Communication Guidelines

Data interchange between NBS Market Participants and eSett
07 January 2025
PUBLIC

eSett Oy

Table of contents

1 Communication Guidelines

1.1 Terms and Definitions

Table 1 Terms and definitions

Term	Definition
NBS	Nordic Imbalance Settlement, common balance settlement mechanism and method for Finland, Denmark, Norway and Sweden.
BRS	Business Requirement Specification, available at ediel.org.
Market Participant	Member of the Nordic Imbalance Settlement. Roles for the Market Participant can be: Balance Settlement Responsible (BRP), Distribution System Operator (DSO) or Retailer (RE).
MPS	Market Participant System – Market Participant's application communicating together with eSett's Imbalance Settlement System.
Message	Data sent between MPS and eSett's Imbalance Settlement System. Message must the requirements of supported dataflow.
NBS Handbook	Overview to the Nordic Imbalance Settlement Model from market participant's perspective available at http://www.esett.com/handbook/.
Inbound	Message sent from MPS to Imbalance Settlement System.
Outbound	Message sent from Imbalance Settlement System to MPS.
Messaging Service	eSett hosts a component called Messaging Service, which is responsible of receiving and delivering the settlement data.
ECP	Energy Communication Platform - software solution owned by ENTSO-E and based on MADES communication standard.
EDX	ENTSO-E Data Exchange - extension built on ECP. EDX is a distributed messaging system, which allows the transfer of messages between network participants.
MADES	Market Data Exchange Standard (The definition of the communication protocol and surrounding business processes for operating a network. Published as international standard IEC 62325-503)

ENTSO-E	European Network Transmission System Operators for Electricity (Regulation (EC) No 714/2009)
AMQP	Advanced Message Queuing Protocol

1.2 Introduction

This document is intended to help members of the Nordic Imbalance Settlement with data interchange together with eSett.

eSett acts as the Imbalance Settlement party on behalf of Nordic Transmission System Operators (TSOs).

Purpose of this document is to describe what is needed in order to deliver and receive the data for settlement purposes.

Depending on the Market Participants role, the data which the party is sending and receiving varies.

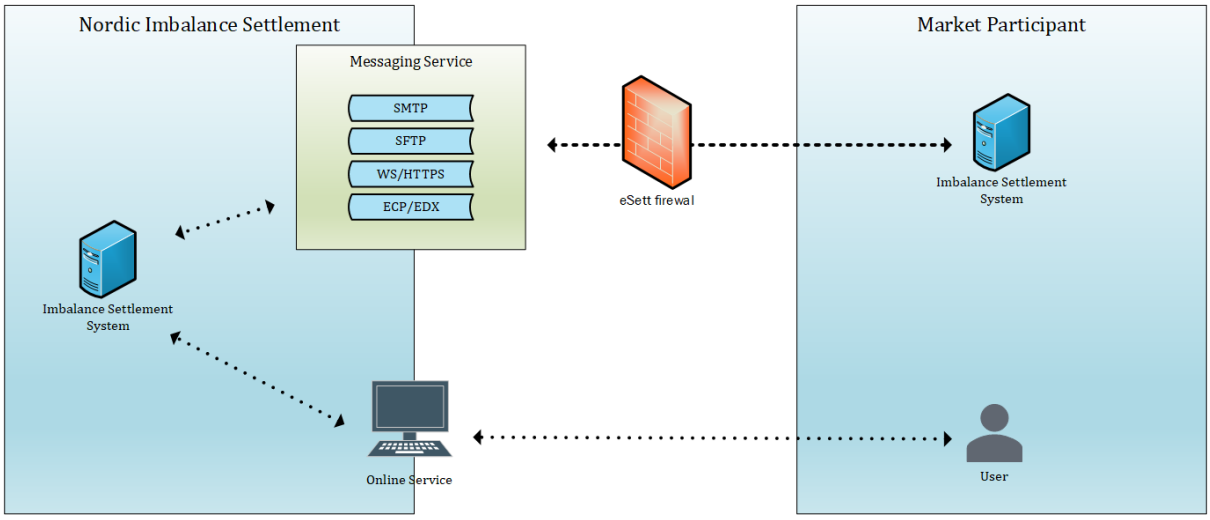

Figure 1: Simplified illustration of integration to and from Imbalance Settlement System

The figure above depicts the main context of the integration. Imbalance Settlement System implements two subsystems, which realize the integration – Messaging Service and Information Service. Both subsystems expose interfaces and channels defined below and interact with the Imbalance Settlement System (BSS) in order to store/retrieve data. Market Participant Systems (MPS) integrate to the defined interfaces in order to realize the physical data exchange (logically represented by Messages). Market Participant users can also use Online Service to configure some aspects of the integration (like Security) and inspect the messages flowing between MPS and Imbalance Settlement System.

Messaging Service enables Imbalance Settlement System and MPS to exchange Messages necessary for the Settlement process – Inbound Messages (e.g. Bilateral Trades) and Outbound Messages (e.g. Settlement Results).

Information Service enables Market Participants to retrieve information related to the Settlement process (e.g. Settlement Structure).

1.3 Available channels

Currently there are 4 different channels available for the integration between Market Participants system and eSett's Messaging Service:

- SMTP (email)
- SFTP
- Webservice
- ECP/EDX

2 eSett address information and credentials to services

2.1 Technical interface addresses

Information to establish connectivity between market participants' information systems and eSett's services (IP addresses, e-mail addresses and such), as described below, are informed to each market participant separately upon registration to eSett.

2.2 Credentials to services

Market participant's main contact person receives required credentials to eSett's services after registration to eSett. Main contact person has administrative user rights and is able to create new users for Online Service and adjust channel of electronic communication.

All communication towards eSett (Online Service and technical interfaces towards eSett) requires strong passwords that meet predefined requirements:

- Minimum 8 characters
- At least one capital letter
- At least one number
- At least one special character

Table 2 List of special characters

Character	Name	Character	Name	Character	Name
!	Exclamation	.	Full stop	|	Vertical bar
@	At sign	,	Comma	<	Less than
#	Number sign (hash)	;	Semicolon	>	Greater than
$	Dollar sign	:	Colon	'	Single quote
%	Percent	?	Question mark	{	Left brace
^	Caret	~	Tilde	}	Right brace
&	Ampersand	-	Minus	[	Left bracket
*	Asterisk	(	Left parenthesis	]	Right bracket
_	Underscore	)	Right parenthesis		
+	Plus	/	Slash		

2.3 Public service addresses for data interchange

2.3.1 Data interchange towards eSett

Channel	Port/protocol	Address	IP address
SFTP	22/tcp	service.esett.com	193.66.248.245
SMTP	25/tcp	service.esett.com	193.66.248.241
Webservice	443/tcp	service.esett.com/MSGS/ /messaging ServiceInputInterface	193.66.248.245

2.3.2 Data interchange from eSett towards Market Participant

eSett calls Market Participants from following IP addresses:

- 193.66.248.234
- 193.66.248.235

3 Integration towards eSett and to Messaging Service

3.1 Interfaces

Market participants in different roles are expected to deliver data towards eSett for imbalance settlement purposes. Delivery of this data is done via self-contained XML file in pre-defined structure that is delivered in integration component of Nordic Imbalance Settlement System called Messaging Service. Market participants are able to deliver these XML files to Messaging Service via four supported channels:

1. E-Mail message via SMTP
2. file via File Transfer Protocol
3. Webservice POST request
4. file via ECP/EDX.

After a successful delivery, the Nordic Imbalance Settlement System processes data and responds back to Market Participant, whether submission was successful. The response is asynchronous, and usually sent within minutes of receiving the original message. See sample XML schemas below.

3.2 Sender/Receiver Representation

The correct identification of Sender and Receiver of the Message is necessary to properly route the Message and deliver it to correct recipient. In Imbalance Settlement System, the Messages contain these identifications directly in the Message body (XML) – there are no additional metadata (on channel-specific level, e.g. filename encoded information or http headers), which describe either Sender or Receiver. The identifications representation differs based on the format of the particular Message. There are currently four format families used in Imbalance Settlement System – ENTSO-e,ebIX,CIM and UTILTS (EDIFACT). All of these formats utilize codes and coding schemes in order to identify Sender/Receiver. Following examples describe usage of these in all of the format families (the identification related is highlighted in yellow in the XML samples).

eSett's sender/receiver code in machine-to-machine communication is EIC code: **44X-00000000004B**

For purposes of delivering SPTI dataflow from Selecting Service the receiver EIC code is 45V000000000066Q with Coding Scheme A01 (EIC).

Codes and schemes in UTILTS (EDIFACT) are in UTILTS Format – Ediel-ID (NSE – National Sweden Code). Code used for eSett (Ediel-ID) is 71100.

ENTSO-E example:

```
<ScheduleDocument
xsi:schemaLocation="urn:entsoe.eu:wgedi:ess:scheduledocument:4:1 urn-entsoe-eu-wgedi-ess-scheduledocument-4-1.xsd"
xmlns="urn:entsoe.eu:wgedi:ess:scheduledocument:4:1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <DocumentIdentification v="ESS schedule for bilateral trade"/>
    <DocumentVersion v="1"/>
    <DocumentType v="A01"/>
    <ProcessType v="Z05"/>
    <ScheduleClassificationType v="A02"/>
    <SenderIdentification v="67800" codingScheme="NSE"/>
    <SenderRole v="A08"/>
    <ReceiverIdentification v="44X-00000000004B" codingScheme="A01"/>
    <ReceiverRole v="A05"/>
    <CreationDateTime v="2014-08-22T09:30:47Z"/>
```

…

ebiX example:

```
<rsm:AggregatedDataPerMGAForSettlementForSettlementResponsible
xsi:schemaLocation="un:unece:260:data:EEM-AggregatedDataPerMGAForSettlementForSettlementResponsible ebIX_AggregatedDataPerMGAForSettlementForSettlementResponsible_2013pA.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:rsm="un:unece:260:data:EEM-AggregatedDataPerMGAForSettlementForSettlementResponsible">
    <rsm:Header>
        <rsm:Identification>Aggregated data for consumption - 01</rsm:Identification>
        <rsm:DocumentType listAgencyIdentifier="260">E31</rsm:DocumentType>
        <rsm:Creation>2014-08-22T10:10:15Z</rsm:Creation>
        <rsm:SenderEnergyParty>
            <rsm:Identification schemeIdentifier="TEST1" schemeAgencyIdentifier="260">93245</rsm:Identification>
        </rsm:SenderEnergyParty>
        <rsm:RecipientEnergyParty>
            <rsm:Identification schemeAgencyIdentifier="305">44X-00000000004B</rsm:Identification>
        </rsm:RecipientEnergyParty>
    </rsm:Header>
    <rsm:ProcessEnergyContext>
```

…

CIM Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<Publication_MarketDocument xmlns="urn:iec62325.351:tc57wg16:451-3:publicationdocument:7:1"
xmlns:ecl="urn:entsoe.eu:wgedi:codelists">
        <mRID>7f5d89499a5d4226a7c3b4601ab3e84c</mRID>
        <revisionNumber>1</revisionNumber>
        <type>A52</type>
        <sender_MarketParticipant.mRID codingScheme="A01">17X100A100M006F3</sender_MarketParticipant.mRID>
        <sender_MarketParticipant.marketRole.type>A11</sender_MarketParticipant.marketRole.type>
        <receiver_MarketParticipant.mRID codingScheme="A01">45V0000000000520</receiver_MarketParticipant.mRID>
        <receiver_MarketParticipant.marketRole.type>A36</receiver_MarketParticipant.marketRole.type>
        <createdDateTime>2019-06-06T11:15:42Z</createdDateTime>
        <period.timeInterval>
                <start>2019-06-06T22:00Z</start>
                <end>2019-06-07T22:00Z</end>
        </period.timeInterval>
        <domain.mRID codingScheme="A01">10Y1001A1001A91G</domain.mRID>
        <TimeSeries>
                <mRID>65</mRID>
                <auction.mRID>7f5d89499a5d4226a7c3b4601ab3e84c1</auction.mRID>
                <auction.type>A01</auction.type>
                <businessType>A69</businessType>
                <in_Domain.mRID codingScheme="A01">10YCB-GERMANY--8</in_Domain.mRID>
                <out_Domain.mRID codingScheme="A01">10YCB-GERMANY--8</out_Domain.mRID>
                <quantity_Measure_Unit.name>MAW</quantity_Measure_Unit.name>
                <currency_Unit.name>EUR</currency_Unit.name>
                <curveType>A01</curveType>
                <Period>
                        <timeInterval>
                                <start>2019-06-06T22:00Z</start>
                                <end>2019-06-07T22:00Z</end>
                        </timeInterval>
                        <resolution>PT60M</resolution>
                        <Point>
                                <position>1</position>
                                <price.amount>48.95</price.amount>
                        </Point>
                </Period>

        </TimeSeries>

</Publication_MarketDocument>
```

UTILTS (EDIFACT)

```
UNA:+.?'
UNB+UNOC:3+51900:ZZ+71100:ZZ+230327:1145+LPRI479++23-DDX-E31-S++1'
UNH+1+UTILTS:D:02B:UN:E5SE1B'BGM+E31::260+LPRI479+9+AB
'DTM+137:202303101145:203
'DTM+735:?+0100:406
'MKS+23+E02::260
'NAD+MS+51900:SVK:260
'NAD+MR+71100:SVK:260
'NAD+DDX'IDE+24+LPRI479T001
'LOC+239+ABC:SVK:260
'LIN+++8716867000030:::9
'PIA+1+Z04:PC:SVK:260+Z51:PT:SVK:260+Z02:OT:SVK:260+Z55:LOD:SVK:260+Z04:BAP:SVK:260
'DTM+324:202305010000202305020000:719
'DTM+354:15:806
'DTM+368:202303101145:203
'STS+7++E44:SVK:260
'MEA+AAZ++KWH
'CCI+++E02::260
'CAV+E02::260
'SEQ++1
'QTY+136:453
'STS+8+56'SEQ++2'QTY+136:453'STS+8+56'SEQ++3'QTY+136:453'STS+8+56'SEQ++4'QTY+136:453'
+56'SEQ++10'QTY+136:16'STS+8+56'SEQ++11'QTY+136:10'STS+8+56'SEQ++12'QTY+136:11'STS+8+
6'SEQ++18'QTY+136:104'STS+8+56'SEQ++19'QTY+136:15'STS+8+56'SEQ++20'QTY+136:16'STS+8+5
EQ++26'QTY+136:102'STS+8+56'SEQ++27'QTY+136:103'STS+8+56'SEQ++28'QTY+136:104'STS+8+56
++34'QTY+136:13'STS+8+56'SEQ++35'QTY+136:101'STS+8+56'SEQ++36'QTY+136:102'STS+8+56'SE
+42'QTY+136:11'STS+8+56'SEQ++43'QTY+136:12'STS+8+56'SEQ++44'QTY+136:13'STS+8+56'SEQ++
50'QTY+136:16'STS+8+56'SEQ++51'QTY+136:10'STS+8+56'SEQ++52'QTY+136:11'STS+8+56'SEQ++5
```

Identification is done using a unique Code (assigned to each Market Participant) and a Coding Scheme (preselected by Market Participant). Additionally, in ENTSO-E messages, Role is also part of identification process. Role defines whether the identified subject acts as BRP, TSO, DSO or Imbalance Settlement responsible. In ebiX messages, this role is automatically recognized based on the message type itself. More information on Coding Schemes and their usage is available in NBS Handbook.

The usage of Code and Identifier schemes is documented in chapter "4.4 Code and Identifier schemes" in "NEG Common XML rules and recommendations", see https://www.ediel.org, "NEG Common Documents".

3.2.1 Alternative Code/Coding Scheme logic

For incoming messages there is implemented a feature that enables using of Alternative Code and Alternative Coding Scheme attributes in the message.

This feature is implemented for purpose of receiving messages where eSett is not a primary receiver and the delivered message is resent by another market subject which figures as the primary recipient.

Typical usage example is delivering of SPTI messages, which are from Market Operators delivered to Selecting Service (the primary recipient) and then the Selecting Service as service provider resends the message to eSett as the alternative recipient.

Messaging Service currently uses attributes *Sender Code* and *Sender Coding Scheme* for identifying of message sender. Market Parties in Imbalance Settlement System are allowed to have Alternative Code and Alternative Coding Scheme as non-mandatory business dimension attributes. In the incoming message there will be still one attribute for Code and one for Coding Scheme. At the message recognition and validation process there needs to be implemented a logic comparing the sender's Code and Coding Scheme in the message with Alternative Code and Alternative Coding Scheme if there is a mismatch with regular Code and Coding Scheme in Imbalance Settlement System.

In the message there is expected only combination of Code and Coding Scheme or combination of Alternative Code and Alternative Coding Scheme. There is no possibility of combination Code and Alternative Coding Scheme. Such combinations don't pass validation process and the message is rejected.

For UTILTS (EDIFACT) communication the Market Party must be in Sweden and have a code + coding scheme/Alternative code + alternative coding scheme combination using Swedish National coding scheme (EDIEL-ID) in order to receive or send dataflows in UTILTS format.

Areas involved in UTILTS (EDIFACT) communication must also use a NSE code + coding scheme combination to be used in outgoing or incoming communication. MBA has specific UTILTS Code + Coding Scheme attributes which should be set up as NSE (Swedish National code).

3.2.1.1 Validation process description

Basic flow description – combination of Code and Coding scheme is invalid, combination of Alternative Code and Alternative Coding Scheme is valid. Other attributes then Code/Coding Scheme are supposed to be valid:

- Message is initiated to be processed
- Sender's Code and Coding Scheme attributes are validated

- Combination of Code and Coding Scheme attributes from the message is validated against valid Code and Coding Scheme combinations in MSGS configuration. Combination is not found.
- Combination of Code and Coding Scheme attributes from the message is validated against valid Alternative Code and Alternative Coding Scheme combinations in MSGS configuration.
- Valid combination found
- Message is accepted successfully

Alternative flow 1 description – combination of Code and Coding Scheme is valid, combination of Alternative Code and Alternative Coding Scheme is invalid. Other attributes then Code/Coding Scheme are supposed to be valid:

- Message is initiated to be processed
- Sender's Code and Coding Scheme attributes are validated
- Combination of Code and Coding Scheme attributes from the message is validated against valid Code and Coding Scheme combinations in MSGS configuration. Valid combination is found.
- Validation of combination of Code and Coding Scheme message attributes against Alternative Code and Alternative Coding Scheme combinations is skipped
- Message is accepted successfully

Alternative flow 2 description – combination of Code, Coding Scheme and combination of Alternative Code, Alternative Coding Scheme are invalid. Other attributes then Code/Coding Scheme are supposed to be valid:

- Message is initiated to be processed
- Sender's Code and Coding Scheme attributes are validated
- Combination of Code and Coding Scheme attributes from the message is validated against valid Code and Coding Scheme combinations in MSGS configuration. Combination is not found.
- Combination of Code and Coding Scheme attributes from the message is validated against valid Alternative Code and Alternative Coding Scheme combinations in MSGS configuration. Combination is not found.
- Valid combination not found
- The validation fails and the message is rejected

Alternative flow 3 description – combination of Code and Coding Scheme is valid, combination of Alternative Code and Alternative Coding Scheme is valid. Other attributes then Code/Coding Scheme are supposed to be valid:

- Message is initiated to be processed
- Sender's Code and Coding Scheme attributes are validated
- Combination of Code and Coding Scheme attributes from the message is validated against valid Code and Coding Scheme combinations in MSGS configuration. Valid combination is found.
- Validation of combination of Code and Coding Scheme message attributes against Alternative Code and Alternative Coding Scheme combinations is skipped
- Valid combination found
- Message is accepted successfully

Other alternative scenarios are not supported and considered.

Table for illustration of valid attributes combinations (✓).

	Code	Coding Scheme	Alternative Code	Alternative Coding Scheme
Code	-	✓	-	-
Coding Scheme	✓	-	-	-
Alternative Code	-	-	-	✓
Alternative Coding Scheme	-	-	✓	-

3.3 Channels

Messaging Service offers four channels to physically realize the logical message transfer. These are FTP, Email, Web Services and ECP. Each of the interfaces is described in detail in subsequent sections of this chapter.

MPS chooses and implements one of them to exchange Messages with Messaging Service. The Online Service provides visual use-case to manually upload a Message – this serves as a fall back option for cases when the channel doesn't work for some reason.

Country specific limitations on communication channels from the NBS handbook available at www.esett.com.

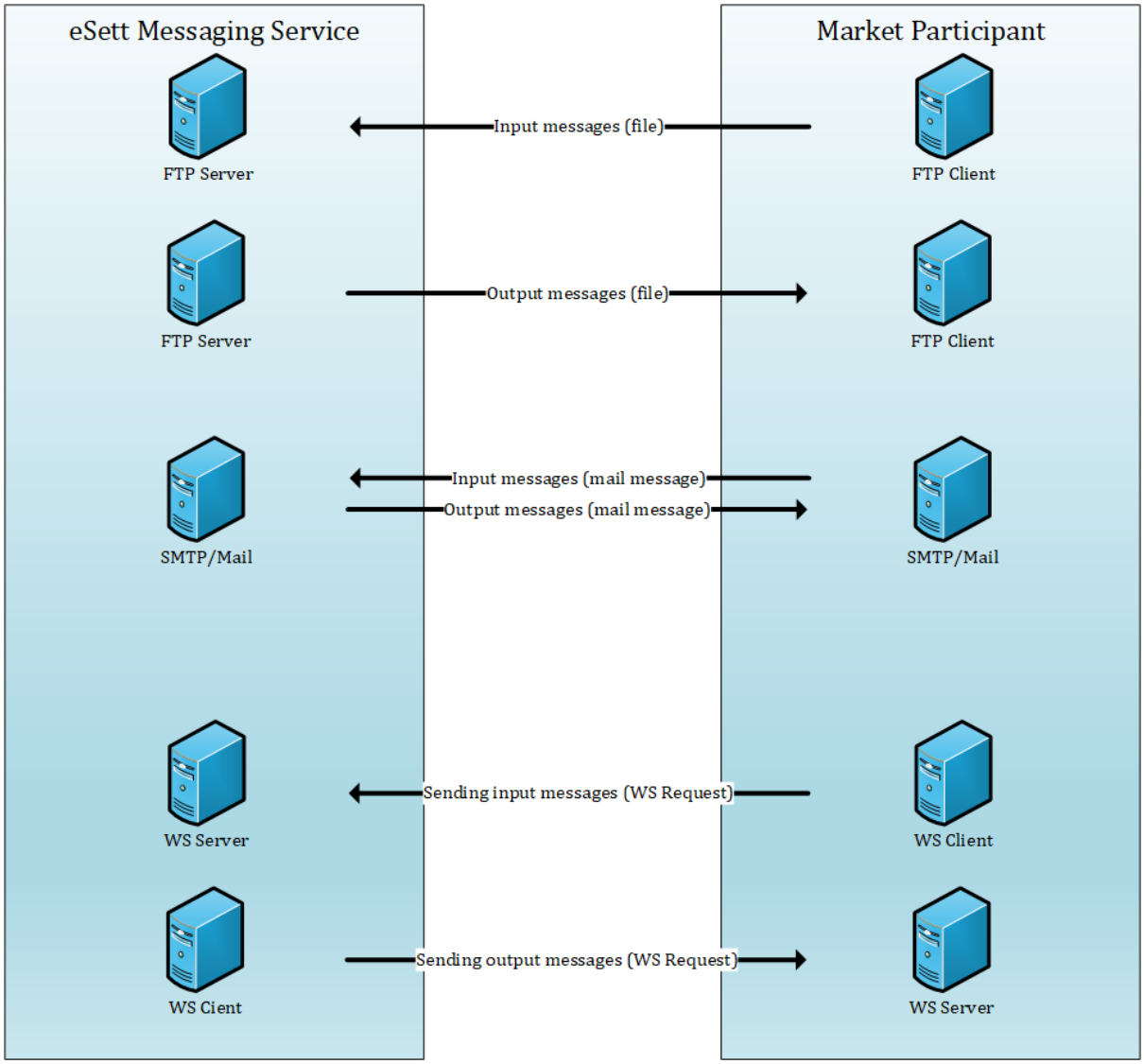

Figure 2: Messaging Service scheme for SMTP, SFTP and Webservice

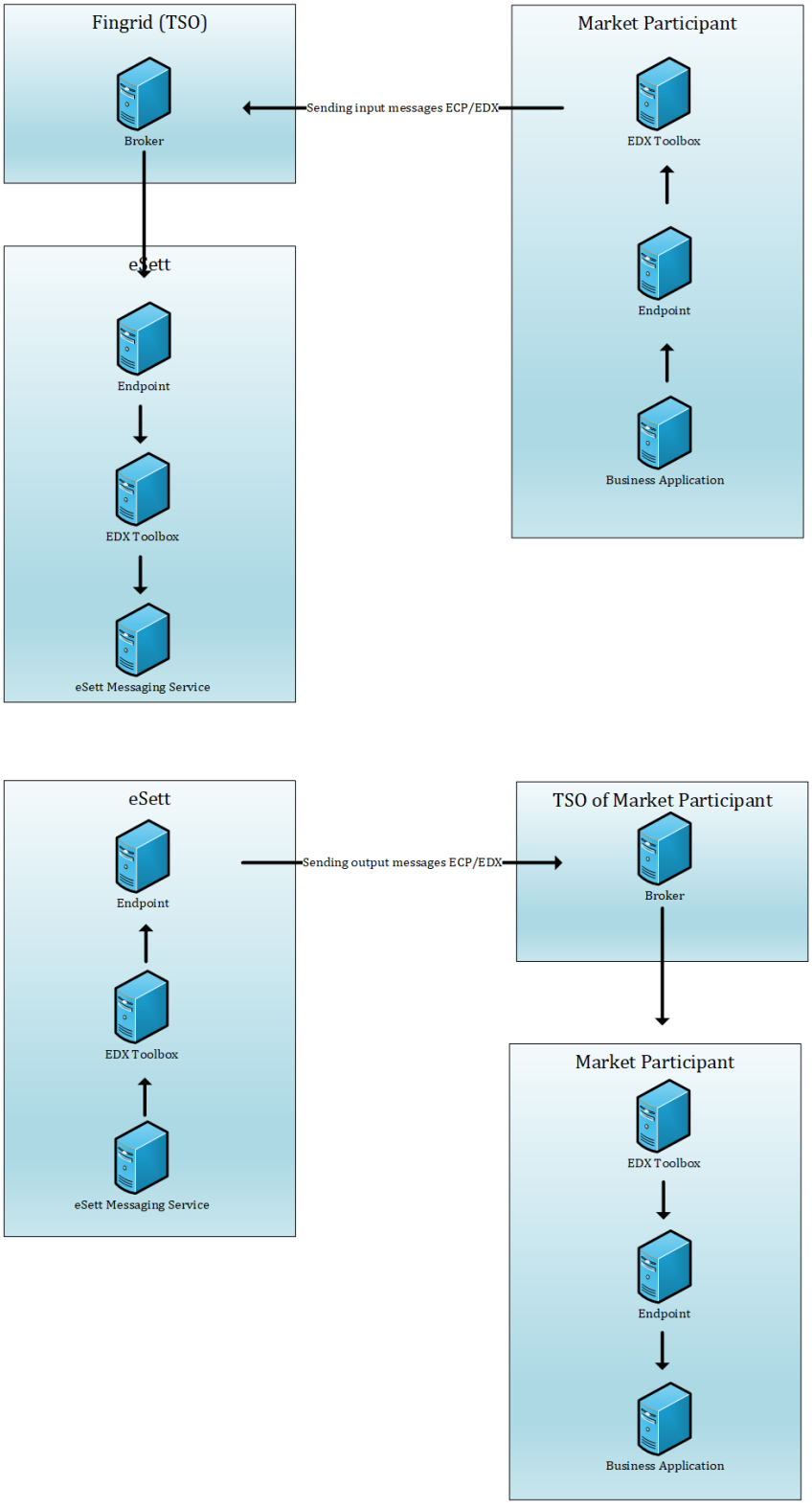

Figure 3: Messaging Service scheme for ECP/EDX

3.3.1 SFTP

The Messaging Service of the Nordic Imbalance Settlement System uses dedicated SFTP Server that supports SFTP only, plain FTP is not allowed for security reasons.

The Market Participant is expected to connect to eSett's SFTP server by using URL listed at Online Service homepage.

In order to make the connection, the IP address of the system that will initiate the connection to Messaging Service has to be as stated to eSett in the Connection details template/form. If a connection is successfully established, the Market Participant is supposed to log in using credentials as provided by eSett. However, those can be updated anytime in Online Service.

After logging in is completed, the Market Participant places the file according to the instructions listed in chapter "Folder Structure" below.

The Nordic Imbalance Settlement System will process the message and afterwards open the connection to the SFTP Server which is administered by Market Participant, using the credentials supplied by the Market Participant. Nordic Imbalance Settlement System will place the XML file which contains the information about processing results and closes the connection afterwards. This process is the same also when delivering results data and data packages ordered by the Market Participant.

3.3.1.1 Folder Structure

The folder structure of the Messaging Service FTP (used for Inbound flows) is defined by the following example. The structure of Market Participant's FTP (used for Outbound flows) is the responsibility of the Market Participant – it is possible to configure a folder where Outbound messages will be placed in MPS FTP. Each Market Participant has its own folder with the Inbound folder. The Market Participant folder is defined during Market Participant creation and cannot be changed further.

- Root
    - Inbound (folder where the messages should be placed)
        - Processes (folder where XML files are moved automatically after processing).

3.3.1.2 FTP User Accounts

Each Market Participant can define its FTP account (username and password) using Online Service. Each Market Participant FTP account can only access its folder (and subfolders); e.g. MARKET_PARTY_A.

3.3.1.3 Inbound FTP

Inbound FTP Interface periodically checks (polls) all INBOUND subfolders and attempts to download the files placed there. Inbound files, that are processed are then moved to subfolder Processed.

3.3.1.4 Outbound FTP

Outbound FTP Interface is used to deliver the Message using FTP. The Interface creates file (using naming convention specified below) and uses Message as the file content. The file is then uploaded to folder in Market Participant FTP Server.

The convention to create the filename is following:

YYYYMMDD_<Data flow code>_<Sender>_<Recipient>_<DocumentId>.xml

3.3.1.5 Security

As stated above, Market Participants are authenticated using username/password (no other authentication method is supported). The data transport is automatically protected by SSH encryption mechanism (encryption algorithm is diffie-hellman-group14-sha1) – there is no need to setup any certificates.

Market participants FTP server static IP address or predefined IP range behind domain must be communicated to eSett or firewall rules.

3.3.2 Mail

The e-mail message is expected to have a single file attachment. The e-mail subject and body do not have any business semantics. Attachments must be declared as “application/xml”.

Message delivered can be up to 50MB in size.

3.3.2.1 Inbound Mail

Inbound e-mail means messages delivered by Market Participant to NBS Settlement System.

Content of the attachment is treated as Message in Messaging Service. The email subject and body don’t have any business semantics.

The sending SMTP server (located in Market Participant’s premises) can optionally use STARTTLS to secure the SMTP-to-SMTP communication. TLS versions 1.0, 1.1 and 1.2 are supported.

3.3.2.2 Outbound Mail

Outbound Mail Channel is used by Messaging Service to deliver the Message from NBS Settlement System to Market Participants using SMTP.

The Channel creates file (using the naming convention: YYYYMMDD_<Data flow code>_<Sender>_<Recipient>_<DocumentId>.xml) and uses Message as the file content.

The email message is created using following rules:

- Created file is attached
- The subject of the email is set to be the same as the filename of the attachment
- Target e-mail address (recipient) is set based on Channel configuration. The configuration is accessed by Market Participant using Online Service.
- Sender of the email is set according to fixed Messaging Service configuration

3.3.2.3 Security

As stated above, Market Participants are not directly authenticated. Market Participants SMTP server can use plain communication (which is vulnerable to wiretapping) or secured STARTTLS transport, which needs to be configured with certificate issued by widely accepted certification authority (using self-signed or non-trusted certificates is not supported). In such case data transport is automatically protected (encrypted) with TLS (using the configured certificates).

3.3.3 Web Service

In order for eSett's Webservice server to receive messages from Market Participants, it is expected from the Market Participant to create a Webservice Client that will submit messages using Simple Object Access Protocol (SOAP).

The client can be generated from WSDL, which is available from the URL published in Online Service.

The Market Participant is expected to authorize itself by using username and password provided by eSett. The credentials can be administered in Online Service.

A request to submit messages needs to utilize the envelope which is described below. Actual data is supposed to be stated in the Content data section (noted by CDATA element).

eSett will immediately respond with a confirmation that the request has been accepted (or that request fails due to authorization or basic format).

Actual results of the processing are delivered in asynchronous response, which is usually delivered within a matter of a few minutes.

While eSett is sending acknowledgements or delivering settlement data towards the Market Participant, the credentials provided by Market Participant are utilized.

3.3.3.1 Inbound Web Service

Inbound WS Channel is directly called from WS Server every time an MPS Client invokes it. The Message is extracted from the WS Request, processed and a WS Response is sent back to MPS.

3.3.3.2 Outbound Web service

Outbound WS Channel is used by Messaging Service to deliver the Message using Web Services (HTTPS). The Channel creates WS Request (using the Message) and uses WS Client to

deliver the Message to external WS Server. The physical URL is resolved from configuration defined by MPS in Online Service.

3.3.3.3 *Web Service API*

Following figure outlines the Web Service API. The API has single method *uploadRequest* with single parameter, which represents the Message content (CDATA value). The WS-Security is used in order to secure the message with username/password. The username/password is stored in the Imbalance Settlement System and configured by Market Participant users using Online Service.

The method returns the InternalId of the Message and result code of the operation. In case the message is refused (e.g. due to some failure), the SoapFault is raised using standard fault code and message, complemented with custom list of refusal reasons.

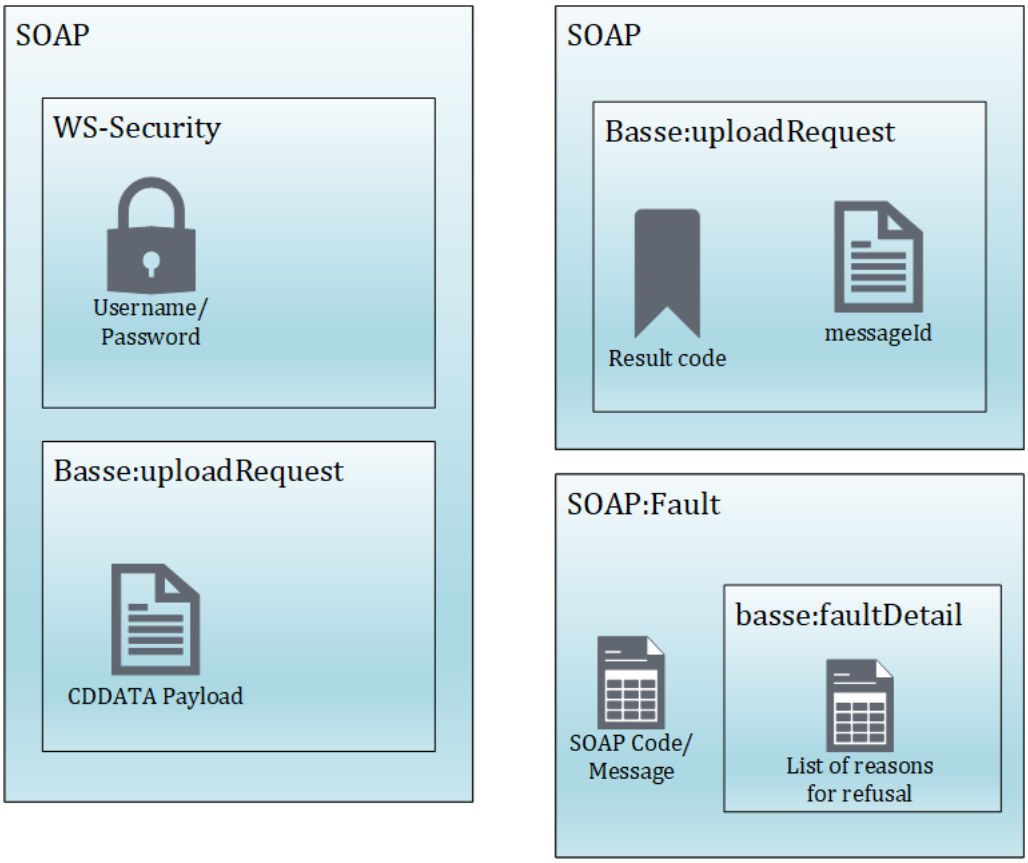

Figure 4: Web Service Endpoint API

Following describes both cases in more detail.

3.3.3.4 *Message successfully uploaded*

Standard web service response if the message is processed by Messaging Service and SOAP fault in the case of error (Below). Message is uploaded successfully only in the case when Messaging Service returns response code MESSAGE_RECEIVED.

Successful Upload Example:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap:Body>
      <mss:uploadResponse xmlns:mss="http://www.nbs.coop/messaging-service-1.0">
           <result_code>MESSAGE_RECEIVED</result_code>
           <message_id>f94ebc859e1a49de890fcc4d694d0ce9</message_id>
      </mss:uploadResponse>
   </soap:Body>
</soap:Envelope>
```

When a message is successfully uploaded to the Messaging Service, Messaging Service returns "uploadResponse" element with additional nested elements:

- "result_code", contains MESSAGE_RECEIVED in case of successful upload and
- "message_id" which is internal message id assigned to message by Messaging Service.

Message can be searched by the message_id in Online Service. For every incoming message the Messaging Service generates also an acknowledgement document with information about processing of message. This acknowledgement will be delivered asynchronously back to the sender.

3.3.3.5 *Failed upload message*

Failed upload message example:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
        <mss:uploadResponse xmlns:mss="http://www.nbs.coop/messaging-service-1.0">
             <result_code>USER_IS_NOT_SENDER</result_code>
             <message_id>e8bfaf1be6ed441483e50fd343bf7512</message_id>
             <acknowledgement_id>da9b7c70c8f34bc4a0538800936884e4</acknowledgement_id>
        </mss:uploadResponse>
    </soap:Body>
</soap:Envelope>
```

In unsuccessful scenario the Messaging Service returns "result_code" different code then MESSAGE_RECEIVED. The internal id of generated acknowledgement document is part of the response as well.

Supported Result Codes

Code	Description

MESSAGE_RECEIVED	Message is received by system and will be processed
DIRECTION_UNRESOLVED	Receiver in the message is not Imbalance Settlement System
NOT_VALID_DATA_FLOW	Sent message is not valid. This result code can be returned when message is technical invalid, usually because of XSD validation.
UNRESOLVED_DATA_FLOW	Message is not recognized to be any data flow supported by Messaging service.
NOT_UNIQUE_MESSAGE	This code is returned when message with same document id and version was already received from Market Party
USER_IS_NOT_SENDER	This code is returned in the case when user used for authentication does not have permissions for Market Party for which the message is sent.

Security error user is not authenticated

Authentication Failure example:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
       <soap:Body>
           <ns1:Fault xmlns:ns1="http://www.w3.org/2003/05/soap-envelope">
             <faultcode xmlns:ns2="http://ws.apache.org/wss4j">ns2:SecurityError</faultcode>
             <faultstring>A security error was encountered when verifying the message</faultstring>
           </ns1:Fault>
       </soap:Body>
</soap:Envelope>
```

This SOAP Fault response is returned when sender in WS-Security header of SOAP request is not authenticated in the system.

And internal server error technical error on server

This SOAP Fault response is returned when system is not able to process message. This error can have different reasons - in this case please contact support.

Technical error on Messaging Service example:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
      <soap:Body>
         <ns1:Fault xmlns:ns1="http://www.w3.org/2003/05/soap-envelope">
              <faultcode>ns1:Receiver</faultcode>
              <faultstring>Fault occurred while processing. Internal server error.</faultstring>
         </ns1:Fault>
      </soap:Body>
</soap:Envelope>
```

3.3.3.6 Security

As stated above, Market Participants are authenticated using WS-S username/password (no other authentication method is supported). Both eSett and Market Participant Web Service

endpoints (https/TLS) must be configured with certificate issued by widely accepted certification authority (using self-signed or non-trusted certificates is not supported). The data transport is automatically protected with TLS (using the configured certificates).

3.3.4 ECP/EDX

ECP (Energy Communication Platform) is an application based on MADES Communication Standard and software solution owned by ENTSO-E. EDX (ENTSO-E Data Exchange) can be considered as an extension, which communicates with ECP over AMQP. eSett is utilizing both of these and for the Market Participant to be able to send and receive messages towards and from eSett, an ECP Endpoint with EDX Toolbox is required. Below there are two tables of the main components of ECP and EDX.
eSett's ECP endpoint codes are 44V000000000029A for production and 44V000000000028C for test environment

Component	Description
Component Directory	The component directory is the center of trust in the ECP network. It contains a list of all trusted components (Brokers & Endpoints), as well as a list of Message Paths in the network. Managed by Transmission System Operators (TSO).
Broker	A broker is an optional component in an ECP network, which acts as a gateway between two endpoints. This facilitates non-repudiation of messages in the network, by introducing a third party in the message exchange and further enables deployment in segregated networks. In ECP4 the Broker is implemented by using the Apache ActiveMQ library with a custom authentication plugin.
Endpoint	An Endpoint is the component, which is the entry point to an ECP network for the business applications in the participants IT landscapes. It provides an abstraction of the services required for addressing, routing and secure exchange of messages. It achieves this by signing and encrypting the payload for the intended recipient and ensuring that delivery is (eventually) possible.
Message Type	To enable usage of one Endpoint for multiple independent business processes, the concept of Message Type is introduced. This, essentially, works like the subject field on an e-mail and lets business applications on the receiving side select for which business process they want to retrieve messages.
Message Path	The ECP interface provides a complete abstraction of the underlying infrastructure, but to provide routing capabilities between endpoints, the concept of Message Path defines the route a given message shall take between its source endpoint, and an optional broker before reaching its destination endpoint. In this way Message Paths enables separation of traffic as well as transparent migration from one broker to another to facilitate high availability. A message path is selected based on recipient and Message Type and is stored in and distributed via the Component Directory.

3.3.4.1 Inbound ECP/EDX

Inbound ECP/EDX Endpoint is used for message receiving. Received messages that should be delivered by the AMQP output channel are sent to the configured AMQP destinations and placed it to Reception Pipeline. ECP/EDX Response is sent back to External System.

3.3.4.2 Outbound ECP/EDX

Outbound ECP/EDX Endpoint is used by Distribution Pipeline to deliver the Message using AMQP. To send or publish a message using the AMQP integration channel MSS puts the message into configured input queue (direction:in) AMQP channel with at least mandatory properties. Message payload is in the message body (AMQP application-data).

3.3.4.3 Security

Market Participants are authenticated using ECP/EDX username/password (no other authentication method is supported). Both eSett and Market Participant ECP/EDX endpoints (https/TLS) must be configured with certificate issued by widely accepted certification authority (using self-signed or non-trusted certificates is not supported). The data transport is automatically protected with TLS (using the configured certificates).

3.4 Manual data submit via Online Service

There is also an option to submit messages manually, which can be done by Market Participant via Online Service. Every Market Participant is given access to this service, which is a web portal, where users can view all market structures and their hourly data that belong to this Market Participant.

3.5 Supported Data flows

Following table lists the data flow types supported by Messaging Service. Please refer to Business Requirement Specification for more details. XSD for all data flow types (along with message examples and format description) can be found at https://www.ediel.org.

For the Outbound data flows, the Message Identification is generated using following pattern:

YYYYMMDD_<Data flow code>_<Sender>_<Recipient>_<DocumentId>.xml

Example of Message Identification is 20160210_SERO_44X-00000000004B_BRP01_197844d55474efe96114.

Messages with same format (e.g. SERO and MGIO) follows the same basic message structure but the content of the elements differ. For example different identifiers and recipient are presented.

Table 3 Messaging Service data flows

Data flow code	Data flow	Process	From	Format
PXTI	PX Market Trade	Scheduling	NPS or TSO (optional)	ENTSO-E ESS Schedule Document v4r1
PXFI	PX Market Flow	Scheduling	NPS	ENTSO-E ESS Schedule Document v4r1

Data flow code	Data flow	Process	From	Format
SPTI	Spot Price	Scheduling	NPS	ENTSO-E ECAN Publication Document
SPCI	Spot Price	Scheduling	Selecting Service	CIM Publication Document UML Model and Schema – version 1.1 (2018-05-02)
BITI	Bilateral Trade	Scheduling	BRP or TSO	ENTSO-E ESS Schedule Document v4r1
BICO	Bilateral Trade Confirmation Report	Scheduling	eSett	ENTSO-E ESS Confirmation Report v4r1
PRPI	Production Plan	Scheduling	TSO	ENTSO-E ERRP Planned Resource Schedule Document v5r0
ACRI	Activated Reserve	Scheduling	NOIS (on behalf of TSOs)	NEG (based on ENTSO-E ERRP) Reserve allocation result document
CREI	Capacity Reserves	Capacity	TSO	NEG (based on ENTSO-E ERRP) Reserve allocation result document
REPI	Regulation Prices	Scheduling	NOIS (on behalf of TSOs)	NEG (based on ENTSO-E ECAN) Publication Document
RPMI	Production	Metering and settlement	DSO	NEG (ebIX® based) Validated Data for Settlement for Aggregator (E66, E44)
RECI	Consumption	Metering and settlement	DSO	NEG (ebIX® based) Aggregated Data per MGA for Settlement Responsible (E31, E44)
MGXI	MGA Exchange	Metering and settlement	DSO	NEG (ebIX® based) Aggregated Data per Neighbouring Grid for Settlement Responsible (E31, E44)
MGCO	MGA Exchange Confirmation Report	Metering and settlement	eSett	NEG Confirmation of Aggregated Data Per Neighbouring Grid From Settlement Responsible (A07/A08), E44)
SERO	Settlement Result	Metering and settlement	eSett	ENTSO-E Energy Account Report Document (EAR) v1r2

Data flow code	Data flow	Process	From	Format
MGIO	MGA Imbalance	Metering and settlement	eSett	ENTSO-E Energy Account Report Document (EAR) v1r2
MGRI	MGA Imbalance Retailer – IN	Scheduling	DSO	NEG Party Master Data Document
PRUI	Production Unit – IN	Scheduling	DSO	NEG Resource Object (Production Unit) Master Data Document
CONI	Conusmption MEC – IN	Scheduling	DSO	NEG Party Master Data Document
BTRI	Bilateral Trade MEC – IN	Scheduling	BRP	Ediel Request Trade Structure Document version 1.0
PXMI	PX Market Trade MEC – IN	Scheduling	Market Operator	Ediel Request Trade Structure Document version 1.0
EPFI	External PX Flow	Scheduling	TSO	ENTSO-E Publication document – UML model and schema version 1.1 The document must be compliant with the XSD: Schedule_MarketDocument v5.1
PLSI	Preliminary Loadshares per MGA per BRP	Reconciliation	DSO	UTILTS & APERAK model and schema version: IG-version: E5SE1B IG-revision: 12 Document name code : S03
LPRI	Load Profile per MGA	Reconciliation	DSO	UTILTS & APERAK model and schema version: IG-version: E5SE1B IG-revision: 12 Document name code: E31 Reason for transaction: E44
FLSI	Final Loadshares per MGA per BRP	Reconciliation	DSO	UTILTS & APERAK model and schema version: IG-version: E5SE1B IG-revision: 12 Document name code: E31

Data flow code	Data flow	Process	From	Format
				Reason for transaction: E43
DERI	Delivered Reserves	Metering and settlement	TSO, BSP, Datahub	CIM Activation_MarketDocument Document type: **A83** (Activated balancing quantities)

Note: Examples of each listed data flow can be found at https://www.esett.com/customers/data-communications/

3.6 Acknowledgements

After delivery of message from Market Participant to Messaging Service, Participant will be acknowledged about the results of delivery by Acknowledgement message.

The Acknowledgement is treated as a special kind of Message, which is not tied to any particular Process, Direction or System – the Format is ENTSO-E AcknowledgementDocument v6r0.

Purpose is to inform Market Participant about result of message processing, whether positive or not, in which case reason of processing failure is stated.

Details how Acknowledgement is structured and how to recognize contained information about processing results are published in the Business Requirement Specification.

Acknowledgements for UTILTS messages are also in EDIFACT format (UTILTS-ERR, APERAK, CONTRL).

3.7 Integration Procedure

This chapter describes the technical tasks which need to be performed in order to implement the integration.

The main prerequisite for integration is ability to create and process Messages (of ENTSO-E, ebIX or CIM formats).

3.7.1 FTP

- MPS user configures the FTP channel using Online Service
- FTP folder name
- FTP user name (can be changed later)
- FTP password (can be changed later)

- MPS implements an FTP Client (supporting SSH FTP) and configures it with URL and port (provided by eSett) and username/password (configured by MPS in previous step)
- Note: Connecting to FTP using provided credentials will allow MPS to access it's folder
- MPS connects to FTP and places Inbound messages to the INBOUND folder
- MPS connects to FTP server and uses outbound folder configured in Messaging Service as Outbound channel.

3.7.2 Mail

- MPS user configures the Mail channel using Online Service
- Recipient e-mail address (where Messaging Service sends the Outbound Message to)
- MPS implements Mail Client configured with MPS based SMTP and POP3/IMAP server
- MPS uses the client to send Inbound Messages to Imbalance Settlement System Messaging Service e-mail address (all MPS use the same address)
- MPS uses the client to poll the Outbound Messages (using POP3 or IMAP) from their INBOX

3.7.3 Web Service

MPS user configures the Web Service channel using Online Service

- WS Username
- WS Password
- MPS implements a WS Client (WSDL available from the endpoint/see Information Service Guide for details) and configures it with URL (provided by eSett) and sets WS-Security username/password to credentials configured by MPS in previous step. MPS uses this WS client to send Inbound Message to Messaging Service.
- MPS implements a WS Server (WSDL available from the endpoint/see Information Service Guide for details) and deploys it to a server which is accessible to Messaging Service over internet (the URL of this WS Server is configured in first step). Messaging Service then sends requests with Outbound

Messages to this server (and uses WS-Security username/password configured by MPS in first step.

3.7.4 ECP/EDX

- MPS user configures the ECP/EDX channel using Online Service
- Outgoing EDX Receiver Endpoint Code
- Outgoing EDX Sender Application
- Incoming EDX Sender Endpoint Code
- Incoming EDX Sender Application
- ECP/EDX Username
- ECP/EDX Password

MPS implements an ECP/EDX endpoint

3.8 EDIFACT incoming and outgoing messages

EDIFACT (UTILTS, UTILTS-ERR, APERAK, CONTRL) messages are sent by E-mail. Each Market Party is responsible to fill out its UTILTS Email and Interchange Party ID in the electronic channel communication settings. In case that UTILTS Email is missing the system may still attempt to send messages through the preferred channel. Incoming EDIFACT messages through different channels may be rejected.

The system does not support partial-accepted status. If there is any error in the content of the EDIFACT message, then the whole message is rejected. Errors about the incorrect parts are reported through ACK or error log in Online Service.

3.8.1 Incoming messages

Incoming EDIFACT messages should be sent by **email** channel. Messages sent from the UTILTS Email must be in EDIFACT format or they will be rejected. An exception would be made if the same email is used for regular email communication and also UTILTS communication.

3.8.2 Outgoing messages

Outgoing EDIFACT messages will always be sent by email channel to the UTILTS Email address, unless the recipient does not have UTILTS Email filled in.

4 Setting up the connectivity for the first time

When the Market Participant is setting the connectivity towards and from eSett for the first time, there are preconditions and process to follow, which both are described in this chapter.

4.1 Prerequisites and firewall openings

In order for a Market Participant to submit and receive data to and from eSett, following prerequisites have to be met:

1. The Connection details template/form is filled in.
2. The Market Participant has submitted a service request containing Connection details template/form as an attachment to eSett's customer service either via email (settlement@esett.com) or preferably via web form

4.2 Process description

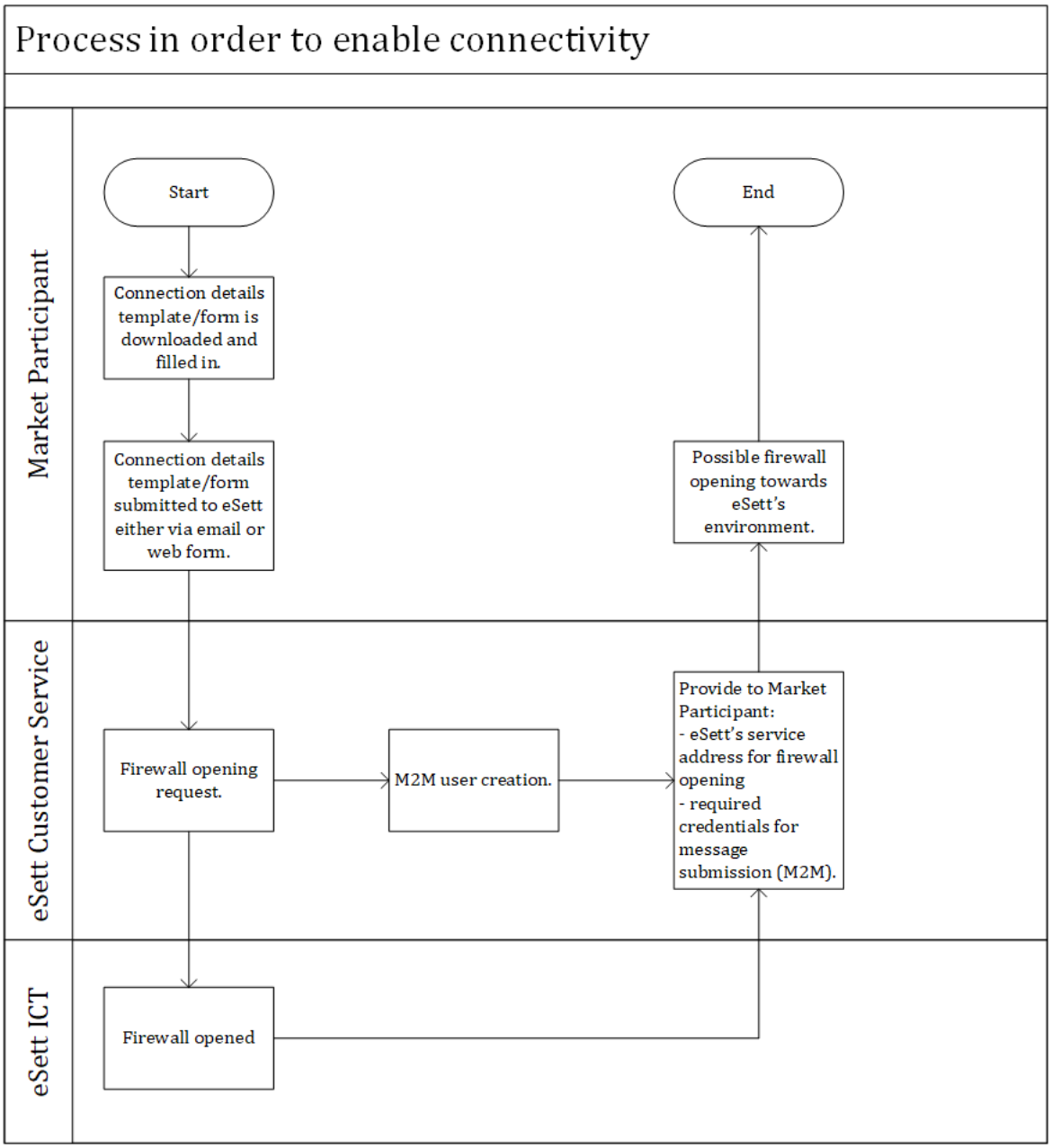

Figure 5: Process description in order to enable connectivity between the Market participant and eSett

4.3 Connection details excel and detailed instructions

Below are detailed instructions on how to fill in the Connection details template/form. The form contains multiple tabs, the Market Participant is required to fill in all fields only in the tab of the submission channel that the Market Participant wishes to use.

The Market Participant can use multiple ways to deliver data at once, but needs to select a primary channel that will be used to deliver data back towards the Market Participant (e.g. SMTP can be used as default channel and SFTP can be used as a backup channel.

eSett however will always try to return Settlement results to SMTP, since it is chosen as the primary channel).

Company							
Party	Business ID	Country	Coding scheme	Code	Name of main contact person	Mobile phone number	E-mail address

Figure 6: Company details

Each tab first contains section "Company" which is same regardless of channels used. Fill it in as follows:

- Party – Business name of the company.
- Business ID – ID of Market Participant's company as registered in national trade register.
- Country – Country where company is registered.
- Code and Coding scheme – Unique identification code that fills the requirements of National Scheme, EIC or GS1. Please see the Handbook for details. This code will be used in every message Market Participant sends or receives and it is used to connect the message to sender's company.
- Name of the main contact person – The person that will be contacted by eSett primarily in case of issues with the settlement process.
- Mobile phone number – Number where the Contact person can be reached.
- E-Mail address – E-Mail where the Contact person can be reached.

4.3.1 SMTP

Company							
Party	Business ID	Country	Coding scheme	Code	Name of main contact person	Mobile phone number	E-mail address

Fill required information for message submission				
Prefered Delivery Channel	Public IP Address of your SMTP	SMTP Server Address	SMTP port	Email address from which you send messages
SMTP				

Fill required information for message reception	
SMTP server IP address	Email address where you want to receive

Figure 7: SMTP channel details

In case that the Market Participant decides to use e-mail as the primary channel to deliver and receive messages, please fill in the tab "SMTP" with following information:

In Section "Fill required information for selected primary service"

- Preferred Delivery Channel– fill in SMTP to this cell if SMTP is used as the primary channel. Otherwise, choose any other channel you will use as the primary way of delivering data and e-mail will work as secondary. Please note that eSett always uses the primary channel to deliver settlement results.
- Public IP Address of your SMTP – IP Address from which the MP will send messages, meaning that this is the address from which the Market party's SMTP server opens connections. Make sure to list a public address, not an internal one if NAT is used.
- SMTP Server address – Public address of Market Participant's SMTP Server, usually in format smtp.example.com or similar.
- SMTP Port – Port which Market Participant is using while sending the email.
- E-Mail address for SMTP Communication – The e-mail address from which MP will send the messages towards eSett.
- Fill in required information for message reception
- SMTP Server Address – IP of Market Participant's SMTP, which is used to whitelist E-Mail delivery to the Market Participant's inbox.
- Email address where the messages from eSett are sent – eSett will deliver the results to this inbox, make sure it can receive up to 50MB per message, as some files (Mainly Data Packages) may reach this size

4.3.2 SFTP

Company							
Party	Business ID	Country	Coding scheme	Code	Name of main contact person	Mobile phone number	E-mail address
Fill required information for selected primary service							
Prefered Delivery Channel (FTP/SFTP)	Public IP Address of your FTP server	Protocol eSett should use to deliver FTP messages to you	Host (IP Address of your FTP where messages will be delivered)	Port (Default for SFTP is 22)	Username (credentials that eSett should use to connect to your FTP)	Password	FTP folder (leave blank if root folder is where you wish messages to be placed)
SFTP		SFTP					

Figure 8: SFTP channel details

In case that the Market Participant decides to use SFTP as the primary channel to deliver and receive messages, please fill in table "FTP" with following information:

In section:" Fill required information for selected primary services."

- Preferred Delivery Channel – In case that SFTP is wanted to be used as primary method to deliver and receive data, SFTP is filled into this cell, otherwise the Market Participant can choose whichever channel will be used as primary. The ability to use SFTP as secondary channel for data delivery will not be influenced, but eSett will always deliver settlement results to the primary channel only.
- Public IP Address of your SFTP server – the IP where Market Participant's SFTP Server is located. This is used to whitelist the address in eSett's firewall, so delivery of results can be done. The Market Participant needs to make sure this address is static.
- The protocol – SFTP
- Host – The address where eSett will deliver the data, this address needs to be reachable from eSett's IP Address which is listed on the homepage of Online Service.
- Port – Port which eSett uses to deliver the results.
- Username – eSett will use this username to deliver the material to Market Participant's server.
- Password – See above.
- FTP Folder – In case it is wanted for eSett to place data to specific folder, list it here. If messages are wanted to be delivered directly to root folder, this can be left empty.

4.3.3 Webservice

Company							
Party	Business ID	Country	Coding scheme	Code	Name of main contact person	Mobile phone number	E-mail address

Fill required information for selected primary service			
Prefered Delivery Channel	You Web Service URL (to receive Settlement Results)	Web Service username (to authorize eSett's result delivery)	Web Service password
WebService			

Figure 9: Webservice channel details

In case that the Market Participant decides to use WebService as its primary channel to deliver and receive messages, please fill in table "WebService" with following information:

In section: "Fill required information for selected primary service"

- Preferred Inbound Connections – In case that the Market Participant wants to use WebService channel as the primary one, fill in WebService to this cell, otherwise choose whatever channel which will be used as the primary way of delivering data.
- Web Service IP Address – IP from which the Market Participant's WebService will submit data to eSett, this is used to whitelist IP for connections to eSett.
- Fill in required information for delivery of results from eSett o Web Service URL – Address where eSett will submit results to Market Participant.
- Web Service username – Credentials that eSett uses to authorize to Market Participant's service
- Web Service password – See above
- Web Service IP Address – IP Address where Market Participant's WebService where eSett submits data, this is used to whitelist IP for delivery.

4.3.4 ECP

Company							
Party	Business ID	Country	Coding scheme	Code	Name of main contact person	Mobile phone number	E-mail address

Fill required information for selected primary service	
Prefered Delivery Channel	Endpoint Code
ECP/EDX	

Figure 10: ECP/EDX channel details

In case that the Market Participant decides to use ECP/EDX as the primary channel to deliver and receive messages, please fill in table "ECP-EDX" with following information:

- Fill in the Component Code of Market Participants Endpoint

5 Information Service Integration

5.1 Interfaces

Information Service interface allows MPS to request data from Imbalance Settlement System. The request is represented by an ENTSO-E Status Request Message. Based on the request, Imbalance Settlement System creates a response, consisting of the business document (one of the supported ENTSO-E or ebIX formats) and passes it back to MPS as a Message. Using this interface, MPS can retrieve information related to the Settlement process.

Information Service provides Web Service as a channel to access the information. MPS must implement specific WS Client in order to use Information Service. The details of the Web Service Channel are specified in section below.

See Information Service Guidelines at https://www.esett.com/customers/data-communications/ to see more specific requests and responses.

5.1.1 Request Format

The Information Service uses ENTSO-E Status Request Document 2.0 as a request format. The document gives sufficient flexibility to request the data from Information Service. The identification of Data Flow and any parameters that need to be passed as data filtering criteria can be represented using the RequestComponent element (see example below).

Example document (request for Bilateral Trades for given time period and given optional parameter (example shows also WS Security header)):

```
<soap:Envelope xmlns:inf="http://www.basse.eu/information-service-1.0"
xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:entsoe.eu:wgedi:components">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"><wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd"><wsse:UsernameToken wsu:Id="UsernameToken-
F50D6C2297C7D81D1F1449669355941134">
<wsse:Username>User_name</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordText">password</wsse:Password><wsse:Nonce
```

```
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary">GFoemDPGx9N0+tGnshjnGQ==</wsse:Nonce>

<wsu:Created>2015-12-09T13:55:55.941Z</wsu:Created>

</wsse:UsernameToken></wsse:Security><wsa:Action>http://www.basse.eu/information
-service-
1.0/IInformationService/GetData</wsa:Action><wsa:To>https://localhost:44301/Info
rmationService.svc</wsa:To></soap:Header>
   <soap:Body>
    <inf:GetData >
        <inf:request  DtdVersion="1" DtdRelease="0">
            <urn:DocumentIdentification v="XYZ"/>
            <urn:DocumentType v=""/>
            <urn:SenderIdentification v="SENDER_CODE " codingScheme="A01"/>
            <urn:SenderRole v="A04"/>
            <urn:ReceiverIdentification v="44X-00000000004B"
codingScheme="A01"/>
            <urn:ReceiverRole v="A05"/>
            <urn:CreationDateTime v="2015-01-21T18:00Z"/> <urn:RequestComponent>
                <urn:RequestedAttribute v=" DataFlow "/>
                <urn:RequestedAttributeValue v="RPM" />
            </urn:RequestComponent>
            <urn:RequestComponent>
                <urn:RequestedAttribute v="TimeInterval"/>
                <urn:RequestedAttributeValue v="2014-11-25T22:00Z/2015-11-
30T23:00Z" codingScheme=""/>
            </urn:RequestComponent>
            <urn:RequestComponent>
                <urn:RequestedAttribute v="TimeResolution"/>
                <urn:RequestedAttributeValue v="PT1H" codingScheme=""/>
            </urn:RequestComponent>
            <urn:RequestComponent>
                <urn:RequestedAttribute v="OPTIONAL_PARAMETER "/>
                <urn:RequestedAttributeValue v="MBAEXAMPLECODE"
codingScheme="A01"/>
            </urn:RequestComponent>
            </inf:request>
    </inf:GetData>
</soap:Body>
</soap:Envelope>
```

The available attributes for given data flows are documented in detail below. The RequestComponent attributes is designed in order to use standard message attributes (e.g.

DocumentType or ProcessType) where possible. For header construction, please note following security notes:

- Add into soap header wsse:Security element with username and plain password.
- Add default wsa:Action and add default wsa:To

Roles and the corresponding codes in requests:

- Balance Responsible Party (Sender role code A08)
- Balancing Service Provider (A46)
- Retailer (Sender role code A12)
- Distribution System Operator (Sender role code A18)

5.1.2 Result Format

Response from method 'GetData' is in an XML format that corresponds to the data that is received. Please see following section for more details. For a basic idea of how the message is encapsulated see the following example.

In this example a response for 'Production' dataflow is returned. Please see that the actual response is an XML document encoded in the CDATA section.

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <s:Header>
      <a:Action s:mustUnderstand="1">http://www.basse.eu/information-service-
0.1/IInformationService/GetDataResponse</a:Action>
      <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <u:Timestamp u:Id="_0">
            <u:Created>2015-06-29T15:35:00.487Z</u:Created>
            <u:Expires>2015-06-29T15:40:00.487Z</u:Expires>
         </u:Timestamp>
      </o:Security>
   </s:Header>
   <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <GetDataResponse xmlns="http://www.basse.eu/information-service-1.0">
         <GetDataResult>

            <Content><![CDATA[<?xml version="1.0" encoding="utf-8"?>
<ValidatedDataForSettlementForAggregator
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="un:unece:260:data:EEM-
```

```
ValidatedDataForSettlementForAggregator">
                        ......
</ValidatedDataForSettlementForAggregator>
              ]]>
            </Content>
          </GetDataResult>
        </GetDataResponse>
    </s:Body>
</s:Envelope>
```

5.1.3 Supported Data Flows

The table below describes

- *Name* and *Description* of the Data Flow supported by Information Service
- *Format* of document that is returned by the Information Service
- Available *Selection Parameters* which a Market Participant can use when querying the Information Service.

Table 4 Information Service data flows

Data Flow	Description	Counterparty / System	Result Format
Bilateral Trades	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Bilateral Trade	BRP	ENTSO-E ESS Schedule Document v4r1
PX Market Trades	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of PX Market Trade	BRP, NPS	ENTSO-E ESS Schedule Document v4r1
PX Market Flows	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of PX Market Flow	BRP, NPS	ENTSO-E ESS Schedule Document v4r1
MGA Exchanges	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of MGA Exchanges.	DSO	NEG (ebIX® based) Aggregated Data per Neighbouring Grid for Settlement Responsible (E31, E44)

Data Flow	Description	Counterparty / System	Result Format
MGA Exchange Trades	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of MGA Exchange Trades	BRP, RE	ENTSO-E ESS Schedule Document
Consumption	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Consumption	BRP, DSO	NEG (ebIX® based) Aggregated Data per MGA for Settlement Responsible (E31, E44)
Production	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Production	BRP, DSO	NEG (ebIX® based) Validated Data for Settlement for Aggregator (E66, E44)
Production Plan	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Production Plans	BRP	ENTSO-E ERRP Planned Resource Schedule Document v5r0
Activated Reserves	Hourly/aggregated values of Activated Reserves	BSP	NEG (based on ENTSO-E ERRP) Reserve allocation result document
Capacity Reserves	Hourly/aggregated values of Capacity Reserves	BSP	ENTSO-E ERRP Reserve Allocation Result Document
Imbalance Adjustment	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Imbalance Adjustment	BRP	ENTSO-E ERRP Reserve Allocation Result Document
Prices	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Prices that are used for settlement	BRP, DSO, NPS	NEG (based on ENTSO-E ECAN) Publication Document
Consumption Imbalance	Hourly/aggregated values of all settlement results – Consumption Imbalance (volumes, amounts, ...)	BRP	ENTSO-E Energy Account Report Document (EAR) v1r2

Data Flow	Description	Counterparty / System	Result Format
Production Imbalance	Hourly/aggregated values of all settlement results – Production Imbalance (volumes, amounts, ...)	BRP	ENTSO-E Energy Account Report Document (EAR) v1r2
MGA Imbalance	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of all settlement results – MGA Imbalance (volumes, amounts, ...)	BRP, DSO	ENTSO-E Energy Account Report Document (EAR) v1r2
Production per Production Unit Type and MGA	Hourly (for period before 15MTP) or 15-minutes (for period after 15MTP) values of Production per Production Unit Type and MGA	TSO	Basse Time Series Document
MGA-MBA Relations	Service provides MGA-MBA relations in country specified in the request.	DSO, TSO, BRP, RE	NBS BRS for Master Data v1r8A - 20180606 (Ediel.org)

5.1.4 Handling of Optional Parameters

Some of the request parameters of Information Service are marked as optional. If any of these parameters are left out of the request XML document, it is assumed that the sender wants to get information about all of the values, which are accessible to the sender.

E.g. when requesting Production hourly data, one can leave the Production Unit parameter out. The Information Service will then return values for all Production Units the sender is entitled to access.

Please consider that in this scenario the response might (especially for large service providers) surpass the limit for maximal response size. The preferred solution is then to query smaller time intervals (e.g. one day instead of one week).

5.2 Web Service Channel

The request channel uses WS-Security envelope to transmit the user's credentials. The request itself is then composed as ENTSO-E Status Request document. See Information Service Guide for examples.

The response is either the XML document in format defined by each Data Flow (see section above) or, in case of error in processing, a SOAP fault document with detailed information about the error (e.g. user is not entitled to see given data etc).

The channel uses a common Request-Reply synchronous communication pattern.

5.2.1 Request Limitations

The technical configuration of Information Service allows setting following parameters to limit the usage. In case any of these limitations is exceeded by the caller of the Information Service; an appropriate exception is returned to the caller.

Limitation	Default Value	Description
Maximum Data Values in Request	74.000	Maximum number of data values in a single Request.
Maximum Number of Values per Minute	740.000	Maximum number of values requested by 1 Market Participant per one minute. This throttles the communication with single Market Participant and protects Information Service against abnormal usage.

5.3 Usage Patterns

This section describes behaviour of the Information Service users (Market Participant Systems). The motivation is to ensure that Information Service will be used with respect to overall Imbalance Settlement System solution performance.

Information Service is expected to be used based on "events" distributed by Imbalance Settlement System Solution. These "events" might include outgoing e.g. data flows or reports, which are actively distributed from Imbalance Settlement System solution to Market Participant Systems.

Information Service is expected to be used on periodical basis with at most hourly frequency. The expected pattern is to fetch data after periodical gate closure times (hourly, daily, weekly, monthly, or yearly).

Information Service is not expected to be frequently polled (with frequencies lower than 1 hour) for some data or event to appear in the system. All basic needs for outgoing data from eSett shall be fulfilled by using data flows, reports, or data packages.

Information Service is not expected to be directly used as a data source for any Market Participant located application (GUI, Reporting Engine, etc.). If there is need to display data fetched from Imbalance Settlement System, these data should be fetched and stored in Market Participant System – these stored data can then be used for other applications located in Market Participant's premises.

5.4 Integration Procedure

This chapter describes the technical tasks which need to be performed in order to implement the integration.

The main prerequisite for integration is the ability to create ENTSO-E Status Request and process the returned Messages (of ENTSO-E or ebIX formats).

5.4.1 Web Service

MPS implements a WS Client and configures it with Information Service URL (provided by eSett) and sets WS-Security username/password to credentials provided by eSett. MPS uses this WS client to send Status Request Messages to Information Service and gets set of requested information contained in ENTSO-E or ebIX document

6 Integration via Online Service

This chapter describes how configuration of communication with Messaging Service can be adjusted using user interface of Online Service.

6.1 Prerequisites and firewall openings

Should the Market Participant choose to alter communication method with eSett, it is the Market Participant's responsibility to first make sure, that possible firewall openings are done on Market Participant's environment and that firewall opening from eSett has been ordered according to the process

6.2 Communication Channel Configuration

This use case allows Market Participants to configure their communication channel for Messaging Service. Before starting with message delivery, it is necessary to choose preferred communication channel and fill in required information based on the choice. The following chapter describes how to select the channel and do the basic setup via Online Service.

6.2.1 Configuration Overview

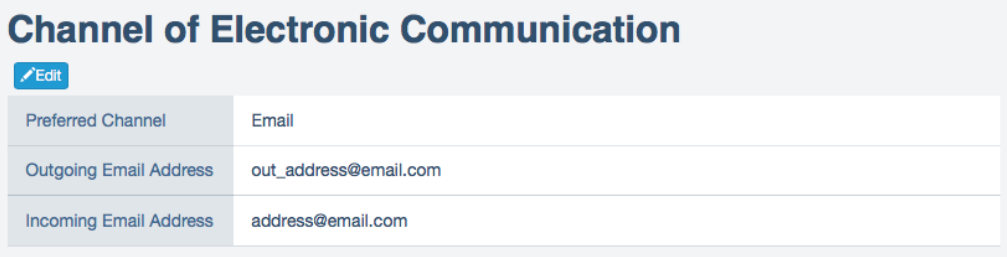

Figure 12: Example of Channel configuration

6.2.1.1 Channel of Electronic Communication

This table will be visible only to users of respective company (Market Participant), which have assigned role External Interface at least in mode Read.

Detailed description of all channels of electronic communication is described in chapters above.

Column Name	Description
Preferred Channel	Preferred channel of electronic communication. Options are 1. FTP 2. E-mail 3. Web Service 4. ECP/EDX
Incoming FTP Folder	Name of the folder, which has been assigned to a Market Participant. This is the folder where NBS Settlement System will expect messages to be delivered. Market Participant is forwarded to this location after connection.

Incoming FTP Username	Username used for login via FTP to a server
Incoming FTP Password	Password used to connect to FTP server, Market Participant can set and alter this password. Password has to contain at least 8 characters, one of which has to be capital letter, one special character and one number.
Outgoing FTP Address	URL of Market Participant's FTP server, where outgoing messages and acknowledgements from NBS Settlement system will be delivered.
Outgoing FTP Port	Port used for connection to Market Participant's FTP server
Outgoing FTP Protocol	Protocol used for connection to Market Participant's FTP server, i.e. "sftp"
Outgoing FTP Folder	Name of the folder, which should be used on Market Participant's FTP server for exchange of data between MP and eSett
Outgoing FTP Username	Username used for login via FTP to a server
Outgoing FTP Password	Password used to connect to Market Participant's FTP server.
Recipient Address	E-mail address of a recipient used for electronic communication used by NBS Settlement System to deliver outgoing messages and acknowledgement to Market Participant.
Incoming WS URL	URL of the web service used by Market Participant to connect to deliver messages into NBS Settlement System. This information is distributed by eSett.
Incoming WS Username	Username used for authentication of web service communication used by Market Participant to connect to Messaging Service to deliver messages to NBS Settlement System.
Incoming WS Password	Password used to connect to Web Service, Market Participant can set and alter this password. Password has to contain at least 8 characters, one of which has to be capital letter, one special character and one number.
Outgoing WS URL	URL of the web service, where outgoing messages and acknowledgements should be delivered to Market Participant.
Outgoing WS Username	Username used for authentication of outgoing web service communication.
Outgoing WS Password	Password used to connect to market Participant's Web Service.
ECP/EDX Endpoint Code	Market Participant's Component code for the Endpoint.
ECP/EDX Sender Application	Optional field for the application name.
UTILTS Email	UTILTS Email address used for UTILTS communication.
Interchange Party ID	Interchange Party ID used for UTILTS communication in UNB segment.

7 Usage of Certificates

7.1 General Consideration

Certificates in Information Service and Messaging Service are used to secure the machine-to-machine communication between Imbalance Settlement System and Market Participants. All of these are only used as server-side domain certificates, i.e. they are installed on server in order to secure its identity (e.g. preventing man-in-the-middle attack) and to encrypt the communication between server and its client. These certificates can be any type of domain certificate (e.g. Single Domain, Multiple Domain or Wildcard) and must be issued by commonly trusted certification authorities (Imbalance Settlement System doesn't support adding public keys/certificates for untrusted certification authorities or self-signed certificates). Certificates are not supported for any other purpose (like client authentication or signatures) than server-side domain certification.

7.2 Web Services

All eSett communication web servers (Messaging Service Web Service and Information Service Web Service) are configured with trusted server-side domain certificate - Market Participant clients shouldn't need any configuration in order to establish secured (TLS) communication with them. Market Participant located web servers (Messaging Service Web Service - used to receive messages from Imbalance Settlement System) must be configured with trusted server-side domain certificate - if not so, Imbalance Settlement System will not trust these servers and will not establish secured (TLS) communication with them.

7.3 E-Mail

Machine-to-machine communication using e-mail can be optionally secured with STARTTLS. In that case, both communicating SMTP servers (Messaging Service SMTP and Market Participant SMTP) must be configured for STARTTLS with trusted server-side domain certificate (the same certificate as for Web Services can be used in case the domain is the same).

7.4 ECP/EDX

Both eSett and Market Participant ECP/EDX endpoints (https/TLS) must be configured with certificate issued by widely accepted certification authority (using self-signed or non-trusted certificates is not supported). The data transport is automatically protected with TLS (using the configured certificates).