Attachment 1

DirectTrust-Carequality and DirectTrust-eHealth Exchange Profiles

Introduction

This document specifies the X.509 version 3 certificate that include:

- DirectTrust-Carequality certificates
- DirectTrust-eHealth Exchange certificates

The profiles serve to identify unique parameter settings for certificates issued for use within the DirectTrust Trust Framework.

These Profiles are based on the DirectTrust Certificate Policy v2.0.

Two types of certificates can be issued under the profiles defined in the following worksheets: production (PRD) certificates and validation (VAL) certificates.
For historical reasons to support interoperability, this document specifies certain fixed values for the subject Organizational Unit and the Subject Alternative Name extension of certificates issued under the profiles defined in the following worksheets. For clarity, it is explicitly noted that certificates issued under these profiles SHALL NOT be interpreted to express an organizational affiliation (as that term is used in Section 1.3.5.2 of the DirectTrust CP) of the Subscriber with the U.S. Department of Health and Human Services (HHS), the Office of the National Coordinator for Health Information Technology (ONC), Carequality, or the Nationwide Health Information Exchnage (NHIN or NwHIN) or its successor the eHealth Exchange, and that the following fixed values SHALL NOT be interpreted to represent the Subscriber, an Affiliated Organization, or the names of organizations asserted in a certificate that require verification by the CA/RA prior to inclusion in the certificate. The fixed values are:

a. In the Subject, the organizationalUnitName attribute values of
    i. "CAREQUALITY" in Worksheet A for production certificates, or
    ii. "CAREQUALITY-TEST" in Worksheet A for validation certificate, or
    iii. "NHIN" in Worksheet B for production certificates, or
    iv. "NHIN-Test" in Worksheet B for validation certificates
b. In the Subject Alternative Name extension for a Carequality validation or production certificate, a uniformResourceIdentifier entry with a value of "HTTP://WWW.CAREQUALITY.ORG/V01" in Worksheet A.

VAL certificates SHALL be issued from a different intermediate CA certificate than PRD certificates and SHALL chain to a different root CA certificate than PRD certificates. VAL certificates are intended for testing and not for production use. As such, identification and authentication procedures for VAL certificates are NOT required to comply with the DirectTrust CP, and the CA/RA is not required to verify the identity of the Subscriber or Sponsor, or any information asserted in a VAL certificate.

For VAL certificates, the CA/RA MAY omit the certificate policy OIDs listed in the profiles below and/or add additional annotations to the subject attributes to indicate the non-production nature of these certificates.

Worksheet A: DirectTrust-Carequality Certificate Profile

Worksheet A: DirectTrust-Carequality 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 either the full name of the state or province or in conformance with the second part (Subdivision name) of the corresponding ISO 3166-2 code.
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)		US	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be either the full name of the state or province or in conformance with the second part (Subdivision name) of the corresponding ISO 3166-2 code.
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<Subscriber Org Name>	Required
organizationalUnitName (2.5.4.11)		<Choice>	Required; “CAREQUALITY” (PRODUCTION) or “CAREQUALITY-TEST” (VALIDATION); Additional OU values may also be present.
commonName (2.5.4.3)		Fully Qualified Domain Name (FQDN) of the End Point	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	
keyEncipherment		1	
dataEncipherment		0	
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		
dNSName		Domain Name	Required; Domain Name expressed as a dNSName, e.g. abc.example.com
uniformResourceIdentifier		HTTP://WWW.CAREQUALITY.ORG/V01	Required
certificatePolicies	FALSE		
policyIdentifier		1.3.6.1.4.1. 41179.0.2.0	Required; DirectTrust CP OID
policyIdentifier		1.3.6.1.4.1.41179.1.5	Required; DirectTrust Identity Level of Assurance OID for IAL2
policyIdentifier		Healthcare Category OID	Required if organization is asserted in Certificate subject.
policyIdentifier		1.3.6.1.4.1.41179.3.1	Required; DirectTrust Device OID
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 B: DirectTrust-eHealth Exchange Certificate Profile

Worksheet B: DirectTrust-eHealth Exchange 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 either the full name of the state or province or in conformance with the second part (Subdivision name) of the corresponding ISO 3166-2 code.
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)		US	Required; Two letter country code in conformance with ISO 3166-1
stateOrProvinceName (2.5.4.8)		(Optional)	Optional; If expressed, must be either the full name of the state or province or in conformance with the second part (Subdivision name) of the corresponding ISO 3166-2 code.
localityName (2.5.4.7)		(Optional)	Optional
organizationName (2.5.4.10)		<Subscriber Org Name>	Required
organizationalUnitName (2.5.4.11)		<Choice>	Required; Either NHIN-Test (VALIDATION) or NHIN (PRODUCTION); Additional OU values may also be present
commonName (2.5.4.3)		Fully Qualified Domain Name (FQDN) of the End Point.	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	
keyEncipherment		1	
dataEncipherment		0	
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		
dNSName		Domain Name	Required; Domain Name expressed as a dNSName, e.g. abc.example.com
certificatePolicies	FALSE		
policyIdentifier		1.3.6.1.4.1. 41179.0.2.0	Required; DirectTrust CP OID
policyIdentifier		1.3.6.1.4.1.41179.1.5	Required; DirectTrust Identity Level of Assurance OID for IAL2
policyIdentifier		Healthcare Category OID	Required if organization is asserted in Certificate subject.
policyIdentifier		1.3.6.1.4.1.41179.3.1	Required; DirectTrust Device OID
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			