

I-SEM Technical Specification (ITS)

VOLUME B: TECHNICAL VOLUME V9.1

COPYRIGHT NOTICE

All rights reserved. This entire publication is subject to the laws of copyright. This publication may not be reproduced or transmitted in any form or by any means, electronic or manual, including photocopying without the prior written permission of EirGrid plc and SONI Limited.

DOCUMENT DISCLAIMER

Every care and precaution is taken to ensure the accuracy of the information provided herein but such information is provided without warranties express, implied or otherwise howsoever arising and EirGrid plc and SONI Limited to the fullest extent permitted by law shall not be liable for any inaccuracies, errors, omissions or misleading information contained herein.

Table of Contents

Table of Contents.....	2
Table of Figures.....	3
Table of Tables.....	4
1 Disclaimer and Content Information.....	6
2 Introduction	7
2.1 Scope of this Volume.....	7
2.2 Structure of this Volume.....	8
3 Architecture Overview	10
3.1 General Architecture Overview	10
3.2 Common Solution Elements.....	11
3.2.1 Type 2 Vs Type 3 Communication Channels.....	11
3.2.2 Minimum System Pre-requisites for Access	11
3.2.3 SecuRity and Encryption Summary	12
4 Balancing Market Solution	13
4.1 Architectural Overview	13
4.1.1 Physical Overview.....	13
4.1.2 Logical Overview.....	14
4.2 Messaging Overview.....	15
4.2.1 WSDL Overview.....	15
4.2.2 Data Schemas – General Validation.....	20
4.2.3 Transaction Handling	20
4.2.4 General Considerations.....	24
4.3 Security And User Management	24
4.3.1 Two factor Authentication.....	24
4.3.2 Factor 1: Digital Certificates	24
4.3.3 Factor 2: MPI Application Password Authentication Process (Type 2)	28
4.4 Balancing Market Toolkit User Guide	29
4.4.1 Toolkit Overview	29
4.4.2 Toolkit Installation Process.....	30
4.4.3 Testing with the toolkit.....	34
5 SEMOpX Ex-Ante Markets Solution	36
5.1 Architectural Overview	36
5.2 Day-Ahead and Intraday Auction Markets	37
5.2.1 Messaging Overview.....	37
5.2.2 ETS Security	38
5.3 Intraday Continuous Market	39
5.3.1 Messaging Overview.....	39
5.3.2 M7 Security.....	40
5.4 Settlement & Clearing	40
5.4.1 Overview.....	40
5.4.2 Messaging Overview.....	40
5.4.3 SMSS Security.....	41
5.5 Process to Access Ex-Ante Market Technical Documentation.....	42
6 Capacity Market	43
6.1 Overview.....	43
6.2 Type 2 Activities.....	43
6.3 User Roles.....	44
6.4 Security	44
6.5 Minimum System Requirements	44

Table of Figures

Figure 1: I-SEM Architecture – Overview.....	10
Figure 2: Messaging Architecture - Logical Overview	14
Figure 3: WSDL Extract: Definitions section	16
Figure 4: Request Type to Schema Mapping	16
Figure 5: WSDL Extract: Request Types for participants	17
Figure 6: WSDL Extract: Attachment Types	19
Figure 7: WSDL Extract: Attachment Operations	19
Figure 8: Some Transactions may contain multiple Requests.....	21
Figure 9: Sample of Meter Data xml	23
Figure 10: Digital Signature Generation Process	27
Figure 11: Data Transfer Process	27
Figure 12: Non-Repudiation Process	27
Figure 13: Overview of Balancing Market Toolkit	30
Figure 14: Overview of SEMOpX Market Solution	36
Figure 15: Auction Markets Interface Mechanisms.....	37
Figure 16: Continuous Markets Interface Mechanisms	39
Figure 17: Continuous Markets Interface Mechanisms	39
Figure 18: Process for Requesting API documentation	42
Figure 19: Capacity Market solution overview	43

Table of Tables

Table 1: I-SEM Technical Specification Volumes	7
Table 2: Minimum System Pre-requisites for clients to access markets	11
Table 3: Summary of encryption standards across markets.....	12
Table 4: Mapping of New Request Types to existing types and schemas	17
Table 5: Processing Statistics Data Fields.....	23
Table 6: Minimum Browser Requirements for Capacity Market Portal	44

Document History

Version	Date	Comment
1.0	08/07/2016	Initial Draft.
2.0	05/09/2016	Updates for Release 3 of the I-SEM Technical Specification
3.0	28/10/2016	Addition of Section 6 (Capacity Market)
4.0	31/01/2017	Update to certificate naming convention Further detail on hash function used.
5.0	05/05/2017	Inclusion of Balancing Market Toolkit Guide Update on WSDL Further clarification on encryption Update on digital signature generation
6.0	17/07/2017	Updates to Balancing Market Toolkit Guide
7.0	13/10/2017	Change name from NEMO to SEMOpX CCQT/PIT Connectivity information included Minor update to Digital Certificate Installation
8.0	01/12/2017	Updated instructions for Type 3 Connectivity
9.0	31/07/2018	Updated Balancing Market Toolkit URL
9.1	13/12/2018	Updated Balancing Market Toolkit URL

Distribution List

Name
All participants

Source / Reference Documents

Document Name	Document Reference
I-SEM_Technical Specification (ITS) Volume C: Balancing Market	9.1

1 DISCLAIMER AND CONTENT INFORMATION

This document has been prepared to provide participants with sufficient information in order to develop their own systems to interface with the I-SEM.

The following disclaimers relate to the content of this document and associated volumes and any use by participants of the information provided therein.

1. EirGrid and SONI accept no responsibility for decisions made or actions taken by participants as a result of the information presented in this document or associated documents. Furthermore, EirGrid and SONI do not indemnify any commercial or organisational decisions made by participants in relation to the information herein.
2. This document represents the most up-to-date information on the I-SEM Systems as they have been developed. With this in mind, it is not appropriate simply to compare the document against the market rules; instead, the document is aligned with a release of the I-SEM Systems.
3. The information provided in this document is based entirely on documentation and information provided by the software vendor. Although EirGrid and SONI have made all reasonable efforts to ensure that the information presented is correct, they cannot guarantee the information provided.
4. Further changes to the technology described in this document may result as new information comes to light during future phases of the market development. To mitigate the impact of such changes, EirGrid and SONI will be issuing planned updates to this document and associated documents (where appropriate).

2 INTRODUCTION

2.1 SCOPE OF THIS VOLUME

The I-SEM¹ Technical Specification (ITS) comprises a number of volumes which provide participants with the information necessary for them to develop their own systems to interface with the I-SEM central market systems.

The volumes of the I-SEM Technical Specification are:

Volume	Document
A	ISEM TS (Overarching Volume)
B	ISEM TS (Technical Volume)
C	ISEM TS (Balancing Market Volume)
D	ISEM TS (SEMOpX Ex-Ante Markets Volume)
E	ISEM TS (Capacity Market Volume)
F	Intentionally blank
G	ISEM TS (Glossary)

Table 1: I-SEM Technical Specification Volumes

This document covers the **technical aspects** of the interfaces which are available for participants to communicate with the I-SEM Systems.

The focus of this document is the Type 3 Communication Channel, i.e. submission and retrieval of I-SEM Data Transactions via computer based mechanisms such as web services or API (Application Programming Interfaces). In addition, some information is also provided on the connectivity requirements to facilitate Type 2 Communication Channel (i.e. data submission and retrieval using Graphical User Interfaces (GUI) by participant users.

The functional aspects of these interfaces and the information on the data schemas are contained in the *I-SEM Technical Specification Volume C: Balancing Market* and *Volume D: SEMOpX Ex-Ante Markets*.

Definitions and terms contained within the *I-SEM Technical Specification Volume G: Glossary* provide information to support the understanding of the content presented in the volumes of the I-SEM Technical Specification.

Notes:

1. References in this document to “query” relate to the retrieval of data from the I-SEM Systems as opposed to the concept of formal queries as defined in the Trading and Settlement Code.
2. Whilst this document refers to the market as “I-SEM”, the market will continue to legally be referenced as the “Single Electricity Market (SEM)”.
3. For the avoidance of doubt, please note that references in this document to ‘NEMO’ relate to SEMOpX.

¹ The market arrangements and associated delivery project are known as the I-SEM, but parties are asked to note that the legal name for the new arrangements will be the Single Electricity Market (SEM).

4. *This version of the technical volume covers the Balancing Market and SEMOpx Market. The technical volume will be updated to cover the Capacity Market following publication of Volume E, as well as any corrections or amendments arising from updates to the Balancing and SEMOpx markets.*

2.2 STRUCTURE OF THIS VOLUME

The information in this document is organised to present the technical information relevant to each specific market within its own section of the document.

The document is structured as follows:

- **Section 3** Architectural Overview provides an architectural overview and some general information relevant to all markets.
- **Section 4** Balancing Market provides technical information relating to the Balancing market presented as follows:
 - Messaging Overview – outlines the integration mechanism for Type 3 interfaces covering protocols, data format and explanation of the Balancing Market WSDL.
 - Security – describes how security is implemented and how digital certificates are handled across both Type 2 and Type 3 interfaces.
 - Connectivity Requirements – lists the software and hardware requirements for both Type 2 and Type 3 integration.
- **Section 5** SEMOpx Ex-Ante Markets provides technical information relating to the Day-Ahead Auction Market, the Intraday Auction Market and the Intraday Continuous Market presented as follows:
 - Architectural Overview – presents a high level view of how the SEMOpx market is structured from a physical and logical perspective
 - Day-Ahead and Intraday Auction Markets:
 - Messaging Overview – provides summary view and linkages to detailed documents covering protocols, data format and explanation of the ETS API.
 - Security – provides summary and linkages to detailed documents that describe how security is implemented for both Type 2 and Type 3 interfaces using ETS.
 - Connectivity Requirements – lists the software and hardware requirements for both Type 2 and Type 3 integration for using ETS client and API respectively.
 - Intraday Continuous Market:
 - Messaging Overview – provides summary view and linkages to detailed documents covering protocols, data format and explanation of the M7 API.
 - Security – provides summary and linkages to detailed documents that describe how security is implemented for both Type 2 and Type 3 interfaces using M7.
 - Connectivity Requirements – lists the software and hardware requirements for both Type 2 and Type 3 integration for using M7 client and API respectively.

Note: The ETS and M7 API Technical Specifications are not publically available. Participants can obtain the API documentation following the signing of a Non-

Disclosure Agreement (NDA). The details on how to request access are outlined in Section 6.2 in I-SEM Technical Specification Volume D: SEMOpX Ex-Ante Market.

- **Section 6** Capacity Market provides technical information relating to the Capacity Market. The information presented will cover similar technical aspects as presented for the other markets. Please note this section will be provided in later versions of this document.

3 ARCHITECTURE OVERVIEW

3.1 GENERAL ARCHITECTURE OVERVIEW

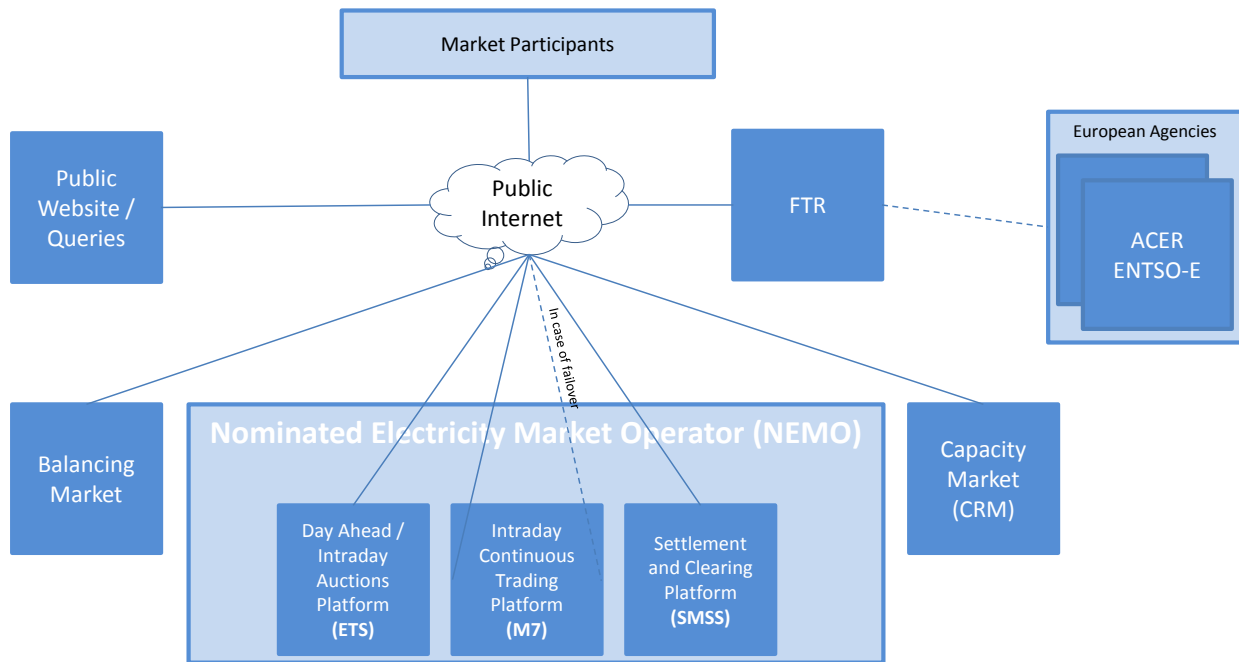


Figure 1: I-SEM Architecture – Overview

Figure 1 above presents the overall architecture for the I-SEM solution. The elements of note for participants are:

- A public website will be hosted by EirGrid/SONI which will be accessible via a single URL over the public internet.
- The Balancing Market solution is located across two physical data centres. This is accessible to participants via a single URL for each Communication Type. Connectivity is over the public internet.
- SEMOpix accessible to participants via different URLs:
 - Day-Ahead / Intraday Auctions Platform (ETS Application)
 - Intraday Continuous Trading Platform (M7 Application)
 - Settlement and Clearing Platform (Spot Market Settlement System (SMSS))
 - Resilience for each service is managed by the Nominated Electricity Market Operator and is transparent to the participant for all interfaces with the exception of the Type 3 interface for Continuous Trading. In a Fail Over scenario participants are responsible for choosing a second URL to maintain access to this service.
- The Capacity Market solution is accessible to participants via a single URL. Connectivity is over the public internet.
- The Financial Transmission Rights (FTR) solution is offered as a service via JAO (Joint Allocation Office). Participants will directly engage with JAO.
- EirGrid/SONI will establish connectivity between each of the market component solutions for a number of functional reasons. However, participants will need to establish direct connectivity to each market solution to participate in that particular market.

- Connectivity to a number of European agencies will be established for several reasons including REMIT (Regulation of wholesale Energy Market Integrity and Transparency).
- A Query Management Portal will also be available for participants to log queries in relation to their engagement with the market and view the status of existing queries. The connectivity details for this element will be communicated in an updated version of this Technical volume.

3.2 COMMON SOLUTION ELEMENTS

3.2.1 TYPE 2 VS TYPE 3 COMMUNICATION CHANNELS

- The Type 2 Communication Channel is screen (Graphical User Interface (GUI)) based, to provide a human-to-computer interface. In most markets these requests are processed by the same back end technology as is used for the Type 3 Channel. For example, the Balancing Market utilises the same web services to facilitate both Type 2 and Type 3 Communications.
- Type 3 Communications refer to automated, computer-to-computer interfaces. They generally use web services as the I-SEM preferred standard for integration. Some Type 3 Communications will be via vendor prescribed technologies, such as the AMQP based M7 API for the SEMOpX Intraday Continuous Market.
- In certain cases, the Type 2 Channel will provide additional functionality that is not supported directly by the Type 3 Channel.

3.2.2 MINIMUM SYSTEM PRE-REQUISITES FOR ACCESS

Table 2 outlines the minimum pre-requisites for a client system for access across all market interfaces.

Area	Requirement
Operating System	Windows 7 - 64 bit Windows 10 (<i>except M7 which will not be supported on Windows 10 until End of 2017</i>)
Other Software	MS Excel 2007, 2010, 2013, . <i>Formats used .csv and .xlsx (Excel 2007 or later)</i> Adobe Reader Java Version 1.8 _91 or higher
Browsers	Internet Explorer 11 or higher
Minimum Hardware Specifications	CPU: Intel i5 over 2GHz 8 GB RAM 6 GB Hard drive for installations

Table 2: Minimum System Pre-requisites for clients to access markets

- Table 2 provides a list of the minimum pre-requisites to run ETS, M7 clients and browser access to the Balancing Market, the Ex-Ante Market Settlement and Clearing and the Capacity Market.
- The table is based on an aggregation of individual vendor inputs from each market for each interface access type.

- EirGrid is not certifying the list of pre-requisites as a single specification running all applications and/or browser access. Neither have we tested this in operation.
- Many participants may also choose to use separate machines for different markets according to their business needs. In this case, participants may choose to follow the individual pre-requisites for each relevant market.
- The pre-requisites list will be updated following the publications of I-SEM Technical Specification Volume E

3.2.3 SECURITY AND ENCRYPTION SUMMARY

Table 3 provides a summary view of the encryption standards used across the markets.

Interface	Encryption Algorithm	Transport Encryption	Notes
Ex-Ante Auction Markets ETS Client	*SHA2 (SHA-256)	TLS 1.2	*ETS will move from SHA1 to SHA2 with the version release for I-SEM Go-Live
Ex-Ante Auction Markets ETS API	SHA2 (SHA-256)	TLS 1.2	
Ex-Ante Continuous Trading M7 (Client & API)	SHA2 (SHA-256)	**TLS 1.2	**M7 will move from TLS 1.0 to TLS 1.2 by the end of 2016
Balancing Market	SHA2 (SHA-256)	TLS 1.2	

Table 3: Summary of encryption standards across markets

4 BALANCING MARKET SOLUTION

4.1 ARCHITECTURAL OVERVIEW

4.1.1 PHYSICAL OVERVIEW

The diagram in Section 3.1 *Figure 1: I-SEM Architecture – Overview* presents the physical connections in place to the I-SEM Balancing Market Solution.

From the internet, the Market Web Interfaces for CCQT/PIT can be accessed via:

- <https://mpc.sem-o.com/mws/> for Web Service access
- or
- <https://mpc.sem-o.com/mpi/> for Internet access (GUI)

An external service (load balancer) will continuously monitor both production web interfaces and redirect traffic to the alternate site should there be a problem with one of the web interfaces.

Participants should not make any assumptions on which site they are connecting to as the site will vary according to the Market Operator's operational decisions.

Details on the Production URL for Market Trial will be presented in a future Technical Liaison Group (TLG) Meeting.

	Type 2	Type 3
Balancing Market	https://mpc.sem-o.com/mpi/	https://mpc.sem-o.com/mws/
Capacity Market	TBC	N/A
SEMOpx	ETS Client M7 Client	Connectivity details available via SEMOpx API NDA process

Table 4: Summary CCQT/PIT connectivity across markets

Note: Accessing the market directly via IP address is not supported.

4.1.2 LOGICAL OVERVIEW

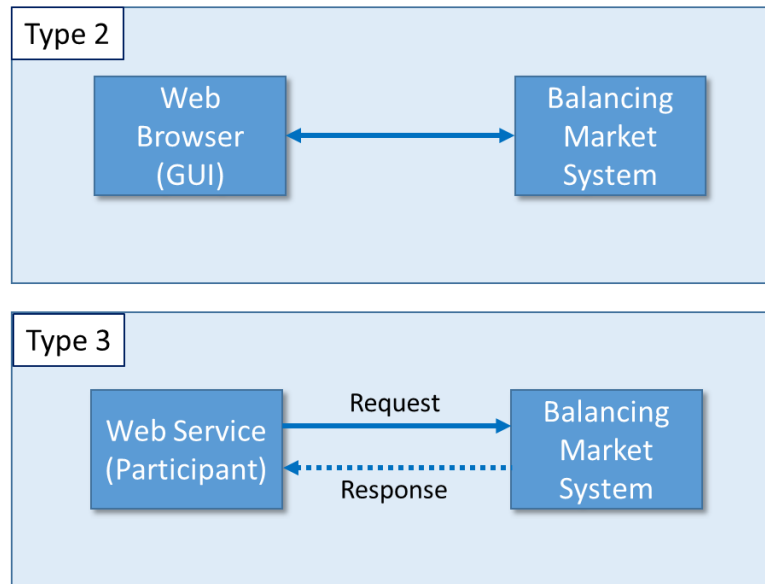


Figure 2: Messaging Architecture - Logical Overview

Figure 2 above gives a logical overview of the messaging architecture for Type 2 and Type 3 Communication Channels. The below items provide some further details on this.

- All connections are initiated external to the Balancing Market Solution (i.e. by participants, Meter Data Providers, etc.) and operate in a synchronous request-response mode.
- For Type 2 Communications, the participant's authorised user connects to the Market Participant Interface (MPI) and is authorised by selecting the appropriate Digital Certificate and entering their application password at initial login. From here, they can select one of the following options: Trading; Registration; Reports; File Exchange; or Settlements.
- For Type 3 Communications, the participant's system also needs to present the appropriate Digital Certificate on connection to the Balancing Market web server. The web service request will indicate the specific schema to be utilised for this purpose. A single web service now covers both metering and the other market functions.
- The web services for accessing the Balancing Market have been developed using Java technology AXIS 2.0.
- All data submitted to the Balancing Market is required to be in XML format.
- The specific format for each report is outlined in the *I-SEM Technical Specification Volume C: Balancing Market*.
- Further information on digital certificates is outlined in Section 4.3 Security And User Management.
- Access to market information for non-participants will be described in a subsequent I-SEM document at a later date.

4.2 MESSAGING OVERVIEW

This section provides an overview of interfacing using the Type 3 Communications Channel for the Balancing Market. Further details are available in the Balancing Market Toolkit User Guide section of this document and within the Balancing Market Participant Web Services Client Toolkit itself.

To interface with the Balancing market system through Type 3 Communications Channel:

- 1) Create request xml with required data using an appropriate schema
 - a. See *I-SEM Technical Specification Volume C: Balancing Market* for details of request schemas.
 - b. See section 4.2.1.2 below for details of Request Types.
- 2) Use a valid I-SEM certificate to generate a digital signature based on this request xml
 - a. See section 4.3.2.3.1 below for details on generating the digital signature
- 3) Generate a request input xml using the submitAttachment method based on the mi-webservice WSDL.
 - a. See section 4.2.1.3 for details on the submitAttachment method and steps 4 through 6
- 4) Populate the requestSignature element of the RequestAttInfo element with the digital signature generated in Step 2
- 5) Populate the requestData element of the RequestAttInfo element with the request xml created in Step 1. This request xml must be Base64 encoded and populated as an MTOM SOAP attachment.
- 6) Set appropriate values for remaining elements within RequestAttInfo
- 7) Submit the input request to the I-SEM Balancing Market system
- 8) Where a response is provided, the responseData element of the ResponseAttInfo element will be populated. The same schema will be used as was used in the request. The responseData content will be Base64 encoded and in-line. A SOAP attachment is NOT used in the response.

There is a single Web Service Definition Language (WSDL) that is used by all web service interfaces to the Balancing Market solution. Using the WSDL, the participant specifies the appropriate schema in their request. The specific validation rules associated with each schema are defined in the *I-SEM Technical Specification Volume C: Balancing Market*

This volume provides a view of how the WSDL is structured, the validation applicable across all schemas, and some general messaging considerations.

4.2.1 WSDL OVERVIEW

The WSDL is published on the I-SEM public website [here](#).

The following section provides an overview of a number of items on the WSDL that are noteworthy.

4.2.1.1 DEFINITIONS

The Definitions section of the WSDL outlines the standard WSDL definitions applicable to the web service. The namespace structure has changed to reflect standard use of “urn:” naming convention. The *mime* definition has moved to the newer *xmime* definition.

```
<?xml version="1.0" encoding="UTF-8"?>
<wSDL:definitions name="MiWebService" targetNamespace="urn:abb.com:project/sem" xmlns:wSDL="http://schemas.xmlsoap.org/wSDL/"
xmlns:soap="http://schemas.xmlsoap.org/wSDL/soap/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xmime="http://www.w3.org/2005/05/xmime" xmlns:types="urn:abb.com:project/sem/types" xmlns:tns="urn:abb.com:project/sem">
```

Figure 3: WSDL Extract: Definitions section

4.2.1.2 REQUEST TYPES

The request types are used to link by the calling web service to identify the specific schema to be utilized to parse the request as outlined in *Figure 4* below.

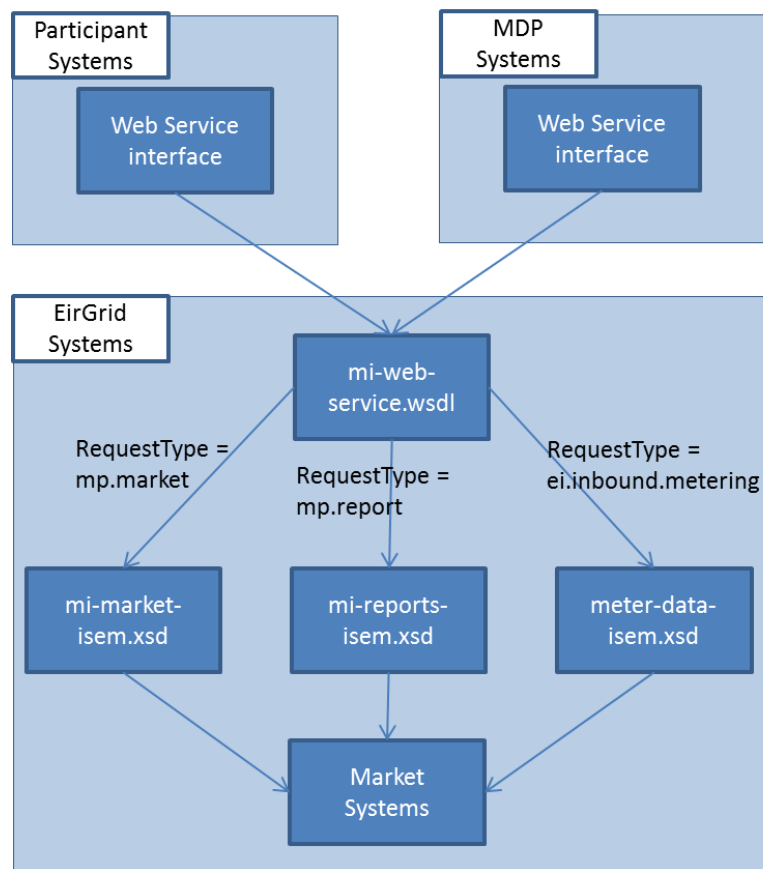


Figure 4: Request Type to Schema Mapping

The *RequestType* naming convention has changed from a two tier type and identifier structure in the current market, to a single tier (more extensible) format. Request Types beginning with “mp.” are relevant to participants. *Table 4* identifies how these request types map to the existing request types.

New WSDL	Current WSDL		Schema
<u>Request Type</u>	<u>Request Type</u>	<u>Request Identifier</u>	
mp.market	MPI	BID	mi-market-isem.xsd
mp.report	MPI	RPT	mi-report-isem.xsd
mp.registration	MPR	REG	mpr-isem.xsd

ei.inbound.metering	N/A	N/A	meter-data-isem.xsd
csb.report	STTL	Various	csb-report.xsd.

Table 4: Mapping of New Request Types to existing types and schemas

The current Settlement Request Types have now been replaced with the csb.report Request Type.

Note: The mp.info request type is no longer relevant to the I-SEM relating to market message functionality. Market messages in I-SEM are accessed via the MPI GUI. As such this has been removed from the WSDL.

The metering data schema is identified using the ei.inbound.metering Request Types.

```

<!-- Request Type -->
<xsd:simpleType name="RequestType">
  <xsd:annotation>
    <xsd:documentation>
      Identifies the request type. Valid values are:

      mp.market:
      Market participant market data requests (submit, query)

      mp.report:
      Market participant report requests (report list, report
download)

      mp.registration:
      Market participant registration requests

      csb.report:
      CSB report requests (report list, report download)

      ei.inbound.metering
      External Interface inbound data from MDPs. Meter Data
Provider
      data requests (submit, query)

    </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="mp.market" />
    <xsd:enumeration value="mp.report" />
    <xsd:enumeration value="mp.registration" />
    <xsd:enumeration value="csb.report" />

    <xsd:enumeration value="ei.inbound.metering" />
  </xsd:restriction>
</xsd:simpleType>

```

Figure 5: WSDL Extract: Request Types for participants

4.2.1.3 ATTACHMENTS AND ATTACHMENT OPERATIONS

4.2.1.3.1 SUBMITTING REQUEST PAYLOADS USING THE SUBMIT ATTACHMENT

The WSDL maintains and extends the usage of the *submitAttachment* operation which was previously the recommended method for submissions in the existing WSDL. This operation allows the web service to handle binary types.

All the data that is submitted to the MMS via the web service must be delivered as SOAP attachment encapsulating the XML payloads (compliant with corresponding schema) making use of the submit attachment operation.

As part of the submitAttachment method the RequestAttInfo element must be populated with the details to be submitted to the Balancing Market system as follows:

Element Name	Details
requestType	The type of request (e.g.mp.market)
adminRole	Always should be set to "false"
requestDataCompressed	Always should be set to "false"
requestDataType	Always should be set to "XML"
sendRequestDataOnSuccess	Include request data in the response even if it is successful. Optional "true" or "false".
sendResponseDataCompressed	Always should be set to "false"
requestSignature	The digital signature of the request payload.
requestData	This should contain the request payload xml. It must be Base64 encoded.

The usage of the submitAttachment operation also extends the size of message that can be handled. The revised recommendation on maximum message size is now **6 MB**. However, this is a recommendation and will not be enforced. The submission of larger messages may be possible but may suffer poor performance or otherwise prove to be problematic.

The *submitBody* operation has been retired which was limited to test only submissions. It is replaced by the submitAttachment method.

4.2.1.3.2 SUBMITTING ATTACHMENTS

In addition to the XML data payload, additional attachments in other formats (e.g. PDF, etc.) can also be submitted. Previously submitted XML payloads can be queried using the submit attachment operation. However, the additional attachments will only be listed as part of the response XML. The additional attachments themselves can be retrieved using the retrieve attachment operation. The remove attachment operation can be used to delete any previously submitted additional attachments.

NOTE: An additional update to this document and WSDL will confirm the operation of the proposed attachment mechanism at a later date.

```

<!-- Attachment -->
<xsd:complexType name="AttachmentType">
  <xsd:sequence>
    <xsd:element name="success" type="xsd:boolean" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="documentType" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="documentMimeType" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="fileName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="binaryData" type="xsd:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="signature" type="types:AttachmentSignature" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="AttachmentReferenceType">
  <xsd:sequence>
    <xsd:element name="success" type="xsd:boolean" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="documentId" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="documentType" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="documentMimeType" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="fileName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
<!-- Request Data -->

```

Figure 6: WSDL Extract: Attachment Types

Two new operations have been provided:

1. retrieveAttachments – allows participants to request an attachment by Attachment ID
2. removeAttachments – allows participants to remove an attachment that was previously provided based on Attachment ID

```

<!-- For soap file attachment based requests -->
<wsdl:operation name="submitAttachment">
  <soap:operation soapAction="urn:abb.com:project/isem/submitAttachment"/>
  <wsdl:input>
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>
<!-- For soap body based requests -->
<wsdl:operation name="retrieveAttachment">
  <soap:operation soapAction="urn:abb.com:project/isem/retrieveAttachment"/>
  <wsdl:input>
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>
<!-- For soap body based requests -->
<wsdl:operation name="removeAttachment">
  <soap:operation soapAction="urn:abb.com:project/isem/removeAttachment"/>
  <wsdl:input>
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>

```

Figure 7: WSDL Extract: Attachment Operations

4.2.1.4 FUTURE PROOFING AND ADMINISTRATION

The WSDL has been written with future flexibility in mind. It contains a number of items that are not directly relevant for participants or for the I-SEM implementation. These include:

- Compression – Both the request and response messages contain elements that may be used in future to support compression.
- adminRole – This attribute is for internal use only and is not relevant to participants.

Note: Reference to JSON as a future capability has been removed from the WSDL for clarity.

4.2.2 DATA SCHEMAS – GENERAL VALIDATION

When participants submit data requests, the following processing is performed in the order outlined below:

1. The submitted data is first validated to ensure it is valid XML and complies with the Schema; (The data can only be submitted in XML file format).
2. The security permission for the combination of participant and participant user is checked – including some checks against Registration data, e.g. resource name is valid, the participant owns the resource etc.
3. When data has been successfully validated and processed, this is indicated to the participant through information messages. When data has failed validation and has not been processed the failure is indicated by error messages.
4. If any validation fails, then all subsequent validations are also performed to the extent possible so that all errors are reported to the participant. However, there are some critical validations like “market not open” or “invalid resource”, which will stop further validations.
5. Validation rules specific to individual Requests are detailed in the relevant sections of the accompanying *I-SEM Technical Specification Volume C: Balancing Market* document.

The specific XML format validation rules that are applied are as follows:

- An XML data stream is a simple text file containing American Standard Code for Information Interchange (ASCII) characters only. Each data field in the data stream begins with a pre-defined XML begin tag and ends with a pre-defined XML end tag. No hidden formatting information is allowed. The XML data streams submitted must adhere to the corresponding schema provided.
- Blank lines are permitted in the data streams and are ignored by the XML parser. White space in the number data field is also ignored.
- Comment lines must begin with “<!--” and end with “-->”. Any text between these two tags will be interpreted as a comment and will be ignored.
- All data information in a given template must be included in exactly the same order as listed in the defined XML schema. Any additional information or omissions will be considered as an error and the relevant transaction will be rejected.
- For the submitted XML template, an optional field can have a value of null. If a value has been entered, it will take precedence over the default value.
- All mandatory fields must have values entered.

4.2.3 TRANSACTION HANDLING

A transaction may contain a number of processing requests – details on which transactions support multiple requests are specified on a Transaction Type or specific Transaction level can be found in the *I-SEM Technical Specification Volume C: Balancing Market* document.

For Type 3 Communications, the entire XML data stream will be considered as one Transaction.

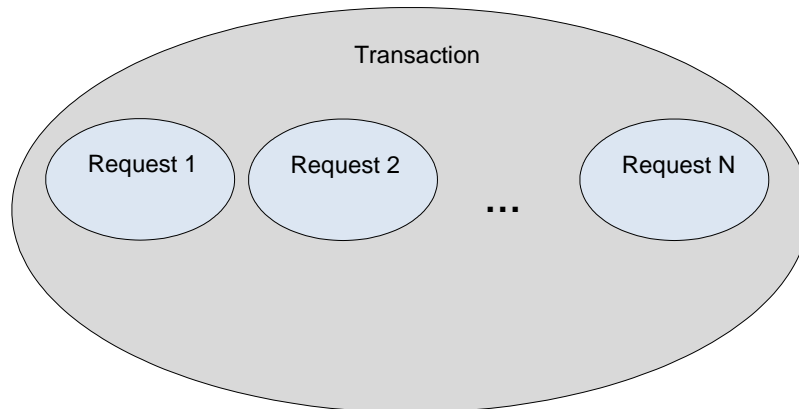


Figure 8: Some Transactions may contain multiple Requests

4.2.3.1 I-SEM TRANSACTION ID

The I-SEM Balancing Market system will assign a Transaction ID. This Transaction ID is a unique 10-character code that will be received by the participant in the response message. There is one Transaction ID per XML stream, regardless of how many Requests form part of that stream.

4.2.3.2 EXTERNAL ID

Participants have the option of submitting an External ID as part of a submission. These External IDs are optional items at a Request level, so a submitted Transaction made up of five Requests could have External IDs provided for none, or up to all five, of those Requests.

The External ID is not used by the Balancing Market system in processing and is treated as a pass-through field. The last External ID (if applicable) used to submit Market Interface and Registration Data is also returned when a Query is run against that data.

The External ID is returned as part of the Transaction response, at a Request level, and may be used by participants for their own tracking purposes.

4.2.3.3 MULTIPLE TRANSACTIONS

- Transactions received will be generally processed on a first-come first-served basis. However, sequencing cannot be guaranteed. The solution architecture for I-SEM is cognisant of the fact that there are multiple users on multiple channels that may be submitting updates to the same data.
- If a participant identifies a specific need to sequence their submissions then that participant should implement appropriate business and system processes to meet this requirement.
- For example, a participant who chooses to only use the Type 3 Channel from a single user with a single login could configure their application such that each transaction is submitted in sequence and a subsequent transaction is not submitted until a response has been received.
- Please note many interactions support submissions by multiple users on multiple channels and do not require sequencing of submissions.
- Users may initiate multiple sessions using the same Digital Certificate.
- Sessions will be timed-out at the Firewall after 15 minutes of inactivity.

4.2.3.4 SOAP MESSAGE STRUCTURE OVERVIEW

The specific details of the Simple Object Access Protocol (SOAP) envelope and header structures can be made visible by using the toolkit provided with this document.

A few specific points are worth noting below:

- All submissions are handled as synchronous request response messages as is the case in the existing market.
- The transport mechanism is Hypertext Transfer Protocol (HTTPS).

4.2.3.5 REQUEST

Each request type is associated with a specific schema as outlined in the WSDL description.

Each schema will have a specific header.

In the case of MDP and MI schemas, the XML tags for request and response are the same. The attributes differentiate a request from a response. This facilitates a response being re-used as a submission if required.

Meter Data Example

For all XML templates in this schema (Submission, Response Successful, and Response failed), we are using the same tag IMPORT_METER_REQUEST. The full XML examples will be released as part of Release 3 of the I-SEM Technical Specification.

Submission:

```
<IMPORT_METER_REQUEST xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="meter-data-isem.xsd"
  >
```

Response successful:

```
<IMPORT_METER_REQUEST xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="meter-data-isem.xsd"
SUCCESS="true"
VALIDATION="PASSED">

Response failure:
<IMPORT_METER_REQUEST xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="meter-data-isem.xsd"

SUCCESS="false"
VALIDATION="FAILED">
```

Figure 9: Sample of Meter Data xml

4.2.3.6 RESPONSE

The response header will remain same as per current usage.

Each Transaction submitted receives a Response, which consists of:

- Processing Statistics;
- Messages; and
- Original Data Submitted by the participant.

Table 5 describes the processing statistics data fields:

Data Field	Description
Valid	The number of valid Requests
Invalid	The number of invalid Requests
Received	The number of received Requests
time_ms	The time spent in processing the data in milliseconds
time_stamp	Received time (string format as below)
transaction_id	Transaction ID is a unique 10-character code generated during processing

Table 5: Processing Statistics Data Fields

The time_stamp field is not designed for automated consumption – the XML_time_stamp field is recommended for this.

The time_stamp field is a string of the following form:

dow mon dd hh:mm:ss zzz yyyy

Where:

- dow is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat);
- mon is the month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec);
- dd is the day of the month (01 through 31), as two decimal digits;
- hh is the hour of the day (00 through 23), as two decimal digits;
- mm is the minute within the hour (00 through 59), as two decimal digits;
- ss is the second within the minute (00 through 59), as two decimal digits;

- zzz is the time zone (and may reflect daylight saving time). Standard time zone abbreviations include those recognized by the method parse. If time zone information is not available, then zzz is empty – that is, it consists of no characters at all;
- yyyy is the year, as four decimal digits.

Note: All time on Type 3 interfaces is represented in UTC.

4.2.4 GENERAL CONSIDERATIONS

The following sections detail items that should be considered when making submissions to the Balancing Market.

4.2.4.1 PERFORMANCE

All Transactions to the Balancing Market are synchronous. The total processing time of the transactions is affected by a number of factors:

- The number of Requests that are part of the Transaction;
- The volume of data to be downloaded (mostly in the case of reports);
- The participant's internet connection speed;
- The participant's Web Service implementation;
- The participant's network implementation;
- The validation (Meter data) during a synchronous call; and
- The size of any submission.

4.2.4.2 GENERAL RECOMMENDATIONS

- Transactions should be kept to less than 6MB in size.
- If participants are unsure whether a Data Transaction was successfully submitted, it is recommended they query their data to ensure that their transaction came through and was successfully validated.

4.3 SECURITY AND USER MANAGEMENT

4.3.1 TWO FACTOR AUTHENTICATION

Participants who are accessing the Balancing Market via Type 2 interfaces will require two independent forms of authentication – a valid digital certificate and an application password.

Type 3 interfaces will not require an application password. However, the existing certificate password will continue to be used for digitally signing market submissions.

4.3.2 FACTOR 1: DIGITAL CERTIFICATES

- The Balancing Market utilizes digital certificates for communications with participants. The digital certificates are used to both encrypt the messages between participants and the systems and to validate the authenticity of the message.
- A new Symantec Public Key Infrastructure (PKI) client will be used in I-SEM for interactions with the Balancing Market Systems. It will allow the automatic installation of client certificates onto the user's PC where the existing certificate, expiry dates and other details can be viewed. The specific details regarding installation are outlined in the CCQT Market Participant Guide, found on the SEMO website [here](#).
- Digital certificates are x.509 compliant.
- The digital signature element in the SOAP message is optional as not all Transactions (such as downloading reports) require Digital Signatures. However, the server-side code ensures that the Digital Signatures are mandatory for any data submit Transactions. If a participant does not provide a Digital Signature for these Transactions an error message will be returned.
- There is no Digital Signing of details returned by the Market Operator to participants.
- In the case of multiple Requests in the same Transaction, a single Digital Signature is created relating to all data submitted. Where attachments are submitted with a request, an additional digital signature per attachment may be used.

4.3.2.1 DIGITAL CERTIFICATES AND USERS

- Each user identifies themselves to the Balancing Market using a Digital Certificate. This includes both Type 2 (screen-based users accessing the MPI) and Type 3 (computer to computer Web Services) communications.
- Users are associated uniquely with a single participant. Each user with access to a particular Functional Area will be able to view or enter information for the entire Functional Area. For example, a user with access to the Trading Functional Area will be able to trade for all Units registered to the participant.
- The above does not preclude a person, e.g. working for a Data Processing Entity, acting as a user for two participants, but that person must have a Digital Certificate for each user/participant.
- It is recommended that the display name of each Digital Certificate is renamed on enrolment within the PKI client to avoid any confusion in later use.

4.3.2.1.1 DIGITAL CERTIFICATE EXPIRY

- Digital certificates are issued with a specific expiry date (one year after issuing) after which the certificate is no longer valid and needs to be renewed. This is a key element in maintaining the validity of the certification process.
- It is the responsibility of the participant to manage the expiry date of their certificate(s) and ensure they are renewed in advance.
- For Type 2 Communications, a pop-up window will now be displayed when a participant logs into the MPI if their digital certificate is due to expire in less than one month. This reminder pop up will be displayed each time the user logs into the MPI.
- Information (text only) will be provided on screen outlining the implications of not renewing in time along with instructions on how to go about renewing the certificate.
- The user will be required to acknowledge the reminder by selecting 'OK' before proceeding with MPI activities.

- The registered email address for the certificate will also receive an email in advance of the expiry date advising that the certificate will expire.

4.3.2.2 DIGITAL CERTIFICATE NAMING CONVENTION

- The username is determined from the Digital Certificate used to establish the TLS connection.
- The Certificate Name (CN) will have the format *user_name@party_name*. The user name is the individual who will use the certificate. The party name will take the form of **PY_xxxxxx** where xxxxxx is a unique identifier typically assigned to the organisation for whom the individual is acting. (Note: Volume C of the Technical Specification describes the relationship between User, Party and Participant.)
- This username must match the user_name/party_name in the request XML.
- New certificates will be required to access the I-SEM Balancing Market (Note the same certificate will be used for the Capacity Market). The current SEMO certificates can continue to be used for read access to the existing market for a period of time post I-SEM go-live.

4.3.2.3 NON-REPUDIATION PROCESS

The Digital Signature is used date to support Non-Repudiation of submitted data.

The I-SEM Balancing Market solution requires Digital Signatures for data submitted by participants as follows:

- Market Interface data submit Transactions;
- Registration data submit Transactions;
- Meter Data submitted by Meter Data Providers; and
- Any Market Interface data submitted through the Type 2 Channel will be Digitally Signed by the application automatically.

4.3.2.3.1 CLIENT SIDE

A Market Interface Client (i.e., Browser for Type 2 or a Web Service client for Type 3) creates the Digital Signature for the XML data being submitted to the Market Interface Web Service. The Digital Signature is created as the RSA encrypted SHA2 (SHA-256) digest of the canonicalised XML data. The steps a Market Interface Web Service client needs to follow to create the Digital Signature are:

1. Create a DOM representation of the XML data;
2. Create a canonicalised representation of the DOM data. The canonicalised representation should follow the form described in <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>;
3. Create the signature RSA encryption of the SHA2 (SHA-256) digest of the canonicalised representation. The signature is encrypted using the participant's private key;
4. Encode the binary signature into a base64-encoded string;
5. Place the Signature string in the SOAP message;
6. Store the XML data as it may be needed later to support Non-Repudiation of the submitted XML data.

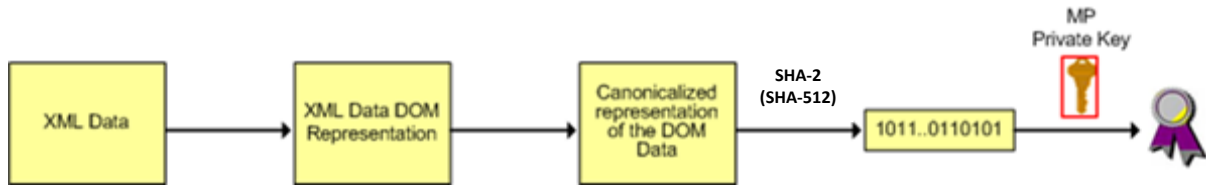


Figure 10: Digital Signature Generation Process

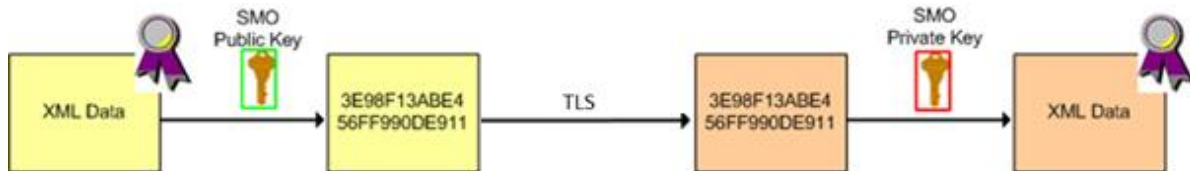


Figure 11: Data Transfer Process

- In Figures Figure 10, Figure 11, Figure 12 the yellow boxes represent the steps on the participant side and the salmon coloured boxes represent the steps happening on the I-SEM side.
- The XML data along with the Digital Signature is then encrypted using the Market Operator public key. This encrypted data is sent within a TLS tunnel to the Market Operator web server.

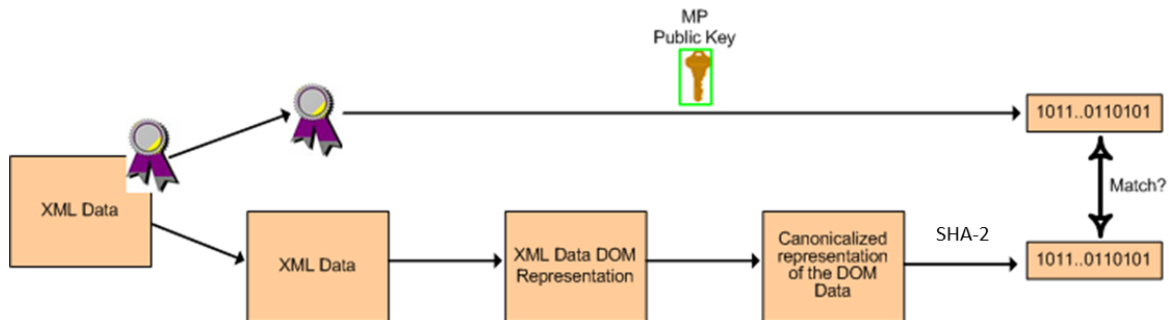


Figure 12: Non-Repudiation Process

NOTE: The inclusion of irrelevant whitespace, line feeds and carriage returns within the xml file has been found to generate issues particularly when generating submissions from a .NET IDE.

For reference as a guide when designing an integration mechanism we have included the following example of .NET code. It performs an initial formatting operation which participants may find useful.

```
Create xml DOM and remove whitespace, carriage return and line feeds
Dim objXMLDoc As New XmlDocument
objXMLDoc.LoadXml(strRequestXMLData)
'loop through every text node

For Each Node As XmlNode In
doc.SelectNodes("//text()")
Node.Value
=
System.Text.RegularExpressions.Regex.Replace(Node.Value, "\s+",
" ").Trim
Next
strRequestXMLData = objXMLDoc.OuterXml
```

```
strRequestXMLData = Replace(strRequestXMLData,  
vbCrLf, "")
```

where StrRequestXMLData contains the initial xml request file

4.3.2.3.2 CONTESTING

The contesting party should send the “original” XML file to an agreed third party. Using a dedicated offline application, the agreed third party would generate the SHA2 hash code for the file being contested and compare it with the hash code obtained by using the participant Public Key to decrypt the Digital Signature which was stored against the original Transaction.

4.3.3 FACTOR 2: MPI APPLICATION PASSWORD AUTHENTICATION PROCESS (TYPE 2)

The following descriptions outline the high level process flows for I-SEM MMS two-factor authentication.

4.3.3.1 LOGIN PROCESS

- a. The participant attempts to login via the MPI URL on their web browser. The browser will ask for the Symantec client certificate to be submitted.
- b. The solution verifies that the Certificate is not revoked by checking the Certificate Revocation List (CRL). If the Certificate is revoked the connection will be terminated.
- c. If the Certificate Name is verified, a password window will be shown on the participant's browser.
- d. The participant enters their application password.
- e. Once the password is validated the MPI home page will be displayed on the browser.

If the password is not validated another password request will be sent to the browser. After 5 unsuccessful password attempts the user will be directed to follow the “forgot password” link to choose a new password.

4.3.3.2 FORGOTTEN PASSWORD

- a. The participant attempts to login to the MPI, submitting a valid client certificate as described above until a password window is displayed prompting the participant to enter a password.
- b. The participant selects the “Forgot Password” link in the password window.
- c. An email will be sent to the registered email address of the authorized user with an authorization code.
- d. The participant enters this information into the “Forgot Password” window.
- e. Upon successful validation of the entered information, a new window with “New Password” and “Confirm New Password” will be displayed.
- f. After entering the new password, the participant will need to re-login into the MPI using the new password.

4.3.3.3 CHANGING THE APPLICATION PASSWORD

- a. The MPI application passwords will expire every 45 days.
- b. The “Change password” process will be similar to “Forgot Password” process.
- c. When a user logs in the MPI application will alert the user that their password is about to expire with a message to screen. This will continue to happen once the expiry date is less than 30 days away.
- d. If the participant does not change the password before it expires they will be directed to follow the “forgot password” link to choose a new password.

4.3.3.4 FIRST TIME LOGIN (INITIAL PASSWORD)

- a. The user logs into the MPI for the first time.
- b. The system will send the user a random string to their registered email address and a window will pop-up on the MPI for the user to enter the string. The user needs to enter this string within 5 minutes.
- c. The string will be validated on the MI App Server and upon successful validation a new window with “New Password” and “Verify New Password” will show up. User needs to enter new password into this window.
- d. The password on the MPI URL will only be asked once, during initial login. The MPI sessions do not timeout.

4.3.3.5 CERTIFICATE AND MPI APPLICATION PASSWORDS

The Certificate Password is required when the participant is signing data as part of the submission process to the Balancing Market. It is not required to view or query data via Type 2 interfaces. This is a continuation of the existing market practice,

As previously stated (See Non-Repudiation Process), all data submitted by the participants will be signed using the certificate private key.

The MPI Application password is distinct and independent of the Certificate password. It is strongly recommend that a different password is chosen for each of these passwords.

4.4 BALANCING MARKET TOOLKIT USER GUIDE

The Balancing Market Toolkit has been opened for participant access. The URL required for access is: <https://mpc.sem-o.com/mws/>

4.4.1 TOOLKIT OVERVIEW

The Balancing Market Toolkit is an optional tool that market participants can use to perform informal interface testing with the Balancing Market.

It includes a number of elements as follows:

- Client installed on an environment local to the participant.
- Server installation on the I-SEM Toolkit environment
- Sample Request xml messages
- Standard security certificate for connectivity to the EirGrid environment

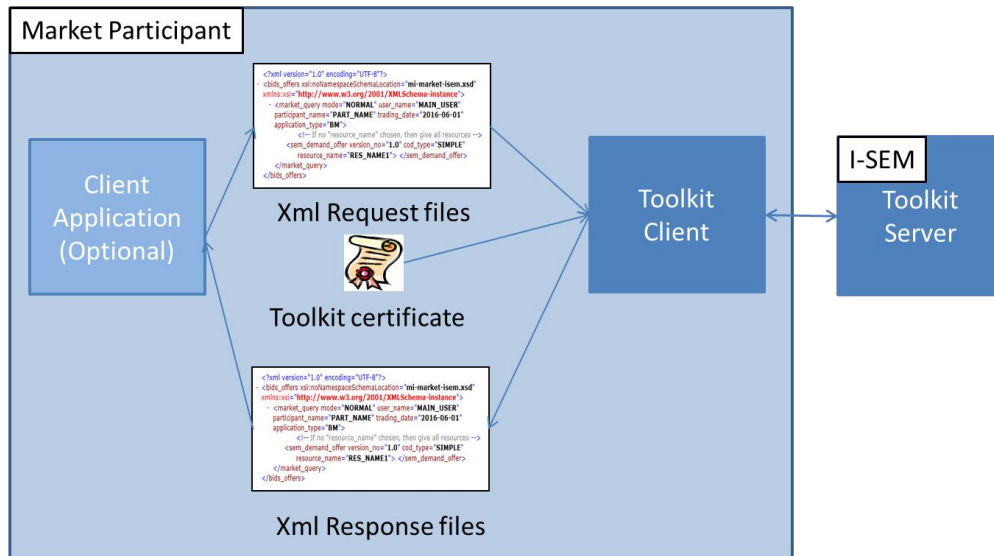


Figure 13: Overview of Balancing Market Toolkit

The toolkit can be used by a participant to validate correctly formatted xml requests through the toolkit client and server and receive response files.

A typical configuration is shown in the diagram above where a client's application generates the xml request file to be validated and picks up the response generated from the server.

Alternatively a participant may choose to incorporate the java classes provided with the toolkit into their own application or connect directly with the toolkit server to test their application interfaces directly.

It is proposed that participants utilise the toolkit as part of their interface development and test activities. It is not a substitute for Market Participant Interface Testing and Communication Channel Qualification Testing (CCQT).

The toolkit covers the Balancing Market only. The toolkit server provides a limited implementation of the balancing market system. It does not provide business meaningful responses. Participants are advised to align their test data with the data contained in the sample files provided to ensure that successful response messages are returned.

4.4.2 TOOLKIT INSTALLATION PROCESS

In summary the installation process for the toolkit is as follows:

1. Install required software to meet system pre-requisites.
2. Download and unpack the toolkit from [here](#) onto the target environment.
3. Install client certificate.
4. Test the toolkit installation.

4.4.2.1 INSTALL REQUIRED SOFTWARE TO MEET SYSTEM PRE-REQUISITES.

4.4.2.1.1 SETUP

1. Ensure that the environment to host the toolkit meets the minimum requirements as described in section 3.2.2.
2. Java SDK 1.8.x *(JDK) should be installed – available [here](#). The environment variables JAVA_HOME and PATH should be set properly.
3. Apache Ant 1.9.x *(software tool suitable for building Java projects) should be installed – available [here](#). Similarly ANT_HOME and PATH should be set properly.

The ant.bat script makes use of three environment variables - ANT_HOME, CLASSPATH and JAVA_HOME. Ensure that ANT_HOME and JAVA_HOME variables are set, and that they do **not** have quotes (either ' or ") and they do not end with \ or with /. CLASSPATH should be unset or empty.

*NOTE: Java SDK Version 1.8.0 131 and Ant 1.9.9 have been used by I-SEM in our testing. An updated more specific version may be communicated before Go-Live if required.

4.4.2.1.2 EXAMPLES

```
PATH=C:\Java\jdk1.8.0_131\bin;C:\Ant\bin;  
ANT_HOME=C:\Ant  
JAVA_HOME=C:\Java\jdk1.8.0_131
```

4.4.2.1.3 VALIDATION

To validate the installation the following commands must be run without any problem in a console (e.g. Windows Command Prompt).

```
java -version  
ant -version
```

Expected successful outcomes should look like the following:

```
C:\mi-isem-ws-client-5.0.1-b104>java -version  
java version "1.8.0_131"  
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)  
Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)
```

```
C:\mi-isem-ws-client-5.0.1-b104>ant -version  
Apache Ant(TM) version 1.9.9 compiled on February 2 2017
```

4.4.2.2 DOWNLOAD AND UNPACK THE TOOLKIT ONTO THE TARGET ENVIRONMENT

4.4.2.2.1 SETUP

Unzip the "mi-isem-ws-client-5.0.1-b<NNN>.tgz" into an empty directory where NNN is three digit identifier for package number.

Note: The entire path to this empty directory should not contain space(s).

4.4.2.2.2 EXAMPLES

C:\mi-isem-ws-client-5.0.1-b104

4.4.2.2.3 VALIDATION

You should see the following directory structure and files under the "isem-ws-client" directory.

Directory/File	Description
certs/	Party client certificate issued by EirGrid should be placed in this directory.
certs/server-ca.jks	The Java keystore which is pre-populated with the I-SEM Toolkit CA certificate.
certs/*.p12	The toolkit public certificate is located here.
config/	WSDL and XML Schema files (for reference only). This directory also contains "log4j.properties" for configuring Apache log4j logging.
dist/	Web service client jar is in this directory.
request-files/	Sample XMLs for various Web Service request type in sub-directories.
request-files/ws-client.properties	Main configuration file, which has all the property setting for running the Web Service client.
Response-files/	Responses from the web service request are stored in this directory.
Third-party/	Third party libraries (Axix2 and XML Security) are in this directory.
build.xml	Build script for web service client.
README.html	instructions for toolkit installation.

4.4.2.3 INSTALL CLIENT CERTIFICATE

4.4.2.3.1 SETUP

The toolkit has been prepopulated with the necessary general certificates to perform secure testing. No further certificate setup is required.

For reference:

The toolkit public certificate `TOOLKITUSER@PY_034000` is pre-populated in the certs directory. This is a general cert to be used by all participants. Participants will not be provided with individual certs for toolkit use.

The I-SEM Toolkit CA is pre-populated in the Java keystore located in certs/server-ca.jks.

4.4.2.3.2 EXAMPLES

Public toolkit certificate:

```
C:\mi-isem-ws-client-5.0.1-b104\certs\TOOLKITUSER@PY_034000
```

4.4.2.3.3 VALIDATION

The validity of the public cert can be confirmed using the CertUtil command from the window command prompt as follows:

```
CertUtil -dump c:\mi-isem-ws-client-5.0.1-b104\certs\TOOLKITUSER@PY_034000
```

Enter the PFX password 123456 when prompted to do so.

The contents of the java keystore can be checked using the keytool command as follows:

```
Keytool -list -keystore C:\mi-isem-ws-client-5.0.1-b104\certs\server-ca.jks
```

4.4.2.4 TEST THE TOOLKIT INSTALLATION

4.4.2.4.1 SETUP

1. The ws-client.properties file has been configured for an initial test. However the actual URL for accessing the I-SEM toolkit server will need to be set. (Note: this will be provided in a separate communication)

```
ws.client.end.point=https://****
```

2. In the Window command prompt window set the current directory to the mi web services home directory

```
C:\mi-isem-ws-client-5.0.1-b104
```

3. Enter the Ant command to run the test as follows:

```
ant -Dcfg.file=ws-client.properties
```

4.4.2.4.2 VALIDATION

After executing the test the following should appear

```
Buildfile: /abbrrt/appmi/isem-ws-client/build.xml
run.client:
[java] INFO Started web service client...
```

```
[java] INFO Config File: ./request-files/ws-client.properties
[java] INFO ClientCert: ./certs/TOOLKITUSER@PY_034000.p12
[java] INFO EndPoint: https://mpc.sem-o.com/mws/
[java] INFO Keystore: ./certs/server-ca.jks
[java] INFO Request Type: mp.report
[java] INFO Admin Role: false
[java] INFO Reading input: ./request-files/rpt-list.xml
[java] INFO Writing file: ./response-files/rpt-list-sig.txt
[java] INFO Submitting attachment...
[java] INFO Submitting attachment returned
[java] INFO Success: true
[java] INFO Warning: false
[java] INFO Writing response to file: ./response-files/rpt-list-out.xml
[java] INFO Finished client.
BUILD SUCCESSFUL
Total time: 1 seconds
```

The Web Service response rpt-list-out.xml should now be found in the "response-files" sub-directory.

C:\mi-isem-ws-client-5.0.1-b104\build.xml

For reference:

The properties file is located at request-files/ws-client.properties

The specific properties have been set as follows:

```
ws.client.end.point      = https://*****
ws.client.cert.file      = TOOLKITUSER@PY_034000
ws.client.cert.password  = 123456
ws.client.request.type   = mp.report
ws.client.input.file     = rpt-list.xml
```

4.4.3 TESTING WITH THE TOOLKIT

The toolkit can be used to test other request xml as follows:

1. Update the properties file to submit the required xml request file and save as a new version of the properties file.

```
ws.client.request.type   = <Request-Type>
ws.client.input.file     = <XML-Request-File>
```

Save as:

```
C:\mi-isem-ws-client-5.0.1-b104\
  <My-Test>.properties
```

2. In the Window command prompt window set the current directory to the mi web services home directory

```
C:\mi-isem-ws-client-5.0.1-b104
```

3. Enter the Ant command to run the test as follows:

```
ant -Dcfg.file=<My-Test>.properties
```

5 SEMOPX EX-ANTE MARKETS SOLUTION

EirGrid and SONI provide the service of the Power Exchange (SEMOpX) systems for both the Day-Ahead Auction Market (DAM) and Intraday Auction Market (IDM). Section 5 provides technical information relating to the SEMOpX Day-Ahead Auction Market, the Intraday Auction Market and the Intraday Continuous Market.

5.1 ARCHITECTURAL OVERVIEW

Figure 14 provides a high level view of how the SEMOpX market solutions are structured from a physical and logical perspective.

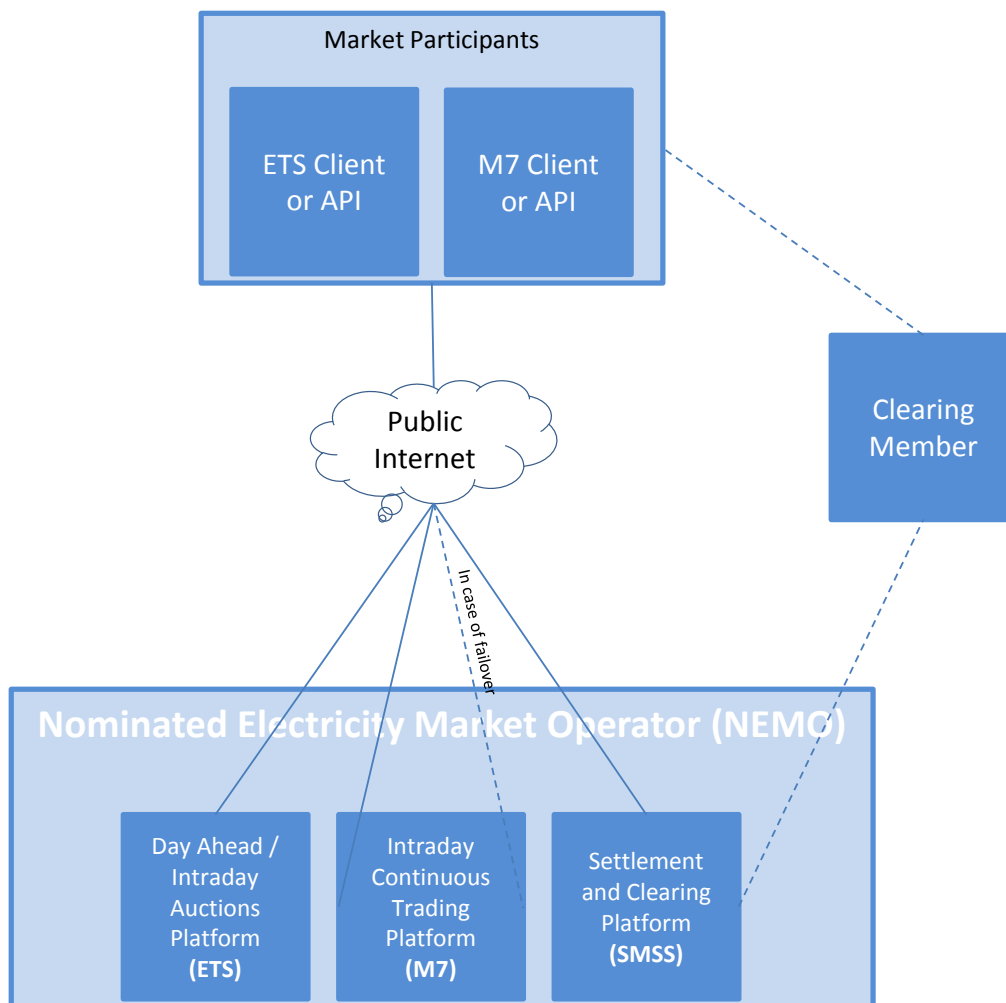


Figure 14: Overview of SEMOpX Market Solution

SEMOpX uses ETS (EPEX SPOT Trading System) as the system for the Day-Ahead and Intraday Auction markets. For the Intraday Continuous market, the trading system application is M7 (ex-ComXerv). Access to the settlement systems for trading participants is provided via the Spot Market Settlement System (SMSS) Member Area. Participants can connect using either a Type 2 or a Type 3 interfaces to the SEMOpX Auction and Continuous Trading Platforms. For Settlement purposes, the participant can either connect via a bank (clearing member) that interacts with SMSS or can connect directly to SMSS Application.

5.2 DAY-AHEAD AND INTRADAY AUCTION MARKETS

The SEMOpX Ex-Ante Market offers two auction based markets. Both of these markets, Day-Ahead and Intraday, utilize the same software solution. This solution is based on the EPEX Trading System (ETS) technology.

ETS supports 2 modes of access:

- Type 2: ETS Client
 - By locally installing an ETS client on a participants PC, participants can access a GUI that provides the full range of trading and reporting functionality available for these markets.
- Type 3: ETS API
 - This API provides a web services based mechanism allowing participants to automatically access the same range of functionality as available from the ETS client with some exceptions (including functionality specific to ETS client settings). The API operates independently of the ETS client and is used typically by participants wishing to integrate their systems with the SEMOpX.

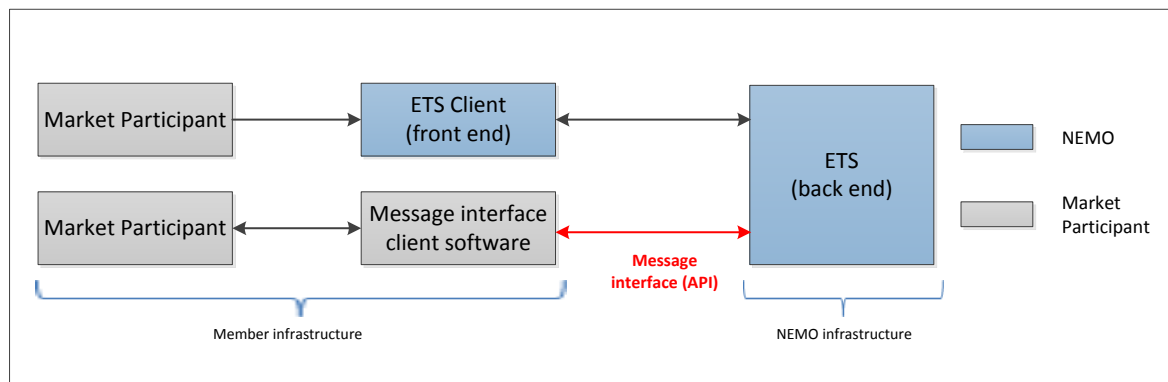


Figure 15: Auction Markets Interface Mechanisms

Further details are outlined in the *I-SEM Technical Specification Volume D: SEMOpX Ex-Ante Markets*.

5.2.1 MESSAGING OVERVIEW

The ETS API provides a web services based, SOAP 1.1., synchronous request-response integration mechanism for participants to automate their interaction with the SEMOpX market and integrate with their own IT systems.

The ETS API works as follows:

- The participant's client web services enabled application takes on the role of the ETS API client.
- An initial call is made to establish the connection with an Open Access SOAP Server. It passes the ETS username and password via a secure HTTPS connection.
- The Open Access SOAP server validates the login credentials with the ETS server and returns a valid Session token. This session token is required to be submitted in the SOAP Header of any subsequent requests.

- The participant's client makes a synchronous call to an Open Access SOAP Server with the required request.
- The Open Access SOAP Server performs the requested action, connecting with the ETS server as required.
- Once complete a response message is returned by the Open Access Server to the calling participant ETS API client.

5.2.2 ETS SECURITY

5.2.2.1 TYPE 2: ETS CLIENT SECURITY

The basic security mechanism restricts access based on authenticated users providing both a valid username and password to the client. Only participants who have completed the required registration steps with EirGrid/SONI will be provided with login credentials.

All communication traffic between the client and ETS is Transport Layer Security (TLS) encrypted.

The use of an HTTP CONNECT Proxy server is also supported if required.

5.2.2.2 TYPE 3: ETS API SECURITY

Security for communications via the API is based on the use of encryption using HTTPS and a digital certificate.

- All communications between ETS API Clients (member application) and ETS API Server are encrypted, using HTTPS.
- Client certificate are required to connect and provide a two-way authentication mechanism. This information is provided in Section 5.2.2.2.1.
- A username and password is also required.

The following protocols should be utilized to ensure compatibility:

- TLS 1.2*SHA1 cryptographic hash function with RSA encryption for public key (Recommended)

Note: ETS will move from SHA1 to SHA2 (SHA-256) with the version release for I-SEM Go-Live

5.2.2.2.1 DIGITAL CERTIFICATES FOR ETS API

As part of the registration process, participants will be issued with a digital certificate from the licenced supplier (EPEX) acting as a Certificate Authority. The participant will use the signed certificate and a private key they have generated during the application process to communicate via the API.

5.3 INTRADAY CONTINUOUS MARKET

The technology solution for the continuous market is uses the M7 technology solution.

M7 supports 2 modes of access:

- Type 2: ComTrader Client
 - By installing a client locally, each participant can access a GUI that provides the full range of trading and reporting functionality available for these markets.
- Type 3: M7 API
 - This API provides an Advanced Message Queuing Protocol (AMQP) , XML based mechanism allowing participants to automatically access the same range of functionality as available from the M7 ComTrader client with the some exceptions.

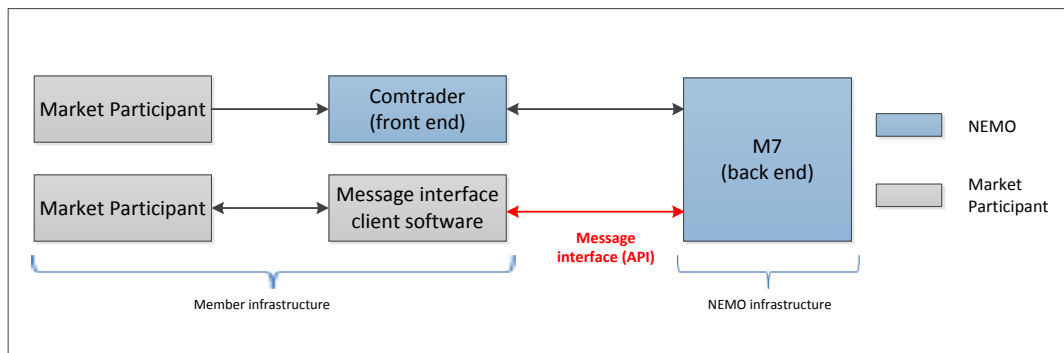


Figure 16: Continuous Markets Interface Mechanisms

Further details of the ComTrader Client and the M7 API are outlined in the *I-SEM Technical Specification Volume D: SEMOpX Ex-Ante Markets*.

5.3.1 MESSAGING OVERVIEW

The Message Interface (API) is a communication channel which can be used by participants to send/receive specially formatted standardized messages to/from the M7 Trading Platform System.

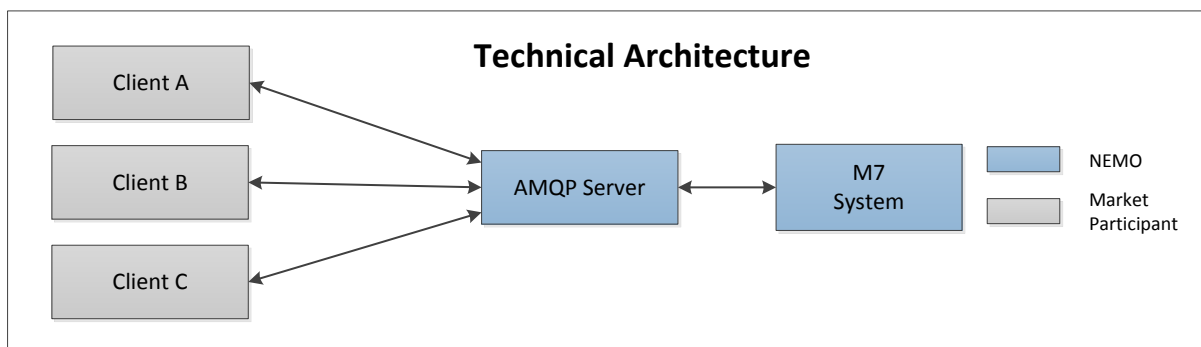


Figure 17: Continuous Markets Interface Mechanisms

The communication with the M7 System is based on Advanced Message Queuing Protocol (AMQP) as a transport layer, while the messages are formatted in XML.

The participant will need to download any AMQP compatible client software for integrating via this API. The recommendation from the M7 supplier is to utilize the RabbitMQ client for this purpose. *(Note: Please refer to the vendor's documents for more details on this client.)*

AQMP is a freely licensed wire protocol standard for message-queuing. More information on the protocol itself is available from the AMQP website www.amqp.org

5.3.2 M7 SECURITY

5.3.2.1 TYPE 2 SECURITY

The details of Type 2 security are outlined in the *I-SEM Technical Specification Volume D: SEMOpX Ex-Ante Markets Section 6.4.1*.

5.3.2.2 TYPE 3 SECURITY

Security for the M7 client is based on the digital certificates x.509 and TLS 1.0 encryption.
Note: M7 will move from TLS 1.0 to TLS 1.2 by the end of 2016.

As part of the registration process, participants will be issued with a digital certificate from EPEX. This will be used as part of communications protocol.

5.4 SETTLEMENT & CLEARING

5.4.1 OVERVIEW

Settlement and clearing are one of the functions for SEMOpX

For Type 2 Communications, participants can connect to the Members Area on the ECC website to access Settlement Reports, to see details of transactions, and to perform administration functions.

A Type 3 Communications interface is also offered which enables participants to download reports from a file transfer server.

Further details are outlined in the *I-SEM Technical Specification Volume D: SEMOpX Ex-Ante Markets*.

5.4.2 MESSAGING OVERVIEW

The Type 3 interface for the settlement function is based on file retrieval via SFTP or FTPS from the member's file transfer server.

It is also possible for a participant to setup an email subscription to specific reports via the user administration function on the Type 2 Communications interface.

5.4.3 SMSS SECURITY

5.4.3.1 TYPE 2 SECURITY

Access to the members' area website is controlled via a username and password login. Login details are provided as part of the registration process.

5.4.3.2 TYPE 3 SECURITY

The same username and password setup for Type 2 access is used for access to the File Transfer Protocol (FTP) server for authentication.

Two security protocol options are available to participants to secure the file transfer process from the FTP server.

1. FTPS (FTP with explicit SSL/TLS) – this provides encoding of both the control and data channel via either Secure Sock Layer(SSL) or TLS
2. SFTP – This option works in combination with a RSA2 public key generated by the participant and shared with EirGrid.

Note: Final security protocol will be clarified in an updated version.

5.5 PROCESS TO ACCESS EX-ANTE MARKET TECHNICAL DOCUMENTATION

The detailed API documentation referenced within this document is available upon request following completion and return of a signed Non-Disclosure Agreement (NDA) between a prospective participant and EirGrid.

The process is outlined in *Figure 16* below:

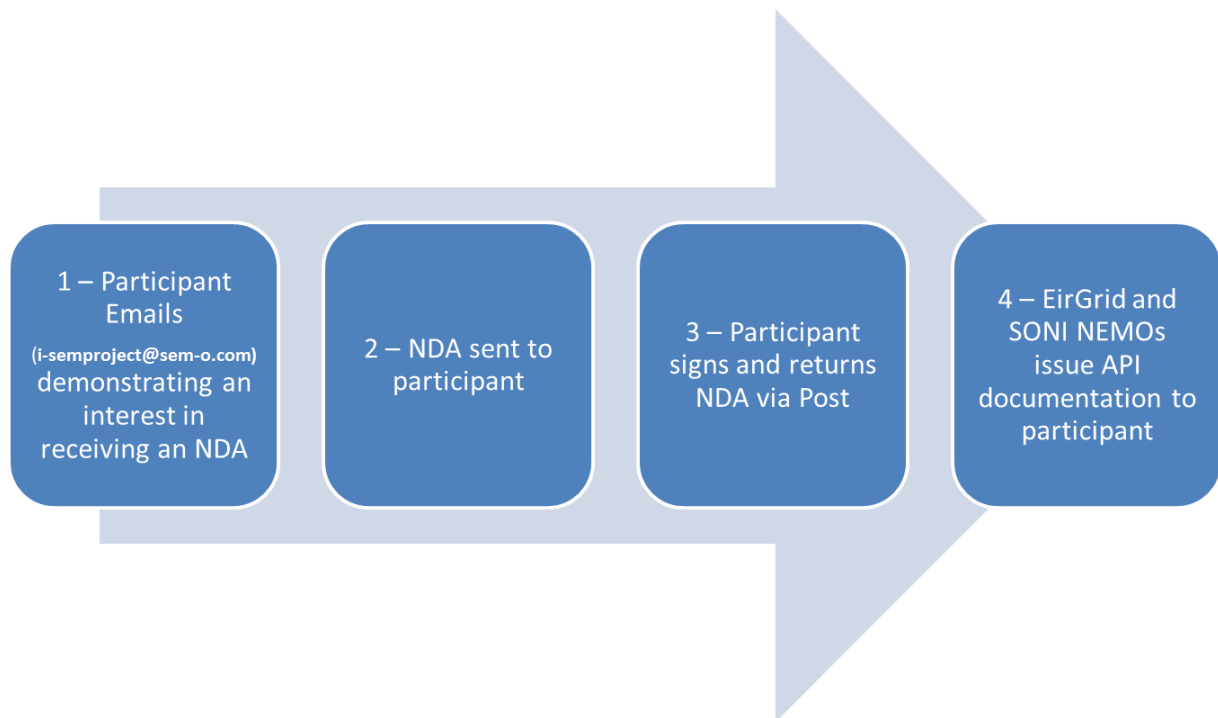


Figure 18: Process for Requesting API documentation

Postal address for return of two signed completed NDAs:

Derek Lawler,
I-SEM Project
EirGrid, The Oval, Block 2
160 Shelbourne Road,
Ballsbridge, Dublin 4.

An updated process will be outlined in due course for receipt of the API materials themselves.

Further details can be found on the I-SEM website.

6 CAPACITY MARKET

This section provides technical information relating to the Capacity Market.

The information below provides a view of the technology for the solution. The information presented in this section will be reviewed and amended as necessary, as the remaining design and build phases progress.

6.1 OVERVIEW

The Capacity Market system architecture supports market participants accessing the Capacity Market system via the public internet. Participant access to the Capacity Market system will be via the Capacity Market Portal, which is a browser-based portal interface, as illustrated in Figure 19.

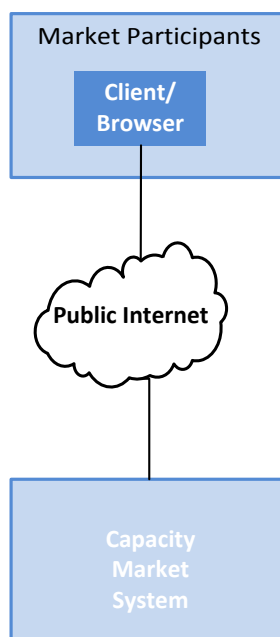


Figure 19: Capacity Market solution overview

No Type 3 access to the Capacity Market System is possible.

6.2 TYPE 2 ACTIVITIES

The Capacity Market Portal (i.e. Type 2 interface) will enable Participants to conduct the following functions including:

- Submission of auction bids;
- Retrieval of reports (principally Capacity Market results by market and for the Participant); and
- Notifications – general messages for participants
- View of Qualification Registration Data

Capacity Market results can be viewed via the Capacity Market Portal and may also be downloaded as a .csv file.

These functions are described in more detail in the I-SEM Technical Specification (ITS) - Volume E: Capacity Market Volume.

6.3 USER ROLES

User access to the Capacity Market Portal will be separated into the following roles:

1. **Trading Access:** Users with trading access privileges will have read-write access to submit offers to Primary Auctions and/or Secondary Auctions.
2. **Reporting Access:** Users with reporting access privileges will have read only access to reports only.
3. **Participant Administration:** Users with Participant administration access will have the capability to set up and configure access rights for other users within their organisation.

6.4 SECURITY

Participant access to the Capacity Market Portal utilises x.509 certificates in combination with a Capacity Market specific username and application password to control access to the system.

Web browser communications support HTTPS and TLS v1.2.

Where a Participant already possesses an I-SEM Balancing Market certificate, this certificate will also be valid for Capacity Market access.

Information on gaining access to the Capacity Market is outlined in ITS Volume E.

6.5 MINIMUM SYSTEM REQUIREMENTS

Table 6 sets out requirements in relation to browser access to the Capacity Market Portal.

Area	Requirement
Browsers	<ul style="list-style-type: none">• Internet Explorer – 11 (I-SEM standard) <p>Note: Internet Explorer 8, 9, 10 in compatibility mode and latest versions of Mozilla Firefox are also supported</p>

Table 6: Minimum Browser Requirements for Capacity Market Portal