CHESS Replacement Project

Connectivity & Integration Working Group

20 November 2019

ASX

Important Information – Competition Law Policy

Working group members are reminded to have regard to their obligations under competition law. In particular, please note recent changes to the Competition and Consumer Act to prohibit a corporation from engaging with one or more persons in a concerted practice that has the purpose, effect or likely effect of substantially lessening competition.

Agenda

- CDE Updates
- Connectivity Updates
- ISO Message Signing
- High Availability
- Questions

CDE Update

CDE 4 Now available

New functionality including;

- Unilateral and Bilateral Settlement Instructions
- Batch Settlement
- Corporate Actions, ex-period
- Security Sub-register Status Notification

Connectivity now available for;

- Approved Market Operators via FIX Gateway (including an uplift in technical documentation)
- Payment Providers (SWIFTNet, AMQP or Ledger API)
- DAML Extractor (requires DAML SDK 0.13.35)

Test Tooling

- Trade Ingest for self service trade reporting (C&S participants and their vendors)
- Corporate Action headers
- Payment Provider cash settlement to faciliate batch settlement

Security Uplift

- Mutual TLS implemented AMQP, FIX Gateway & Trade Ingest

Notes

- Mutual TLS for Ledger API & Extractor will be implemented in CDE 5
- Netting reversal - scheduled job that runs each Wednesday has been suspended for CDE 4
- CDE 4 will be re-set every 2 weeks for scheduled ASX maintenance

Documentation Update

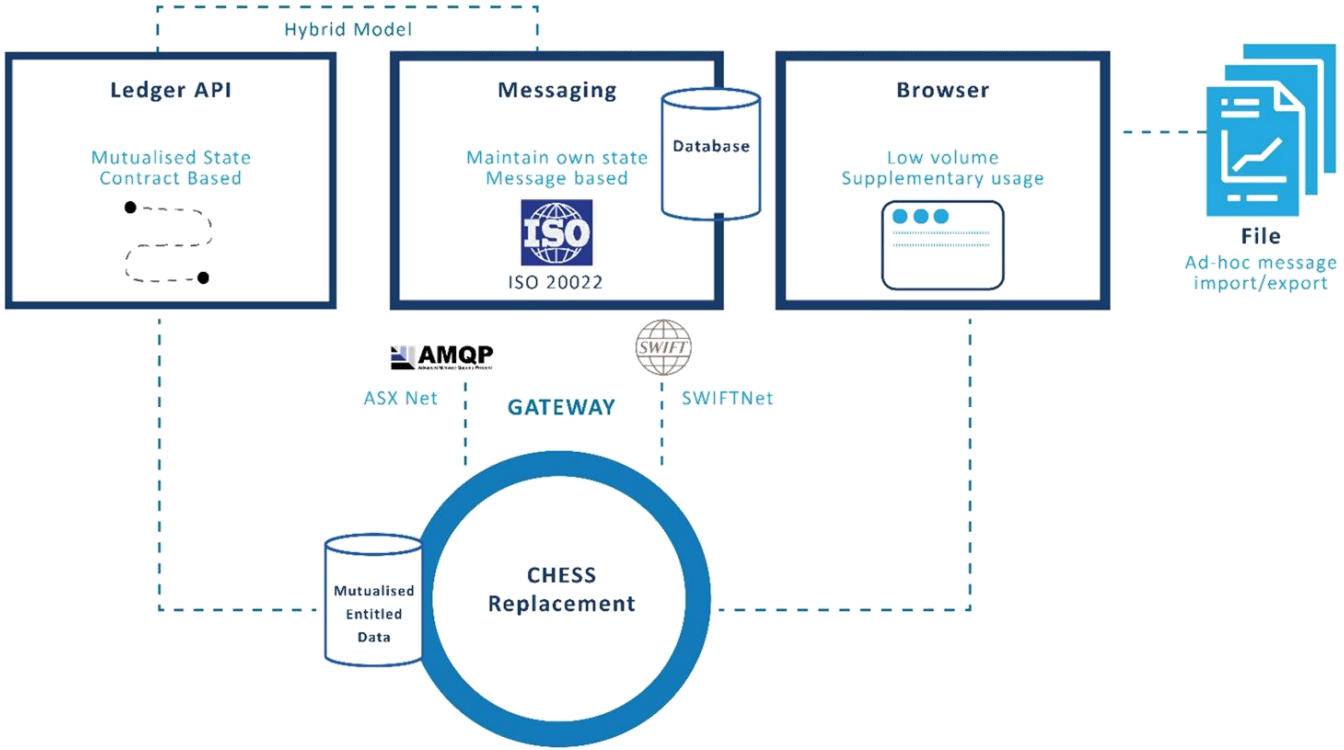
There has been an update to the **'What's New'** technical documentation;
11 November 2019 - Corporate Actions, Environments and Known Issues and Limitations Updates.

This update includes the following:

- **Corporate Actions Update** – new table that brings together the Corporate Action Lifecycles, Corporate Action Functional and Messaging Specifications
- **Environments Timeline Update** – new high level timeline based on the Implementation & Transition Working Group on the 25 October
- **Known Issue & Limitations table** updated with any new defects

Connectivity Updates

Connectivity Overview



ISO 20022 XML Message Signing

ISO Message Signing

- Message signing process **normalises**, **digests**, and **encrypts** information within the KeyInfo, BizMsg, and Document sections of the ISO 20022 XML message
- Will follow ISO 20022 Business Application Header Message Usage Guideline v1.9
- Targeting CDE 6 release, Feb 2020
- Will be configurable as to whether signatures are validated during CDE
- Only applicable for AMQP messaging customers
- Separate certificate will be required for message signing

https://www.iso20022.org/sites/default/files/documents/general/ISO_20022_BusinessApplicationHeader_MUG_v1_9.pdf

Message Signature XML Tag

Wildcard Signature Inclusion

```xml
<?xml version="1.0" encoding="UTF-8"?>
<BizMsg xmlns="urn:iso:std:iso:20022:tech:xsd:head.002.001.01" xmlns:xsi=
    <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01" xmlns:
        <Fr>···
        </Fr>
        <To>···
        </To>
        <BizMsgIdr></BizMsgIdr>
        <MsgDefIdr>DRAFT6reda.018.001.01</MsgDefIdr>
        <BizSvc>acct_001_001_02_!p</BizSvc>
        <CreDt></CreDt>
        <Sgntr>
            <n1:auto-generated_for_wildcard/>
        </Sgntr>
```

Full ISO 20022 XML Signature Section

```xml
<!-- signature section not included in the calculation for business application header signing -->
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n2#"/>
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <!--this reference section contains digest of KeyInfo section -->
        <Reference URI="#Unique-id-to-KeyInfo" Type="http://www.w3.org/2000/09/xmldsig#KeyInfo">
        </Reference>
        <!-- this reference section contains digest of ISO 20022 XML business application header section -->
        <Reference URI=""> ···
        </Reference>
        <!-- this reference section contains digest of ISO 20022 XML document section -->
        <Reference URI=""> ···
        </Reference>
    </SignedInfo>
    <SignatureValue><!-- value from signing and encryption of <SignedInfo> section --></SignatureValue>
    <KeyInfo Id="Unique-id-to-KeyInfo"> ···
    </KeyInfo>
</Signature>
```

Creating a Signature

Normalize XML

- Standardize XML formatting prior to signing
- Ensures validator processes without breaking signature

Data Integrity

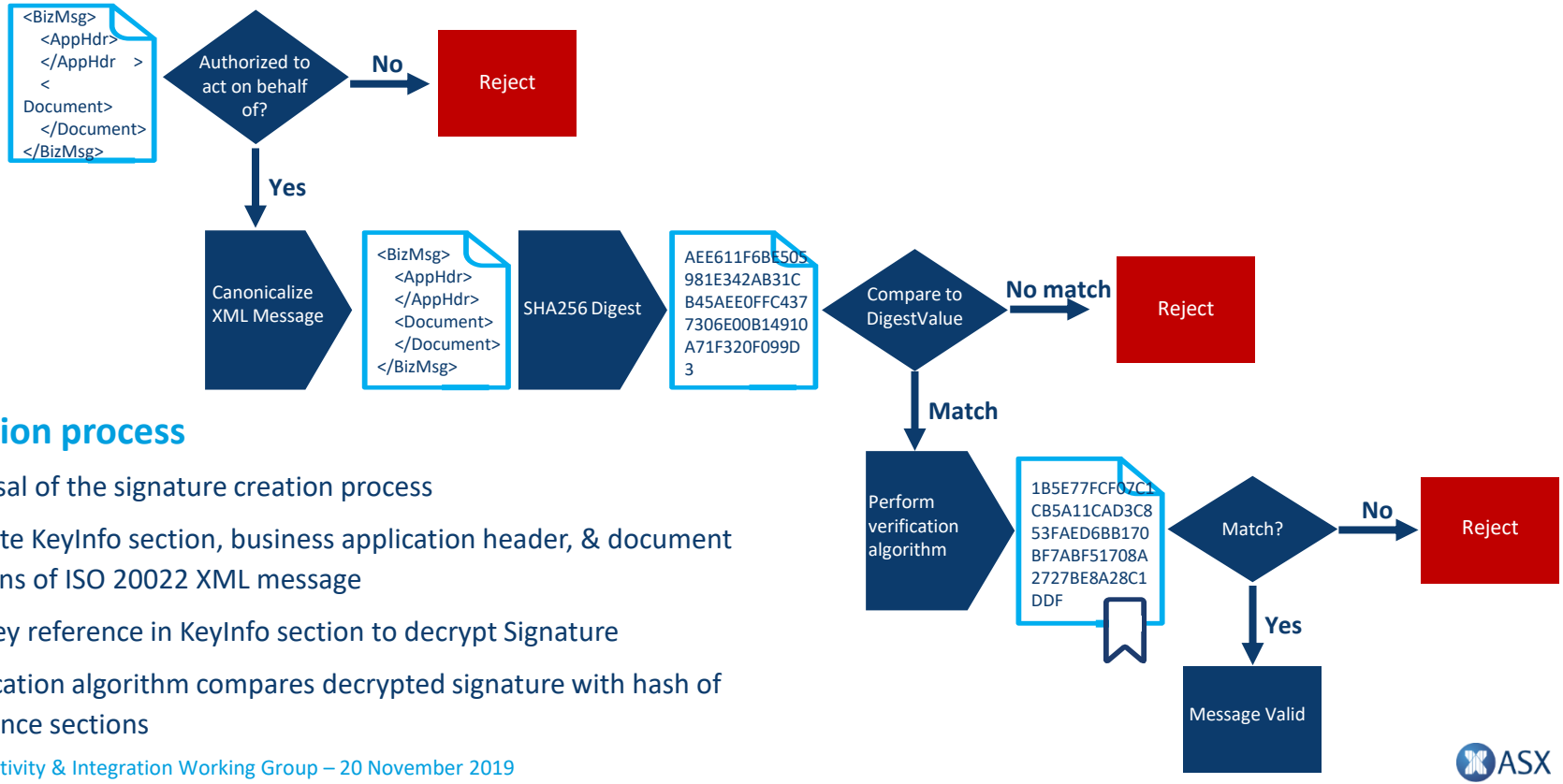
- Guarantees message has not been altered in transit
- Allows for audit of message

Authentication & Non-repudiation

- Guarantees message actually came from sender
- Sender can't deny having sent or signed message

AMQP users note, business message wrapper is not included in the signature calculations

Validate Signature



Validation process

- Reversal of the signature creation process
- Validate KeyInfo section, business application header, & document sections of ISO 20022 XML message
- Use key reference in KeyInfo section to decrypt Signature
- Verification algorithm compares decrypted signature with hash of reference sections

Key Takeaways – Message Signing

- Message signing process **normalises**, **digests**, and **encrypts** information within the KeyInfo, BizMsg, and Document sections of the ISO 20022 XML message
- Following ISO 20022 Business Application Header Message Usage Guideline for signature creation and validation
- Relevant for AMQP messaging channel only, targeting CDE 6 release (with documentation in Dec 2019)
- AMQP users should not include the business message wrapper in the message signature creation process
- Common cryptography libraries have the ability to create a signature of defined XML sections based on a provided signing private key
- ASX will provide a documentation uplift in December to provide more information

High Availability

High Availability (HA) Design Patterns

Client Side

- Application Layer
  - Behavioural (e.g. batch, retry)
  - Configuration (e.g. dns, git)
  - Framework (e.g. Spring Cloud)
- Application Local
  - Proxy (e.g. Envoy)

Somewhere in the Middle

- Network
  - Multicast / Anycast
- Service Mesh
  - e.g. Consul

Server Side

- DNS
  - Simple
  - Complex
- Load Balancer
  - Reverse Proxy
  - Direct Server Return
- Application Layer
  - Symmetrical / Asymmetrical

ASX

HA Design Pattern Analysis

Client Side

- **Pro**
  - Transparent system state*
  - Client side control / choice
  - Infrastructure simplicity
- **Con**
  - Application complexity

* Somewhat dependent on which client side approach is taken

Somewhere in the Middle

- **Pro**
  - Semi-transparent to client
- **Con**
  - Semi-transparent to client
  - Infrastructure complexity

Server Side

- **Pro**
  - Application simplicity
- **Con**
  - Opaque system state
  - Client has no control
  - Infrastructure complexity

CHESS Replacement Approach

For Ledger API, High Availability concerns must be implemented on the client (i.e. application) side.

This allows for greater flexibility both in normal operations (e.g. hot/hot) and failure scenarios.

CHESS Replacement System Properties

State Awareness

Applications can determine committer connectivity status and success / failure of operations.

Idempotency

CHESS Replacement ensures duplicate operations are safe.

Streaming

Client applications can pause / restart Ledger API streams at (somewhat) arbitrary points in time.

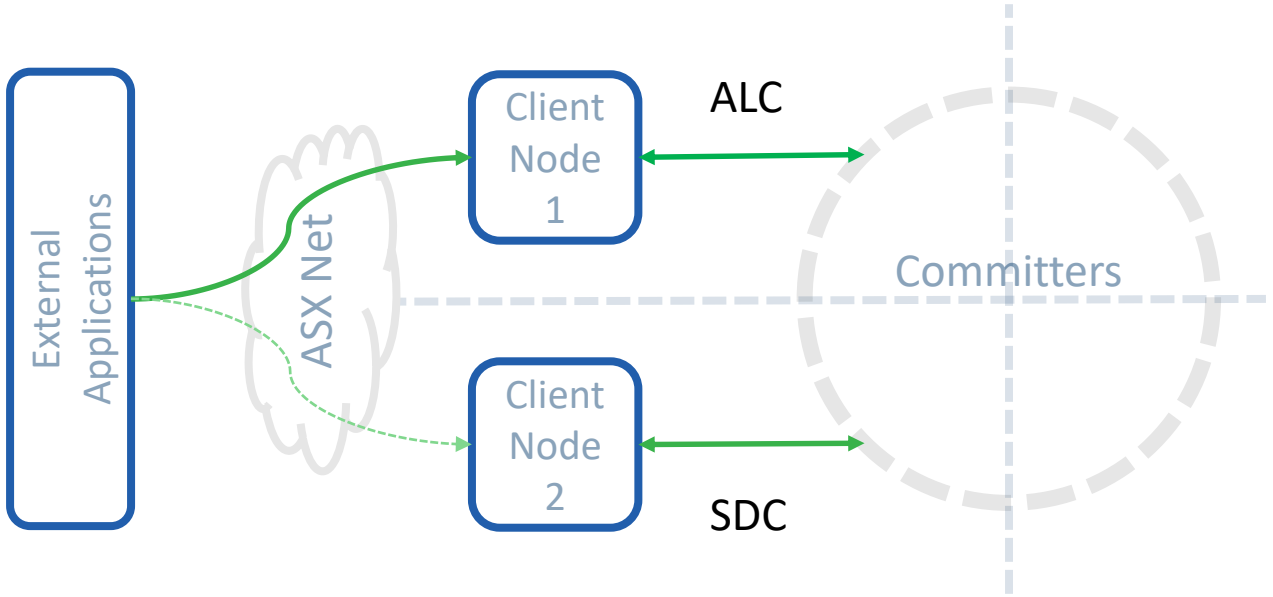
See https://docs.daml.com/app-dev/app-arch.html for guidance.

Failure Scenario Discussion

High Level Example

For the purpose of discussing failure scenarios, we'll assume an application uses Client Node 1 during normal operation and Client Node 2 in failure scenarios only.

ALC and SDC primary ASX Datacentres, which are geographically dispersed.

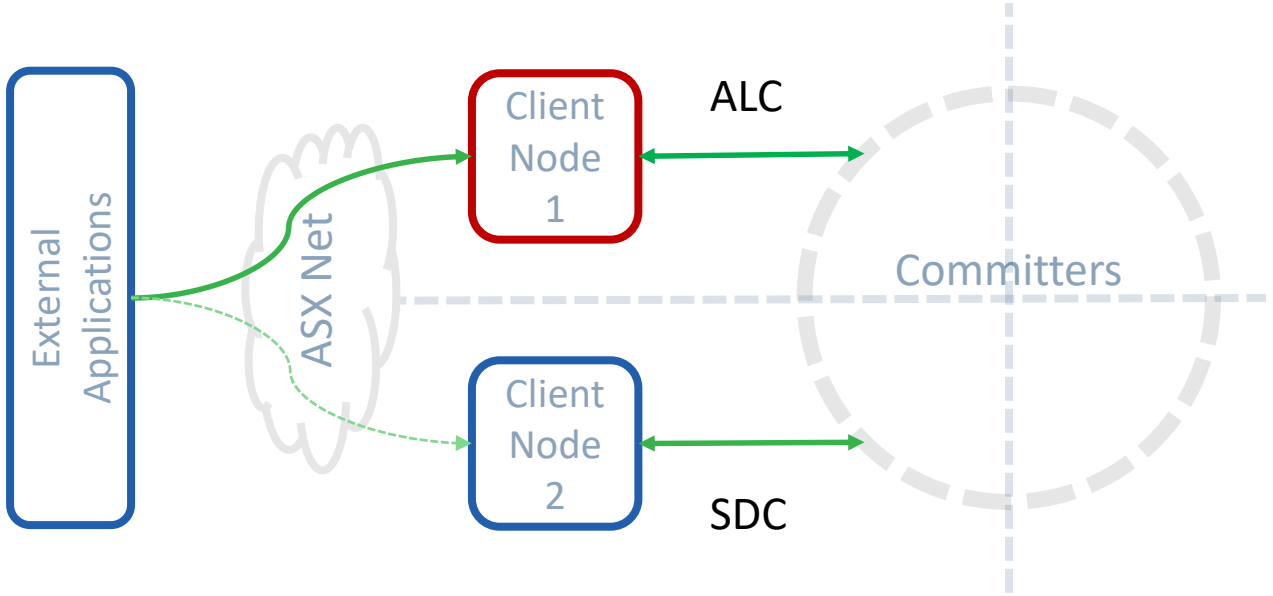


Failure Scenario

Client Node Failure

Network connectivity to Client Node 1 is up, but the Client Node itself is down.

Applications can't any submit operations to Client Node 1. Can be highly confident of what has failed, and use a number of strategies to failover and resume operations on Node 2.



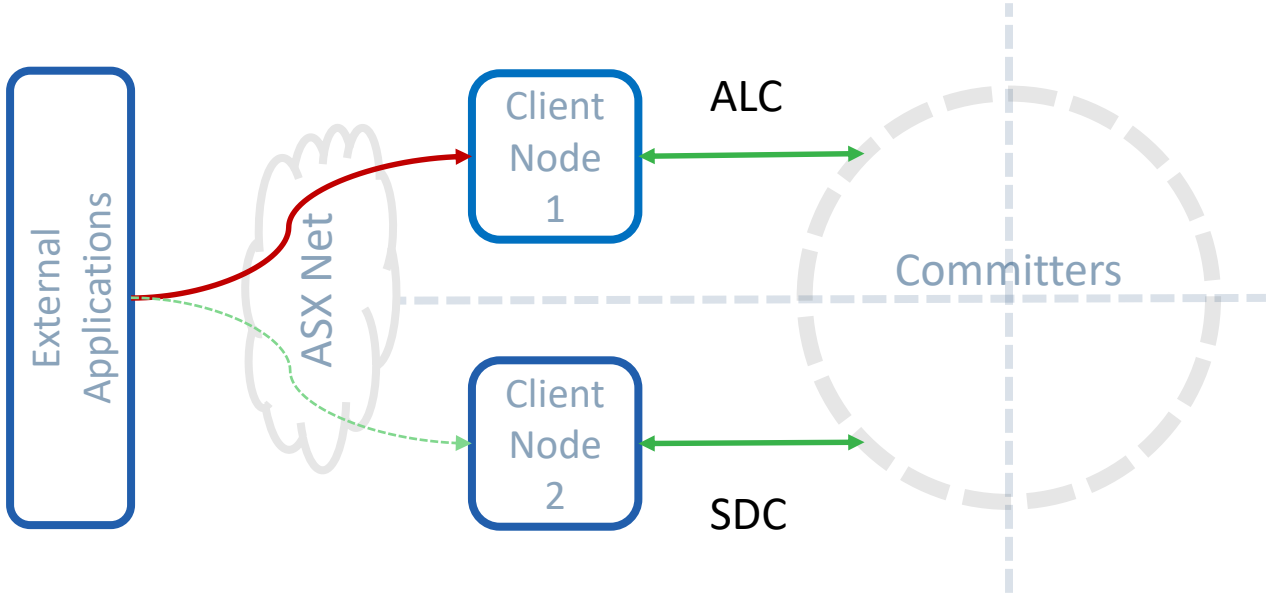
Failure Scenario

Network Failure

The network path between customer application and Client Node 1 is down, but the client node itself is up.

This could be due to a client side network failure, an ASX Net Gateway failure, an ASX Net router/switch failure, etc.

Depending on the nature of the failure, applications may or may not choose to failover to Client Node 2.

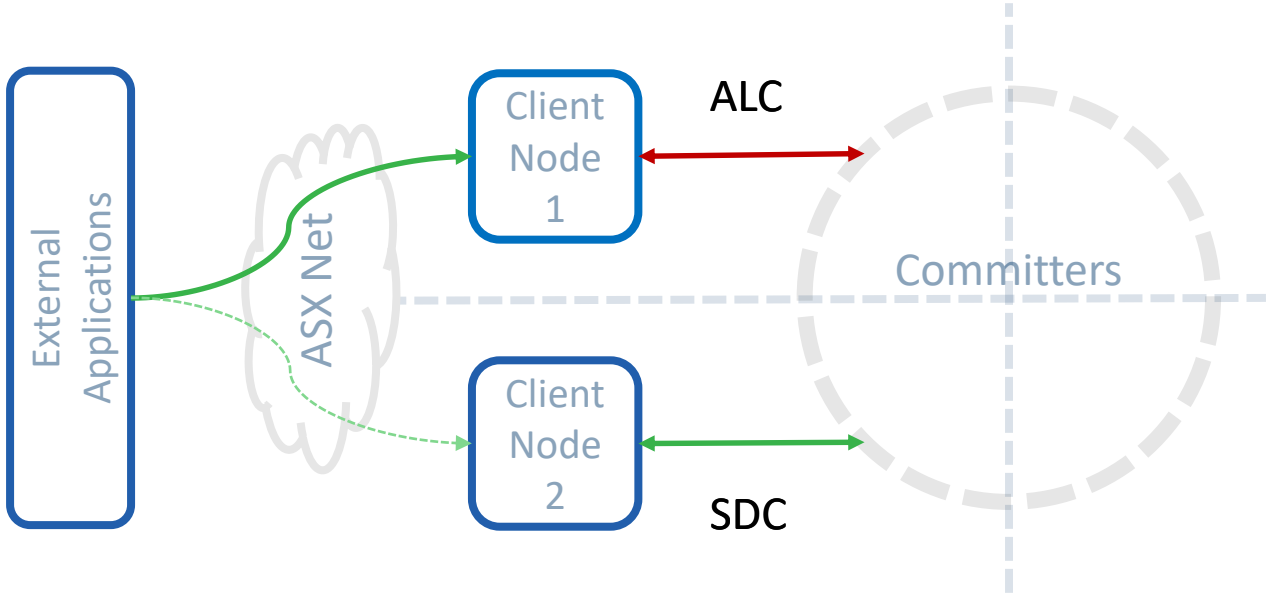


Failure Scenario

Backend Network Failure

Network connectivity to Client Node 1 is up, Client Node 1 itself is up, but it cannot communicate with the backend committers.

Applications can submit Ledger API operations, but none are successful. Can be reasonably confident as to what has failed, and use a number of strategies to failover and resume operations on Node 2.

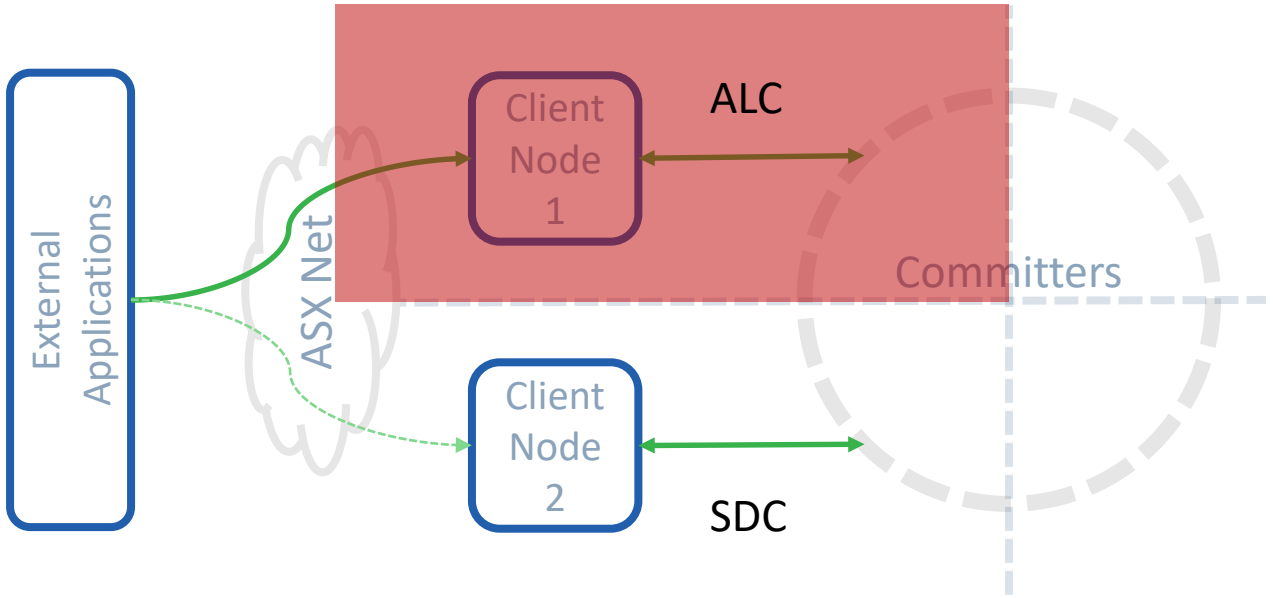


Failure Scenario

Datacentre Failure

The ALC datacentre is down, taking out the ASX Net path to Client Node 1, Client Node 1 itself, and any committers located in the ALC.

Applications can't any submit operations to Client Node 1. Can use a number of strategies to failover and resume operations on Node 2. May choose to invoke their own topology change (e.g. invoke DR).



High Availability – Message-based Options

AMQP

- Single connection IP:port provided to customers
- Highly available service at primary and secondary sites
- ASX manages roll-over to secondary site in event of failure
- Application must manage duplicate detection
- Requires request to ASX for replay of previously acknowledged messages

SWIFT

- Managed by SWIFT
- No changes from today
- Application must manage duplicate detection
- Requires request to ASX for replay messages

FIX Gateway

- Single connection IP:port provided to customers
- Highly available service at primary and secondary sites
- ASX manages roll-over to secondary site in event of failure
- Can replay messages from the current business day

Summary

In summary, CHESS Replacement is a highly available system that uses different HA strategies, based on what is optimal for the client application:

Ledger API

- 2 active Ledger API endpoints provided, each in a geographically dispersed location
- Greater application insight to state of the system
- Implement HA strategies in your application (i.e. client side)

AMQP / FIX

- Single endpoint to highly available services

Questions

Next Working Groups

26 November

- ISO 20022 Technical Committee – including a review of reporting changes

29 November

- Implementation & Transition Webinar; focus on CHESS Registration Conversion

4 December

- Connectivity and Integration Working Group
- Forward view of CDE 5
- Reporting change (summary of Technical Committee updates)
- Secure Browser (overview of new Browser functional capabilities)

Thank you

Disclaimer

This document provides general information only and reflects matters put forward for discussion at a point in time. You should obtain independent advice before making any decisions. ASX Limited (ABN 98 008 624 691) and its related bodies corporate ("ASX") makes no representation or warranty with respect to the accuracy, reliability or completeness of the information. To the extent permitted by law, ASX and its employees, officers and contractors shall not be liable for any loss or damage arising in any way (including by way of negligence) from or in connection with any information provided or omitted or from anyone acting or refraining to act in reliance on this information.