
uniformResourceIdentifier		Idap://	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
ReasonFlags	1		Any combination of reasons may be asserted.
unused	1	1	
keyCompromise	1	1	1
cACompromise	1	1	
affiliationChanged	1	1	
superseded	1	1	
cessationOfOperation	1	1	
certificateHold	1	1	
privilegeWithdrawn	1	1	
aACompromise	1	1	
aAcompromise		1	If present this field indicates that the distribution point is an
CRLIssuer GeneralNames			indirect CRL.
GeneralName	1		
directoryName	1		
Name			
PDNSequence	1	1	
PolotivoDiotingvishadNama			
Attribute i ypeAndValue		015	
Attribute I ype		UID	
AttributeValue		see comment	See preamble text on naming.

FreshestCRL	FALSE		If delta-CRLs are issued that cover this certificate, then either this certificate or the complete for scope CRL that corresponds to the delta-CRLs should include the FreshestCRL extension
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
BelativeDistinguishedName			
AttributeTypeAndValue			
AttributeTypeAnd Valde		OID	
Attribute l'ype		COD commont	See proomble text on paming
		see comment	See preamble text on Halling
		Idap://	See preamble text on URIS.
nameRelative FockLissuer			
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
		1	Any combination of reasons may be asserted.
keyCompromise		1	
cACompromise		1	
offiliationChanged		1	
anniaionChanged		1	
superseded		1	
cessationOroperation			
certificateHold		1	
privilegewithdrawn		1	
aACompromise		1	If present this field indicates that the distribution point is an
cRLIssuer			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 paming
		See comment	authorityInfoAccess consists of a sequence of accessMethod and
authorityInfoAccess	FALSE		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
AccessPresentier			this certificate.
AccessDescription			Access Method #1 When this access method is used, the access location should use
accessMethod		id-ad-calssuers	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		Idan://	See preamble text on LIDIs
AccessDescription		iuap.//	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		http://	See proomble test on LIDIa
Designed by Robert Moskowitz (ICSA) and modified by Rooz Alle	en & Hamilton	nup://	See preamble text on UKIS.

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
subjectPublicKeyInfo			Certificates and CRLs issued by this subject CA
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 Cupye Algorithms
		1.2.040.10045.2.1	Emplie Guive Algonamis
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters i 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		
keyldentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyldentifier	FALSE		
keyldentifier		OCTET STRING	Match the authority key identifier included in certificates and CRLs signed by the subject with this public key.
KeyUsage	IRUE		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	1		

policyldentifier		OID	
policyQualifiers			Use of policy qualifiers is optional, but limited to qualifier types
PolicyQualificitate			identified below.
policyQualifierId	-	id at opp	
qualifier		cPSuri	LIRI for publishing CPS Lise IA5String
PolicyQualifierInfo		or our	defined policy gualifier #2
policyQualifierId		id-at-unotice	
qualifier			
UserNotice			UserNotice should only appear in EE or CA certs issued to other
noticeRef			organizations to prevent multiple duplicate displays.
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			
Attribute I ypeAndValue		010	
Attribute i ype		OID	
Attribute\/alue		see comment	See preamble text on naming
AttributeValue issuerAltName	FALSE	see comment	See preamble text on naming. In general, this extension will not appear in certificates.
AttributeValue issuerAltName GeneralNames	FALSE	see comment	See preamble text on naming. In general, this extension will not appear in certificates.
AttributeValue issuerAltName GeneralNames GeneralName	FALSE	see comment	See preamble text on naming. In general, this extension will not appear in certificates.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name	FALSE	IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA
AttributeValue issuerAltName GeneralNames rfc822Name dNSName	FALSE	IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames rfc822Name dNSName directoryName	FALSE	IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames rfc822Name dNSName directoryName Name	FALSE	IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence	FALSE	IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName rtc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName	FALSE	See comment IA5String IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue	FALSE	IA5String IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType	FALSE	See comment	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA. This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeState	FALSE	See comment IA5String IA5String OID See comment	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType CA	FALSE	See comment IA5String IA5String OID See comment TRUE	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA. This field contains the dns name of the issuing CA.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType Constraints cA pathLenConstraint	FALSE	IA5String IA5String IA5String OID see comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeValue basicConstraints cA pathLenConstraint nameConstraints	FALSE	IA5String IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType Constraints pathLenConstraint permittedSubtrees	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. Extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees workap, the excluded subtree takes precedence. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue AttributeType AttributeType AttributeTotalue basicConstraints cA pathLenConstraint permittedSubtrees GeneralSubtree	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. The use of a path length constraint is optional. This extension of permitted and excluded subtrees may appear. If permitted and excluded subtrees overlap, the excluded subtree takes precedence. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue basicConstraints cA pathLenConstraint permittedSubtrees GeneralSubtree base	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA. This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. This extension of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees overlap, the excluded subtree takes precedence. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeType AttributeType generalits cA pathLenConstraints generalSubtrees GeneralSubtree base GeneralName	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA. This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees overlap, the excluded subtree takes precedence. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName dNsName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeValue basicConstraints cA pathLenConstraint permittedSubtrees GeneralName GeneralName directoryName	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. 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. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeType CA pathLenConstraints GeneralSubtrees GeneralSubtree base GeneralName	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. 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. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeValue basicConstraints cA pathLenConstraint permittedSubtrees GeneralSubtree base GeneralName directoryName Name RDNSequence	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees ma
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue basicConstraints cA pathLenConstraint permittedSubtrees GeneralName directoryName Name REDNSequence RelativeDistinguishedName	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue pathLenConstraints cA permittedSubtrees GeneralSubtree base GeneralName directoryName Name RDNSequence RelativeDistinguishedName	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. This always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue AttributeType AttributeTypeAndValue AttributeTypeAndValue pathLenConstraints cA pathLenConstraint generalName directoryName Mame RDNSequence RDNSequence AttributeSubtrees GeneralName directoryName Name RDNSequence RDNSequence AttributeTypeAndValue	FALSE	See comment IA5String IA5String OID See comment TRUE INTEGER INTEGER OID OID	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue basicConstraints cA pathLenConstraint generalSubtrees GeneralSubtree base GeneralName directoryName Name RDNSequence RelativeDistinguishedName AttributeType	FALSE	See comment IA5String IA5String OID See comment INTEGER OID OID See comment IA5Ctring OID	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees takes precedence. minimum is always zero, maximum is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue basicConstraints cA pathLenConstraint generalSubtree base GeneralName directoryName Name RDNSequence AttributeType AttributeType AttributeSubtrees GeneralName directoryName Name RDNSequence RelativeDistinguishedName AttributeType AttributeType AttributeType AttributeType AttributeType AttributeType	FALSE	See comment IA5String IA5String OID See comment INTEGER INTEGER OID See comment IA5String IA5String IA5String IA5String IA5String	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA. This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear. If minimum is always zero, maximum is never present. See preamble text on naming. See preamble text on naming is never present.
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue basicConstraints cA pathLenConstraint generalSubtree base GeneralName directoryName Name RDNSequence cA pathLenConstraint nameConstraints GeneralName directoryName Name RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue AttributeTypeAndValue AttributeType AttributeType AttributeType AttributeType AttributeValue mame minimum	FALSE	See comment IA5String IA5String OID See comment INTEGER OID OID See comment IA5String IA5String IA5String IA5String I	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. 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. minimum is always zero, maximum is never present. See preamble text on naming.
AttributeValue issuerAltName GeneralNames GeneralName rfc822Name dNSName directoryName Name RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeValue basicConstraints cA pathLenConstraint permittedSubtrees GeneralSubtree base GeneralName directoryName Name RDNSequence AttributeValue	FALSE	See comment IA5String IA5String OID See comment INTEGER OID OID See comment IA5String IA5String IA5String IA5String IA5String 0	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates. If present, any combination of permitted and excluded subtrees may appear. If permitted and excluded subtrees may appear and the specied and excluded subtrees may appear and the specied and excluded subtrees may appear and the specied and excluded subtrees may appear. If permitted and excluded subtrees may appear and the specied and excluded subtrees may appear and the specied and excluded subtrees may appear and the specied and excluded subtrees and appear and the specied and excluded subtrees may appear and the specied and excluded subtrees and appear and the specied and excluded subtrees and appear and the specied and excluded subtrees and the specied and excluded subtree
AttributeValue issuerAltName GeneralNames GeneralName dNSName directoryName Name RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeValue basicConstraints cA pathLenConstraint generalSubtrees GeneralSubtree base GeneralName Mame RDNSequence RelativeDistinguishedName AttributeTypeAndValue AttributeType AttributeType AttributeValue rfc822Name dNSName minimum excludedSubtrees GeneralSubtrees	FALSE	See comment IA5String IA5String IA5String OID See comment INTEGER OID See comment IA5String IA5String IA5String IA5String 0	See preamble text on naming. In general, this extension will not appear in certificates. This field contains the electronic mail address of the issuing CA This field contains the dns name of the issuing CA. See preamble text on naming. This extension must appear in all CA certificates. The use of a path length constraint is optional. This extension is optional in CA certificates may appear. If permitted and excluded subtrees may appear. If See preamble text on naming.

base			
GeneralName	i i		
directorvName	1		
Name	1		
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
Attribute TypeAnd Value		OID	
Attribute lype		OID see comment	See preamble text on naming
rfc822Name		IA5String	See preamble text on naming.
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
SkinCerts		INTEGER	
inhibitPolicyManning			Should be asserted if local policy prohibits policy mapping
SkinCerte		INTEGER	chould be asserted in local policy prohibits policy mapping
cRI DistributionPoints	FALSE	INTEGER	This extension is required in all CA certificates
DistributionPoint	THEOL		This extension is required in an or certificates.
distributionPoint			
fullName			
Generalivames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		Idap://	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
DeserverElene			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.
FreshestCRL	FALSE		If delta-CRLs are issued that cover this certificate, then either this certificate or the complete for scope CRL that corresponds to the delta-CRLs should include the FreshestCRL extension
DistributionPoint	1		
distributionPoint	1		
DistributionPointName			
fullName	1		
GeneralNames	1		
ConorolNemo			
	<u> </u>		
directoryName			
Name			

ResubrokasingusherName Image: constraint of the second secon	RDNSequence	T		
Antibala Type OID Antibala Type OID Antibala Type OID number Antibala Type See prantile tors on naming nameR data Type Antibala See prantile tors on naming Antibala Type Antibala OID Antibala Type Antibala See prantile tors on naming Antibala Type Antibala I Antibala Type	RelativeDistinguishedName			
Attendar/Spain OD Attendar/Spain See presented test on naming uniformResource/departure Idep/II See presented test on naming Internet/Product/Secure Idep/II See presented test on naming Relative/Distriguish OD See presented test on naming Attribute/Type OD See presented test on naming Attribute/Type OD See presented test on naming Attribute/Type OD See presented test on naming Resource See presented test on naming See presented test on naming Resource See presented test on naming See presented test on naming Resource See presented test on naming See presented test on naming Resource See presented test on naming See presented test on naming Resource See presented test on naming See presented test on naming Resource 1 If present See presented test on naming	AttributeTypeAndValue			
Attituativalue see connent See preamble text on naming marrefreidever CGRUssauri idep// See preamble text on UBs. marrefreidever CGRUssauri idep// See preamble text on UBs. Attituatify Type. NOTO OD See preamble text on UBs. Attituatify Type. NOTO OD See preamble text on naming Attituatify Type. NOTO OD See preamble text on naming Attituatify Type. NOTO OD See preamble text on naming masses See preamble text on naming Harder text on naming masses See preamble text on naming Harder text on naming masses Control Harder text on naming masses Immediate Harder text on naming masses	AttributeType		OID	
uniform ResourceManning Idag/// See preamble test on URIs. RestativeDatingsatesManne AttitudeType OD RescortFags 1 unused 1 unused 1 assperated 1	AttributeValue		see comment	See preamble text on naming
Insertification of Comparison of an optimization of a construction of construction of a construction of construction of a constructio	uniformResourceIdentifier	ł	Idan://	See preamble text on LIRIs
Relative/Disriguis/end/size Image: constraint of the second	nameRelativeToCRLIssuer		iddp#////	
Antibact Type Image: Control of Contr	RelativeDistinguishedName			
Antibularity or OD Antibularity or set commant Antibularity or set commant Rescoring is present in the individual is associated or maning Number of the individual is associated or maning Set of the individual is associated or maning Associate or maning Associate or maning Associate or maning Associate or maning Name Restrict Office or maning Associate or maning Associate or maning	AttributeTupeAndValue			
Autobary Space Dut Space Autobary Space If present, this field disclose that the scans are covered, this space and scans are covered, the space and the space are covered. unused 1 Any continuation of reasons may be asserted. unused 1 Any continuation of reasons are be asserted. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. assperable 1 Image: Continue of the space are covered. asspective of the space are covered. Image: Continue of the space are covered. asspective of the space are covered. Image: Continue of the space are covered. asspec	AttributeTure		OID	
Autodarvalue one Continue The present, the set of granted table of maining distribution point. If months all issues are accessed. ReasonFlags 1 Any combination of masons may be assented. usuad 1 Image: Comparison of the combination of masons may be assented. allisation/Changed 1 Image: Combination of masons may be assented. allisation/Changed 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. asspended 1 Image: Combination of masons may be assented. assented combination 1 Image: Combination of masons may be assented. assented combination 1 Image: Combination of masons may be assented.	Attribute / ype		OID	Cae preemble text on noming
reasons Production point. If anited all reasons are covered, ino distribution point. If anited all reasons are covered all reasons are covered. research wave assession/Opuration 1 constant hold 1 privilege/Windrawn 1 directory frame 1 GeneralNames 1 GeneralNames 1 RobitSquence 1 Name 1 Name 1 Attributor TypeInd Value 0ID Attributor TypeInd Value authorityIntAAccess FALSE FALSE accessMethod 1 accessMethod <td< td=""><td>Attributevalue</td><td></td><td>see comment</td><td>if present this field indicates which reasons are covered by this</td></td<>	Attributevalue		see comment	if present this field indicates which reasons are covered by this
Rescorfiage Image: market in the second se	reasons			distribution point. If omitted all reasons are covered by this
unused 1 keyCompromise 1 okCompromise 1 affiliationChanged 1 superseded 1 centicationChanged 1 centicationChanged 1 centicationChanged 1 centicationChanged 1 centicationChanged 1 centicationChanged 1 privilegeWithdrawn 1 a&Compromise 1 centicationChanged 1 generalNames 1 GeneralName 1 GeneralName 1 GeneralName 1 RbNSequence 1 RbNSequence 1 Attribute TypeAnd/slaue see comment Attribute TypeAnd/slaue see comment AccessDescription KaccessDescription AccessDescription 1 AccessDescription	ReasonFlags			Any combination of reasons may be asserted.
wc/Compromise 1 adCompromise 1 alfinition/Changed 1 superselfed 1 cessation/Operation 1 cessation/Operation 1 centificate/Add 1 adCompromise 1 adCompromise 1 centificate/Add 1 adCompromise 1 additional status 1 additional status 1 additional status 1 additional status 1 authority/infoAccess 1 authority/infoAccess 1 authority/infoAccess 1 accessMethod 1 <td< td=""><td>unused</td><td></td><td>1</td><td></td></td<>	unused		1	
adfiator/Changed 1 adfiator/Changed 1 superseded 1 cessatisor/Operation 1 continua-Hold 1 continua-Hold 1 privilege/Windrawn 1 al/Componise 1 dRLission 1 dRLission 1 GeneralNames 1 GeneralName 1 drector/Name 1 Rollwebolics 1 Name 1 Rollwebolics 1 AttributeTypeAndYalue 1 AttributeTypeAndYalue 1 authorityInfoAccess FALSE accessDescription 1 accessDescript	keyCompromise		1	
attiluitor/Changed 1 superseded 1 cessation/Operation 1 centificate/idd 1 privilege/Whatram 1 aACompromise 1 defuse/Whatram 1 aACompromise 1 refulsation/Operation 1 defuse/Whatram 1 defuse/Whatram 1 defuse/Whatram 1 defuse/Operation 1 defuse/Operation 1 defuse/Operation 1 defuse/Operation 1 AttributeTypeAndValue 2 AttributeTypeAndValue 3ee comment authorityInfoAccess FALSE FALSE FALSE descess/Method #1 3ee preamble text on naming. authorityInfoAccess 1 accessMethod 1 accessMethod 1 accessMethod 1 descess/Method #1 3ee preamble text on naming. unformResourcedomifier 1 accessMethod	cACompromise		1	
superseded 1 cessationODeerstion 1 centificateHold 1 privilegeWindrawn 1 dRCurspromise 1 rectificateHold 1 orRLissuer If present, this field indicates that the distribution point is an indirect CRL. GeneralName 1 GeneralName 1 directoryName 1 RSINSequence 1 RAthoutsTypeAndValue see comment AttributeTypeAndValue See preamble text on naming. authorityInfoAccess FALSE authorityInfoAccess FALSE accessDescription 1 accessMethod id-ad-calssuers id-ad-calssuer id-ad-calssuers denorabinities id-ad-calssuers denorabinities id-ad-calssuers accessMethod id-ad-calssuers </td <td>affiliationChanged</td> <td></td> <td>1</td> <td></td>	affiliationChanged		1	
cessation/00peration 1 cessation/00peration 1 privilege/Mintraon 1 aACompromise 1 cRussur 1 cRussur 1 cRenariName 1 GeneralNames 1 GeneralName 1 Mame 1 RNDsequence 1 AttributeTypeAndValue 1 AttributeTypeAndValue 1 AttributeTypeAndValue 2 AttributeTypeAndValue 2 authorityInfoAccess FALSE accessMethod id-ad-calssuers accessMethod id-ad-cac	superseded		1	
certificateHold 1 privilegeWithdrawn 1 aACompromise 1 rectoryName 1 GeneralName	cessationOfOperation		1	
pixilegeWithdrawn 1 aACompromie 1 dRUsser 1 right 1 GeneralNames 1 GeneralName 1 Indirect CRL. 1 GeneralName 1 IndirectOrName 1 RDNSequence 1 RtituteDistinguishedName 1 AttributeType AndYalue 000 AttributeType 010 AttributeType 010 AttributeType AndYalue see preamble text on naming. authorityinfoAccess FALSE accessDescription AccessDescription accessMethod id-ad-catssuers accessLocation 1 accessDescription AccessDescription accessLocation 1 accessLocation 1 accessLocation 1 accessLocation 1 accessLocation 1 accessLocation Id-ad-catssuers accessLocation Id-ad-cocsp. accessLocation	certificateHold		1	
aACompromise 1 oRLissuer 1 GeneralNames 1 GeneralName 1 drectoryName 1 Name 1 RDNSequence 1 AttributeTypeAndValue 0ID AttributeTypeAndValue 0ID AttributeTypeAndValue 0ID AttributeTypeAndValue 0ID AttributeTypeAndValue 0ID AttributeTypeAndValue 0ID AttributeTypeAndValue See preamble text on naming. authontlyInfoAccess FALSE accessDescription Idead-calssuers accessDescription Idead-calssuers accessLocation Idead-calssuers decessLocation Idead-calssuers accessLocation Idead-calssuers acc	privilegeWithdrawn		1	
cRLisser If present, this field indicates that the distribution point is an indirect CRL. GeneralNames indirect CRL. GeneralName indirect CRL. idedCoyName indirect CRL. Name indirect CRL. RoNSequence indirect CRL. AttributeTypeAndName indirect CRL. AttributeTypeAndName indirect CRL. AttributeTypeAndName OID AttributeTypeAndName indirect CRL. authorityInfoAccess FALSE FALSE id-ad-calssuers id-ad-calssuers tid-ad-calssuers id-ad-calssuers tid-ad-calssuers id-ad-calssuers tid-ad-calssuers id-ad-calssuers tid-ad-calssuers id-ad-calssuers tid-ad-calssuers uniformResourcidentifier Idap://	aACompromise	ł	1	
cReversilvanes indirect CRL GeneralNames indirect CRL GeneralName indirect CRL GeneralName indirect CRL Mame indirect CRL Name indirect CRL RDNSequence indirect CRL RatibuteTypeAndValue indirect CRL AttributeType OID AttributeType OID AttributeType OID AttributeType OID authorityInfoAccess see preamble text on naming. authorityInfoAccess authorityInfoAccess consists of a sequence of accessMethod and accessSuection pair. Two access methods are defined: one for locating entificate issued to the certificate issue and one for locating an OCSP server that provides are defined. AccessDescription id-ad-calssuers accessIdentod id-ad-calssuers accessIdentod id-ad-calssuers accessIdentod id-ad-calssuers accessIdentofier id-ad-calssuers accessIdentofier id-ad-calssuers accessIdentifier id-ad-calssuers accessIdentofier id-ad-calssuers accessIdentifier id-ad-calssuers accessIdentofier id-ad-calssuers accessIdentofier id-ad-calssuers accessIdentofier id-ad-calssuers		ł		If present, this field indicates that the distribution point is an
GeneralName	CRLISSUER			indirect CRL.
GeneralName	GeneralNames			
Name Image: Constraint of the constr	GeneralName			
Name Image: Constraint of the second sec	directoryName			
RDNSequence Image: constraint of the second sec	Name			
RelativeDistinguishedName Image: constraint of the consthere. AccessDescription <td>RDNSequence</td> <td></td> <td></td> <td></td>	RDNSequence			
AttributeTypeAndValue OID AttributeType OID AttributeType OID AttributeValue see comment authorityInfoAccess consists of a sequence of accessMethod and access.Location pairs. Two access methods are defined: one for locating certificate issuer and one for locating an CCSP server that provides status information about this certificate. AccessDescription AccessDescription accessLocation id-ad-calssuers GeneralName id-ad-calssuers uniformResourceIdentIfier Idap:// AccessDescription Access Description AccessDescription For this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory serve where certificate issued to the issuer of this certificate issue and this certificate issue access location should use the URI name form to specify the location of an CSP server that provides status information about this certificate. accessLocation Id-ad-ocsp GeneralName Id-ad-ocsp uniformResourceIdentIfier Idap:// accessLocation Access method is certificate. accessLocation Id-ad-ocsp accessLocation Access method is used, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this	RelativeDistinguishedName			
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 ant CCSP server that provides status information about this certificate. AccessDescription FALSE When this access method is used, the access location of an LDAP accessible access heathod is used, the access location should use the URI name form to specify the location of an LDAP accessible accessMethod accessLocation id-ad-calssuers When this access method, if a access location of an LDAP accessible access location accessLocation accessLocation Idap:// See preamble text on URIs. accessLocation Idap:// See preamble text on URIs. accessLocation Id-ad-ocsp name form to specify the location af an UCSP server that provides status information about this certificate. accessLocation Id-ad-ocsp name form to specify the location af an UCSP server that provides status information about this certificate. accessLocation Id-ad-calspect subjectInfoAccess consists of a sequence of accessMethod for use in CA cec	AttributeTypeAndValue			
AttributeValue see comment See preamble text on naming. authorityInfoAccess FALSE authorityInfoAccess consist of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificate issuer and one for locating an OCSP server that provides status information about uses the defined. AccessMethod AccessMethod #1 accessMethod id-ad-calssuers accessMethod When this access method is used, the access location should use the the UR name form to specify the location of an DAP accessIble directory server where certificate issued to the issuer of this certificate. accessMethod Idap:// accessMethod Idad-ac-osp accessMethod	AttributeType		OID	
authorityInfoAccess FALSE authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating an OCSP server that provides status information about this certificate. AccessDescription AccessMethod #1 AccessDescription AccessMethod #1 accessLocation pairs Men 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 certificate issuer of this certificate. accessLocation Idad-calssuers withortMinfoAccess Idad-calssuers AccessDescription Idad-calssuers accessLocation Idad-calssuers GeneralName Idad-d-calssuers uniformResourceIdentifier Idap:// AccessSDescription Access method, the access location should use the URI and the access location is should use the URI and the access location is should use the URI and the access location is should use the URI and the access location should use the URI and the access location should use the URI and the access location is and use the URI and the access location of an OSP server that provides status information about this certificate. accessLocation Idad-calses GeneralName Idad-calses <t< td=""><td>AttributeValue</td><td></td><td>see comment</td><td>See preamble text on naming.</td></t<>	AttributeValue		see comment	See preamble text on naming.
authorityInfoAccess FALSE FALSE AccessDescription Idcasting certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificates AccessDescription Idcasting certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about the certificates issued to the certificate issuer of this accessMethod id-ad-calssuers id-ad-calssuers id-ad-calssuers id-ad-calssuers certificate issued to the issuer of this certificate may be found. accessDescription Idap:// AccessDescription Idap:// accessMethod id-ad-cosp accessMethod id-ad-cosp accessMethod id-ad-cosp accessLocation Image: formation about this certificate. generalName Image: formation about this certificate. uniformResourceIdentifier http:// uniformResourceIdentifier http:// subjectInfoAccess FALSE accessMethod id-ad-caRepository id-ad-caRepository id-ad-caRepository accessMethod id-ad-caRepository id-ad-caRepository id-ad-caRepository				authorityInfoAccess consists of a sequence of accessMethod and
Inclusion	authoritvInfoAccess	FALSE		locating certificates issued to the certificate issuer and one for
AccessDescription this 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 certificate issued to the issuer of this certificate may be found. accessLocation Idap:// See preamble text on URIs. accessLocation Idad-cocsp name form to specify the location of an OCSP server that provides status information about this certificate. accessLocation Idad-cocsp name form to specify the location of an OCSP server that provides status information about this certificate. accessLocation Ittp:// See preamble text on URIs. subjectInfoAccess FALSE subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only on access method is used, the accessible directory server where certificates. accessLocation Id-ad-caRepository When this access method is used, the accessible directory server where certificates issued by the subject of this certificates may be found. accessLocation	,	-		locating an OCSP server that provides status information about
AccessDescription AccessMethod ±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 certificate issued to the issuer of this certificate may be found. accessLocation Idap:// See preamble text on URIs. uniformResourceIdentifier Idap:// See preamble text on URIs. accessMethod id-ad-ocsp name form to specify the location of an OCSP server that provides status information about this certificate. accessMethod id-ad-ocsp name form to specify the location of an OCSP server that provides status information about this certificate. accessLocation Ida-d-ocsp name form to specify the location of an OCSP server that provides status information about this certificate. accessLocation Ida-d-ocsp subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is defined for use in CA certificates. subjectInfoAccess FALSE when this access method is used, the access location should use the URI name form to specify the location of an DAP accessible directory server where certificates issued by the subject of this certificates. accessLocation Ida-d-ocsp subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is used, the access location should use the URI name form to specify the location of an L				this certificate.
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 UDAP accessible directory server where certificates issued to the issuer of this certificate may be found. accessLocation Idap:// See preamble text on URIs. GeneralName Idap:// See preamble text on URIs. uniformResourceIdentifier Idap:// Access Method #2 accessMethod id-ad-cosp 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 Idad-cosp subjectInfoAccess consists of a sequence of accessMethod and accessLocation of an OCSP server that provides in CA certificates. subjectInfoAccess FALSE SubjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access Method is defined for use in CA certificates. 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 certificate is subd by the subject of this certificate. accessLocation 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 certificate is subd by the subject of this certificate may be found. accessLocation	AccessDescription			Access Method #1
accessMethod id-ad-calssuers id-ad-calssuers id-ad-calssuers id-ad-calssuers id-ad-calssuers accessLocation id-ad-calssuers id-ad-calssuers uniformResourceIdentifier Idap:// See preamble text on URIs. AccessDescription Access Method #2 Access Method #2 accessLocation 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 id-ad-ocsp name form to specify the location of an OCSP server that provides status information about this certificate. uniformResourceIdentifier http:// See preamble text on URIs. 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 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 id-ad-caRepository When this access method is used, the access location should use the URI name form to specify the locati				When this access method is used, the access location should use the LIPI name form to specify the location of an LDAP accessible.
accessLocation certificate may be found. accessLocation certificate may be found. GeneralName ldap:// uniformResourceIdentifier ldap:// AccessDescription Access Method #2 accessMethod For this access nethod, 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 for this access nethod. uniformResourceIdentifier http:// subjectInfoAccess FALSE subjectInfoAccess method is used, the access location should use the URI accessLocation pairs. Only one access methods is defined for use accessLocation pairs. Only one 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 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 access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server where certificate may be found. accessLocation id-ad-caRepository accessLocation id-ad-caRepository accessLocation id-ad-caRepository accessLocation id-ad-caRepository when this access method is used, the subje	accessMethod		id-ad-calssuers	directory server where certificates issued to the issuer of this
accessLocation Idap:// GeneralName Idap:// uniformResourceIdentifier Idap:// AccessDescription Access Method #2 accessMethod 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 Id-ad-ocsp GeneralName subjectInfoAccess uniformResourceIdentifier http:// subjectInfoAccess FALSE accessDescription subjectInfoAccess method is used, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate. subjectInfoAccess FALSE accessDescription http:// accessMethod id-ad-caRepository id-ad-caRepository id-ad-caRepository accessLocation certificate may be found. accessLocation certificate m		ļ		certificate may be found.
GeneralName Idap:// uniformResourceIdentifier Idap:// AccessDescription Access Method #2 accessMethod 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 Id-ad-ocsp GeneralName subjectInfoAccess uniformResourceIdentifier http:// subjectInfoAccess FALSE AccessDescription id-ad-caRepository when this access method is used, the access location should use the URI name form to specify the location of an OCSP server that provides status information about this certificate. subjectInfoAccess FALSE accessDescription subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is defined for use in CA certificates. accessMethod id-ad-caRepository 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 Idap:// See preamble text on URIs. accessLocation Idap:// See preamble text on URIs. accessLocation Idap:/	accessLocation			
uniformResourceIdentifier Idap:// See preamble text on URIs. AccessDescription Access Method #2 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			
AccessDescription Access Method #2 accessMethod 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 Image: SubjectInfoAccess generalName Image: SubjectInfoAccess uniformResourceIdentifier http:// subjectInfoAccess FALSE AccessDescription SubjectInfoAccess method is used, the access location should use the used in CA certificates. AccessDescription Image:	uniformResourceIdentifier	ļ	Idap://	See preamble text on URIs.
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	AccessDescription	ļ		Access Method #2
access/location in-ad-dcsp Infan form to specify the location of an OCOF server that provides status information about this occurs server that provides status information about this certificate. access/Location in-ad-dcsp infan form to specify the location of an OCOF server that provides status information about this certificate. GeneralName informResourceIdentifier 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 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 certificate issued by the subject of this certificate may be found. accessLocation id-ad-caRepository accessLocation id-ad-caRepository accessLocation id-ad-caRepository	access Mathe		id ad assa	For this access method, the access location should use the URI
accessLocation GeneralName uniformResourceIdentifier http:// subjectInfoAccess FALSE subjectInfoAccess FALSE AccessDescription id-ad-caRepository accessLocation generalName accessLocation id-ad-caRepository accessLocation certificate may be found. accessLocation generalName uniformResourceIdentifier Idap:// Subject InfoAccess See preamble text on URIs. accessLocation subject InfoAccess method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server where certificate issued by the subject of this certificate may be found. GeneralName Idap:// uniformResourceIdentifier Idap:// See preamble text on URIs. See preamble text on URIs.	accessmethod		id-ad-ocsp	status information about this certificate.
GeneralName 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 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 certificate issued by the subject of this certificate may be found. accessLocation certificate certificate may be found. GeneralName Idap:// See preamble text on URIs. UniformResourceIdentifier Idap:// See preamble text on URIs.	accessLocation			
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 when this access method is used, the access location should use directory server where certificates issued by the subject of this access. accessLocation when this access method is used, the access location of an LDAP accessible directory server where certificates issued by the subject of this access. GeneralName Idap:// See preamble text on URIs. Designed by Robert MoSowitz (CSA) and modified by Booz Allen & Hamilton Idap:// See preamble text on URIs.	GeneralName			
subjectInfoAccess FALSE subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access methods is defined for use in CA certificates. AccessDescription 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. GeneralName Idap:// See preamble text on URIs.	uniformResourceIdentifier		http://	See preamble text on URIs.
subjectInfoAccess FALSE accessLocation pairs. Only one access methods is defined for use in CA certificates. AccessDescription 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 certificates certificates GeneralName Idap:// See preamble text on URIs. Designed by Robert Mosowitz (UCSA) and modified by Booz Allen & Hamilton Idap:// See preamble text on URIs.				subjectInfoAccess consists of a sequence of accessMethod and
AccessDescription In CA Certificates. accessDescription id-ad-caRepository accessMethod id-ad-caRepository accessLocation certificates issued by the subject of this certificates issued by the certificate issued by the certificate issued by the certificates issued by the certificate issued by the cerificate issued by the certificate issued by the certif	subjectInfoAccess	FALSE		accessLocation pairs. Only one access methods is defined for use
accessMethod id-ad-caRepository id-ad-caRepository directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the subject of this directory server where certificates issued by the directory server where certificates issued by	AccessDescription			in CA certificates.
accessMethod id-ad-caRepository 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 certificate may be found. GeneralName certificate may be found. uniformResourceIdentifier Idap:// Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton See preamble text on URIs.				When this access method is used, the access location should use
accessLocation certaincates issued by the subject of this certificate may be found. Certificate may b	accessMethod		id-ad-caRepository	the URI name form to specify the location of an LDAP accessible
accessLocation GeneralName uniformResourceIdentifier Usigned by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton				certificate may be found.
GeneralName uniformResourceIdentifier Idap:// See preamble text on URIs.	accessLocation			
uniormicesourceidenmier ldap:// See preamble text on URIs.	GeneralName	<u> </u>	lder://	One are areful to the UDIs
	uniformicesourceidentifier Designed by Robert Moskowitz (ICSA) and modified by Rooz Alle	en & Hamilton	idap://	See preample text on URIS.

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	ļ!		
RDNSequence	[C= ; O= ; OU= ; CN= ; and DC= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType	 	OID	See preamble text on paming
validity		See comment	See preamble text on naming.
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			
Algorithmldentifier	[Public key algorithm used.
algorithm	Į!		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	and issuer have different parameters. If parameters are inherited, omit
· · ·			field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	
extensions			
authorityKeyIdentifier	FALSE		
keyldentifier	511.05	OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		De la la la di Olità di bash af dia sublia basi
keyldentifier	 	OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		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.,
PolicyInformation			Ully use for access to www.agency.gov), otherwise set as non-onaca.
policyldentifier		OID	
		0	Use of policy qualifiers is optional, but limited to qualifier types identified
policyQualitiers			below.
PolicyQualifierInfo	1		defined policy qualifier #1

policyQualifierId		id-at-cps	CPS
guelifier			UDI for publishing CDC Line IAECtring
quainer		CFSull	URI für publisning CPS. Use IASSung.
PolicyQualitierInto			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.
noticeBef			
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			
rfe@22Name		IAE String	This field contains the electronic mail address of the subject
rrc822Name		IASString	I his 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			
BDNSequence	1		
KDNSequence			
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
dNSNomo		IAEString	This field contains the dree name of the issuing CA
unsname		ASSUING	This field contains the dris name of the issuing CA.
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeApd\/alue			
Attribute Type		OID	
AttributeType		OID	One are apple to day a serie a
Attribute value	EALSE	see comment	See preamble text on naming.
Distribution Doint	TALGE		
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
ConcrelName			
director blor -		l	1
directoryiname			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeTupe	1		
Attribute lype		OID	Cae preamble text on paming
uniformResourceIdentifier		Idar://	See preamble text on Halling.
		iuap.//	See preamble text on URIS.
nameRelative I oCRLIssuer			
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	<u> </u>	1	
offiliationChanged		4	1
anniauononanged	ļ	1	
superseded		1	
cessationOfOperation		1	

aartificatal lald		4	
		1	<u>↓</u>
privilegeWithdrawn		1	
aACompromise		1	
cRLlssuer			If present, this field indicates that the distribution point is an indirect CRI
CaparalNamaa			
Generalivalles			
GeneralName			matches the DN in the issuer field of the corresponding CRL
directoryName			
Name			
Naille			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
			If delta-CRLs are issued that cover this certificate, then either this
FreshestCRL	FALSE		certificate or the complete for scope CRL that corresponds to the delta-
			CRLs should include the FreshestCRL extension
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName	l		
GeneralNames	l		
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
uniformResourceIdentifier		Idap://	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
1000000			if present, this field indicates which reasons are covered by this distribution
Teasons			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 consists of a sequence of accessMethod and
	541.05		accessLocation pairs. Two access methods are defined: one for locating
authorityInfoAccess	FALSE		certificates issued to the certificate issuer and one for locating an OCSP
			server that provides status information about this certificate.
AccessDescription			Access Method #1
· ·			When this access method is used, the access location should use the URI
accessMethod		id-ad-calssuers	name form to specify the location of an LDAP accessible directory server
	i l		where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceldentifier		Idap://	See preamble text on URIs.
AccessDescription			Access Method #2
			For this access method, the access location should use the URI name form
accessMethod	i l	id-ad-ocsp	to specify the location of an OCSP server that provides status information
	i I	p	about this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://	See preamble text on URIs.
Designed by Robert Moskowitz (ICSA) and modified by	Booz Allen & Hamilton		
and mounted by			

Key Management Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate	, v		
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlaorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm			Choice of following three algorithms
agonan		1 2 840 113549 1 1 5	SHA-1WithRSAEncryption
		1 2 840 10040 4 3	id-dea-with-sha-1
		1 2 840 10045 4 1	acted with SHA1
parametera		1.2.840.10045.4.1	Only populate when using SHA 1With PSAE populate
parameters		NOEL	Only populate when using SHA-TWITINSAETICIY puoli
Issuer			
Name			
RDINSequence			C=; $O=$; $OU=$; $CN=$; and $DC=$ are recommended
RelativeDistinguishedName			
Attribute I ypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
notBerore			
lime			
utclime		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		
keyldentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyldentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		As specififed 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	
kevAgreement		1	Used when subject public key is DH or ECDH
keyCertSign		0	
cRLSign	1	0	
encipherOnly		0	There is no requirement to support this key usage
decipherOnly		0	There is no requirement to support this key usage
		, v	Set as critical if policy is designed to restrict usage of the certificate
certificatePolicies	See comment.		(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.

PolicvQualifierInfo			defined policy qualifier #1
policyQualifierId		id-gt-cps	CPS
qualifier		cPSuri	URI for publishing CPS. Use IA5String.
PolicyQualifierInfo			defined policy qualifier #2
policyQualifierId		id-gt-unotice	
qualifier			
UserNotice			UserNotice should only appear in EE or CA certs issued to other
noticeRef			organizations to prevent multiple duplicate displays.
NoticeReference			
organization			
DisplayText		See comment	visableString bmpString or utf8String
noticeNumbers			Housidening, Shipening of directing
explicitText			
DisplayText		See comment	visableString hmpString or utf8String
Display Toxe		occ comment.	This extension is optional. Any name types may be present; only the
subjectAltName	FALSE		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		Idap://	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	1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	1

		1	
certificateHold		1	
privilegeWithdrawn		1	
privilegewinididwi			4
aACompromise		1	
cPI lequer			If present, this field indicates that the distribution point is an indirect
CIVEISSUEI			CRL.
GeneralNames			
GeneralName			matches the DN in the issuer field of the corresponding CPI
Generalivatile			matches the DN in the issuel held of the corresponding CNL
directoryName			
Name			
BDNSequence			
RDNOequeilce			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeTure		OID	
Attribute i ype		UID	
AttributeValue		see comment	See preamble text on naming.
			If delta-CRLs are issued that cover this certificate, then either this
FreshestCRI	FALSE		certificate or the complete for scope CRL that corresponds to the delta
Treshestone	171202		CRI s should include the EreshestCRI, extension
DistributionPoint			CILES SHOULD INCIDE THE THESHESTORE EXTENSION
distribution Boint			
DistributionPoint			
DistributionPointName			
ruiiname			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming
uniformResourceIdentifier		Idan://	See preamble text on LIRIs
	-	iuap.//	See preamble text on ortis.
Relative Distinguished Name			
AttributeTupeAppl/clue			
Attribute i ypeAnd value		015	
Attribute l ype		OID	
AttributeValue		see comment	See preamble text on naming
reasons			if present, this field indicates which reasons are covered by this
10030113			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	
cessation		1	
certificateHold		1	
privilegeWithdrawp		1	
aACompromise		1	
aAcompromise		1	If present this field indicates that the distribution point is an indirect
cRLIssuer			Il present, unis nelo indicates triat the distribution point is an indirect
O			URL.
GeneralNames			
GeneralName			4
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
			autionlyinioAccess consists of a sequence of accessmethod and
authorityInfoAccess	FALSE		accessLocation pairs. I wo 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
//0000000000000000000000000000000000000			When this access method is used, the access location should use the
			LIPI name form to specify the location of an LDAP accessible directory
accessMethod		id-ad-calssuers	server where certificates issued to the issuer of this certificate may be
			server where certificates issued to the issuer of this certificate may be
-			formal
accord apption			found.
accessLocation			found.
accessLocation GeneralName			found.
accessLocation GeneralName uniformResourceIdentifier		ldap://	found. See preamble text on URIs.
accessLocation GeneralName uniformResourceIdentifier AccessDescription		Idap://	found. See preamble text on URIs. Access Method #2
accessLocation GeneralName uniformResourceIdentifier AccessDescription		Idap://	found. See preamble text on URIs. Access Method #2 For this access method, the access location should use the URI name
accessLocation GeneralName uniformResourceIdentifier AccessDescription accessMethod		ldap:// id-ad-ocsp	found. See preamble text on URIs. Access Method #2 For this access method, the access location should use the URI name form to specify the location of an OCSP server that provides status
accessLocation GeneralName uniformResourceIdentifier AccessDescription accessMethod		id-ad-ocsp	found. See preamble text on URIs. Access Method #2 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 uniformResourceldentifier AccessDescription accessMethod accessLocation		id-ad-ocsp	found. See preamble text on URIs. Access Method #2 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 AccessDescription accessMethod accessLocation GeneralName		id-ad-ocsp	found. See preamble text on URIs. Access Method #2 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 uniformResourceldentifier AccessDescription accessMethod accessLocation GeneralName uniformResourceldentifier		id-ad-ocsp	found. See preamble text on URIs. Access Method #2 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. See preamble text on URIs.
accessLocation GeneralName uniformResourceIdentifier AccessDescription accessMethod accessLocation GeneralName uniformResourceIdentifier Designed by Robert Moskowitz (ICSA) and modified	by Booz Allen & Hamilton	id-ad-ocsp	found. See preamble text on URIs. Access Method #2 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. See preamble text on URIs.

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			Dublis Los alexañtes con d
Algorithmidentiller			Public key algorithm used.
algoritrim		4 0 040 440540 4 4 4	Choice of following two algorithms.
		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
paramotore		1.2.840.10045.2.1	Elliptic Curve Algorithms
subjectPublicKey		BIT STRING	TO NOA Include NOLL, IOI DOA and LODOA Include parameters.
extensions		Bir officia	
subjectKeyIdentifier	FALSE		This extension is required to assist in path development
keyldentifier		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 be enforced.
cA		TRUE	
Designed by Robert Moskowitz (ICSA) and	d modified by Booz Allen	& Hamilton	1

Self-Signed Certificate Profile

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
GeneralizedTime			revocation date.
certificatelssuer	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		
keyldentifier		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			

	1		
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment	See preamble text on paming
cRI Number	FALSE	INTEGER	Monotonically increasing sequential number
la sula a Distrikution Delat	TRUE	INTEGER	This subscripts are set in a second state of OPL s and indirect OPL s
IssuingDistributionPoint	IRUE		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			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment	See preamble text on paming
uniformResourceIdentifier		IA5String	matches the URI in the crI distribution points extension of certificates covered by this CRL.
onlyContainsUserCerts		BOOLEAN	If set to TRUE, this CRL only covers end entity certificates
		2001 5111	If set to TRUE, this CRL only covers CA certificates. If
onlyContainsCACerts		BOOLEAN	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			reasons, this held is offitted.
Keasonriags			
unused		1	
keyCompromise		1	
cACompromise		1	
affiliationChanged		1	
superseded		1	
cessationOfOperation		1	
		1	
CertificateHold			
privilegewithdrawh		1	
aACompromise		1	
indirectCRL		BOOLEAN	If set to true, this CRL covers certificates that were not issued by the issuer of this CRL.
FreshestCRL	FALSE		If this is a complete for scope CRL, and delta-CRLs are issued for the same scope, then either this CRL or the certificates that it covers should include the FreshestCRL extension. When the FreshestCRL extension is used in a CRL, only the distributionPoint field is used. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence	L		
RelativeDistinguishedName	 		
AttributeType		OID	
AttributeValue	1	see comment	See preamble text on naming
uniformResourceIdentifier		Idap://	See preamble text on URIs.
nameRelativeToCRLIssuer			
RelativeDistinguishedName	ļ		
Attribute I ypeAndValue	 	OID	
Attribute//alue	łł	UID see comment	See preamble text on paming
deltaCRLIndicator	TRUF	See comment	This extension is included if and only if the CRL is a delta CRL
BaseCBI Number		INTEGER	This value shall be identical to the value in the cRLNumber extension of the
Designed by Robert Moskowitz (ICSA) and modified	by Booz Allen & Hamilt	on	base certificate.