DirectTrust X.509 Certificate and Certificate Revocation List (CRL) Profiles

DirectTrust.org Certificate Policy & Practices (CPP) Work Group

December 12, 2018

Revision History Table

Date	Version	Description
Jan 3, 2014	1.0	Initial version of profile
August 10, 2016	1.3	Updated version released in conjunction with DirectTrust CP v1.3.
December 1, 2016	1.3 with errata	Errata to correct name of DirectTrust-EHNAC Accreditation programs.
December 12, 2018	1.3 with errata	Errata to correct LoA and CP OIDs, and device certificate profile subject alternative name.

1. Introduction

This document specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for Direct Organization certificates, Direct Address certificates, and CRLs issued for use with DirectTrust Accredited entities. The profiles serve to identify unique parameter settings for certificates and CRLs issued for use within the DirectTrust Trust Framework.

This Profile is based on the DirectTrust Certificate Policy [1], and also the Federal Public Key Infrastructure (PKI) X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile [13], which is based on the Internet Engineering Task Force (IETF) Public Key Infrastructure (PKIX) profile developed by the PKIX working group [3]. The PKIX profile identifies the format and semantics of certificates and CRLs for the Internet PKI. Procedures are described for processing and validating certification paths in the Internet environment. Encoding rules are provided for all fields and extensions profiled in both the X.509 v3 certificate and v2 CRL. Encoding rules for cryptographic algorithms specified in this profile are specified in [7] and [10].

An approved version of this Profile becomes normative for certificates submitted for inclusion (or issued by such included Trust Anchors) in a DirectTrust Trust Anchor Bundle (TAB).

1.1. Structure

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

1.2. Relationship to DirectTrust Certificate Policy

This Profile serves as appendix to DirectTrust Certificate Policy v1.3. These X.509 version 3 certificate and version 2 CRL profile specifications are deemed normative for certificates submitted for inclusion in a DirectTrust Trust Anchor Bundle (TAB), or for Direct Organization and Address certificates issued by Trust Anchors in that bundle, and their related revocation lists. Failure to comply with these specifications for certificates asserting a CP v1.3 policy OID is potential grounds for exclusion of Trust Anchors from the TAB, or loss of accreditation status through DirectTrust-EHNAC Accreditation.

1.3. Acronyms

AKID Authority Key Identifier

CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
FBCA	Federal Bridge Certification Authority
FPKI	Federal Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PSS	Probabilistic Signature Scheme
RFC	Request For Comments
RSA	Rivest-Shamir-Adelman
SHA	Secure Hash Algorithm
SKID	Subject Key Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universally Unique IDentifier

1.4. References

[1] DirectTrust Community X.509 Certificate Policy, Version 1.3, 10 August 2016.

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

[3] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russel Housley, and Tim Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280, May 2008.

[4] Mark Smith and Tim Howes. *Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator*, RFC 4516, June 2006.

[5] Roy T. Fielding, James Gettys, Jeffrey C. Mogul, Henrik Frystyk Nielsen, Larry Masinter, Paul J. Leach, and Tim Berners-Lee. *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, June 1999.

[6] Steve Lloyd. *AKID/SKID Implementation Guideline*, September 2002.

[7] Tim Polk, Russel Housley, and Larry Bassham. Internet Public Key Infrastructure: *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3279, April 2002.

[8] W. Timothy Polk, Donna F. Dodson, and William E. Burr. *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST Special Publication 800-78-2, February 2010.

[9] Blake Ramsdell and Sean Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*, RFC 5751, January 2010.

[10] Jim Schaad, Burt Kaliski, and Russell Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 4055, June 2005.

[11] Applicability Statement for Secure Health Transport Version 1.2, Aug 2015

[12] Paul J. Leach, Michael Mealling, and Rich Salz. *A Universally Unique IDentifier (UUID) URN Namespace*, RFC 4122, July 2005.

[13] Federal Public Key Infrastructure (PKI) X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile

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 subject's distinguished name, 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 RFC 5280.

CAs create certificates for subject authentication, digital signing, and confidentiality procedures that require a relying party to obtain the user's public key. So that users and relying parties 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, and to bind that information to the cryptographic keys controlled by the applicant – the Public Key of which is part of the certificate contents. The fields in a certificate identify the issuer (i.e., CA), subject (i.e., user/service), 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/service or the CA, depending on the implementation.

3. X.509 v2 Certificate Revocation Lists

CAs use CRLs to publicize the revocation of a subject's certificate. The CRLs are stored in a repository 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 certificates.

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

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

4. Encoding Distinguished Names with Attributes of type DirectoryString

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

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

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

For certificates and CRLs issued for DirectTrust, attributes of type DirectoryString shall be encoded in either PrintableString or UTF8String, in accordance with RFC 5280.

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

Uniform Resource Identifiers (URIs) are used in three different extensions within the certificate and CRL profiles in this document: authorityInfoAccess, policyQualifierIDs (within certificatePolicies), and cRLDistributionPoints. Two different protocols may be referenced in these extensions: LDAP and HTTP. The specifications for URIs for these

protocols may be found in RFC 4516 and RFC 2616, respectively.

NB: ALL URIs as specified in this document are actually URLs and therefore MUST all be resolvable in order for the respective Trust Anchor to be accepted into the TAB.

The scheme portion of all primary URIs must be HTTP (with the exception of CPS Pointer which may be HTTPS), and additional HTTP URIs may also be specified if allowed by the extension. Additional LDAP URIs may optionally be used to indicate that the relevant information is located in an LDAP accessible directory, but only after a primarily URI is specified as being available via HTTP. Specifically for the id-ad-ocsp access method of the authorityInfoAccess, the scheme portion of the URI must be HTTP to indicate that the transport protocol for the OCSP request/response messages is HTTP. The hostname of every URI must be specified as either a fully qualified domain name or an IP address. The information must be made available via the default port number for the relevant protocol (80 for HTTP and 389 for LDAP) and so does not need to be specified in the URI.

In the cRLDistributionPoints extension, the URI is a pointer to a current CRL that provides status information about the certificate. If LDAP is also used, the URI must include the DN of the entry containing the CRL and specify the directory attribute in which the CRL is located (certificateRevocationList, authorityRevocationList, or deltaRevocationList). If the directory in which the CRL is stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI.

When HTTP is used, the URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL (see RFC 2585). When a URI is used as the DistributionPointName in the issuingDistributionPoint extension in a CRL, the value must match the URI in the corresponding distribution points in the cRLDistributionPoints extensions in certificates covered by the CRL.

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

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

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

The authorityInfoAccess extension uses URIs for two purposes. When the id-ad-caIssuers access method is used, the access location specifies where certificates issued to the issuer of the certificate may be found. When HTTP is used, the URI must point to a file that has an extension of ".p7c" or ".p7b" (if a CMS message format is used e.g. when there are multiple certificates identified) –or– ".cer" or ".crt" if a single DER-encoded certificate format is used. If ".p7c" or ".p7b" is used then it must contain a DER-encoded “certs-only” CMS message (see RFC 5751). The CMS message should include all certificates issued to the issuer of this certificate, but must at least contain all certificates issued to the issuer of this certificate in which the subject public key may be used to verify the signature on this certificate. It is acceptable for a CMS message to contain a single certificate in the ".p7c" or ".p7b" file. If an optional LDAP location is used, the URI must include the DN of the entry containing the relevant certificates and specify the directory

attribute in which the certificates are located. If the directory in which the certificates are stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI.

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

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

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

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

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

6. DirectTrust Certificates

The certificate profiles for DirectTrust Certificates are based on the profiles from the Direct Project Applicability Statement for Secure Health Transport [11] and upon discussion and consensus within the DirectTrust Certificate Policies and Practices Work Group.

7. Worksheet Contents

The certificate and CRL profiles consist of five worksheets. Each worksheet lists mandatory contents of a particular class of certificates or CRLs. Optional features that will be widely supported in the DirectTrust Trust Framework 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 DirectTrust Federation to process this additional information. Critical extensions that are not listed in these worksheets MUST NOT be included in certificates or CRLs issued for DirectTrust.

The five worksheets are:

1. The *Issuing CA Certificate Profile* worksheet defines the mandatory and optional contents of issuers of DirectTrust certificates (may also apply to Trust Anchors).
2. The *CRL Profile* worksheet table defines the mandatory and optional contents of CRLs issued by CAs that issue certificates.
3. The *DirectTrust Domain-Bound Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the Direct Domain-Bound Certificate defined in Sections 1.4 and 5.2 of the Applicability Statement[11].
4. The *DirectTrust Address Certificate Profile* worksheet defines the

mandatory and optional contents of certificates that correspond to the Direct Address-Bound Certificate defined in Sections 1.4 and 5.1 of the Applicability Statement[11].

5. The *DirectTrust Device Certificate Profile* worksheet defines the mandatory and optional contents of certificates that correspond to the DirectTrust Device Certificates.

Worksheet 1: Issuing CA Certificate Profile

Worksheet 1: Issuing CA Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
Certificate			MUST be dedicated to issuing Direct certificates ONLY
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		Integer	Unique positive integer
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
parameters		NULL	
issuer			
Name			
RelativeDistinguishedName			
countryName (2.5.4.6)		Two letter country code of Issuer CA	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<NAME of Org responsible for CA's issuer>	Required
organizationalUnitName (2.5.4.11)		(Optional)	
commonName (2.5.4.3)		Name of Issuing CA's Issuer	Required NOTE: May be issued by a higher Root
validity			
notBefore Time		(issue date)	utcTime - YYMMDDHHMMSSZ
notAfter Time		(issue date + up to Max of 20 years)	utcTime - YYMMDDHHMMSSZ
subject			
Name			
RelativeDistinguishedName			
countryName (2.5.4.6)		Two letter country code of Issuer CA	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<NAME of Org responsible for CA>	Required
organizationalUnitName (2.5.4.11)		(Optional)	

Worksheet 1: Issuing CA Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
commonName (2.5.4.3)		Name of Issuing CA	Required
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Algorithm associated with the public key
algorithm		1.2.840.113549.1.1.1	rsaEncryption
parameters		NULL	
subjectPublicKey		key	2048 bit RSA public key
required extensions			
keyUsage (2.5.29.15)	**TRUE**		
digitalSignature		1	Optional - To facilitate direct OCSP signing if required
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
basicConstraints (2.5.29.19)	**TRUE**		
cA		Y	
pathLenConstraint		pathlen=N	Optional. N is the number of the depth of allowed subordinates in a chain. Zero means no subCAs allowed. One means subCAs allowed. Two means subCAs and sub-subCAs allowed etc. Recommend pathlen=0 i.e.no subs for issuing CAs.
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	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. Unless self-signed, Certificates issued under the DirectTrust Certificate Policy must include an authorityInfoAccess extension with at least one instance of the caIssuers access method: one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
accessMethod		On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	(Optional) - required if relying on OCSP services i.e. NO CDPs referenced
accessLocation		<http URL>	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	Required for certificates that are not self-signed - When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or LDAP accessible directory server where certificates issued to the issuer of

Worksheet 1: Issuing CA Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
			this certificate may be found.
accessLocation		pointer to cer or p7c file containing issuer	GeneralName (uniformResourceIdentifier)
cRLDistributionPoints (2.5.29.31)	FALSE		This extension is required in all CA certificates even if OCSP is offered, unless the CA cert is self-signed. At least one HTTP URI is required.
DistributionPointName			
fullName		URL to where CRL is published	
DistributionPointName		(Optional)	
fullName		Optional Additional CDP URL	
extendedKeyUsage (2.5.29.37)	FALSE	Not Present	Prohibited
certificatePolicies (2.5.29.32)	FALSE		
policyIdentifier		OID Representing the Policy(ies) CA is valid to issue certs under	At least one DT CP policy OID (version or subversion) or one CP policy OID that maps to a DT CP OID must be included. anyPolicy (OID 2.5.29.32.0) is permitted.
policyQualifierID		(Optional) URL to CPS	Type = CPS, only permitted when the corresponding OID points to a full CP, i.e. not on other certificate attribute OIDs
policyQualifierInfo		Not Present	Prohibited
policyIdentifier		(Optional) Multiple Policy OIDs may be specified	No qualifiers other than on CP OID (above)
subjectKeyIdentifier (2.5.29.14)	FALSE	(keyID)	
authorityKeyIdentifier (2.5.29.35)	FALSE	(keyID=)	
Signature			
signatureAlgorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
signature			

Worksheet 2: CRL Profile

Worksheet 2: CRL Profile			
Field	**Criticality Flag**	**Value**	**Comments**
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.113549.1.1.12	Sha384WithRSAEncryption
		1.2.840.113549.1.1.13	Sha512WithRSAEncryption
parameters		Null	
issuer			
Name			Issuer name should be encoded exactly as it is encoded in the issuer fields of the certificates that are covered by this CRL.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See Comment.	See preamble text on naming.
thisUpdate			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
nextUpdate			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
revokedCertificates			
userCertificate		INTEGER	serial number of certificate being revoked

Worksheet 2: CRL Profile			
Field	**Criticality Flag**	**Value**	**Comments**
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. The removeFromCRL reason code may only be used in delta CRLs.
invalidityDate	FALSE		This extension may be included if the invalidity date precedes the revocation date.
generalTime		YYYYMMDDHHMMSSZ	use this format for all dates.
crlExtensions			
Extensions			
authorityKeyIdentifier	FALSE		Must be included in all CRLs.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
cRLNumber	FALSE	INTEGER	Monotonically increasing sequential number. Must be included in all CRLs.
issuingDistributionPoint	TRUE	(Optional)	This extension appears in segmented CRLs. If the CRL covers all unexpired certificates issued by the CRL issuer (i.e., all unexpired certificates in which the issuer field contains the same name as the issuer field of the CRL), then this extension does not need to be included. CRLs must cover all reason codes and may not be indirect. Thus, the onlySomeReasons field must be absent and the indirectCRL flag must be false.
distributionPoint		(Optional)	
DistributionPointName		(Optional)	If the issuer generates segmented CRLs (i.e., CRLs that do not cover all unexpired certificates in which the issuer field contains the same name asthe issuer field in the CRL), this field must be present and must specify the same names as are specified in the distributionPoint field of the cRLDistributionPoints extensions of certificates covered by this CRL.
fullName			
GeneralNames			

Worksheet 2: CRL Profile			
Field	**Criticality Flag**	**Value**	**Comments**
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	
uniformResourceIdentifier		IA5String	
onlyContainsUserCerts		BOOLEAN	If set to TRUE, this CRL only covers end entity certificates
onlyContainsCACerts		BOOLEAN	If set to TRUE, this CRL only covers CA certificates. If onlyContainsUserCerts is TRUE, this field must be FALSE.
IndirectCRL		FALSE	

Worksheet 3: Domain-Bound Certificate Profile

Worksheet 3: Domain-Bound Certificate			
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; CAs SHOULD generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
parameters		NULL	
issuer			
Name			MUST match Issuer DN
RDNSequence			
countryName (2.5.4.6)		Two letter country code of Issuer CA	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<NAME of Org responsible for CA>	Required
organizationalUnitName (2.5.4.11)		(Optional)	
commonName (2.5.4.3)		Name of Issuing CA	Required
validity			
notBefore		(issue date)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
notAfter		(issue date + up to 3 years)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
subject			
Name			
RDNSequence			
countryName (2.5.4.6)		Two letter country code of subject	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		Subscriber organization name	Required.
organizationalUnitName (2.5.4.11)		(Optional)	
commonName (2.5.4.3)		Health Domain Name	Required: Health Domain Name in the form of a dNSName;
subjectPublicKeyInfo			

Worksheet 3: Domain-Bound Certificate			
Field	**Criticality Flag**	**Value**	**Comments**
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	Modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	**TRUE**		At least one of the allowed keyUsages must be asserted. A single keyUsage is allowed.
digitalSignature		1	
nonRepudiation		0	Group Certificates SHALL NOT assert the non-repudiation bit.
keyEncipherment		1	
dataEncipherment		1	dataEncipherment is not required for Direct messaging. dataEncipherment is allowed for other use cases.
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
basicConstraints (2.5.29.19)	**TRUE**		
cA		N	
pathLenConstraint		empty	
extKeyUsage	FALSE		
keyPurposeID		1.3.6.1.5.5.7.3.4	Secure Email; other extended key usages may be present
subjectAltName	FALSE		
dNSName		Health Domain Name	Repeats Health Domain Name in the form of a dNSName from CN
certificatePolicies	FALSE		
policyIdentifier		1.3.6.1.4.1. 41179.0.1.3	Required; DirectTrust CP OID
policyIdentifier		Applicable LoA OID	Required; DirectTrust LoA OID, e.g. 1.3.6.1.4.1. 41179.1.3 for LoA3
policyIdentifier		Healthcare Category OID	Required; The appropriate DirectTrust Healthcare Category OIDs shall be asserted, e.g. 1.3.6.1.4.1. 41179.2.1 for a Covered Entity.
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		HTTP URL to where CRL is published	Required
DistributionPointName			

Worksheet 3: Domain-Bound Certificate			
Field	**Criticality Flag**	**Value**	**Comments**
fullName		Optional Additional CRL Distribution Point URL	Optional
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	FALSE		
accessMethod		On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	Optional
accessLocation		URI for OCSP	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		pointer to cer/crt or p7c/p7b file containing issuer	GeneralName (uniformResourceIdentifier)
Signature			
signatureAlgorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
signature			

Worksheet 4: Address Certificate Profile

Worksheet 4: Address Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		(unique random assigned by CA)	
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
parameters		NULL	
issuer			
Name			MUST match Issuer DN
RDNSequence			
countryName (2.5.4.6)		Two letter country code of Issuer CA	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<NAME of Org responsible for CA>	Required
organizationalUnitName (2.5.4.11)		(Optional)	
commonName (2.5.4.3)		Name of Issuing CA	Required
validity			
notBefore		(issue date)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
notAfter		(issue date + up to 3 years)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
subject			
Name			
RDNSequence			
countryName (2.5.4.6)		Two letter country code of subject	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		Subscriber organization name	Required when Subscriber is an Organization. Required absent when Subscriber is a Patient.
organizationalUnitName (2.5.4.11)		(Optional)	

Worksheet 4: Address Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
commonName (2.5.4.3)		Full name of Subscriber + some text to denote Group nature of certificate, the Direct Address, or Description of Direct End Point	Required; E.g. Scott Rea Direct Group Cert; or billing@direct.practice.org; or ER Department DirectHospital; Per CP, a cert whose private keys are accessed by more than one party or held by a HISP ISSO (Group Cert) may not be represented as if it belongs to a single person. Example group status designators include “Group Cert” and “HISP-Managed Certificate”, etc. Alternatively, the group status designator may be listed in the OrganizationalUnitName attribute.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	Modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	**TRUE**		At least one of the allowed keyUsages must be asserted. A single keyUsage is allowed.
digitalSignature		1	
nonRepudiation		0	Group Certificates SHALL NOT assert the non-repudiation bit.
keyEncipherment		1	
dataEncipherment		1	dataEncipherment is not required for Direct messaging. dataEncipherment is allowed for other use cases.
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
basicConstraints (2.5.29.19)	**TRUE**		
cA		N	
pathLenConstraint		empty	
extKeyUsage	FALSE		
keyPurposeID		1.3.6.1.5.5.7.3.4	Secure Email; other extended key usages may be expressed
subjectAltName	FALSE		
rfc822Name		IA5String:Direct End Point Address	Direct End Point Address expressed as an rfc822 name
certificatePolicies	FALSE		

Worksheet 4: Address Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
policyIdentifier		1.3.6.1.4.1. 41179.0.1.3	Required; DirectTrust CP OID
policyIdentifier		LoA OID	Required; DirectTrust LoA OID, e.g. 1.3.6.1.4.1. 41179.1.3 for LoA3
policyIdentifier		Healthcare Category OID	Required; The appropriate DirectTrust Healthcare Category OIDs shall be asserted, e.g. 1.3.6.1.4.1. 41179.2.1 for a Covered Entity.
cRLDistributionPoints (2.5.29.31)	FALSE		This extension is required in all certificates. At least one HTTP URI is required, and HTTP URIs are preferred. The reasons and cRLIssuer fields must be omitted.
DistributionPointName			
fullName		HTTP URL to where CRL is published	Required
DistributionPointName			
fullName		Optional Additional CRL Distribution Point URL	Optional
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	FALSE		
accessMethod		On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	Optional
accessLocation		URI for OCSP	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		pointer to cer/crt or p7c/p7b file containing issuer	GeneralName (uniformResourceIdentifier)
Signature			
signatureAlgorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
signature			

Worksheet 5: Device Certificate Profile

Worksheet 5: Device Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		(unique random assigned by CA)	
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
parameters		NULL	
issuer			
Name			MUST match Issuer DN
RDNSequence			
countryName (2.5.4.6)		Two letter country code of Issuer CA	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<NAME of Org responsible for CA>	Required
organizationalUnitName (2.5.4.11)		(Optional)	
commonName (2.5.4.3)		Name of Issuing CA	Required
validity			
notBefore		(issue date)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
notAfter		(issue date + up to 3 years)	
utcTime -or- generalTime		YYMMDDHHMMSSZ -or- YYYYMMDDHHMMSSZ	UTC may only be used for dates up to and including 2049. General can be used for any dates.
subject			
Name			
RDNSequence			
countryName (2.5.4.6)		Two letter country code of subject	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be in conformance with ISO 3166-2
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		Subscriber organization name	Optional
organizationalUnitName (2.5.4.11)		(Optional)	

Worksheet 5: Device Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
commonName (2.5.4.3)		Device name	Required
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	Modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	**TRUE**		At least one of the allowed keyUsages must be asserted. A single keyUsage is allowed.
digitalSignature		1	
nonRepudiation		0	Group Certificates SHALL NOT assert the non-repudiation bit.
keyEncipherment		1	
dataEncipherment		1	dataEncipherment is not required for Direct messaging. dataEncipherment is allowed for other use cases.
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
basicConstraints (2.5.29.19)	**TRUE**		
cA		N	
pathLenConstraint		empty	
extKeyUsage	FALSE		
keyPurposeID		Optional	Optional; e.g. Server Authentication or other extended key usages may be expressed
subjectAltName	FALSE		
rfc822Name		(Optional) IA5String:Direct Address	Direct Address expressed as an rfc822 name, e.g. johndoe@direct.sunnyfamilypractice.org
dNSName		(Optional) Domain Name	Domain Name expressed as a dNSName, e.g. abc.example.com

otherName		(Optional) Sequence {
		OID: 2.16.840.1.113883.4.6,
		[0] UTF8String: <10-digit Numeric NPI>
		}
			Optional encoding of a verified NPI for Subject
			organization or Subject Individual Covered entity

certificatePolicies	FALSE		

Worksheet 5: Device Certificate Profile			
Field	**Criticality Flag**	**Value**	**Comments**
policyIdentifier		1.3.6.1.4.1. 41179.0.1.3	Required; DirectTrust CP OID
policyIdentifier		LoA OID	Required; DirectTrust LoA OID, e.g. 1.3.6.1.4.1. 41179.1.3 for LoA3
policyIdentifier		Healthcare Category OID	Required if organization is asserted in Certificate subject.
cRLDistributionPoints (2.5.29.31)	FALSE		This extension is required in all certificates. At least one HTTP URI is required, and HTTP URIs are preferred. The reasons and cRLIssuer fields must be omitted.
DistributionPointName			
fullName		HTTP URL to where CRL is published	Required
DistributionPointName			
fullName		Optional Additional CRL Distribution Point URL	Optional
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	FALSE		
accessMethod		On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	Optional
accessLocation		URI for OCSP	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		pointer to cer/crt or p7c/p7b file containing issuer	GeneralName (uniformResourceIdentifier)
Signature			
signatureAlgorithm		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
signature			