Corda Network CRL Profile

15 March 2021

Purpose

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

CRL endpoints

Certificate	**CRL endpoint**
Root	none
Subordinate (CNA 1)	http://crl.corda.network/cnrc.crl
Doorman	http://crl.corda.network/cna1.crl
Node CA	http://crl.corda.network/doorman.crl
Node TLS	http://crl.corda.network/nodetls.crl

TLS Revocation Status

Certificate revocation in Corda currently applies to the TLS certificate chain only. Revocation status is validated on peer-to-peer (P2P) connections between nodes. For every P2P connection (for both peers) every certificate in the TLS chain is validated against the corresponding CRL (certificate revocation list) in this order:

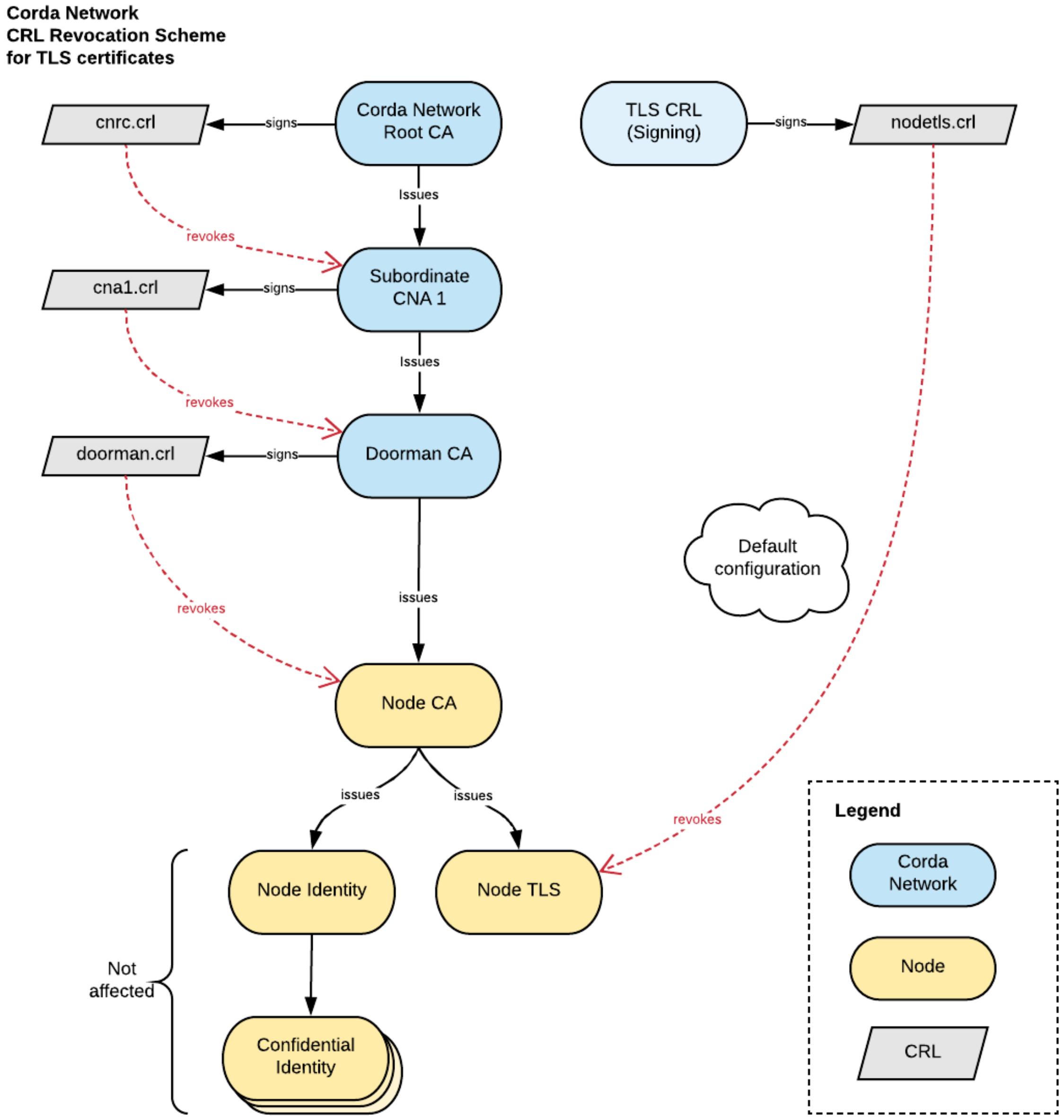
1. Node TLS
2. Node CA
3. Doorman
4. Subordinate
5. Root

Legal Identity Revocation

Note that the revocation status of Legal Identity and Confidential Identity certificates are enforced in Corda 4.

CRL hierarchy

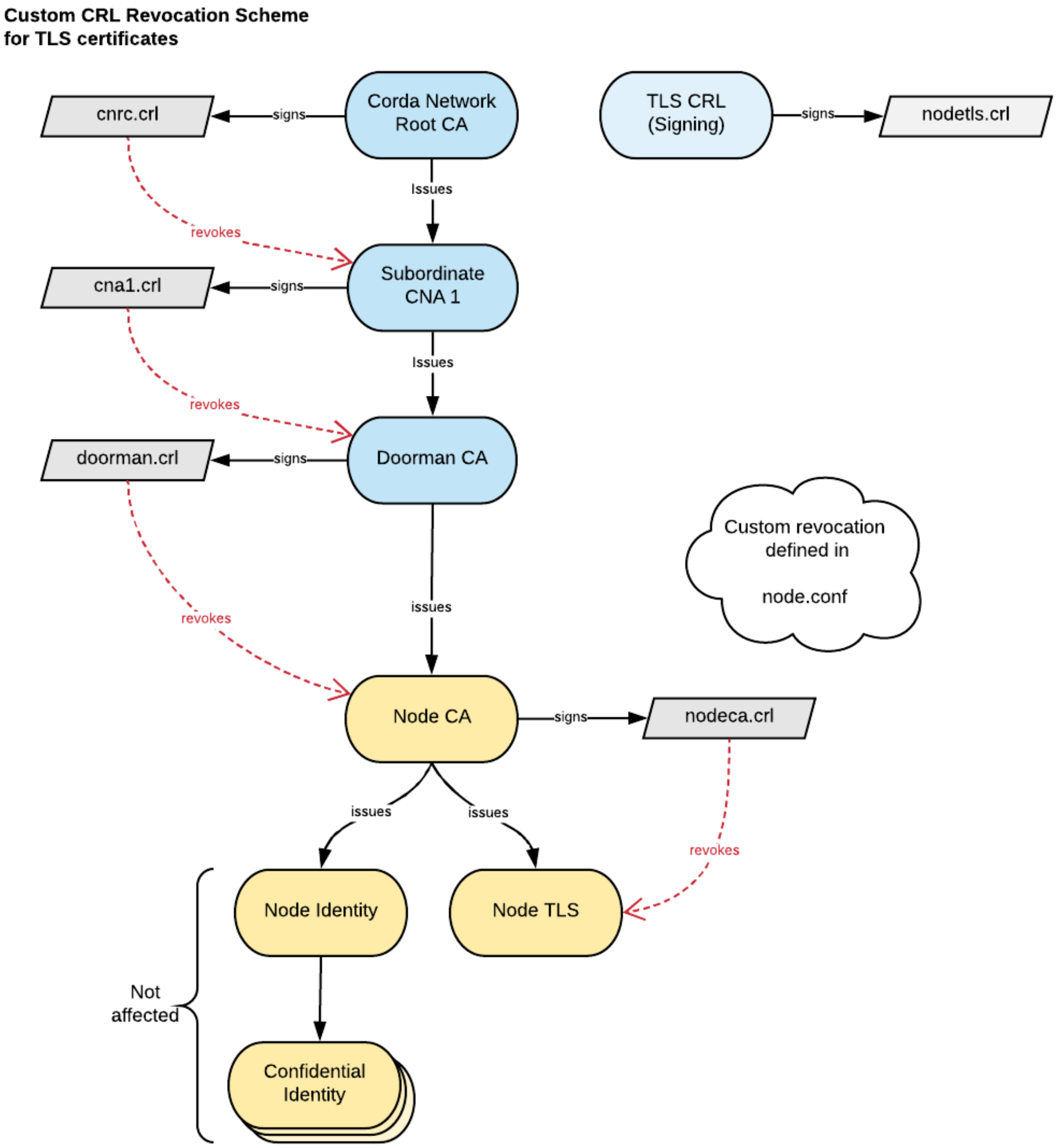
The image below depicts the CRL revocation scheme as defined by the Corda PKI. This is the default configuration that a node will use.



Custom CRL Specification

Nodes can be configured (via node.conf) to specify a custom CRL endpoint for the node TLS certificates. This allows a node operator to control the revocation station of node TLS certificates.

When a node is configured in this way, the CRL scheme will look the image below:



Revocation Process

Node CA

The Network Operator has the ability to revoke Node CA certificates issued by the Doorman. Revocation of a Node certificate also revokes all certificates issued below the Node CA:

- Node TLS
- Legal Identity
- Confidential Identities

Note that the revocation status of the Identity and Confidential Identity certificates is not enforced by Corda.

Node TLS

Whilst the Network Operator technically has the ability to revoke a node's TLS certificate under the node's *default configuration*, this is not a process that the Network Operator expects to perform. The nodetls.crl endpoint will be empty and exists purely to allow the normal operation of TLS communications in a Corda node.

Node operators can choose to host their own revocation endpoint by specifying this in the node's configuration. Under this operating model, Node TLS certificates cannot be revoked by the Network Operator and can only be revoked by the node operator. The Network Operator would still have the power to revoke a Node CA certificate, but this would have no impact on the node's TLS certificate.