Technical Briefing Pack 3.0

Austraclear System

ASXNet Participant

Aug 2025

Contacts

For general enquiries, please contact:

Austraclear and ASX Collateral Service Desk
T 1300 362 257
E 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.

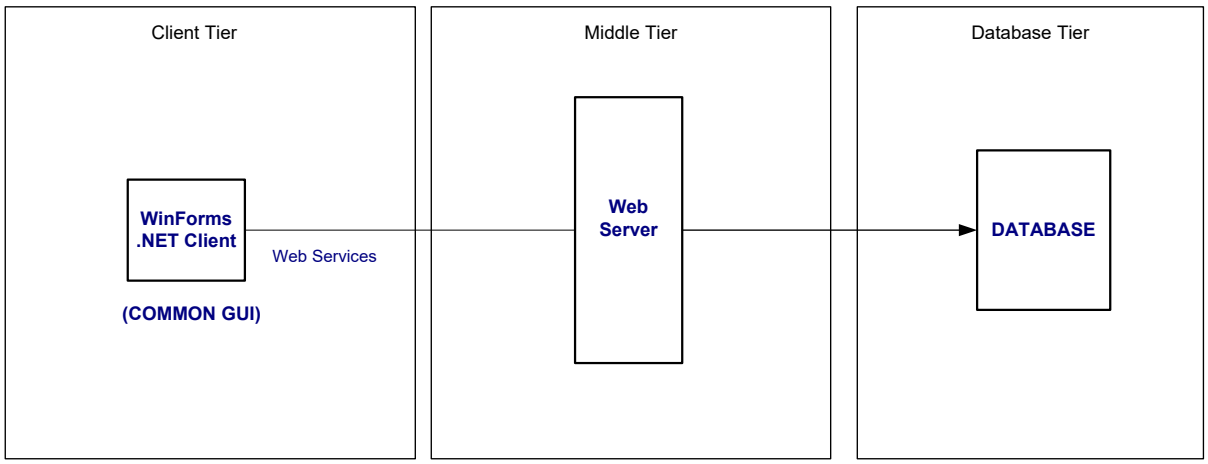
This document does not cover the functionality of the Austraclear system. For further information regarding the content of this document or the ASX Austraclear system, please send any enquires by email to austraclear@asx.com.au

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 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 11 32-bit or 64-bit	Participant
Microsoft EDGE (Supporting TLS 1.2 and TLS 1.3) Google Chrome (Supporting TLS 1.2 and TLS 1.3)	Participant
Microsoft .Net Framework version 4.8	Participant
Microsoft Visual C++2015-2022 Redistributable (x86) product version vs14.44.35208.0 also known as: Visual C++ Redistributable (x86) for Visual Studio 2022 (version 17.14)	Participant

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

https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0

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.

Microsoft Edge can be downloaded from the Microsoft web site: Explore Microsoft.com

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.

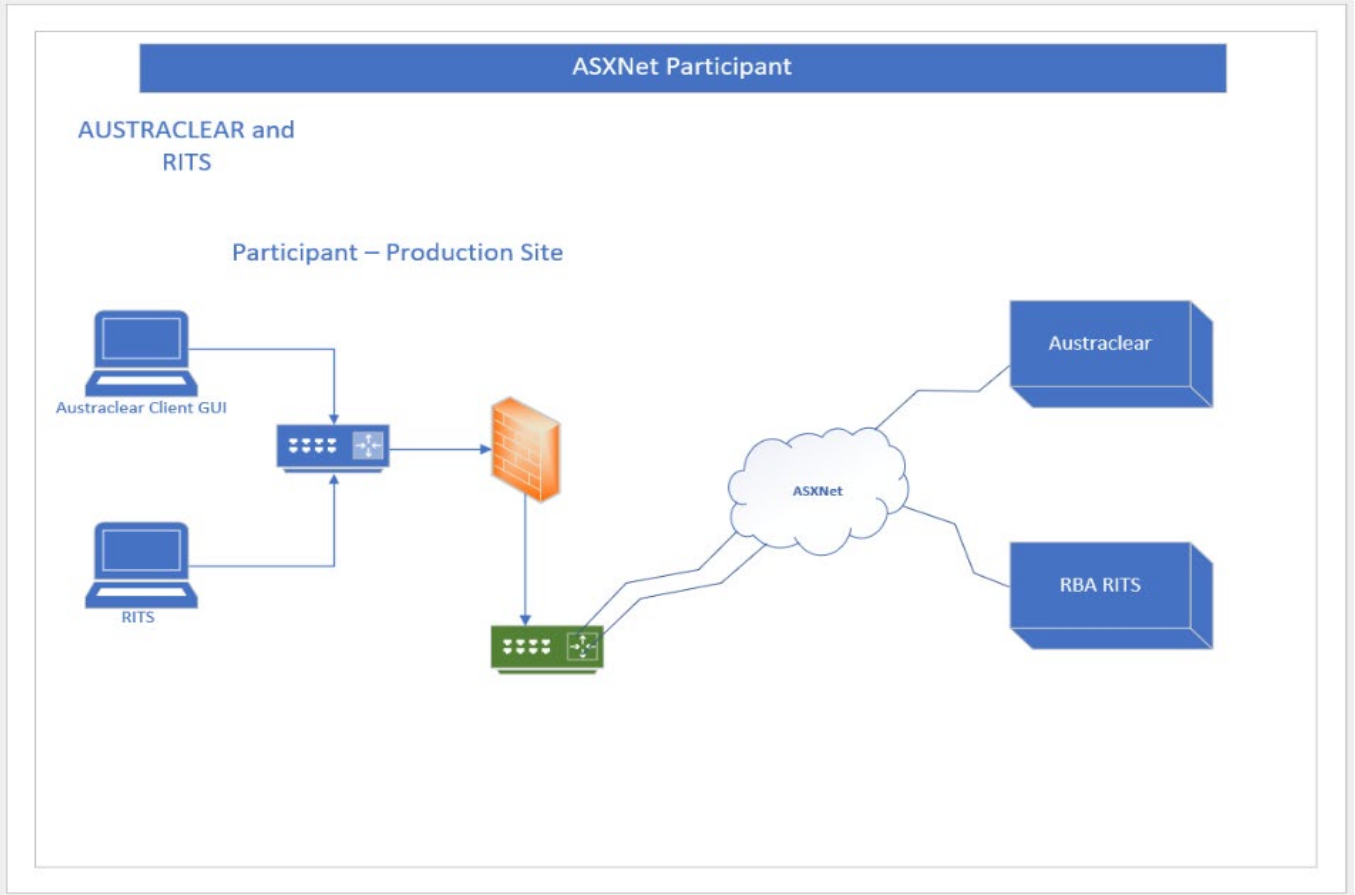
Network and Security Requirements

Table 3: Network and Security Requirements – Production

Requirements	ASX Austraclear	Responsible
Network		
ASXNet connectivity (1 Gb) *	**X**	**Participant**
Security		
Firewall ports required to be opened: • HTTPS (TCP port 443) • DNS (TCP/UDP port 53)	**X** **X**	**Participant**
Client-Side Digital Certificates	**X**	**Participant**

System Connectivity – Typical Configuration

Diagram 2: ASXNet Participant



Network Infrastructure

Connectivity for ASXNet Participants is currently configured to 1GB. Network redundancy is provisioned through the use of a second 1GB service.

Participant Firewalls

Where Participant firewalls are installed, modifications will be required to firewalls in order to communicate successfully with the ASX Austraclear system from the Client Workstation. This information is detailed below in Table 4.

Table 4 - Firewall rules required

ASXNet participants should use one of the two methods of name resolution:

1) Corporate internal DNS servers forwarding requests to the authoritative ASXNet DNS server for austraclear.com.au, which is 203.4.179.50. This request must be sent to the ASXNet network.

TABLE 4.1

Primary Site			
Destination	Port(s)	Action	Description
203.4.179.50	DNS UDP/53	ALLOW	Allow access to Austraclear DNS systems where required.

2) Local hosts files with the entries in Table 4.2 (Refer to Table 6 for further details)

TABLE 4.2

Primary Site			
Destination	Port(s)	Action	Description
203.4.179.224	HTTPS TCP/443	ALLOW	Allow access to the Austraclear Production
203.4.179.230	HTTPS TCP/443	ALLOW	Allow access to Austraclear Test Environment

Proxy Servers

A proxy server is one which sits between a web browser and another server. It intercepts all requests to the real server to see if it can fulfill the request 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 following ASX Austraclear websites.

Austraclear Software and Technical Documents

DNS TCP/IP configuration

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

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

Where DNS-based name resolution is not possible, an alternate mechanism is available to support Business Continuity as specified in Table 6

Table 5: Application access via DNS

Application	URL
Production	https://asx.austraclear.com.au
Test Environment	https://asxta.austraclear.com.au

Participant DNS systems should resolve all name queries for the austraclear.com.au domain as follows:

- Add DNS forwarding entries for the austraclear.com.au domain to your internal DNS servers to directly resolve the austraclear.com.au domain against the Austraclear DNS servers. The authoritative Austraclear name server is 203.4.179.50 for ASXNet participants.

Participants can configure IP addresses in their corporate internal DNS or a local host file on the PC. ASXNet participants can continue to use their corporate internal DNS or the host file. The entries in table 6 have not changed from Release 4.5. They also have the option to forward their DNS requests to 203.4.179.50. Where DNS resolution against the authoritative Austraclear name servers is not possible, the following host file entries or static DNS entries should be used:

Table 6: Application access using "Host files" or static DNS entries at Participant sites.

Application	Host Address	Domain Name
Production	203.4.179.224	asx.austraclear.com.au
Test Environment	203.4.179.230	asxta.austraclear.com.au

BCP/DR Scenario (ASXNet Router failure)

Although unlikely, in the event of an ASXNet access router failure at the ASX Production site, two options are available for participants to continue using the ASX Austraclear system:

1) Connect to the Austraclear system via the internet (authentication via RSA token)
2) Relocate to the Business Continuity Processing / Disaster Recovery site (Some participants will utilise 1GB dedicated links to their DR site while others will utilise internet connectivity).

BCP/DR Configuration Requirements - Internet

For Participants who prefer to use to access Austraclear from their BCP/DR site using Internet connection, the ASX advises a recommended minimum connection speed of 256kbps* for Internet connectivity to the ASX Austraclear system.

The following section provides the basic technical requirements to enable Participants to make the appropriate network configuration changes at their BCP/DR site, in order to be able to access the ASX system via the Internet.

Table 7: Network and Security Requirements – Internet Connection

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

ASXNet Participants with Internet Backup

For ASXNet participants, **who do use internet connected PCs as a backup** (i.e. PC's not using the ASXNet network to connect to Austraclear), it is recommended that these internet PC's resolve using either of the following two methods:

1) Name Resolution Request for asx.austraclear.com.au and asxta.austraclear.com.au are resolvable on public internet.

   Please run nslookup to check name resolution.

   :\>nslookup asx.austraclear.com.au

   Name: asx.austraclear.com.au

   Address: 203.15.145.75

   :\>nslookup asxta.austraclear.com.au

   Name: asx.austraclear.com.au

   Address: 203.15.146.75

2) Local hosts files, with the following entries

   203.15.145.75 asx.austraclear.com.au

   203.15.146.75 asxta.austraclear.com.au

Security

Application authentication in the ASX Austraclear System is currently controlled through various Security controls, such things as:

- End to end encryption of data between the Client and server using SSL
- Three factor application authentication when connecting over the internet (something you know and something you have)
- Comprehensive password policies
- Automatic application lock for idle users

All users will still be required to both have and know something. This includes the use of an ASX issued Client-Side Digital Certificate and a username/password pair for application authentication.

From a security perspective the security controls are related to the application rather than the network. There are no changes in the protocols required.

Production (ASXNet):

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

BCP/DR (Internet):

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

It should be noted that no connections will be initiated from the ASX network (ASXNet) to the Participant site.

As such, Participants should only allow connections to be initiated outbound to ASXNet, 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 FAQs for further details regarding digital certificates.

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.

Austraclear Software and Technical Documents

Frequently Asked Questions

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

Austraclear Software and Technical Documents

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 Microsoft .NET - Build modern apps and powerful cloud services
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
Microsoft Edge	Microsoft Edge	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.
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
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 e.g. 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 running the program. The security policy file will be delivered as MSI (Microsoft Installer) once downloaded (for browser deployment only.).

Get in touch

Austraclear Service Desk
ASX Settlement Operation | 20 Bridge Street | Sydney
NSW 2000
T: 1300 362 257 | Intl: +61 2 8298 8474
E: austraclear@asx.com.au | W: www.asx.com.au