Corda Network Certificate Profile

12 March 2021

Purpose

This document provides the reference for the Certificate Profile, as a component part of the Certificate Policy for the Corda Network.

Certificate Hierarchy

The diagram below illustrates the certificate hierarchy of the Corda Network. The PKI (Public Key Infrastructure) is separated into two components:

- Corda Network certificates which are issued and operated by the Corda Network Foundation (currently R3).
- Corda Node certificates which are issued by the node and controlled by the node operator.

Certificate Cipher Suite and Algorithms

The table below lists the cipher suite and algorithms required by each certificate in the Corda certificate hierarchy.

Certificate	**Cipher Suite**	**Signature Hash**	**Parameters**	**Lifetime**	**Notes**
Corda Foundation Root CA	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Permanently offline
Subordinate (Issuing) CA	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Online subordinate root
Doorman CA	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Network CA (Issues Node certificates)
Network Map	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Signs the Network Map & Network Parameters
Service Identity	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Notary Signing Key

Certificate	Cipher Suite	Signature Hash	Parameters	Lifetime	Notes
Node CA	ECDSA with SHA-256	SHA-256	ECDSA_P256	20 years	Must contain Name Constraint extension
Legal Identity	ECDSA with SHA-256	SHA-256	ECDSA_P256	*20 years	
Node TLS	ECDSA with SHA-256	SHA-256	ECDSA_P256	*20 years	Expiration defined by node operator
Confidential Identity	ECDSA with SHA-256	SHA-256	ECDSA_P256	-	Deprecated

** Node Legal Identity and TLS certificates are issued by the Node CA. The lifespan of these certificates is defined by the node operator, but by default will have the same lifespan as the issuing NodeCA.*

Certificate Profiles

The following section provides the certificate profiles of all certificates in the Corda Network

Root CA Certificate

Extension	Status	Constraints
basicConstraints	**CRITICAL**	This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present
keyUsage	**CRITICAL**	This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
certificatePolicies	**NOT PRESENT**	This extension SHOULD NOT be present
extendedKeyUsage	**NOT PRESENT**	This extension MUST NOT be present

Subordinate CA Certificate

Field	Status	Constraint
certificatePolicies	REQUIRED	This extension MUST be present and SHOULD NOT be marked as critical REQUIRED certificatePolicies:policyIdentifier OPTIONAL certificatePolicies:policyQualifiers:policyQualifierId OPTIONAL certificatePolicies:policyQualifiers:qualifier:cPSuri
cRLDistributionPoints	REQUIRED	This extension MUST be present and SHOULD NOT be marked as critical It MUST contain the HTTP URL of the CA's CRL service
authorityInformationAccess	REQUIRED	With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked as critical It MUST contain the URL of the issuing CA's OCSP responder (access method = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366]
basicConstraints	CRITICAL	This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present
keyUsage	CRITICAL	This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Issuing CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
nameConstraints	OPTIONAL	If present, this extension SHOULD be marked critical
extkeyUsage	OPTIONAL	For Subordinate CA Certificates to be Technically constrained in line with section 7.1.5, then either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present**

All Certificates

All certificates issued under a Corda Subordinate CA must have the following common property:

Field	Status	Constraint
certRole (1.3.6.1.4.1.50530.1.1)	**REQUIRED**	This extension MUST be present and SHOULD NOT be marked as critical certRole is a custom X.509 extension. It has been registered with OID 1.3.6.1.4.1.50530.1.1

Corda uses a custom X.509 extension to represent the purpose of each certificate in the Corda PKI. This extension is referred to as the *Certificate Role* and has an OID of 1.3.6.1.4.1.50530.1.1. The extension contains a single ASN.1 integer which defines the certificate's role.

Certificate Role	Value	ASN.1 encoding
Doorman CA	1	02 01 01
Network Map	2	02 01 02
Service Identity	3	02 01 03
Node CA	4	02 01 04
TLS	5	02 01 05
Legal Identity	6	02 01 06
Confidential Identity	7	02 01 07

Doorman CA

Field	Status	Constraint
basicConstraints	**CRITICAL**	This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field MAY be set to 2
keyUsage	**CRITICAL**	This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Doorman CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
certRole (1.3.6.1.4.1.50530.1.1)	**REQUIRED**	This extension MUST be present and SHOULD NOT be marked as critical certRole is a custom extension with OID 1.3.6.1.4.1.50530.1.1 It SHOULD contain the value 02 01 01 which corresponds to DOORMAN_CA

Network Map

Field	Status	Constraint
basicConstraints	OPTIONAL	If present, the CA field MUST be set to false
keyUsage	CRITICAL	This extension MUST be present and MUST be marked critical. The Bit position for digitalSignature MUST be set.
certRole (1.3.6.1.4.1.50530.1.1)	REQUIRED	This extension MUST be present and SHOULD NOT be marked as critical certRole is a custom extension with OID 1.3.6.1.4.1.50530.1.1 It SHOULD contain the value 02 01 02 which corresponds to NETWORK_MAP

Service Identity

Field	Status	Constraint
basicConstraints	OPTIONAL	If present, the CA field MUST be set to false
keyUsage	CRITICAL	This extension MUST be present and MUST be marked critical. The Bit position for digitalSignature MUST be set.
certRole (1.3.6.1.4.1.50530.1.1)	REQUIRED	This extension MUST be present and MUST be marked critical. certRole is a custom extension with OID 1.3.6.1.4.1.50530.1.1 It SHOULD contain the value 02 01 03 which corresponds to SERVICE_IDENTITY

Node CA

Field	Status	Constraint
basicConstraints	CRITICAL	This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field MAY be set to 1
keyUsage	CRITICAL	This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Node CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

Field	Status	Constraint
nameConstraints	CRITICAL	This extension MUST be present and MUST be marked critical. Permitted Subtree MUST be present REQUIRED DirectoryName MUST be present and should contain the X.500 distinguished name of the node - it's 'Legal Identity' in the Corda Network Excluded Subtree SHOULD NOT be present
certRole (1.3.6.1.4.1.50530.1.1)	REQUIRED	certRole is a custom extension with OID 1.3.6.1.4.1.50530.1.1 This extension MUST be present and SHOULD NOT be marked as critical It SHOULD contain the value 02 01 04 which corresponds to NODE_CA