Corda Network Service Level Agreement (SLA)

User Acceptance Test Environment

January 2019

UAT Service Descriptions & SLAs

1.0 Introduction, Scope & Assumptions

This document defines standard Services and Service Levels offered by R3 LLC in operating User Acceptance Test (UAT) facilities for organisations testing Corda Network implementations ahead of on-boarding to the production Corda Network.

Participants who join Corda Network automatically accept these service levels, unless a separate agreement has been negotiated and put in place.

The difference between UAT, Production and Testnet environments is described below.

Corda Network UAT:

For owners of tested CorDapps with a firm plan to take them into production, a bespoke UAT environment is provided and operated by R3 where such CorDapps can be further tested in the network configuration they will experience in production, utilising relevant Corda Network Services (including Doorman and trusted notaries).

Corda UAT is not intended for customers' full test cycles, as it is expected that the bulk of CorDapp testing will occur in simpler network configurations run by the CorDapp provider, or operating within Corda Testnet, but is available for testing of functionally complete and tested CorDapps in realistic network settings to simulate the real-world business environment, including the production settings of network parameters, Corda network services and supported Corda versions.

UAT is therefore more aligned to the testing of the operational characteristics of networked CorDapps rather than their specific functional features, although we recognise there can be overlap between the two. Realistic test data is therefore expected to be used and may include data copied from production environments and hence representing real world entities and business activities.

It will be up to the introducer of such data to ensure that all relevant data protection legislation is complied with and, in particular, that the terms and conditions under which Corda Network Services processes such data is suitable for their needs. All test data will be cleared down from Corda Network Services on the completion of testing.

Corda Network Live:

Corda Network Live (Production) is a long-lived environment supporting real business activity conducted on the Corda Network. It will be a global network, governed by the independent Corda Network Foundation and operating under a single set of rules. Operators of 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, and the Foundation will seek to define a set of rules are not in conflict with such local rules or legislation, as far as is practicable. Corda Network Live 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 Live will need to be consistent with the high value (and risk) of the activities going on within its applications.

Corda Testnet:

An environment where any individual or company can experiment with Corda, set up and run a Corda node, create, find, deploy and test applications (CorDapps) and interact with other users of those CorDapps. Testnet is meant to be to all intents and purposes a mirror of the production Corda Network, with global participation and a kaleidoscope of participants, applications, business networks and service providers operating in a single network environment. It is fundamentally intended to be a play and practice area, with no surrounding legal framework, security model or other ability to support enforceable and safe business contracts or activity.

There will be no real world assets and any data entered through Testnet applications should be true test data and not represent real world entities. Any data entered to Testnet is at the risk of the entity entering such data and Corda Testnet provides no guarantees or SLAs around the security or longevity of such data. Corda Testnet is intended as a springboard for Corda Network Live, although it is not under the control of the Corda Foundation.

This document defines:

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

This Agreement is valid from date of issue of a Corda Network UAT participation certificate.

Scope

This document applies only to the Corda Network UAT environment and its constituent services as defined herein.

Assumptions

- Corda Network UAT Services are only available to licensed users of Corda Enterprise, those with separately negotiated Support agreements or Corda Triallists. Support processes and incident severity levels are detailed in bespoke support agreements or standard support user guide.
- Expected participant and transaction volumes for the period of use have been previously communicated to R3 and agreed as suitable for this standard SLA.
- Period of usage of the UAT environment will be agreed in advance. At the end of that period, in the absence of further agreement, participant certificates will be revoked and any data held by R3 removed from Corda Network UAT and returned to participant if previously agreed.
- A start date for usage of the services has been agreed at least 4 weeks in advance.
- Other participants may be accessing the specified services during the usage period.
- There is no limit to the number of CorDapps or business networks any particular participant can run or be part of in the Corda Network UAT environment, although each is subject separately to the terms of this agreement

2.0 Service Descriptions

DOORMAN

The Doorman Service controls entry and exit of participants to Corda Network UAT. Prospective participants request signed certificates from the Doorman to enable them to transact on Corda Network UAT. Participants with a certificate signed by the Doorman can use this to communicate their identity to other participants on Corda Network UAT. The Doorman asserts the uniqueness of the certificate and the Distinguished Name supplied by the Participant.

The participant will populate identity and other node configuration information to the Corda Node. During node start-up, the node will automatically send a certificate request to the Doorman for processing and poll for a completed request. The Doorman performs a series of screening checks on the entity before issuing a signed participation certificate to the participant.

The screening checks seek to establish the identity of the participant to a reasonable level of certainty and confirm that the individuals requesting the signed certificates are permitted to act on behalf of the participant. These checks should not be considered to be formal Know Your Customer (KYC)

or Enhanced Due Diligence (EDD) checks, and R3 will not assume any liability for the activity of participants on Corda Network UAT.

Rules for the correct construction of certificate signing requests are included in the User Guide.

R3 reserves the right to deny entry to Corda Network UAT via the Doorman at its sole discretion.

The Doorman also controls exit of participants from Corda Network UAT via the certificate revocation process. On the conclusion of the pre-agreed usage period, should the participant fail to abide by the Corda Network UAT Terms of Use, and or if the participant requests, participant certificates will be revoked and all relevant data removed from Corda Network UAT.

Participants may join Corda Network UAT directly or they may be sponsored by a Business Network Operator. In the latter case Participants should contact their Business Network Operator to understand the details of their sponsoring process.

NETWORK MAP SERVICE

The Network Map service maintains the routing information within Corda Network UAT which allows participants to find and transact with one another. The service receives routing information from the Doorman when new nodes are admitted to Corda Network UAT and then publishes the updated map to one or more sites from where existing Corda participant nodes can download the updated Network Map according to their own schedule.

The Network Map is an automated service accessed by participant nodes which maintain their own local copy of the Network Map. It is the local copy that nodes consult when proposing and responding to transactions.

The Network Map service updates the Network Map when participants enter and exit Corda Network UAT. The certificate revocation process will automatically update the Network Map. It is important to note that Participant Nodes need to download the Network Map before the certificate revocation takes effect for their node.

NOTARY

A notary is a network consensus service that attests that a given transaction has not already signed other transactions that consume any of the proposed transaction's input states, and is used in double spend protection.

Upon being asked to notarise a correctly constructed transaction, a notary will either:

- Sign the transaction – if it has not already signed other transactions consuming any of the proposed transaction's input states
- Reject the transaction and flag that a double-spend attempt may have occurred

In doing so, the notary supports transaction finalization in the system. Until the notary's signature is obtained, parties cannot be sure that an equally valid, but conflicting, transaction will not be regarded as the "valid" attempt to spend a given input state.

The R3 notary maintains a database of all input and output states that it has been notified of and their state of consumption. This data is not accessible by other nodes. Other nodes can only submit transactions containing explicit state references to be used as part of the transaction.

The included notary service is a crash fault tolerant, non-validating service with clustered nodes, run by R3 and operating a RAFT-like consensus algorithm. The particular algorithm being used is a proprietary version based on Galera (http://galeracluster.com/products/). It provides fault tolerance by distributing inbound notarisation requests across n nodes (5 in the current implementation). Any node can notarise and syncs its response with the other n-1 nodes. Requesting customer nodes will automatically retry a notarisation if it times out because the original node was down. The model therefore assumes all nodes are run by a trusted entity. The 5 nodes are distributed across three separate datacentres and the cluster will operate whilst at least three nodes are up and can create a quorum.

Further information on the notary operation and algorithm can be found on the Galera website.

3.0 Service Levels

This service level agreement applies during the period of access to Corda Network UAT agreed with R3 in advance of entry.

3.1 Performance

The following SLAs and performance levels apply as minimum standards of performance.

DOORMAN

Turnaround of certificate signing requests is measured from time of the acknowledged receipt of a correctly formatted signing request by R3 to the time at which we return a response onto the outbound network. The Doorman process can handle multiple certificate signing requests in parallel.

The Doorman process requires the participant to respond to a confirmation request from R3. R3 cannot control the timescale of such a response.

The Doorman 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 recertification, 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.

Details such as the IP address of the node, can be changed by sending a new configuration file directly to the Network Map server (see below).

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

- 95% of valid (see User Guide) Certificate Signing Requests will be completed within 2 working days provided the participant responds to the confirmation request within 24 hours, subject to the below
- A maximum of 50 certificate signing requests can be handled in parallel (across all participants in the environment) without impacting the above service level
- Should the number of outstanding CSRs exceed 50 in any one period the corresponding service level for that period will increase to 10 days
- Certificate revocation requests to the Doorman from a Business Network Operator or a participant will be turned around within five working days, up to a maximum of 10 in any one day

The service levels above only apply during normal hours of business (see section 3.2).

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 doorman 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 certificate signing request being approved by the Doorman
- 95% of Network Map updates for resigning nodes will be completed within 1 hour of the certificate revocation request 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
- Should the number of outstanding Network Map updates exceed 1000 in any one period the corresponding service level for that period will increase to 2 hours

The service levels above only apply during normal hours of business (see 3.2).

NOTARY

The turnaround time for transaction notarization request is measured from the inbound request is received on R3 infrastructure to the point at which the reply leaves R3 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.

- The notarization system will operate at a maximum end-to-end throughput (as defined above) of 4000 transactions per hour (for transactions with an average of 10 or less input states)
- The notarization system will operate at an average end-to-end throughput (as defined above) of 2000 transactions per hour (for transactions with an average of 10 or less input states)
- The number of transactions for which an incorrect response is given by the notary (input state consumed but indicated as not consumer and vice versa) will be less than 1 in 100,000,000
- 95% of transactions with 10 or less input states will be notarised within 60 secs of the previous notarization completing

The service levels above only apply during normal hours of business (see 3.2).

3.2 Availability

Uptime

- Normal business hours are considered as from 00:30 UTC+0 to 21:30 UTC+0 excluding weekends and bank holidays
- Services will be available 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

- The normal maintenance window will be each Wednesday at a time to be advertised at least 5 days in advance

Unscheduled Downtime

- Outside of scheduled maintenance periods all services are designed to be continuously available and operate with hot-cold back-up (see recovery section)
- Each service will operate with 99% availability during normal business hours

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.
- R3 cannot guarantee any particular fix meets this objective but will issue hourly updates on progress to all affected participants

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

3.3 Data Retention

- Test data created in the Corda Network UAT environment as a result of customer activities under this agreement will be held by customer nodes and R3 databases supporting the Notary, Network Map and Doorman Services.
- At the end of the pre-agreed UAT usage period R3 retains the right to remove such data held in its own databases
- Such data as R3 controls can be held for future periods of testing if agreed at least 14 days in advance of the end of the pre-agreed usage period, and subject to separate commercial negotiation (a reasonable fee will apply, based on R3's assessment of incremental costs)

3.4 Release Management

- R3 operates a single Corda Network UAT environment with the intention of simulating the conditions applying in the single production Corda Network.
- It is important that Corda Network production is able to take advantage of new releases without undue delay and so the normal mode of operation is for services in both production and UAT environments to be regularly upgraded.
- Since Corda from version 3.1 onward is fully backwards compatible releases that impact the UAT services offered by R3 do not require customer nodes to upgrade.
- R3 will post intention to upgrade its own services one calendar month in advance of the event on r3.com 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
- R3 will make the upgrade on a specified day published on r3.com as per the notification period above. Customer services may be impacted and such impact will be notified in the upgrade communicaation. In the rare event of issues arising, they should be handled through the normal support channels

3.5 Network Parameter Upgrades ('Flag Days')

- 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 – occasioning a 'flag day'.
- The flag day process incorporates a node polling activity that ensures all node operators see the requested changes in advance and can vote to accept or not accept.
- R3 will consult with customers should there be disagreement over the proposed changes but reserves the right to progress the flag day 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.
- Details of the flag day process can be found in the User Guide which can be obtained from uatdoorman@r3.com.
- Execution of an agreed flag day should be entirely transparent to users, and can be executed during normal working hours. Flag days will be advertised at least ten working days in advance and executed during normal working hours.
- Flag days 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)
- Further details can be found at https://www.docs.corda.net under Corda Networks / Network Map

3.6 Business Continuity

- R3 has fully redundant data center capabilities for all of its services, utilizing Microsoft Azure Cloud infrastructure.
- R3 has a disaster recovery policy which is reviewed and tested semi-annually.
- R3 has a comprehensive security policy incorporating specific security incident management procedures

3.7 Support

R3 support Corda Network UAT Services as follows:

Hours Of Service:

Support desk is open during normal business hours.

Classification of Errors.

Errors will be classified by R3, in discussion with the customer, in accordance with the Support Handbook found here: https://r3-cev.atlassian.net/wiki/spaces/SKB/pages/990544103/The+Corda+Software+Support+Services+Handbook

Resolution of Errors and Support Requests:

R3 will operate according to the service levels documented in the Support Handbook.

It should be noted that, unless agreed by an R3 director and according to special circumstances, Severity 1 incidents cannot arise from any UAT activity and only Severity 2 to 4 incidents apply.

3.8 SLA reporting

Formal SLA reporting will not be operated for the Corda Network UAT environment. R3 will monitor service level performance internally and make changes as required either to maintain service levels or to modify them, at R3's discretion.

3.9 In the event of SLA breach

- Penalties will not apply for SLA non-performance during the pilot period.
- If customers test plans are severely disrupted as a direct result of persistent issues with the Corda Network UAT Services or Corda Software, then representation to R3 Commercial team for appropriate repatriation of any fees payable for UAT services can be made.