Joining Corda Network

A User Guide

Nigel King
October 2018

Draft - work in progress

Joining the Corda Network

This document provides guidance for Node Operators to connect their nodes to the Corda Network. It assumes the Node Operators have:

1. Agreed to licence the Corda Software (Corda, Corda Enterprise) under the appropriate licence.
2. Know which Corda Network environment they wish to join (Corda Production Network, Corda Testnet).
3. Have access to at least one CorDapp that they wish to deploy with the Corda Node.
4. Have conducted the appropriate change management activities within their organisation to authorise set up and operation of the Node.
5. Can supply a dedicated IP address for communications with their node (typical network configurations are described at Corda Firewall.

Introduction

Corda Network participation requires each node to possess a recognised Certificate Authority (CA) certificate (or "Participation Certificate"), which is used to derive other digital certificates required by the node (legal entity / signing certificate, TLS certificate).

The Node CA certificate provides a recognised, human-readable Distinguished Name (DN) for the entity which can be used as a reference in transactions between nodes. The Node is considered a CA in its own right as it issues its own certificates. Node CA certificates must be issued by the Corda Network Manager (Doorman / Network Map), which guarantees that each Distinguished Name (and hence its corresponding public key) is uniquely held by a single party within the network.

In effect, identities are marked by public keys in Corda (only a public key is stored on ledger states, for example), and the identity service enables certificates to be found from public keys. There is a 1:1 binding between the node CA identity and the node. This is explained more at the Identity page on Corda docs.

A Certificate Signing Request (CSR) is a formal request for a node CA certificate conferring ownership of a DN. The CSR is created by the Corda node during its initial registration process, based on information supplied in the node's configuration file (node.conf).

The CSR contains the following information:

- The proposed DN
- A public key for the certificate to be generated. This key, and its corresponding private key, are generated during the initial registration process
- A contact email address
- A signature over the above data using the private key, corresponding to the public key in the CSR

Corda nodes may be operated by third parties, such as Business Network Operators, on behalf of Participants. There may be various forms of contractual relationship between such third parties and participants and such relationships will not generally be known to the Corda Network Operator. It is expected that ownership of ledger assets is defined by the legal entity name included in the signing certificate of the node and applied to states on the ledger, and Doorman checks are to ascertain that an accurate, valid and unique legal name is always assigned to such certificates.

Where a third party is hosting the node and even possibly operating the signing processes on behalf of the Participant, the Corda Network will still consider the Participant to be the name included in the Certificate Signing Request, and will need to know that the same Participant has signed the Terms of Use.

The term 'sponsoring' refers to occasions where a third party sets up and operates a node on behalf of one or more Participants and provides assurance to the Corda Network Operator that:

1. The third party is entitled to operate on behalf of the Participant in setting up and operating its node, putting in place suitable means by which the Participant can control and approve the node operations occurring on its behalf
2. The third party has taken the necessary steps to ensure that the Participant has read and agreed to abide by the Corda Network Terms of Use
3. Ledger records on the node being operated by the Third Party are beneficially owned by the named entity on the Participation Certificate
4. The Participant has been accurately identified and the name on the Participant Certificate is the correct legal name of the entity owning the ledger states

A Sponsor may or may not host the node itself, which could be outsourced to another party (such as a cloud provider).

Sponsors typically wish to manage their own customer relationships and so communications between the Corda Network Operator and the underlying Participant should go via the Sponsor. Typically this means that the contact name on the Certificate Signing Request is of an employee of the Sponsor. Corda Network Support will also be provided via the Sponsor.

Sponsors will be required to provide evidence that they have obtained sufficient approval from the Participant to act upon their behalf.

Sponsored Participants may also operate their own on-premise nodes, in this case the Business Network Operator or other third party can still manage the signing of Terms of Use, communications, and support relationships but this will require some manual co-ordination with the Corda Network Operator (see below) to align such sign-offs with the node set-up procedure being operated by the Participant itself.

If a third party is acting in an agency relationship for its customers it may choose to set up nodes in its own name, in this case the Participant shall be the agent, and its nodes denoted appropriately with the OU field to distinguish them (see below).

A summary of these relationships is shown in the table below. Participants may act in more than one mode if running more than one node (see below).

Model	**Node Identity**	**Node Operator**	**Corda Network Operator Primary Relationship**
Direct	Participant	Participant	Participant
Sponsored on-premise	Participant	Participant	Sponsor
Sponsored hosted*	Participant	Sponsor	Sponsor
Agency	Agent	Agent	Agent

* It remains to be seen how often this model will be deployed in practice due to the need for the Sponsor to hold signing keys for the Participant.

Business Networks

The primary Corda Network model is for Participants to run a single node regardless of how many CorDapps they run. A Participant may join several business networks, each with their own specific membership list (owned and managed by the network itself) and each using a separate CorDapp. However, for system management reasons, Participants may use different nodes to join such networks. This complicates the Doorman checks described here since Corda assumes one node per Participant.

Although not ideal, in the initial stages of the life of the Corda Network, the Doorman will implement manual checks to ensure that Participant entities operating more than one node use DNs with the same root, and we will allow a suffix to denote the different uses of each node (the business networks). Note: the suffix will not be the same as the UUID used to denote privacy of business networks.

Environments

Corda Network comprises several distinct environments for both production and non-production use. Node Operators must determine in advance, in consultation with the Corda Network Operator, the most appropriate environment to use within a given context. Each environment represents a completely separate network (Compatibility Zone) with separate Doorman and Network Map. A given node can only ever be a member of one environment.

There will only be one true Production network, where the appropriate physical and operational controls are in place to secure support for legally-binding contracts held on customer nodes (the ledger itself is distributed and not centralised at service entities). A condition of entry to the Corda Production Network is for each Participant to contractually confirm they have appropriate an security model in place around their node.

With respect to non-production environments in particular, no assumptions should be made regarding the resilience, long term retention of data or service levels, unless specifically agreed with R3.

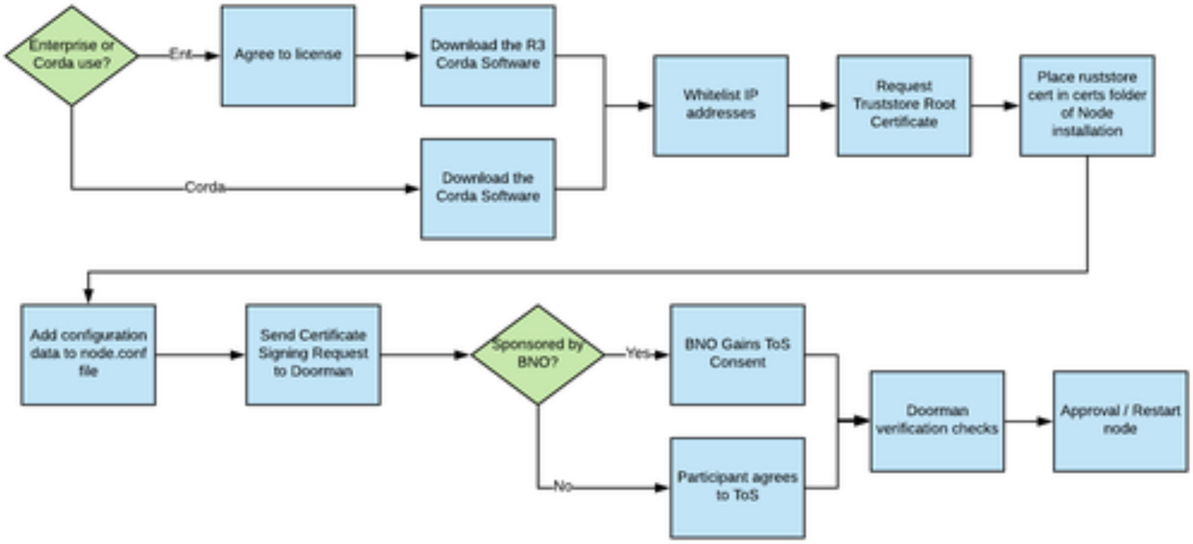
Prerequisites

The following items are essential before you can enlist a node to Corda Network:

- One or more physical or virtual machines upon which to deploy Corda, with compatible operating system and a compatible Java version (e.g. Oracle JDK 8u131+).
- A static external IP address must be mapped to each machine on which Corda will be run.
- Signed Corda Network Terms of Use returned to R3.
- The Corda Software - either Corda Enterprise (license from R3) or Corda (Open Source).
- A root trust certificate for you to verify the source (R3) of returned participation certificates.

Step-by-Step overview

1. Obtain the Corda Software
2. Whitelist your IP address(es)
3. Request the root trust certificate (truststore.jks file)
4. Start up a node
5. Configure the Node, including adding your Distinguished Name
6. Run the initial registration - this sends a CSR to the Doorman
7. Participant signs the Corda Network Terms of Use
8. Doorman verification checks occur
9. Completion


Enterprise or Corda use?
Ent
Agree to license
Download the R3 Corda Software
Corda
Download the Corda Software
Whitelist IP addresses
Request Truststore Root Certificate
Place ruststore cert in certs folder of Node installation
Add configuration data to node.conf file
Send Certificate Signing Request to Doorman
Sponsored by BNO?
Yes
BNO Gains ToS Consent
No
Participant agrees to ToS
Doorman verification checks
Approval / Restart node

Step-by-step details

Step 1 – Obtain the Software

- ***Corda Enterprise:*** your designated R3 sales representative is responsible for giving you access to the software artefacts and set-up and configuration instructions

- ***Corda:*** Corda is an open source project. The source code is freely available in our Github repository under an Apache 2 license. Visit https://github.com/corda to access the software. Further guidance on setting up Corda is found here: https://docs.corda.net/getting-set-up.html

Step 2 – Obtain the Software

Access to Corda Network services is restricted to IP addresses from known partners who have signed the appropriate commercial agreement. Hence, Node Operators will need to determine the IP address(es) or range associated with their Corda deployment, and advise R3 of these prior to raising Certificate Signing Requests. Please send your IP address(es) to 'Corda Network Onboarding' - doorman@r3.com.

Step 3 – Request the root trust certificate (truststore.jks file)

Please request the root trust certificate by emailing 'Corda Network Onboarding', doorman@r3.com. The file will then be transferred to you. You should copy this file to the certificates folder of your Corda directory. Corda nodes reference the root trust certificate chain for every signature they resolve.

Step 4 – Start the node

Deploying a node - Your designated Corda sales representative is responsible for ensuring you have the correct information to enable you to follow the instructions outlined.

Step 5 – Configure Node.conf

As explained in Configuring a node, a node.conf file must be included in the root directory of each corda node.

5.1 Specifying a contact email address

An email address must be specified in the node.conf in relation to the CSR. This email address is retained by the Corda Network Operator for the purposes of contact in relation to identity checks and any administrative issues. It is **not** included in the certificate. The email address should belong to a suitably empowered employee of the Node Operator organisation.

5.2 Guidance on choosing a Distinguished Name

A Distinguished Name (DN) must be unique within the Corda Network. The DN is comprised of separate fields as per the table below. Only O and OU are used for the identity uniqueness check, and the other fields are considered as attributes of the identity.

All data fields must adhere to the following constraints:

- Only uses Latin, common and inherited unicode scripts
- Upper-case first letter
- At least two letters
- No leading or trailing whitespace
- Does not include the following characters: , , = , $, " , ' , \
- Is in NFKC normalization form
- Does not contain the null character

	Mandatory	**Length (chars)**	**Validation**	**Purpose**
Common Name (CN)	N	64	As per above	Available for use by the node operator for their own internal purposes. Often used for home website urls in WWW.
Organisation (O)	Y	128	As per above, and additionally: No double-spacing. May not contain the words “node” or “server”.	Used to define the owning organisation of the node / certificate. In general internet usage, the Organisation usually denotes the highest level parent company, e.g. ABC group. In the Corda Network, we are using the O field for the legal entity which will be the beneficial owner of states on the ledger. IT should therefore be set to the ***legal nam***e of the participant organisation as it appears on the official trade register within the jurisdiction in which the entity is registered.
Organisation Unit (OU)	N	64	As per above	This field is generally used to denote sub-divisions or units of the organisation. In the Corda Network, this field may be used by node operators for internal purposes to separate nodes used for different purposes by the same legal entity.

Locality (L)	Y	64	As per above	The city or town in which the registered head-office of the legal entity is located. If the company operates from New York City but is registered in Wilmington, Delaware then please use Wilmington
Country (C)	Y	2	2-digit ISO code	The country in which the registered head-office of the legal entity is located.
State (S)	N	64	As per above	If your country operates a State or Province system (e.g. USA and Canada) please add the State in which the registered head-office of the legal entity is located. Do not abbreviate. For example, "CA" is not a valid state name. "California" is correct. If the company operates from New York but is registered in Delaware, please use Delaware

Note: The above fields do not allow sponsors to denote their service relationship with the node owner in the current implementation. Further support for sponsors will be delivered in future releases. Records of sponsoring relationships will be held manually by the Corda Network Operator for the time being.

The X509 standard does not impose much constraint on what can be included in these fields. The Corda Network Governing Body owns standards for Network Participants to follow in the creation of Certificate Signing Requests. At this stage the Corda Network Operator operates rules and guidelines as described in the table above.

The above fields must be populated accurately with respect to the legal status of the entity being registered. As part of standard onboarding checks for Corda Network, R3 may verify that these details have been accurately populated and reject requests where the population of these fields does not appear to be correct.

5.3 Specify URL For Initial Registration

For Corda Network, it is http://join.cordaconnect.org/ED5D077E-F970-428B-8091-F7FCBDA06F8C. This needs to be added to the node.conf at the end of the file:

```
compatibilityZoneURL=http://join.cordaconnect.org/ED5D077E-F970-428B-8091-F7FCBDA06F8C
```

Step 6 - Running the initial registration

Once the node.conf file is configured, the following should be typed to the command line "java -jar <corda jar file> --initial-registration". This will send a CSR (with the relevant DN and email) to the Network Manager service (Doorman / Network Map). A message similar to the below will be printed to the console:

```
Legal Name: O=ABC LIMITED, L=New York, C=US

Email: john.smith@abc.com


Public Key: EC Public Key

            X: d14bc17e650f2a317cbcb95e554f1e26808ca80f67ab804bbc911ec16673abbd

            Y: 1978b02a8e693ecd534ceef835091c376cfc4e506decc69b91a872fc13ad1aeb


-----BEGIN CERTIFICATE REQUEST-----

MIIBLTCBywIBADBMMQswCQYDVQQGEwJVUzERMA8GA1UEBwwITmV3IFlvcmsxFjAU

BgNVBAoMDVIzIEhvbGRDbyBMTEMxEjAQBgNVBAsMCUM4MTUyOTE2NzBZMBMGByqG

SM49AgEGCCqGSM49AwEHA0IABNFLwX5lDyoxfLy5XlVPHiaAjKgPZ6uAS7yRHsFm

c6u9GXiwKo5pPs1TTO74NQkcN2z8TlBt7Mabkahy/BOtGuugHTAbBgkqhkiG9w0B

CQExDgwMYWRtaW5AcjMuY29tMBQGCCqGSM49BAMCBggqhkjOPQMBBwNHADBEAiBA

KLF4NLrleNZPKMoxBrr/80fE3kVbFnYtkB2h0JhX1gIgPcV0X0xZQug+njKCyKgf

DkNUdQJPqhkBBEpgVqyZmE8=

-----END CERTIFICATE REQUEST-----

Submitting certificate signing request to Corda certificate signing server.

Successfully submitted request to Corda certificate signing server, request ID:
6CBB63558B4B2D9C94F8C14AB713432F60AF692EB30F2E12E628B089C517F3CF.

Start polling server for certificate signing approval.
```

Important: the Request ID given in the above should be noted and kept safe for future reference. You may need it in the event of a Certificate Revocation Request, for example.

At this point, the node begins automatically polling an endpoint on the Network Manager (Doorman / Network Map). It does this without an action required by the Node Operator and does so at regular intervals in anticipation of a certificate being made available to it for download.

The Node Operator may, if preferred, terminate the process, e.g. in the course of shutting down the machine; this will not cancel or otherwise invalidate the (now pending) CSR. Re-starting the node will cause it to resume polling for a completed certificate.

Step 7 – Participant Signs Terms of Use

- Sponsored model: A Business Network Operator (BNO) requesting approval for a certificate on behalf of the Participant
- Direct model: The Participant requesting a certificate for themselves

Sponsored

As a BNO you will ensure the Node Users/Participants have signed the Terms of Use before they transact on Corda. Please email doorman@r3.com providing assurance that the Node User/Participant has signed the Terms of Use. You may do this as a batch email if you have multiple CSRs in flight. You must specify the precise Distinguished Name in order to confirm that the correct entity has signed and the right certificate will be granted.

Direct

Please go to https://legal.corda.net and complete the Terms of Use. A notification will automatically be sent to the Doorman upon completion.

Step 8 – Doorman verification checks

Upon receipt of a CSR, R3 will conduct a number of identity-related checks before issuing a certificate:

1. The DN accurately reflects a real-world legal entity registered with an appropriate trade register
2. The relevant Business Network Operator has a valid legal agreement with R3
3. The Node Operator (participating entity) has signed the Corda Network Terms of Use
4. The email address provided is valid
5. The owner of the email address is aware of / approves the CSR

Important

- All checks are performed at the discretion of R3. Checks may be supplemented with additional checks as required.

- Identity checks do **not** constitute formal Know Your Customer (KYC) or Enhanced Due Diligence (EDD) checks. Node operators and their users are responsible for carrying out appropriate due diligence on any participant in relation to transactions performed via Corda Connect; all associated liability in relation to this is disclaimed by R3.

Email contact

Identity checks will require R3 to contact the owner of the email address provided in the CSR. It is important that the owner of this email address is aware of and prepared to respond to contact from R3 in relation to identity checks, and that they are able to do so on a timely basis. Inability for R3 to contact and obtain suitable responses from the email address owner may delay or result in rejection of the CSR.

Communications will be sent from 'Corda Network Onboarding' (doorman@r3.com). The email owner should ensure this address is whitelisted by their email provider. Enquires not received in English may take longer to process.

Status enquiries

Parties wishing to enquire as to the status of their CSR should contact doorman@r3.com in the first instance. Enquiries should reference the request ID of the relevant CSR (e.g. "6CBB63558B4B2D9C94F8C14AB713432F60AF692EB30F2E12E628B089C517F3CF"). Enquires not received in English may take longer to process.

Step 9 – Completion

Once identity checks have been completed, a signed node CA certificate will be released by the Network Manager (Doorman / Network Map) to the Node. A node in polling mode will automatically download and install the certificate in its local trust store. It will also automatically generate additional identity and TLS certificates from the node CA certificate, which are required for subsequent operation of the node.

At this point, the node will terminate and will need to be restarted. Type "java -jar <corda jar file>" into the command line. Once restarted, the node will then proceed to download the network map and discover other nodes within Corda Connect.

About R3

R3 is an enterprise software firm working with a network of over 200 banks, financial institutions, regulators, trade associations, professional services firms and technology companies to develop Corda, its blockchain platform designed specifically for businesses. R3's global team of over 160 professionals in nine countries is supported by over 2,000 technology, financial, and legal experts drawn from its global member base.

Learn more at r3.com and corda.net

Locations

New York
11 West 42nd Street, 8th Floor, New York, NY 10036

London
2 London Wall Palace, London, EC2Y 5AU

Singapore
80 Robinson Road, #09-04 Singapore, 068898