

# Communication Guidelines

Data interchange between NBS Market Participants and eSett

19 November 2020

PUBLIC

# Contents

|   |    |
|---|----|
| Contents .....  | 1  |
| Communication Guidelines .....                                      | 3  |
| 1. Terms and Definitions.....                                       | 3  |
| 2. Introduction and purpose of the document.....                    | 4  |
| 2.1. Available channels .....                                       | 4  |
| 3. Integration towards eSett and to Messaging Service .....         | 5  |
| 3.1. Manual data submit via Online Service.....                     | 8  |
| 3.2. Public service addresses for data interchange .....            | 9  |
| 3.2.1. Data interchange towards eSett.....                          | 9  |
| 3.2.2. Data interchange from eSett towards Market Participant ..... | 9  |
| 3.3. About SFTP channel .....                                       | 10 |
| 3.3.3. Folder structure.....  | 10 |
| 3.3.4. Naming conventions .....                                     | 10 |
| 3.3.5. Security.....  | 11 |
| 3.4. About E-mail channel .....                                     | 11 |
| 3.4.6. Acknowledgements specifications.....                         | 11 |
| 3.4.7. Security.....  | 11 |
| 3.5. About Webservice channel.....                                  | 12 |
| 3.5.1. Webservice API .....   | 12 |
| 3.5.1.1. SOAP envelope format .....                                 | 13 |
| 3.5.1.2. Successful message submission .....                        | 14 |
| 3.5.1.3. Failed message submission.....                             | 14 |
| 3.5.1.4. Security error user is not authenticated.....              | 15 |
| 3.5.1.5. And internal server error technical error on server .....  | 15 |
| 3.5.2. Security.....  | 15 |
| 3.6. About ECP/EDX channel.....                                     | 15 |
| 4. Setting up the connectivity for the first time .....             | 20 |
| 4.1. Prerequisites and firewall openings .....                      | 20 |
| 4.2. Process description .....                                      | 21 |
| 4.3. Connection details excel and detailed instructions.....        | 22 |
| 4.3.1. SMTP .....   | 22 |
| 4.3.2. SFTP .....   | 23 |
| 4.3.3. Webservice .....   | 24 |

|   |    |
|---|----|
| 4.3.4. ECP .....                                  | 24 |
| 5. Supported messages.....                        | 26 |
| 5.1. Message creation basics .....                | 27 |
| 6. Acknowledgements .....                         | 29 |
| 7. Certificates .....                             | 29 |
| 7.1. General .....                                | 29 |
| 7.2. Webservices.....                             | 29 |
| 7.3. E-mail.....                                  | 29 |
| 8. Altering an existing communication method..... | 30 |
| 8.1. Prerequisites and firewall openings .....    | 30 |
| 8.2. Process description .....                    | 31 |
| 8.3. Configuration overview .....                 | 31 |

# Communication Guidelines

## 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 <a href="http://ediel.org">ediel.org</a> .  |
| 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 <a href="http://www.esett.com/handbook/">http://www.esett.com/handbook/</a> .         |
| 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 <a href="#">MADES communication standard</a> .   |
| 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 Table: Terms and definitions

## 2. Introduction and purpose of the document

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).

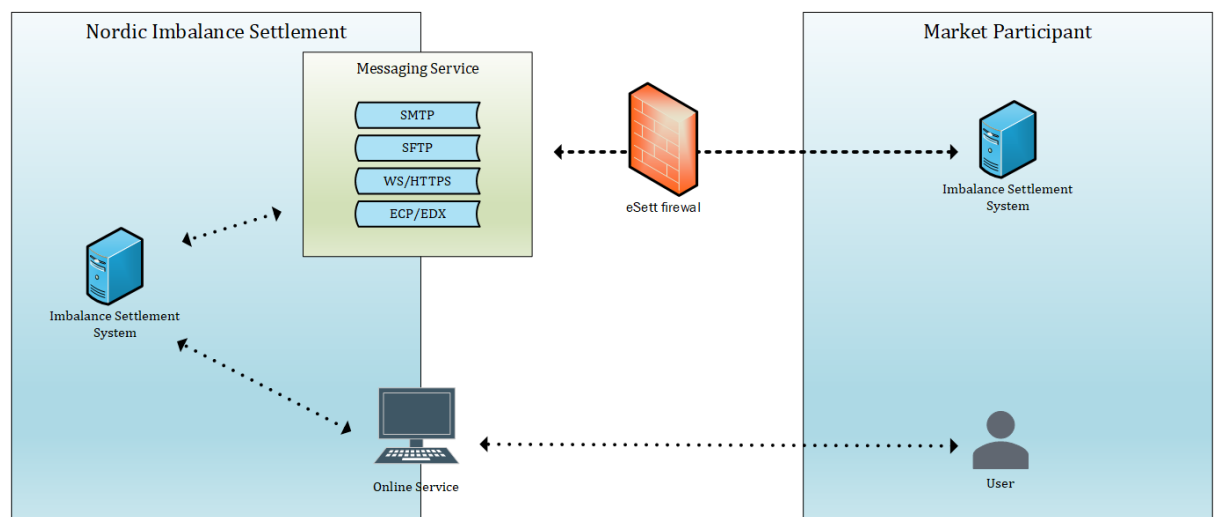
Purpose of this document is to describe what is needed in order to deliver and receive the data for settlement purposes.

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

### 2.1. 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 Simplified illustration of integration to and from Imbalance Settlement System

### 3. Integration towards eSett and to Messaging Service

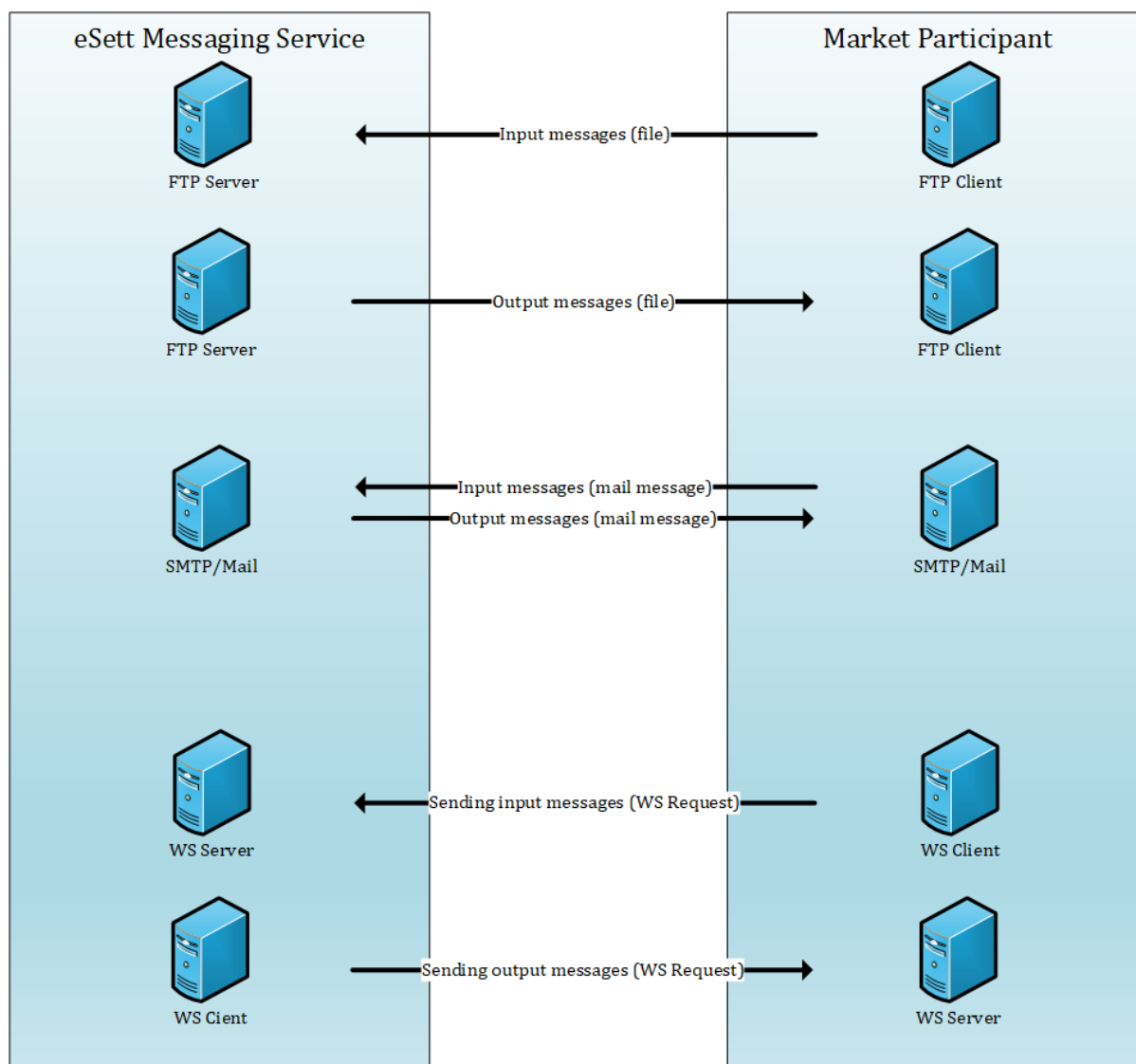
Market participants in different roles are expected to deliver data towards eSett for imbalance settlement purposes.

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.

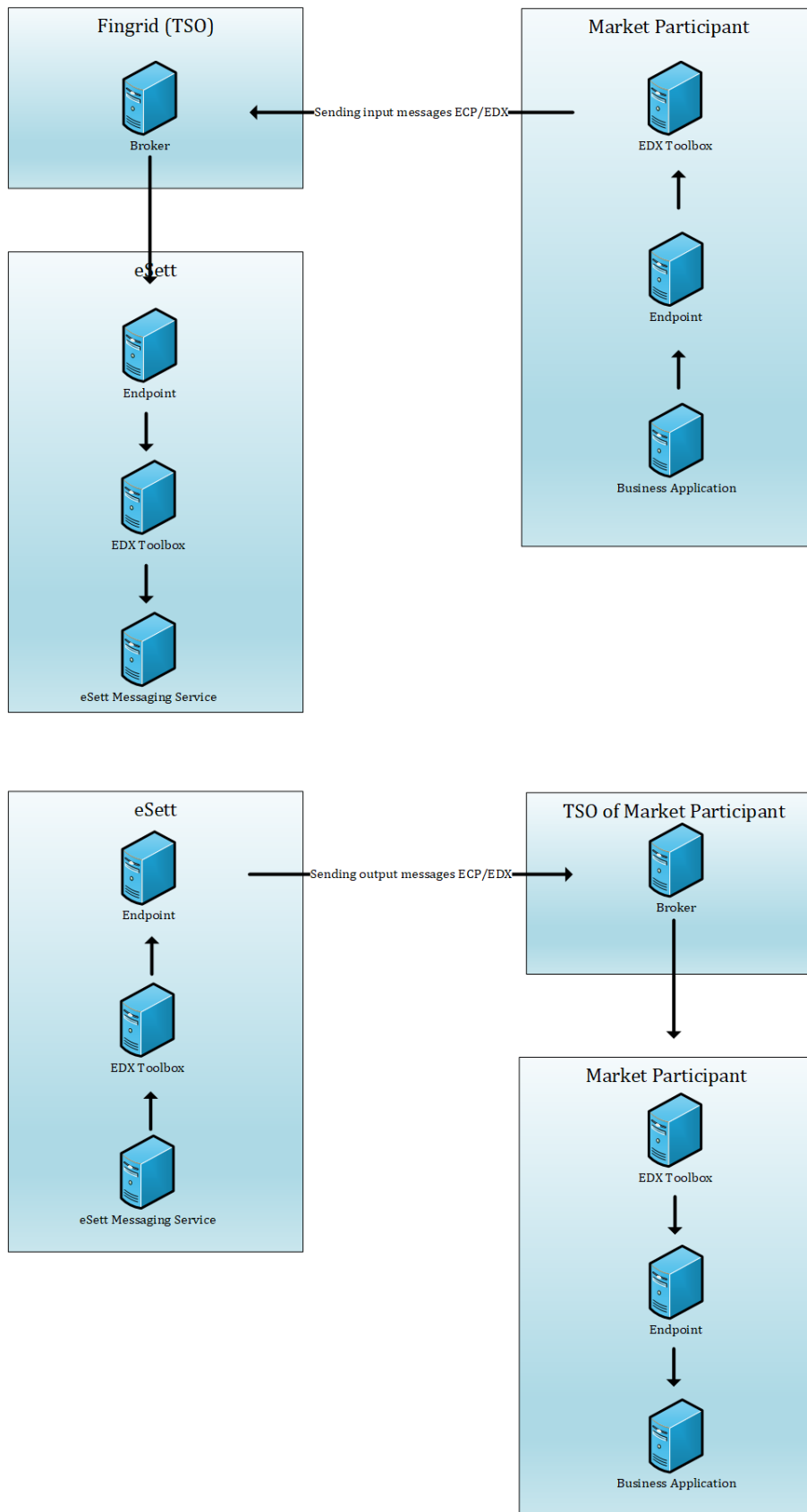
Market participants are able to deliver these XML files to Messaging Service via four supported channels:

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 respond back to Market Participant, whether submission was successful. The response is asynchronous, and usually sent within minutes of receiving the original message. See sample schemas below.



3 Messaging service scheme for SMTP, SFTP and Webservice



#### 4 Scheme for ECP/EDX



### 3.1. 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.

## 3.2. Public service addresses for data interchange

### 3.2.1. 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<br>/MSGs/messaging<br>ServiceInputInterface | 193.66.248.245 |

### 3.2.2. Data interchange from eSett towards Market Participant

eSett calls Market Participants from following IP addresses:

- 193.66.248.234
- 193.66.248.235

### 3.3. About SFTP channel

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.

#### 3.3.3. Folder structure

The folder structure of the Messaging Service SFTP (used for Inbound flows) is defined by following example.

After successful login the user is directed to root folder, where the only available folder is "Inbound". Messages are expected to be delivered inside this folder. The system will read any XML file placed there and will move the file automatically into the folder "Processed".

Only files that cannot be processed (File type is not XML) will stay in the Inbound folder indefinitely.

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

#### 3.3.4. Naming conventions

The convention to create the filename is following:

YYYYMMDD\_Message-code\_Sender\_Recipinet\_Document-id.xml

This is used by Nordic Imbalance Settlement System to ensure that all result files are unique and will not overwrite previous results.

The Market Participant is NOT forced to use this filename conventions, though it is recommended.

What is however necessary is to make sure, that XML files delivered to Nordic Imbalance Settlement System do contain “.xml” suffix, otherwise they will not be processed.

### **3.3.5. Security**

As stated above, the Market Participants are authenticated by 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 Participant needs to inform eSett about their IP address. eSett needs to open firewall based on this information.

About SMTP channel

While using email as the channel to deliver and receive settlement data towards and from eSett, the message is expected to be sent as an attachment.

The Subject and content of the message with exception of attachment is ignored and can be left blank.

However, in order for attached XML file in the e-mail to be processed, it must be declared as attachment type “application/xml”.

Message delivered can be up to 50MB in size.

## **3.4. About E-mail channel**

The e-mail message is expected to have a single file attachment. Content of the attachment is treated as a Message in Messaging Service.

The e-mail subject and body do not have any business semantics.

Attachments must be declared as “application/xml”.

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

### **3.4.6. Acknowledgements specifications**

The Nordic Imbalance Settlement System responds to every e-mail it receives from Market Participants with an acknowledgement message sent as an attachment in an e-mail.

This file is using the following naming conventions:

YYYYMMDD\_message-code\_Sender\_Receiver\_Document-id.xml

The file name is also used in the subject field of the e-mail. Same rules apply also for all Settlement results files and data packages.

### **3.4.7. Security**

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 a 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).

### 3.5. About Webservice channel

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.

#### 3.5.1. Webservice API

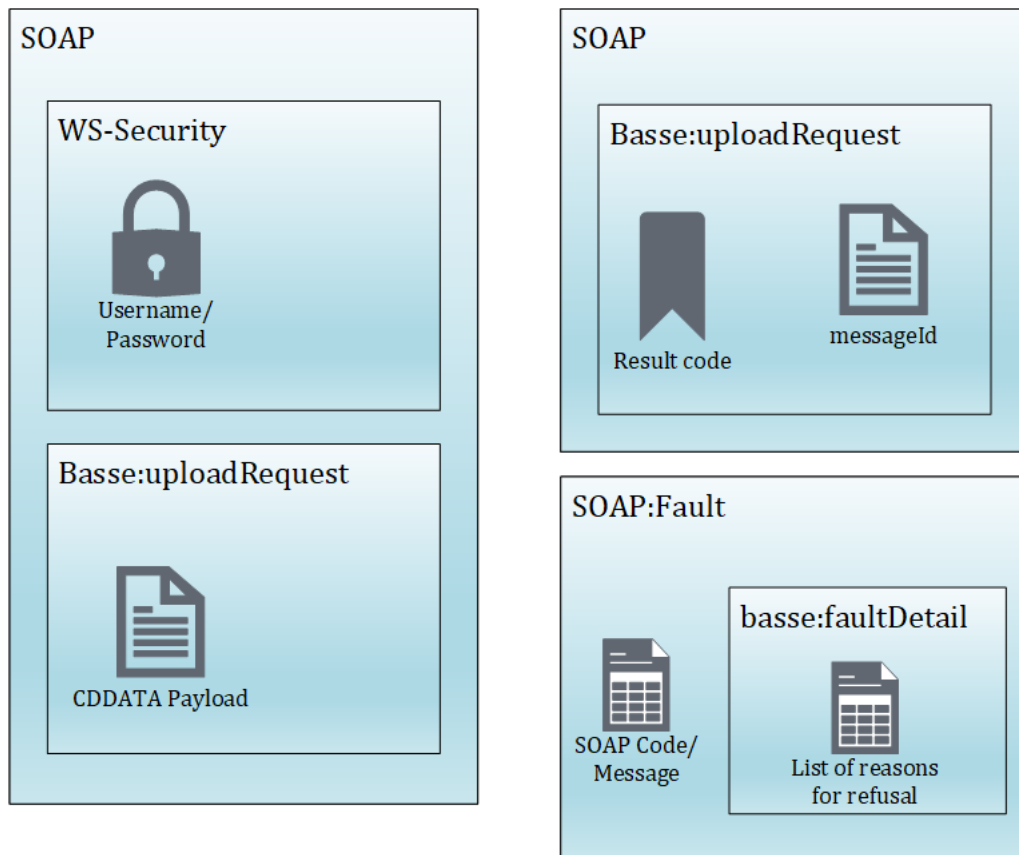
Following figure outlines the Web Service API.

The API has a single method upload Request with a 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 Internal Id of the Message and the result code of the operation. In case that the message is refused (e.g. due to some failure), the SoapFault is raised using a standard fault code and message, complemented with a custom list of refusal reasons.



### 5 Webservice endpoint API

#### 3.5.1.1. SOAP envelope format

In order to perform the submission of data, the Market Participant needs to use a correct envelope to submit content data.

This envelope should be correctly generated if the client is based on the WSDL.

Please verify, that the generated envelope matches the example bellow.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mes="http://www.nbs.coop/messaging-service-1.0">
  <soapenv:Header>
    <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:UsernameToken wsu:Id="UsernameToken-2" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <wsse:Username>username</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:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <mes:uploadRequest><![CDATA[<!-- the actual message is to be place here -->]]></mes:uploadRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

### 3.5.1.2. Successful message submission

Standard webservice response is returned, if the message is processed by Messaging Service and SOAP fault in the case of error.

A message is uploaded successfully only in the case when Messaging Service returns a response code MESSAGE\_RECEIVED.

```
<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, Messaging Service returns "uploadResponse" element with an additional nested elements:

- "result\_code", contains MESSAGE\_RECEIVED in case of successful upload and
- "message\_id" which is internal message id assigned to a message by Messaging Service.

A Message can be searched on by the message\_id in [Online Service](#).

For every incoming message the Messaging Service generates also an acknowledgement document with information about processing of the message. This acknowledgement will be delivered asynchronously back to the sender.

### 3.5.1.3. Failed message submission

In an unsuccessful scenario the Messaging Service returns a result code. The internal id of the generated acknowledgement document is part of the response as well.

| Result code          | Description   |
|----------------------|---|
| 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 a 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 a message with the same document id and version was already received from a Market Participant.          |
| USER_IS_NOT_SENDER   | This code is returned in the case when the username used for authentication does  |

|  |  |
|--|--|
|  | not have permissions for Market Participant for which the message is sent. |
|--|--|

6 Table: result codes for failed delivery

#### 3.5.1.4. Security error user is not authenticated

```
<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.

#### 3.5.1.5. And internal server error technical error on server

```
<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>
```

This SOAP Fault response is returned when the system is not able to process a message. This error can have different reasons - in this case please contact [eSett Customer Service](#).

### 3.5.2. Security

Market Participants are authenticated by using WS-S username/password (no other authentication method is supported).

Both eSett and the Market Participant's Web Service endpoints (https/TLS) must be configured with a 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).

## 3.6. About ECP/EDX channel

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.

| 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.<br>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.<br>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.<br>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.<br>It provides an abstraction of the services required for addressing, routing and secure exchange of messages.<br>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.<br>In this way Message Paths enables separation of traffic as well as transparent |

|  |  |
|--|--|
|  | <p>migration from one broker to another to facilitate high availability.</p> <p>A message path is selected based on recipient and Message Type and is stored in and distributed via the Component Directory.</p> |
|--|--|

7 Table: ECP components

| Component         | Description  |
|-------------------|--|
| Service Catalogue | <p>Complementary to the Component Directory, the Service Catalogue is a shared component, which provides a central source of truth for all subscriptions and publications in the network.</p> <p>The Service Catalogue is implemented as an application, which uses an Endpoint to communicate on the network.</p>   |
| Toolbox           | <p>A Toolbox is essentially a business application, which itself provides the same interfaces as an Endpoint, to its business applications, but adds a set of addressing capabilities to the system.</p> <p>These concerns the ability to publish messages to and receiving from services, as defined in the service catalogue.</p> <p>All actual exchange of data is still handled by the Endpoints and is getting all the promises from the MADES standard, such as non-repudiation, guarantee of delivery and encryption.</p> <p>Toolbox's also supports an optional feature supporting exchange of large files using the claim-based message transfer pattern.</p> |

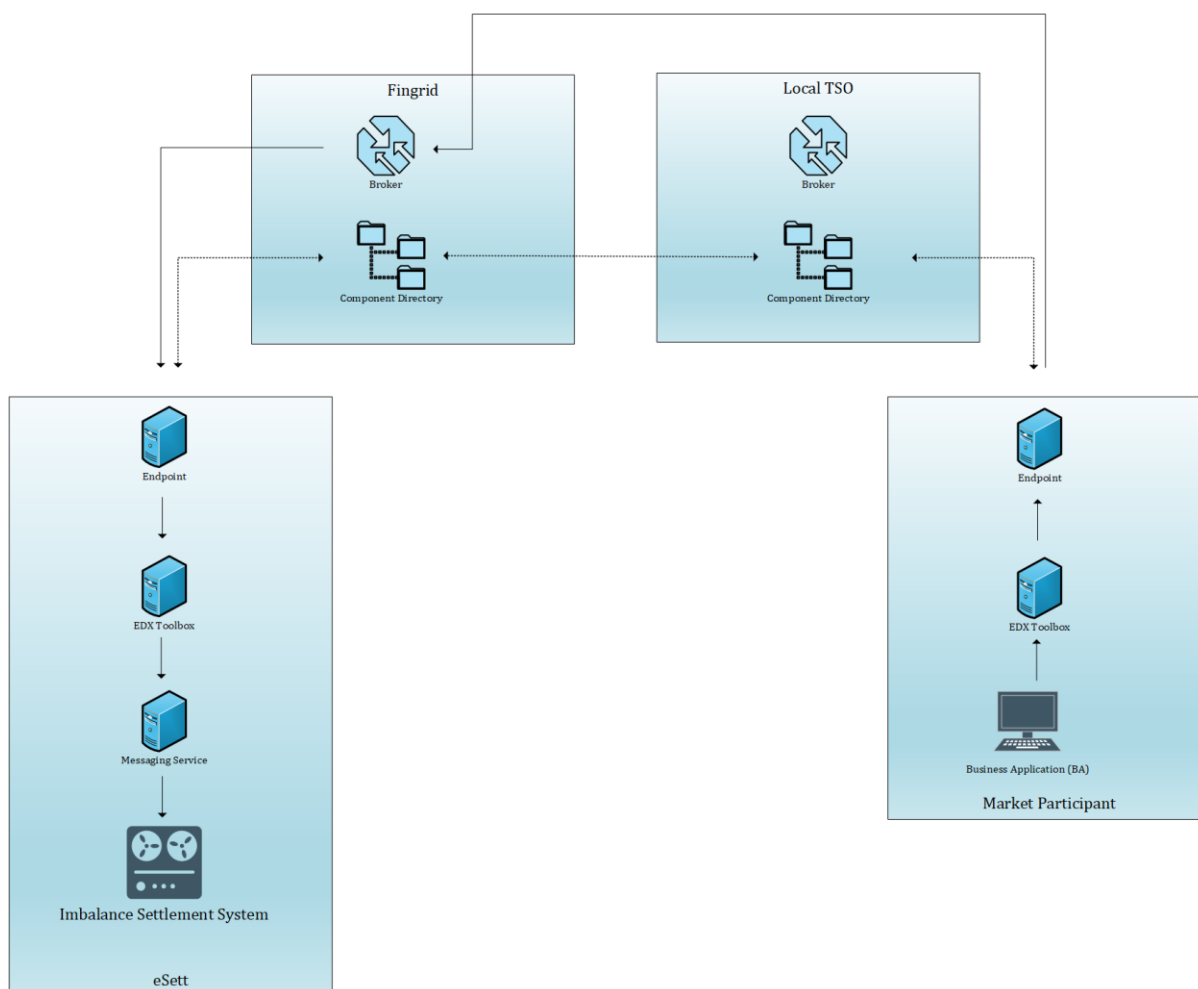
8 Table: EDX components

Installation requirements and installation media for the latest ECP version can be found via [ENTSO-E](#). On top of this, also an EDX Toolbox is required. Installation media can be obtained via the local Transmission System Operator.

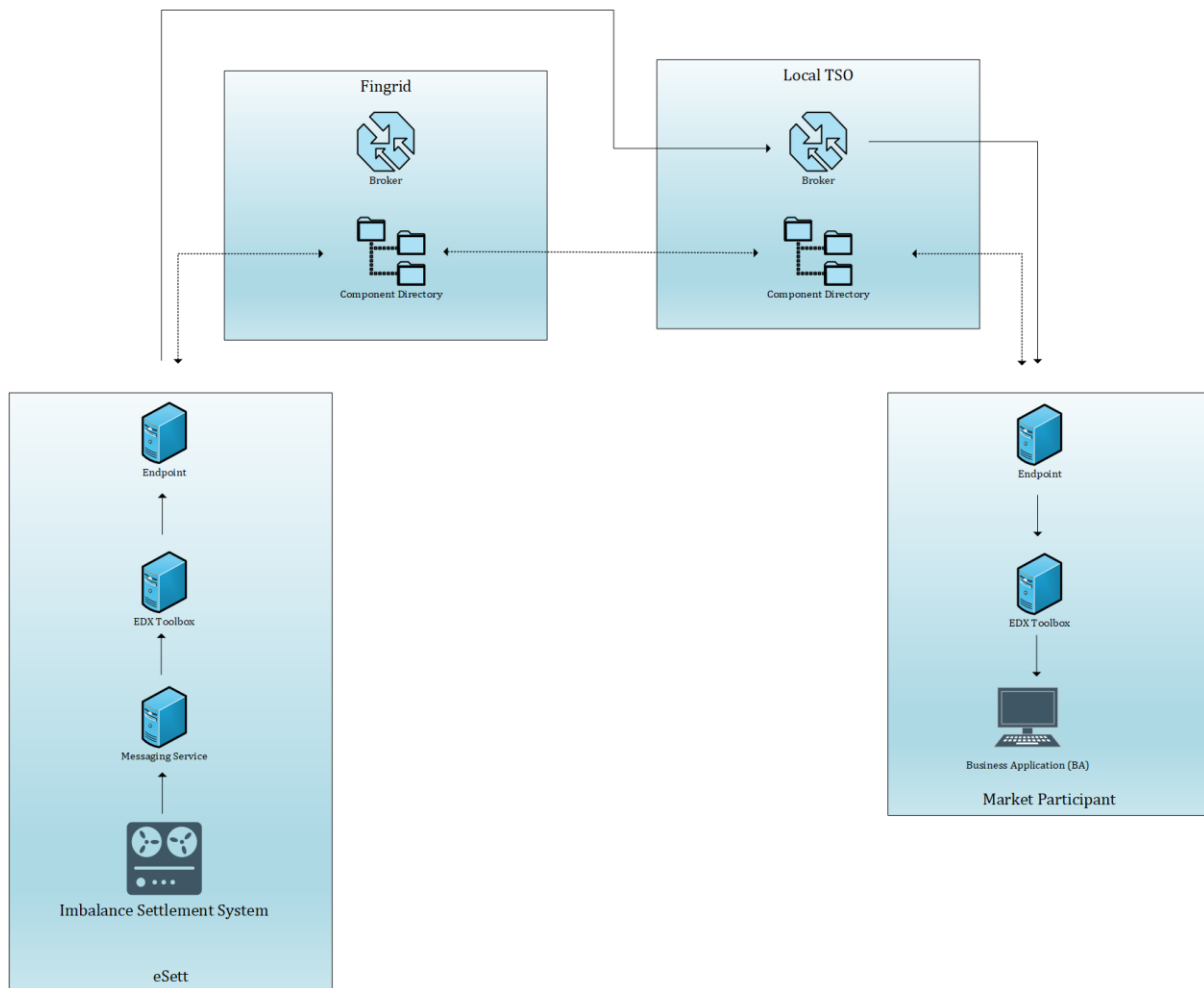
In order for a Market Participant to join Nordic ECP Network, the Market Participant's Endpoint must be registered to the local TSO's Component Directory following the process, which the local TSO has in place.

This enables the Market Party to send and receive messages towards and from eSett.

While submitting a message towards eSett via ECP/EDX, the message is routed via Fingrid's Broker. And while eSett is submitting a message towards Market Participant the message is routed via the local TSO's broker.



9 Message path while sending a message towards eSett via ECP/EDX



10 Message path while eSett is sending toward Market Participant

## 4. Setting up the connectivity for the first time

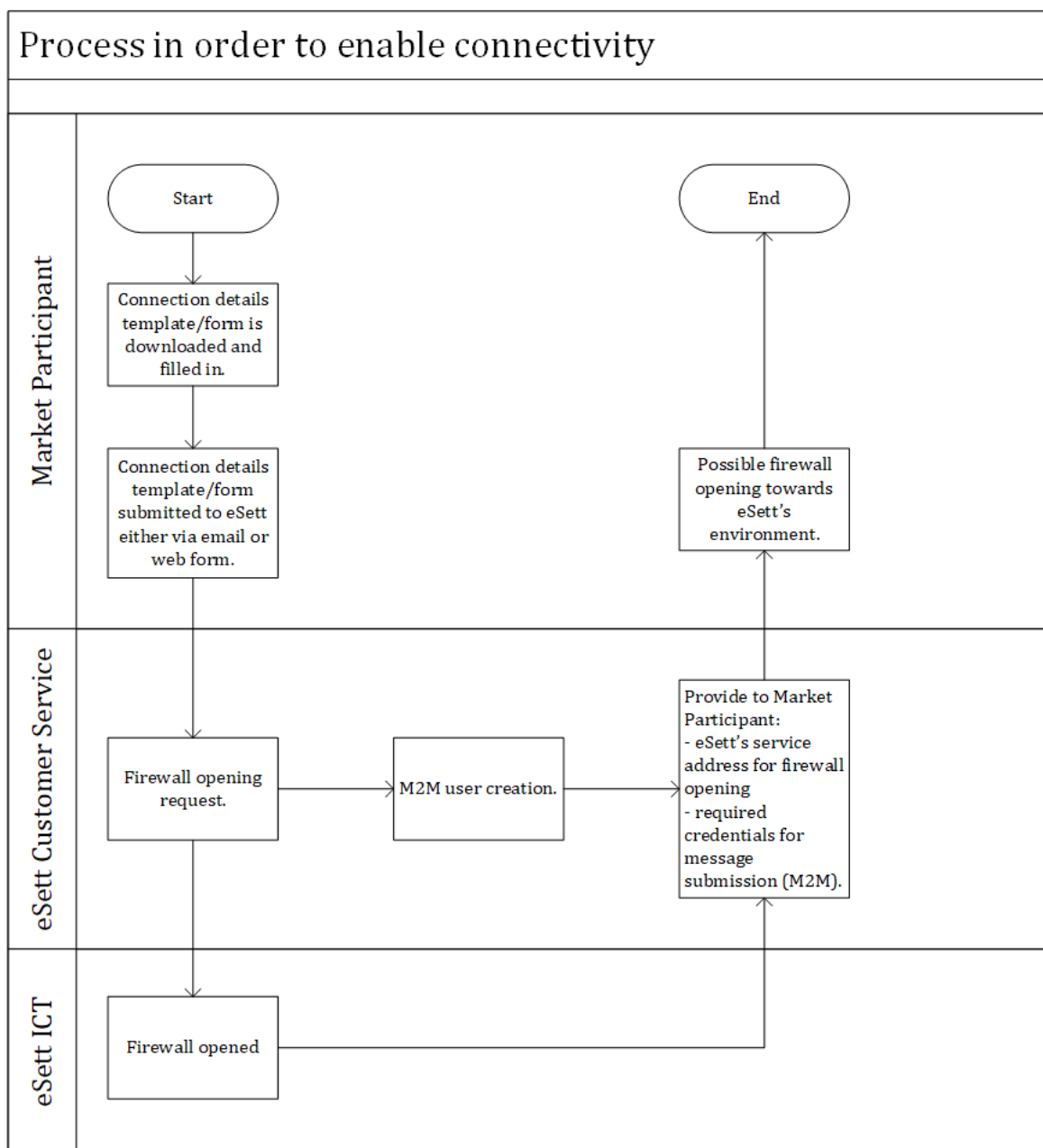
When the Market Participant is setting the connectivity towards and from eSett for the first time, there are preconditions and process to follow, which both are described in this chapter.

### 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](mailto:settlement@esett.com)) or preferably via [web form](#).

## 4.2. Process description



11 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 it is needed 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 |

#### 12 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 |                                |   |               |  |                             |                     |                |  |  |  |  |
| Preferred 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 |               |  |                             |                     |                |  |  |  |  |
|  |                                |   |               |  |                             |                     |                |  |  |  |  |

#### 13 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 |                                      |  |  |                               |   |                     |   |
| Preferred 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   |  |                               |   |                     |   |

#### 14 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 in to 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 need to make sure this address is static.
  - The protocol eSett should use to deliver SFTP messages to the Market Party – Choose the protocol that eSett is supposed to use in order to deliver the results. S



- 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 leaved 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 |   |   |                      |      |                             |                     |                |
| Preferred Delivery Channel                             | You Web Service URL (to receive Settlement Results) | Web Service username (to authorize eSett's result delivery) | Web Service password |      |                             |                     |                |
| WebService   |   |   |                      |      |                             |                     |                |

#### 15 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
  - Web Service URL – Address where eSett will submit results to Market Participant.
  - Web Service username – Credentials that eSett uses in order 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

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.

| 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 |               |
|--|---------------|
| Preferred Delivery Channel                             | Endpoint Code |
| ECP/EDX  |               |

#### 16 ECP/EDX channel details

## 5. Supported messages

Following table lists the NBS messages sent by Market Participants and supported by eSett.

Please refer to the Business Requirement Specification documents maintained by the Nordic Market Expert Group (NMEG) for more details.

XSD for all data flow types (along with message examples and format description) can be found at <https://ediel.org>.

For messages sent by eSett to the Market Participants, please refer to [Data Packages presentation](#) and to [Data Package XML User Guide](#).

| Message code | Data flow             | Process                 | From | Format  |
|--------------|-----------------------|-------------------------|------|---|
| PRPI         | Production Plan       | Scheduling              | TSO  | ENTSO-E ERRP Planned Resource Schedule Document   |
| ACRI         | Activated reserve     | Scheduling              | TSO  | Ediel ERRP Reserve Allocation Result Document   |
| CREI         | Capacity Reserves     | Scheduling              | TSO  | Ediel ERRP Reserve Allocation Result Document   |
| REPI         | Regulation Prices     | Scheduling              | TSO  | Ediel ECAN Publication Document   |
| RPMI         | Production            | Metering and settlement | DSO  | NEG (ebIX® based) Validated Data for Settlement for Aggregator (E66, E44)                     |
| MEPI         | Aggregated Production | Metering and settlement | DSO  | NEG (ebIX® based) Aggregated Data per MGA (E31, E44) - production                             |
| 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) |
| PRUI         | Production Unit       | Scheduling              | DSO  | Ediel (NEG) Resource Object (Production Unit) Master Data Document                            |
| CONI         | Consumption MEC       | Scheduling              | DSO  | NEG Party Master Data Document  |

|      |                     |            |                   |  |
|------|---------------------|------------|-------------------|--|
| MGRI | MGA RE Imbalance    | Scheduling | DSO               | NEG Party Master Data Document         |
| BITI | Bilateral Trade     | Scheduling | BRP, NEMO         | ENTSO-E ESS Schedule Document          |
| BTRI | Bilateral Trade MEC | Scheduling | BRP               | Ediel Request Trade Structure Document |
| PXTI | PX Market Trade     | Scheduling | NEMO              | ENTSO-E ESS Schedule Document          |
| PXFI | PX Market Flow      | Scheduling | NEMO              | ENTSO-E ESS Schedule Document          |
| PXMI | PX Market Trade MEC | Scheduling | NEMO              | Ediel Request Trade Structure Document |
| SPCI | Spot Price          | Scheduling | Selecting Service | ENTSO-E Publication document           |

17 Table: supported messages to be sent to eSett

Please note, that examples of each listed message can be found at <https://www.esett.com/materials/communication-guidelines> and from “Dataflows” section.

## 5.1. Message creation basics

Please note that each message consists of the same basic structure, regardless of the format.

Each message comes with following main parts:

- Document ID number (to ensure that the same document will not be sent multiple times)
- Document type identification (to ensure that document purpose is correctly identified)
- Document sender (sender of the document and it's role)
- Document receiver (receiver of the document, most commonly Nordic Balance Settlement)
- Identification of structure that will receive hourly values (For instance of Consumption point)
- Hourly values.

The information about the usage of each message can be found on <https://ediel.org/> and from the particular BRS document in question.

The correct identification of Sender and Receiver of the Message is necessary to properly route the Message and deliver it to correct recipient.

In the Nordic 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 three format families used in Imbalance Settlement System:

- ENTSO-e

- ebiX
- CIM.

Each of these formats utilize codes and coding schemes in order to identify Sender/Receiver.

Identification is done using Code (assigned to each Market Participant) and Coding Scheme (preselected by Market Participant).

More on Coding Schemes and their usage is available in [NBS Handbook](#).

In ENTSO-E messages Role is also part of the identification process, it defines whether identified subject acts as BRP, TSO, DSO or Balance Settlement responsible. In ebiX messages, the role is automatically recognized based on the message type itself.

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”.

## 6. Acknowledgements

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

The purpose is to inform the Market Participant about the result of message processing, whether it's positive or not, in which case the reason of processing failure is stated.

Details on how the Acknowledgement is structured and how to recognize contained information about processing results are published in the [Business Requirement Specification](#).

## 7. Certificates

### 7.1. General

Certificates in Messaging Service are used to secure the machine-to-machine communication between the Imbalance Settlement System and the Market Participants.

All of these are only used as serverside domain certificates, i.e. they are installed on a server in order to secure its identity (e.g. preventing man -in-the-middle attack) and to encrypt the communication between the 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 does not 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. Webservices

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 should not 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).

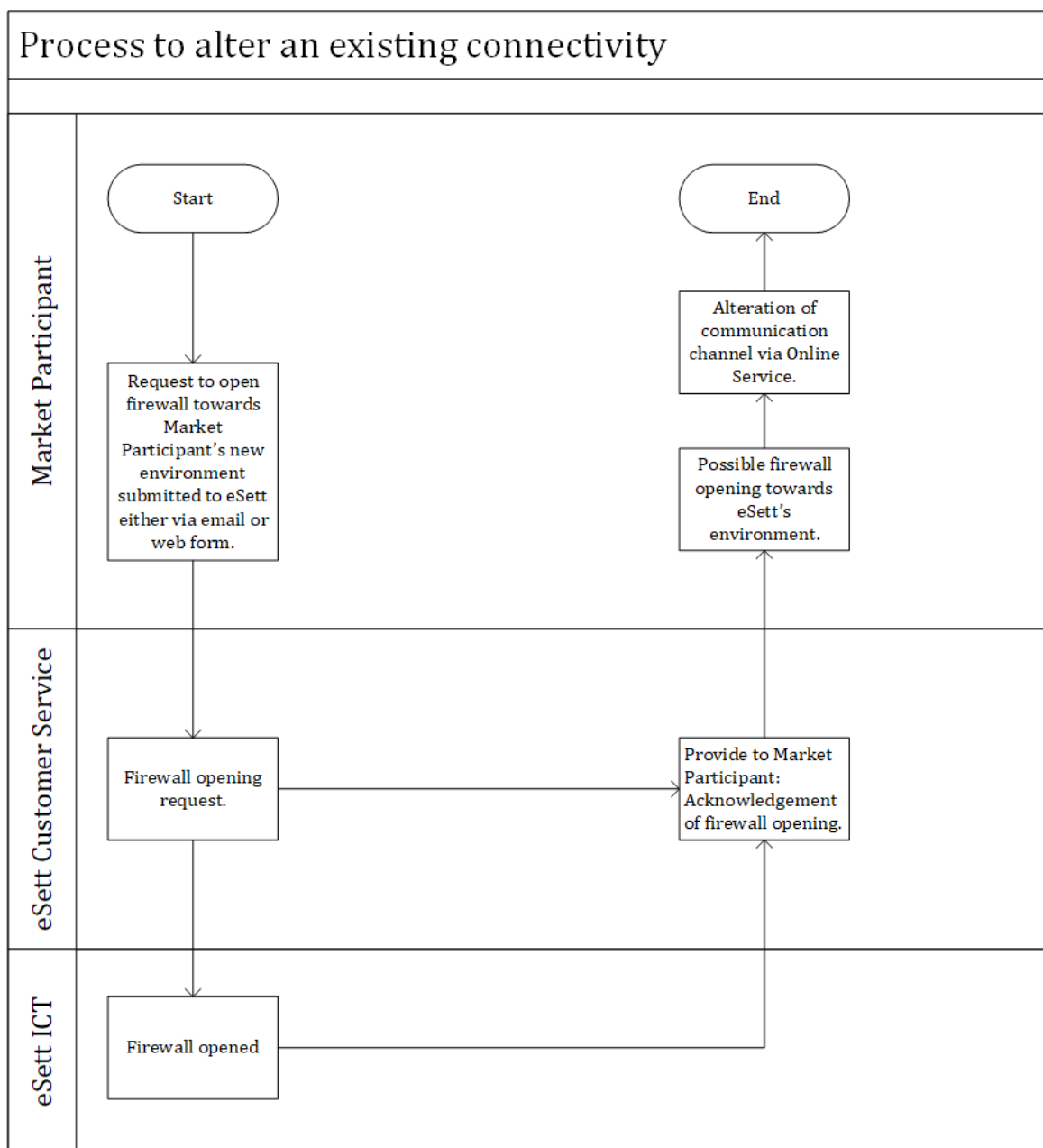
## 8. Altering an existing communication method

This chapter describes how configuration of communication with Messaging Service can be adjusted using user interface of [Online Service](#).

### 8.1. 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.

## 8.2. Process description



18 Process description in order to alter existing connectivity between the Market Participant and eSett

## 8.3. Configuration overview

Channel of Electronic Communication can be altered via Online Service:

ADMINISTRATION > Market Party Details > Channel of Electronic Communication



## Edit Channel of Communication ✕

**Preferred Channel \***

FTP
Email
WS
ECP/EDX

**Incoming Email Address ? \***

john.smith@company.eu

Required field

**Outgoing Email Address ? \***

john.smith@company.eu

Required field

Change in communication settings may take up to one hour to be processed.

Save

Cancel

### 19 Example of altering the configuration

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

| Column name           | Description   |
|-----------------------|---|
| Preferred Channel     | Preferred channel of electronic communication.<br>Options are: <ol style="list-style-type: none"> <li>1. FTP</li> <li>2. Email</li> <li>3. WS</li> <li>4. ECP/EDX</li> </ol>  |
| Incoming FTP Password | Password used to connect to SFTP server,<br>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 SFTP server, where outgoing messages and acknowledgements from NBS System will be delivered.   |
| Outgoing FTP Port      | Port used for connection to Market Participant's SFTP server.  |
| Outgoing FTP Protocol  | Protocol used for connection to Market Participant's FTP server, allowed choice is "sftp".   |
| Outgoing FTP Folder    | Name of the folder, which should be used on Market Participant's SFTP server for exchange of data between MP and eSett.  |
| Outgoing FTP Username  | Username used for login via SFTP to a server.  |
| Outgoing FTP Password  | Password used to connect to Market Participant's SFTP server.  |
| Incoming Email Address | Email address from which Market Participant is sending messages towards eSett.   |
| Outgoing Email Address | Email address of a recipient used for electronic communication used by NBS 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 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 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.                      |

20 Table: description of details in "Edit Channel of Communication" form.