Technical Briefing Pack

Austraclear System Release 9

Internet Participant

March 2020

Contacts

For general enquiries, please contact:

ASX Fixed Income Operations
ASX Settlement Operation | 20 Bridge Street | Sydney NSW 2000

T +61 28298 8474
T 1300 362 257
Intl: +61 2 8298 8474
Email Austraclear@asx.com.au

Contents

Introduction

About this Document

This is the technical briefing paper for the ASX Austraclear system, and will supersede the previously published paper. Its purpose is to assist Participant technology staff in the implementation of the Austraclear system. The information in this document applies to Participants who operate in Australia or overseas.

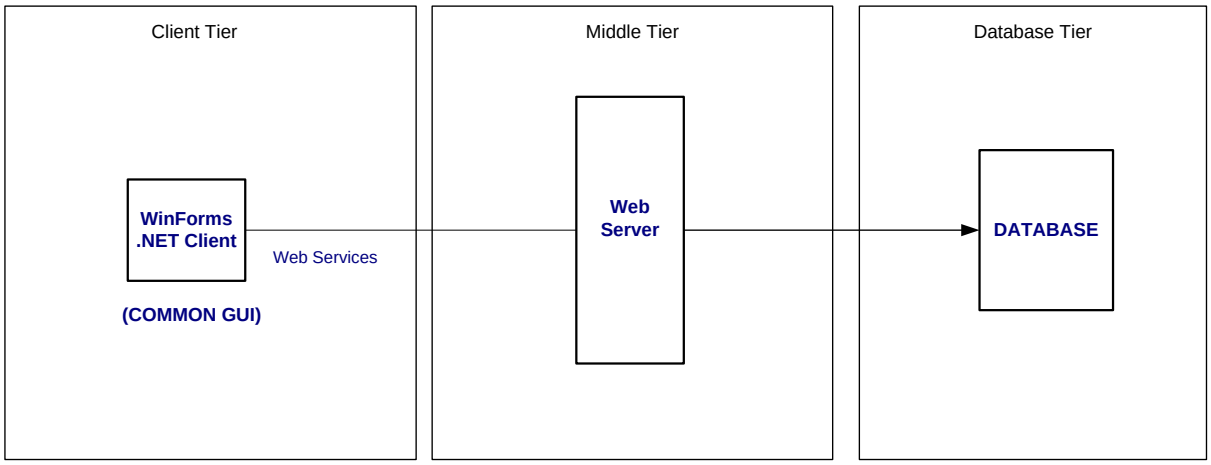
This document does not cover the functionality of the replacement system. For further information regarding the content of this document or the ASX Austraclear system, please send any enquires by email to austraclear@asx.com.au

Background

The ASX Austraclear system is a next generation Central Securities Depository (CSD) system that utilises an open architecture with a Windows Graphical User Interface (GUI) front end Client. The system's Service Release 9 provided improvement onto technical requirements as well as additional and improved functionalities.

The ASX Austraclear system is a .Net Windows Forms application and can be deployed either by browser deployment or file deployment (further information provided in Section 4). The Client application connects to a central web service utilising Microsoft .Net technologies. See Diagram 1 below.

Diagram 1: ASX Austraclear System Architecture Overview.



Client Workstation Requirements

Software Requirements

The following table outlines the software requirements for the ASX Austraclear system. The Participant is responsible for the supply, installation and support of the required Software, as specified below, and the Hardware required for the system.

Table 1: Software Requirements

Software Requirements	Responsible
Microsoft Windows 10 32-bit or 64-bit Microsoft Windows 8 32-bit or 64-bit	Participant
Microsoft Internet Explorer 11 (Supporting TLS 1.2)	Participant
Microsoft .Net Framework version 4.7.2 or higher	Participant

The Microsoft .Net Framework can be downloaded from the Microsoft web site:

https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows

Please note that you need to be logged in with Administrator rights to install the Microsoft .Net Framework, as you would normally do when installing operating system software.

Internet Explorer can be downloaded from the Microsoft web site:

http://www.microsoft.com/downloads/

Hardware Specifications

The minimum recommended PC specification for the ASX Austraclear system is shown below. ASX testing has indicated that performance improvements can be realised with increases in processor speed and memory.

Table 2: Recommended Hardware Requirements

Hardware Requirements	Specifications
PC client	Intel Core 2 3.16 GHz (Or AMD equivalent)
Memory RAM	4 GB
Monitor & screen resolution	17" (1024 x 768)
Disk space	100MB per Windows user profile

Network Infrastructure & Security Requirements

This section outlines minimum Network infrastructure and Security requirements for connecting to the ASX Austraclear system.

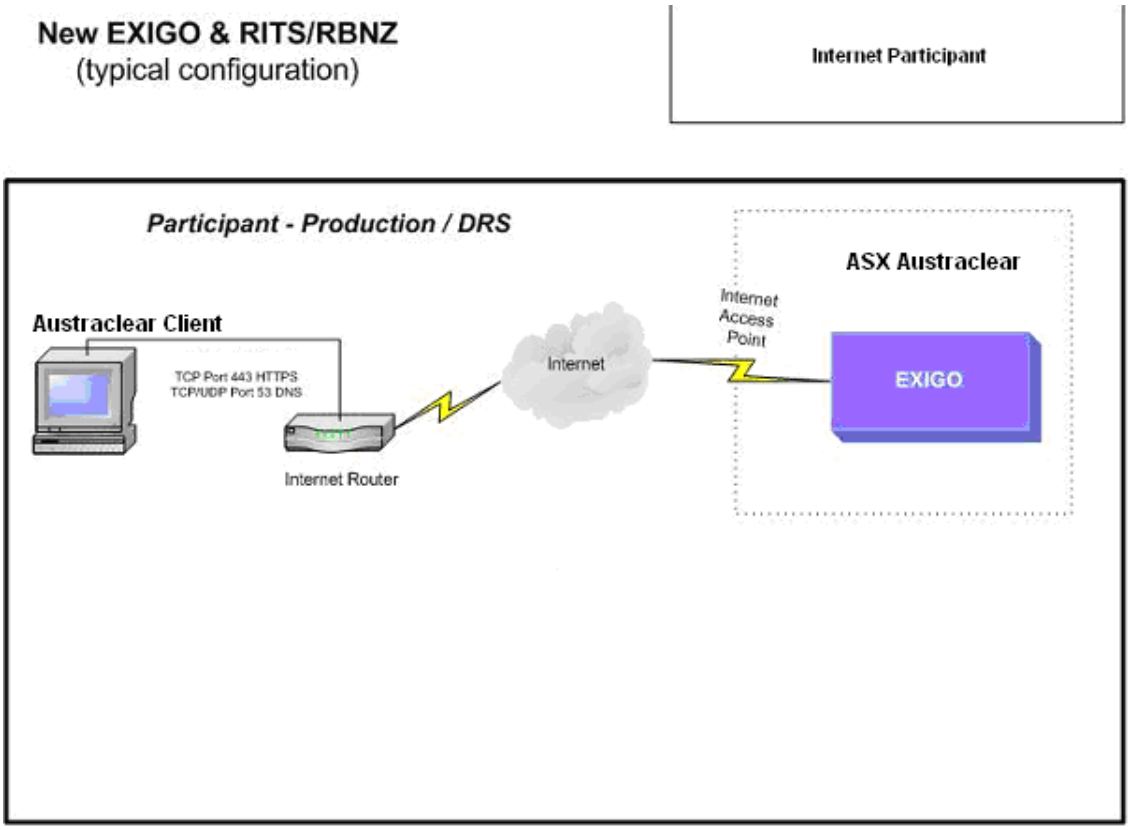
Network and Security Requirements

Table 3: Network and Security Requirements – Production

Requirements	ASX Austraclear	Responsible
Network		
Internet connectivity (256Kbps) *	X	**Participant**
Security		
Firewall ports required to be opened: HTTPS (TCP port 443) DNS (TCP/UDP port 53)	X X X	**Participant**
Client Side Digital Certificates	X	**Participant**
RSA Token (ACE Card)	X	**Participant**

System Connectivity – Typical Configuration

Diagram 2: Internet Participant Typical Configuration



ASX Infrastructure

The ASX advises a recommended minimum connection speed of 256Kbps per active user connectivity for Internet connectivity to the ASX Austraclear system.

Internet connections are the responsibility of the Participant and may include such methods as ADSL/Cable/Broadband/Wireless via an ISP or an existing Participant Internet connection (possibly via a Proxy Server/firewall).

Participant Infrastructure

Participant Internet

Austraclear Internet Participants will use their existing internet connections to access the ASX Austraclear System

Proxy Servers

A proxy server is one which sits between a web browser and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself and if not, forwards the request to the real server. It also can be used to filter requests i.e. to prevent users from accessing a specific web page or sites.

There are two common types of proxy configuration:

- Authenticating
  - Manual – requires all users to authenticate when browsing internet sites
  - Automatic/Integrated – allows users to browse internet sites automatically using a common authentication integrated to each of the user ids.
- Non Authenticating

The ASX Austraclear system is designed to work with proxy servers that support HTTP 1.1 (RFC2616)

Please note that the deployment of the ASX Austraclear system differs according to which method of authentication is used. Please see the appropriate user manual for further details. These will be made available on the ASX Austraclear websites.

https://asxonline.com/content/asxonline/public/documents/austraclear-technical-documents.html

Table 4 - Firewall rules required

Primary Site			
Destination	Port(s)	Action	Description
203.15.145.75	HTTPS TCP/443	ALLOW	Allow access to the Austraclear Production Environment
203.15.145.78	HTTPS TCP/443	ALLOW	Allow access to the Austraclear Online Help Production environment
203.15.146.75	HTTPS TCP/443	ALLOW	Allow access to Test Environment
203.15.146.78	HTTPS TCP/443	ALLOW	Allow access to Test Online Help
203.15.147.70 203.15.147.74	DNS UDP/53	ALLOW	Allow access to ASX DNS systems where required, to allow austraclear.com.au names to be resolved.

DNS TCP/IP Configuration

The design of the Austraclear environment makes provision for dynamic failover between Austraclear processing sites for **Business Continuity** purposes.

TTL or Time To Live should be set to recommended setting of 30 seconds.

It is important that Participants make use of DNS-based name resolution wherever possible. Details are shown in Table 5.

Table 5: Application access via DNS

Application	URL
Production	https://asx.austraclear.com.au
Online Help	https://asxhelp.austraclear.com.au
Test Environment	https://asxta.austraclear.com.au
Test Online Help	https://asxtahelp.austraclear.com.au

BCP/DR Configurations Requirements

Access to the ASX Austraclear system from your BCP/DR site will also be via the Internet. The ASX advises a recommended minimum connection speed of 256Kbps/per active user for Internet connectivity to the ASX Austraclear system. You will need to ensure that the appropriate configuration is implemented at your BCP/DR site.

In addition you will also need to ensure that you have the following available:

- **An RSA token / ACE card** at your DR site, so that you can authenticate to the ASX firewall (Please check availability of a RSA token)
- **Client Side Digital Certificate** - please note that the original client side digital certificate will need to be exported for use on your DR PC (please see the CSDC Import & Export Procedures on the ASX Austraclear website)

Security

Application authentication in the ASX Austraclear System is currently controlled through various Security Controls.

Aside from all users will be required to use a Digital Certificate and a username/password pair for application authentication. Security controls include:

- End to end encryption of data between the client and server using SSL
- Three factor application authentication
- Comprehensive password policies
- Automatic application lock for idle users

Internet ASX Austraclear users

From a network perspective, ASX Austraclear users will be required to authenticate to the ASX firewall using the RSA token, which will then allow access into the system's middle tier. Once past this point, standard application procedures apply.

The system requires the following protocols:

- HTTPS (TCP port 443)
- DNS (TCP/UDP port 53)

It should be noted that connections will not be initiated from the ASX network to the participant site. As such, Participants should only allow connections to be initiated outbound to the ASX Austraclear system, with established connections also allowed through firewalls/router access control lists.

Deployment of the Client Software

Deployment Models

The ASX Austraclear system is installed as a .Net Windows Forms application. There are two options available to deploy the Client on your desktop workstation.

Browser Deployment

This model enables a user to deploy the software using their browser via a regular web address (URL). By clicking on the appropriate link on the ASX Austraclear website, the Weblauncher is initiated which will carry out the initial download and execution of the application.

This model ensures that each time you initiate the login procedure the web launcher will check for updates to the underlying application. The web launcher Security Policy needs to be installed initially in order to configure the trust relationship between the client and the middle tier.

File Deployment

This model enables a user to install the ASX Austraclear system on the local PC client. The installation file can be downloaded from the ASX website, and allows the application to be packaged and distributed if necessary.

It will require some intervention on the Participant's part to download and install the most recent version of software periodically. This model is launched from the Start menu or by using a desktop shortcut and doesn't require the use of the browser to execute the system.

Digital Certificates

Users of the ASX Austraclear system will be required to enrol in the ASX controlled Certificate Authority (CA). Once the user has been validated, a certificate will be issued and downloaded into the user's Web browser. This certificate will be exportable. (E.g. installed at a Participant BCP/DR site).

Use of this exportable capability is a security policy decision owned by the Participant. ASX does not take responsibility for the management of the certificate and authentication process within a Participant's operations.

When logging into the application, a valid certificate and username and password pair will need to be presented to the application. Without these items a user will not be able to login.

Please see the Technical FAQ's for further details regarding digital certificates.

PC Set Up for SR9 IWT and SR9 Go-Live

ASX Austraclear recommends use of PCs that are separate to the current Production environment, for testing during IWT. This approach will minimize any impacts to existing Production PC's used for current Austraclear production version.

Prior to IWT, it is recommended that a PC to be used in the test should meet the software requirements listed in Table 1.

However, if necessary and while not recommended, participants can set up existing production PCs to also be used for SR9 IWT (and therefore go-live). Participants must note that running both current production version and SR9 GUI's on the same PC during IWT poses an operational risk to the user.

To mitigate this risk, the SR9 GUI during IWT is coloured to assist users in differentiating the versions.

Using the same PC for current Production and SR9 may also pose a technical risk if any installation delays are experienced during deployment by participant's internal IT.

Additional set up is required if this approach is to be taken, the details of which are provided below.

1) Install .net to a version that meets the software requirements listed in Table 1, this will replace existing .net 4.5.2

2) Upgrade Internet Explorer to a version that meets the software requirements listed in Table 1.

3) For Browser deployment users (Users who click on the web link to launch the GUI), the new updated version of Weblauncher (EWL_2_17_4.msi) **must be installed**. The previous version must not be uninstalled (EWL_2.8.1.msi) prior to Go Live of SR9. Both versions can coexist on the same PC. Please note that clicking on the new link to launch the SR9, will overwrite the current GUI version in the user's windows profile space. Vice versa, clicking on the current link to launch the current Prod GUI, will overwrite the SR9 GUI. This means that every time the user switches between current Prod and SR9 GUI's, they will be required to download the GUI again.

For File deployment users, both current Prod GUI version and SR9 GUI's can be installed side by side on the same PC. Both can be launched and used at the same time.

ASX Austraclear current production version can work with .net 4.7.2 and Windows 10 with IE11.

Deployment and user guides

All the relevant documentation and user guides relating to the deployment and installation of both the ASX Austraclear system and the related Digital Certificates will be available on the ASX Austraclear websites.

https://asxonline.com/content/asxonline/public/documents/austraclear-technical-documents.html

Frequently Asked Questions

An FAQ register is available on the Austraclear Technical Documents Website and is updated regularly.

https://asxonline.com/content/asxonline/public/documents/austraclear-technical-documents.html

Glossary

Term	Definition	Meaning
ASXNet	ASX Wide Area Network	The network, supported by the ASX that provides access to the Austraclear, RITS & ACNZ systems
Authentication	Login process	Establishes the credentials of a user as an “authorised” user
.Net	.Net Framework	Server based technology designed to provide web based services with minimal need for manual software installation on the desktop. For more details see http://www.microsoft.com/net
Data Encryption	Data Encryption	The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes
Digital Certificates	Digital Certificates	A Digital Certificate is the electronic version of an ID card that establishes your credentials and authenticates your connection when performing transactions over the Internet
DNS	Domain Name System	The Domain Name System is the system that translates Internet *domain names* into *IP numbers*. A "DNS Server" is a *server* that performs this kind of translation.
GUI	Graphical User Interface	The part of the application with which the user interacts. Windows applications interact graphically
HTML	Hyper Text Markup Language	The language used to create Web pages and read by a browser.
HTTP	Hyper Text Transfer Protocol	The protocol used for Internet HTML web pages
HTTPS	Hyper Text Transfer Protocol Secure	The protocol used for Secure Internet HTML web pages
Internet Explorer	Internet Explorer	Software provided by Microsoft used to browse the Internet. Used to view and interact with HTML pages.
RITS	Reserve Bank Information & Transfer System	A simultaneous electronic transfer and settlement system for Commonwealth Government Securities. This facility has now been largely transferred to the Austraclear system
SSL	Secure Sockets layer	This is an industry wide standard for encrypting data securely across the Internet via the HTTP and HTTPS protocols.

Three-Factor Authentication	Three-Factor Authentication	Three-Factor authentication is based on something you know (a password or PIN), and something you have (an authenticator) an RSA token – providing a much more reliable level of user authentication than a reusable password. The 3 factors are Username & password, digital certificate and RSA token
TTL	Time To Live	TTL is set by an authoritative name server for a particular resource record. When a caching name server queries the authoritative name server for a resource record, it will cache that record for the defined period (in seconds) set as a TTL,
URL	Universal Resource Locater	An address for a resource available on the Internet eg www.asx.com.au
Security Policy	Security Policy	This file was provided by the vendor to ensure that assemblies are secure when downloaded. This file also gives access to run the program. The security policy file will be delivered as MSI (Microsoft Installer) once downloaded (for browser deployment only.).

Disclaimer & Copyright