Corda Network Service Level Agreement (SLA)

Production Environment

June 2019

1.0 Introduction

This document defines standard Service Levels offered by the Corda Network Foundation (CNF) for organisations operating live on the Corda Network.

Corda Network operates under a single set of rules and policies set by Corda Network Foundation's Board of Directors, which is comprised of its earliest customers. Further details are available at https://corda.network. The Foundation appoints an operator of the network, who undertakes all day-to-day activities associated with delivering the network services described in Section 2 of this document. The operator is currently R3.

Users of Corda Network applications (CorDapps) in any jurisdiction will need to ensure that their usage of the Corda Network complies with any local rules and legislation to which they are subject. Corda Network will support real-world assets, real-world identities and legally enforceable contracts between counterparties. Data will be long-lived and immutable. As such, the security model for Corda Network is consistent with the high value (and risk) of the activities being undertaken by its participants.

This document defines:

- Services included in the Corda Network
- The appropriate service levels for each service
- Actions on non-performance / remediation

Corda Network participants accept the service levels contained within this document upon signing of the Corda Network Terms of Use, unless otherwise stipulated in such Terms of Use.

Scope

This document applies only to the Corda Network production environment and its constituent services as described in this document, and not to any other environments operated by the Foundation or the Operator.

Assumptions

- Available to all participants of Corda Network – as defined on https://corda.network
- Support processes and incident severity levels are detailed in bespoke support agreements or the Corda Network Support Handbook held on https://corda.network.
- Expected participant and transaction volumes for the period of use have been previously communicated to CNF and agreed as suitable for this standard SLA.
- A start date for usage of the services has been agreed at least 4 weeks in advance.
- Specified services are supplied to all participants of the Corda Network.
- Direct participants may operate more than one application within Corda Network and the Service Levels described here apply to each

2.0 Service Descriptions

For the most up to date, detailed information about the services which Corda Network Foundation provides, consult: https://corda.network/about/concepts.html

3.0 Service Levels

3.1 General information

- Business working days include any normal working day, i.e. excluding weekends and bank holidays, in the territories of the United Kingdom, United States and Singapore
- Normal business hours are considered from **00:30 UTC+0 - 21:30 UTC+0** on any business working day
- All service levels defined herein apply only during normal business hours

3.2 Performance

The following SLAs and performance levels will apply during the term of Participants membership agreement of Corda Network.

Identity Manager

Turnaround of certificate signing requests (CSRs) is measured from the time of receipt of a correctly formatted signing request by the CNF Identity Manager to the time at which a response is submitted to the requesting node. The Identity Manager process can handle multiple certificate signing requests in parallel.

Unless the Participant is being sponsored onto Corda Network by a Business Network Operator with whom such agreement is in place with CNF, the Identity Manager process requires the participant to respond to a confirmation request. Service levels quoted here for turnaround time specifically exclude the duration of such participant response.

The Identity Manager may reject the certificate signing request if the data is not constructed according to the standards set out in the User Guide. Amended CSRs will be subject to the same SLAs as new certificate signing requests.

Participants requesting re-certification, either to generate new keys, or to amend information on an existing and valid certificate, will start a new node and request a new certificate in exactly the same way as the original certificate and this will be subject to the same service levels. The Distinguished Name of the new identity must be unique (not the same as the previous identity).

Details such as the IP address of the node, can be changed without re-certification by sending a new configuration file directly to the Network Map server.

The service levels below are dependent on receiving a correctly formatted CSR.

- **95%** of valid (see User Guide) Certificate Signing Requests (CSR) will be completed within **2 business working days,** excluding wait time for responses to confirmation requests from the participant or Business Network Operator
- **95%** of valid (see User Guide) Certificate Revocation Requests (CRR) to the Identity Manager from a Business Network Operator or a participant will be processed within 2 business working days, excluding wait time for responses to confirmation requests from the participant or Business Network Operator

Network Map Service

Turnaround of Network Map updates as a result of successful certification of a new node is measured from the time a certificate is issued from the Identity Manager, to the time at which the updated Network Map is placed upon on the distribution site(s). Participants are responsible for updating their own nodes with the revised information.

- **95%** of Network Map updates for new nodes will be completed within 1 hour of the CSR being approved by the Doorman
- **95%** of Network Map updates for revoked nodes will be completed within 1 hour of the CRR being executed by the Doorman
- **95%** of IP address changes will be added to the network map within 15 minutes of the network map server receiving the new information from the relevant participant node

Notary

The turnaround time for transaction notarization request is measured from the inbound request is received on CNF infrastructure to the point at which the reply leaves CNF infrastructure and assumes correctly formatted and structured notarization requests.

Notarization requests are treated individually, in sequence of receipt, by the notary working from an inbound queue. The speed of processing of requests depends on the complexity of the transactions received, in particular the number of input states.

- **99%** of transactions with 5 or less input states will be notarised within 60 seconds of the receipt of a valid notarization request
- **99%** of transactions with 10 or less input states will be notarised within 120 seconds of the receipt of a valid notarization request
- **99%** of transactions with 15 or less input states will be notarised within 240 seconds of the receipt of a valid notarization request
- The number of transactions for which an incorrect response is given by the notary (input state consumed but indicated as not consumed and vice versa) will be less than 1 in 100,000,000

3.3 Availability

Uptime

- Each service will operate with **99% availability** during normal business hours
- On UK, US and Singapore bank holidays availability is not supported during the normal office hours of the impacted location(s): (08:30 to 17:30 in local time – adjusted for seasonal variation)

Scheduled Downtime / Service Window

- Maintenance will be carried on outside of normal business hours and notified 5 business days in advance to node operators (via the contact contained in the CSR for the node unless separately advised to doorman@r3.com

Unscheduled Downtime

- Any unavailability of services during normal business hours will be treated as an incident and managed according to the service levels defined in the Corda Network Support Handbook
- Urgent maintenance, for example as a result of real or perceived security threats requiring immediate action, or in order to prevent more severe disruption to services before the next maintenance period that may require cessation of services during normal business hours will be flagged on https://corda.network and executed immediately. All reasonable attempts will be made to avoid such unscheduled downtime.

Back-ups

- Back-ups will occur daily overnight from the hours of 02:00 UTC+0 to 03:00 UTC+0

Recovery Time Objective

- In the event of a failure of any service the recovery time objective will be 2 hours (within normal business hours) from the point of detection.
- CNF cannot guarantee any particular fix meets this objective but will issue hourly updates on progress on https://corda.network

Recovery Point Objective

- In the event of a failure, data will be recovered to the point of last backup
- Transactions occurring after the previous back-up may need to be replayed to the notary and node operators should retain this facility

3.4 Data Retention

- Business data created in the Corda Network environment as a result of customer activities under this agreement will be held by customer nodes and CNF databases supporting the Notary, Network Map and Identity Manager services.
- At the end of the term of Corda Network membership of the participant CNF retains the right to remove such data held in its own databases
- Such data as CNF holds can be retained if agreed at least 30 days in advance of the end of the membership period, and subject to separate commercial negotiation (a reasonable fee will apply, based on CNF's assessment of incremental costs)

3.5 Release Management

- CNF operates a single Corda Network production environment. It is important that Corda Network is able to take advantage of new releases without undue delay and so the normal mode of operation is for services to be regularly upgraded to the latest Corda platform version.
- Corda Network platform version upgrades will not normally require customer nodes to upgrade and will be invisible to users.
- Corda Network upgrades that also require Corda Network participants to upgrade are subject to customer acceptance as defined in the flag day process (see User Guide and also section below).
- CNF will post intention to upgrade its own services one calendar month in advance of the event on https://corda.network and will conduct its own testing in a separate environment before making the upgrade. Customers will be invited to support such testing by operating test nodes in such an environment. It may not be possible to test with every CorDapp, nor should it be necessary
- CNF will make the upgrade on a specified day published on https://corda.network as per the notification period above. Customer services will not normally be impacted. In the rare event of issues arising, they will be handled as per the Corda Network Support Handbook.

3.6 Network Parameter Updates

- All Corda Network participants have agreed to operate with a common set of network-wide parameters that each of their nodes downloads alongside the Network Map.
- From time to time these network parameters need updating.
- The update process incorporates a node polling activity that ensures all node operators see the requested changes in advance and can vote to accept / not accept.
- CNF will consult with customers should there be disagreement over the proposed changes but reserves the right to progress if the majority of participants are in agreement that it should go ahead and reasonable attempts have been made to address any concerns of participants rejecting the change.
- Further details can be found on: https://corda.network/policy/network-params-upgrade.html
- Many types of update processes will be entirely transparent to users, and can be executed during normal working hours. Updates will be advertised at least 10 working days in advance.
- Updates will be required whenever the following occur:
    - A new public notary is added to the environment
    - A participant whitelists a new contract
    - The minimum platform version is upgraded
    - The maximum message and / or transaction sizes are increased
    - The network epoch value is increased
    - The event horizon is changed (the amount of time a node can be un-contactable before being retired from the network)
- Where the update may require participant action, for example where the minimum platform version is increased and certain participants need to upgrade to meet the new minimum, full instructions will be communicated to node operators on https://corda.network
- Further details can also be found at https://www.docs.corda.net under Corda Networks / Network Map

3.7 Business Continuity

- CNF has fully redundant data center capabilities for all of its services, utilizing Microsoft Azure Cloud infrastructure.
- CNF has a disaster recovery policy which is reviewed and tested semi-annually.

- CNF has a comprehensive security policy incorporating specific security incident management procedures

4.0 Support

CNF supports Corda Network Services according to the service levels documented in the Support Handbook found on https://corda.network

Hours Of Service:

Support desk is open during normal business hours.

5.0 SLA reporting

5.1 SLA Reporting

Performance against SLAs defined in this document will be reported on the Corda Network Foundation website within 5 business working days of the end of each calendar month.

SLA reporting will not be customer specific and will not include any identifiable customer details.

5.2 In the event of SLA breach

- In the event of SLA breaches impacting individual customers they will be entitled to repatriation of fees for the specific service affected subject to the following:
    - For each service, a maximum of 100% of fees paid can be claimed in any one calendar year
    - Participant will be expected to provide reasonable evidence of each breach
    - Only one breach can be claimed in any one business day, per service
    - 10% of fees for any service can be claimed where >3 and <10 breaches occurred within the calendar year for which fees were payable
    - 25% of fees for any service can be claimed where >9 and <20 breaches occurred within the calendar year for which fees were payable
    - 50% of fees for any service can be claimed where >19 and <40 breaches occurred within the calendar year for which fees were payable
    - 100% of fees for any service can be claimed where >39 breaches occurred within the calendar year for which fees were payable