GUIDE TO AEMO’S E-HUB APIS

THIS GUIDE PROVIDES DETAILS ABOUT USING AEMO’S E-HUB AS AN INTERFACE TO COMMUNICATE INFORMATION WITH AEMO. IT ASSISTS WHOLESALE ELECTRICITY AND GAS PARTICIPANTS DEVELOPING THEIR OWN APIS.

Version: 1.02
Published: 2 August 2018
IMPORTANT NOTICE

Purpose
The Australian Energy Market Operator (AEMO) has prepared this Guide to AEMO’s e-Hub APIs to provide information about e-Hub APIs. It provides participants with the API technical specifications to assist with the development of their own systems.

Privacy and legal notices
The material in this publication may be used in accordance with the privacy and legal notices on AEMO’s website.

Trademark Notices
Copyright (c) 2002 JSON.org
Oracle and/or its affiliates: Copyright © 1995, 2018. All rights reserved.
postmanlabs/postman is licensed under the Apache License 2.0
YAML: Copyright © 2001-2009 Oren Ben-Kiki, Clark Evans, Ingy döt Net

Distribution
Available to the public.

Document Identification
Application owner: IT Platforms
Document owner: Technology
Prepared by: Technology, Technical Writers
Last update: Thursday, 2 August 2018 11:22 AM

Documents made obsolete
The release of this document changes only the version of Guide to AEMO’s e-Hub APIs.

Further Information
For further information, please visit AEMO’s website www.aemo.com.au or contact:
AEMO Information and Support Hub  Phone: 1300 AEMO 00 (1300 236 600) and follow the prompts.
Email: supporthub@aemo.com.au

Feedback
Your feedback is important and helps us improve our services and products. To suggest improvements, please contact AEMO’s Information and Support Hub.

Version Release History
1.01 Initial creation
1.02 Changed HTTP Request – Header attributes
CONTENTS

1 Introduction ........................................................................................................................................... 5
   1.1 Purpose ............................................................................................................................................. 5
   1.2 Audience ......................................................................................................................................... 5
   1.3 How to use this guide ......................................................................................................................... 5
   1.4 What's in this guide ........................................................................................................................... 5

2 About AEMO’s e-Hub ............................................................................................................................. 7
   2.1 Architecture ...................................................................................................................................... 8
   2.2 API Standard ..................................................................................................................................... 9
   2.3 Design principles ............................................................................................................................... 9
   2.4 URL format ...................................................................................................................................... 9
   2.5 HTTP request .................................................................................................................................... 10
   2.6 HTTP response ................................................................................................................................. 11
   2.7 Traffic Management ......................................................................................................................... 14
   2.8 Connection and read timeout settings ............................................................................................. 14
   2.9 Security .......................................................................................................................................... 14
   2.10 System requirements ...................................................................................................................... 15
   2.11 Swagger files .................................................................................................................................. 16
   2.12 Participant e-Hub Gateway ............................................................................................................ 17

3 Using the API Portal ............................................................................................................................. 18
   3.1 Steps to use APIs ............................................................................................................................. 18
   3.2 Register .......................................................................................................................................... 18
   3.3 Access the e-Hub ............................................................................................................................. 18
   3.4 View the API gallery ....................................................................................................................... 19
   3.5 Obtain a Swagger file ....................................................................................................................... 23

4 Manage Certificates ............................................................................................................................ 25
   4.1 Decide how to use certificates .......................................................................................................... 25
   4.2 Obtain a new certificate .................................................................................................................... 25
   4.3 Use an existing certificate ................................................................................................................ 28
   4.4 Send the certificate to AEMO .......................................................................................................... 28
   4.5 AEMO validates, generates, and issues the certificate .................................................................... 29
   4.6 AEMO and participants install the digital certificate ....................................................................... 29

5 Needing Help ......................................................................................................................................... 30
   5.1 FAQs ................................................................................................................................................. 30
   5.2 Related resources ............................................................................................................................. 30
   5.3 Glossary .......................................................................................................................................... 31
1 INTRODUCTION

1.1 Purpose

This guide provides details about using AEMO’s e-Hub as an interface to communicate information with AEMO. It assists Wholesale electricity and gas participants developing their own APIs.


1.2 Audience

The primary audience is participants’ technical staff responsible for developing APIs. The secondary audience is anyone who has an interest in understanding how AEMO’s APIs work.

1.3 How to use this guide

- This document is written in plain language for easy reading. Where there is a discrepancy between the Rules and information or a term in this document, the Rules take precedence.
- The references listed throughout this document are primary resources and take precedence over this document.
- Text in this format indicates a resource on AEMO’s website.
- Glossary terms are capitalised and have the meanings listed against them in the Glossary section.
- Italicised terms are defined in the Rules. Any rules terms not in this format still have the same meaning.
- This guide assumes you have knowledge of the RESTful programming architecture.
- Actions to complete in the API Web Portal interface are bold and dark grey.

1.4 What’s in this guide

About AEMO’s e-Hub provides an overview of the e-Hub environment, basic requirements, security, and system requirements. It also explains the HTTP request methods and responses, what goes in the header, and provides POST and GET examples.

Using the API Portal provides the steps to access the e-Hub, including URLs. How to register and view the APIs.

Manage Certificates provides guidance about managing certificates and how to set them up.

Needing Help on page 30 provides some FAQs, related resources, and a glossary.
For technical details about individual API specifications, see the generated Swagger files in the API Web Portal. For help, see View the API gallery on page 19.
2 ABOUT AEMO’S E-HUB

The e-Hub is AEMO’s communication platform supporting exchange of information between participants and AEMO. The e-Hub is accessible over MarketNet or the internet and includes:

1. An **API Web Portal** for supporting messaging using web services, see Figure 1 below.
2. An **API Gateway**, see Figure 2 on page 8.

Figure 1 AEMO’s e-Hub and Participant API Gateway
2.1 Architecture

AEMO chose RESTful (REST) for its web services architecture because of its lightweight nature and ability to transmit data using HTTPS and JSON. REST is an alternative to SOAP and WSDL and is cheaper, simpler, and faster. The REST architecture makes it possible to start small; developing what is required with available resources, scaling up as the number of services increase.

AEMO’s goal with this approach is:

1. Performance: quality of responsiveness.
2. Scalability: many users can simultaneously use the systems.
4. Simplicity: no complex interactions, easy to prove the system is doing as it should.
5. Modifiability: extensible in the face of new requirements and technologies.

2.2 API Standard

The standard AEMO uses for APIs is the OpenAPI Specification (OAS). For more details, see OpenAPI-Specification: https://github.com/OAI/OpenAPI-Specification.

2.3 Design principles

The REST approach uses the features of HTTP to make requests using these design principles:

1. HTTPS protocol provides services over MarketNet or the internet.
2. Resources are mapped to a location within a hierarchy of URIs, for example: service host/<system>/<business_function>.
   a. The root of the hierarchy represents the web service or API application and provides the resources available.
   b. The next level provides specific information about the resource,
   c. The final level provides data from the specific resource records. For more details, see URL format below.
3. Accommodates a variety of payloads such as XML, JSON, or a custom schema.

2.4 URL format

API URLs are in the following format:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;protocol&gt;</td>
<td>HTTPS</td>
</tr>
<tr>
<td>&lt;web service host&gt;</td>
<td>Name of the server hosting the service or an external proxy.</td>
</tr>
<tr>
<td>&lt;Business_function&gt;</td>
<td>API Name - The AEMO system providing the services, e.g. GeneratorRecall</td>
</tr>
<tr>
<td>&lt;Resource&gt;</td>
<td>Entities of the business function e.g. /listRecallPlans</td>
</tr>
<tr>
<td>?querystring parameters</td>
<td>Case-sensitive query string parameters for the GET method.</td>
</tr>
</tbody>
</table>
2.4.1 Format example

https://<web service host>/<business_function>/<APIversion>/<resource>?querystring parameters

2.4.2 Internet URL example

https://apis.prod.aemo.com.au:9319/ws/GeneratorRecall/1.0/listRecallPlans

2.4.3 MarketNet URL example

https://apis.prod.marketnet.net.au:9319/ws/GeneratorRecall/1.0/listRecallPlans

2.5 HTTP request

While APIs are defined in either YAML or JSON format, the API request body and other content are not required to be JSON or YAML.

2.5.1 Header

Table 1 Header attributes

<table>
<thead>
<tr>
<th>Header parameter</th>
<th>Description</th>
<th>Allowed values / Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-type</td>
<td>HTTPS request format.</td>
<td>Content-type: application/json</td>
</tr>
<tr>
<td>Accept</td>
<td>HTTPS response format.</td>
<td>Accept: application/json</td>
</tr>
<tr>
<td>Content-length</td>
<td>Content length of file. The value is populated when the request is sent.</td>
<td>Content-length: nnn</td>
</tr>
<tr>
<td>X-initiatingParticipantID</td>
<td>The participant ID</td>
<td>X-initiatingParticipantID: 123456</td>
</tr>
<tr>
<td>X-market</td>
<td>The market type that the request applies.</td>
<td>X-market: GAS</td>
</tr>
<tr>
<td>Authorisation</td>
<td>Specifies basic HTTP authentication containing the Base64[1] encoded username and password. The participant’s URM username and password are concatenated with a colon separator and then Base64 encoded.</td>
<td>Authorisation: Basic QFhQVC0wMDA0Mzoy2ZWRmOGJhYS0wY2I0LTQwZjctOTIyM50yODUxNmM4N2MxNjQ= (For URM username “@XPT-00003” and password “2edf8baa-0cb4-40f7-9221-28516c87c164”)</td>
</tr>
</tbody>
</table>
2.5.2 Methods

<table>
<thead>
<tr>
<th>HTTPS method</th>
<th>Operation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>Retrieve Data</td>
<td>The GET method has the query string parameters in the URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The GET method does not have the Content-Type passed in the HTTP request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not all AEMO’s APIs use the GET method.</td>
</tr>
<tr>
<td>POST</td>
<td>Post Data</td>
<td>The POST method has:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- No query string parameters in the URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- BASIC Authentication details, username and password encoded and passed in the request header.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HTTP request header parameters specific to the API (if any).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ParticipantId&quot;:&quot;PID&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;StartDate&quot;:&quot;2017-11-01T00:00:00+10:00&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;EndDate&quot;:&quot;2017-11-02T00:00:00+10:00&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;StationId&quot;:&quot;PID6&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;DUID&quot;:&quot;AEMO1&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;OutagePlanId&quot;:&quot;MMS_GEN_OUT1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td>DELETE</td>
<td>Delete Data</td>
<td>The DELETE method has the query string parameters in the URL.</td>
</tr>
</tbody>
</table>

2.6 HTTP response

While APIs are defined in either YAML or JSON format, the API response body and other content are not required to be JSON or YAML.

The HTTP Response has:
- A response code and description, with
  - A successful request indicated by 200 OK.
  - Other response codes for technical and Payload validation failures. For details, see CodesError! Reference source not found. Error! Bookmark not defined.
- Optional Payload.
2.6.1 Codes

The e-Hub sends an appropriate HTTP response code and response Payload when any of the technical validations fail.

<table>
<thead>
<tr>
<th>Code</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Indicates a successful request.</td>
<td>OK (2.6.2 below).</td>
</tr>
</tbody>
</table>
| 400  | Invalid API URI | The service cannot be found for the endpoint reference (EPR) <URI>
"Fault": "<SystemMessageExceptionDump>" |
| 401  | Invalid credentials | Unauthorized |
No BASICAuth information in HTTP Request Header
"Exception": "Unauthorized:Invalid UserName or Password"
"Exception": "Unauthorized:Invalid UserName or Password"
| 404  | Resource not Found | "Exception": "Resources for the endpoint URI not found. Endpoint URI: <Resource>" |
| 405  | Invalid Method used (e.g. GET used instead of POST) | "Exception": "Input request HTTP method is <Invalid Method passed> but operation <Resource Name> accepts only: [<Valid Method>]" (see 2.6.3 below) |
| 422  | Business validation failure | Unprocessable entity |
| 500  | e-Hub is operational but downstream systems are not available or malformed payload (JSON) | "Exception": "Application Unavailable" |
| 503  | Exceeds Throttling Limits | Service invocation for API was rejected based on policy violation |

Some APIs may have specific response codes, for details check the individual Swagger file.

2.6.2 Response example - 200 OK with response Payload

HTTP/1.1 200 OK
Content-Type: application/json
2.6.3 Response example - HTTP response code 405

HTTP/1.1 405 Method Not Allowed
Content-Length: nnn
Date: Mon, 01 May 2017 18:00:00 GMT
Connection: close

{
  "Exception": "Input request HTTP method is GET but operation /listRecallPlans accepts only: [POST]"
}
2.7 Traffic Management

To protect the backend service from overload, the e-Hub enforces traffic limits. For details about the traffic limits for each individual API, see the individual API policy. For help, see View the API gallery on page 19.

2.8 Connection and read timeout settings

We recommend participants use the following settings when calling AEMO’s APIs.

<table>
<thead>
<tr>
<th>Type</th>
<th>Problem</th>
<th>Recommended settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection timeout</td>
<td>Cannot connect to the e-Hub’s endpoint (e.g. e-Hub infrastructure is not available).</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Read timeout</td>
<td>Connected to the endpoint but the e-Hub does not respond within the configured time.</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>

2.9 Security

2.9.1 Custom Ports

The API Gateway uses custom ports as a defence against Denial of Service (DoS) attacks. For HTTPS the port is 9319.

2.9.2 SSL certificates

The e-Hub uses SSL certificates to secure encrypted communication and secure interactions between participants’ and AEMO’s systems. All communications between the e-Hub and participants’ gateways use HTTPS. The e-Hub does not support HTTP.

Access to production and pre-production APIs require different SSL certificates.

Participants must obtain a Certificate Signing Request (CSR) to manage their TLS/SSL encryption. Usually, a Private Key and a CSR are created at the same time, making a Key Pair.

The CSR is generated in the API Portal and contains information included in the certificate, such as the company name, common name, locality, and country. It also contains the Public Key included in the certificate.

SSL connectivity for the e-Hub complies with the TLS v1.1 and v1.2 protocols.
2.9.3 Authentication and authorisation

When calling APIs, participants authenticate their identity using Basic Authentication — passing a username and password.

The username and password is provided by your company’s participant administrator (PA) and is encoded into a Base64 authorisation token. To do this you need an application such as Postman (for help, see https://www.getpostman.com/).

The HTTP Basic authentication header takes the following format:

Authorization: Basic {Base64 hash of user:password}, for example:

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

2.10 System requirements

2.10.1 API Portal

To connect to the API Portal, participants’ need:
- Access to MarketNet or the internet. For details about MarketNet, see Guide to Information Systems. If you are an existing participants your company probably already has access to MarketNet.
- API Portal registration, see Register on page 18.
- A valid SSL certificate, see Manage Certificates on page 25.
- A user ID and password with access rights for the API provided by your company’s Participant Administrator (PA). For help, see User rights access below.

2.10.2 API Gateway

To connect to the API Gateway, participants’ need:
- Their IP address range white listed by AEMO.
- SSL authentication using digital certificates.

2.10.3 User rights access

For access to APIs, participant administrators select the relevant entity in the MSATS “Maintain Rights” menu and assign the right to their participant users. For help, see Guide to User Rights Management.

For example, the entity required for the Generator Recall APIs is:
- EMMS - Offers and Submissions - Generator Recall
This is the username and password that goes in the authorisation header. For help, see Authentication and authorisation on page 15.

2.11 Swagger files

2.11.1 What are they?

Swagger files are one of the tools of the OpenAPI Specification (OAS). It is the specification of the API detailing its resources and operations in a human and machine readable format for easy development, discovery, and integration. AEMO uses Swagger files in its API Portal.

![Swagger file example](image)

For more details and examples, see OpenAPI Specification: https://swagger.io/specification/

2.11.2 How to use

You can use the Swagger tools to view, inspect, and test the Swagger file before integrating it into your systems.

To download an AEMO API, see Obtain a Swagger file on page 23.
2.12 Participant e-Hub Gateway

Participants can implement their own API Gateway to interact with AEMO’s API Gateway.

To set up your own gateway define your URL and API names. The e-Hub uses the resources and methods to push the messages to your gateway.
3 USING THE API PORTAL

3.1 Steps to use APIs

Follow these steps to begin using AEMO’s APIs:

1. Register
2. Access the API Portal
3. View the API gallery
4. Decide how to use certificates
5. Send the certificate to AEMO
6. AEMO validates, generates, and issues the certificate
7. AEMO and participants install the digital certificate
8. If required, set up your Participant e-Hub Gateway (see page 17).

3.2 Register

To register:

1. Send an email to AEMO’s Support Hub: suporthub@aemo.com.au.

2. Once your registration is complete, the Support Hub emails your access credentials so you can login, view, and download the API Swagger files. See Obtain a new certificate on page 25.

3.3 Access the e-Hub

3.3.1 Access the API Portal

1. Access the API Portal using one of the following URLs:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Pre-production</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>MarketNet</td>
<td><a href="https://apiportal.prod.marketnet.net.au">https://apiportal.prod.marketnet.net.au</a></td>
<td><a href="https://apiportal.prod.marketnet.net.au">https://apiportal.prod.marketnet.net.au</a></td>
</tr>
</tbody>
</table>

2. In the top-right corner, click Log in.
3.3.2 Access the API Gateway URLs

To access AEMO’s API Gateway, use the following URLs:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Pre-production</th>
<th>Production</th>
</tr>
</thead>
</table>

3.3.3 e-Hub to Participant Gateway IP addresses

You see the following source IP addresses when the e-Hub connects to your Participant API Gateways.

<table>
<thead>
<tr>
<th>Connection</th>
<th>Pre-production</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>MarketNet</td>
<td>146.178.211.91</td>
<td>146.178.211.92</td>
</tr>
<tr>
<td>Internet</td>
<td>202.44.76.204</td>
<td>202.44.76.204</td>
</tr>
</tbody>
</table>
<pre><code>          | 202.44.78.204  | 202.44.78.204 |
</code></pre>

3.4 View the API gallery

The API gallery provides access to AEMO’s APIs that you have access to. To view the API Gallery:

1. Access the API Portal. For help, see page 18.
2. At the top of the portal, click API Gallery.
3. Find the API, and click View details.
4. The following details about the API display.
3.4.1 API resources

Drill down to see details about the API’s resources with examples of request details and responses.

API resources

Below is a list of resources available in the API. Click each resource to view more details.

**POST** /submitRecallPlan

**POST** /listRecallPlans

**POST** /getRecallPlan

3.4.2 API documents

This is where you can download the Swagger file for the API. For details, see Swagger files on page 16.
API documents

Here you find the list of all documents for the API:

Generated Swagger file: GeneratorRecall.json

3.4.3 API policies

Under API policies you can find specific throttling and security details for the API.

API policies

Traffic Management

Classify the actions that are specific to Traffic Management message flow.

Throttling Traffic Optimization

The API enforces traffic limits to protect the backend service from becoming overloaded

**Soft Limit:** 3 invocations per 1 Minutes

**Hard Limit:** 5 invocations per 1 Minutes - further requests will be blocked

Security

Classify the actions that are specific to Security message flow.

Evaluate HTTP Basic Authentication

The API requires the usage of HTTP Basic authentication header to allow access.

The HTTP header takes them following format:

**Details:** Authorization: Basic {Base64 hash of user:password}

**Example:** Authorization: Basic QWxhZGRptpjpcGVuiHNIc2FlZQ==
3.4.4 Access API

A list of default, test, and development endpoints.

### Access API

**Uncategorized**

- **List of default end points**
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7320/ws/GeneratorRecall/1.0
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7320/ws/GeneratorRecall/1.0
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7319/ws/GeneratorRecall/1.0
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7321/ws/GeneratorRecall/1.0

**System Integration Test**

Testing endpoints can be used for all non-production usage. These endpoints have limited availability and higher response time SLAs.

**Development**

The development endpoints can be used while developing your applications. It may have restricted features and limited availability.

- **End point URL**: https://apiportal.prod.marketnet.net.au:7321/ws/GeneratorRecall/1.0
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7321/ws/GeneratorRecall/1.0
  - **End point URL**: https://apiportal.prod.marketnet.net.au:7321/ws/GeneratorRecall/1.0

3.5 Obtain a Swagger file

To obtain a Swagger file:

1. Access the API Portal on page 18.
2. Click API documents and click Generated Swagger file.
3. Save the Swagger file to your local computer.
About GeneratorRecall

API resources

API documents

Here you find the list of all documents for the API:

Generated Swagger file: GeneratorRecall.json
4 MANAGE CERTIFICATES

You require a different Certificate to connect to each environment — pre-production and production.

4.1 Decide how to use certificates

Before obtaining an SSL certificate, determine if you need a new certificate or you can use an existing one.

4.1.1 New e-HUB participants

If you are a new e-HUB participant, you can do one of the following:

1. Have one certificate for multiple participant IDs.

2. Have one certificate for each participant ID.

4.1.2 Existing e-HUB participants

If you are an existing e-Hub participant (already having a Certificate), you can do one of the following:

1. Request to use an existing certificate for multiple participant IDs.

2. Have one new certificate for multiple participant IDs.

3. Have one new certificate for each additional participant ID.

4.2 Obtain a new certificate

To obtain an SSL certificate, you must generate a Certificate Signing Request (CSR) that identifies your server. Instructions for generating the CSR depend on your server and operating system.

For help generating a CSR for your server/operating system, consult your vendor’s guide.
### 4.2.1 Information required for your CSR

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN (common name)</td>
<td>If required, call AEMO’s Support Hub who can provide your Organisation ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Single Participant ID</strong></td>
</tr>
<tr>
<td></td>
<td>`&lt;ORGANISATION ID&gt;_&lt;PreProd</td>
</tr>
<tr>
<td></td>
<td>30187_PreProd_Jun2017</td>
</tr>
<tr>
<td></td>
<td><strong>Multiple Participant IDs</strong></td>
</tr>
<tr>
<td></td>
<td>If you are using the same certificate for more than one organisation the format is:</td>
</tr>
<tr>
<td></td>
<td>`&lt;ORGANISATION ID1&gt;<em>&lt;ORGANISATION ID2&gt;</em>&lt;..._&lt;PreProd</td>
</tr>
<tr>
<td></td>
<td>30187_30188_PreProd_Jun2017</td>
</tr>
<tr>
<td></td>
<td>The length of the CN field is limited to 64 characters.</td>
</tr>
<tr>
<td>Challenge password</td>
<td><strong>Do not</strong> set the Challenge password.</td>
</tr>
<tr>
<td>OU</td>
<td>For the OU and remaining fields in the subject attribute, enter any description relating to your organisation.</td>
</tr>
<tr>
<td>Public key algorithm</td>
<td>You must use RSA encryption with a key length of 1024 bits or preferably 2048 bits</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>You must use RSA encryption with a SHA1 hash</td>
</tr>
</tbody>
</table>
The request will look similar to this example:

```
Certificate Request:

Version: 2 (0x2)
Subject: C=AU, ST=Test State, L=Test City, O=Test Organisation, OU=Test Organisational Unit, CN=*
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key (2048 bit):

-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAqAwzELMAkGA1UEBhMCVVMxDTALBgNVBAgMBFV0YWgxDzANBgNVBAYTAlVT

-----END CERTIFICATE REQUEST-----
```

The CSR file contains text that looks similar to the following example. The BEGIN and END lines must be present.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAqAwzELMAkGA1UEBhMCVVMxDTALBgNVBAgMBFV0YWgxDzANBgNVBAYTAlVT

-----END CERTIFICATE REQUEST-----
```
4.3 Use an existing certificate

To use an existing certificate, send an email to AEMO's Support Hub with the following information:

<table>
<thead>
<tr>
<th>To</th>
<th><a href="mailto:supporthub@aemo.com.au">supporthub@aemo.com.au</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Participant email</td>
</tr>
<tr>
<td>Subject</td>
<td>AEMO e-Hub SSL certificate update</td>
</tr>
<tr>
<td>Body</td>
<td>AEMO Support Hub</td>
</tr>
<tr>
<td></td>
<td>We have an existing SSL certificate with the following Thumbprint: &lt;Thumbprint&gt;.</td>
</tr>
<tr>
<td></td>
<td>Please update the participant IDs below to use this certificate:</td>
</tr>
<tr>
<td></td>
<td>- &lt;Participant ID 1&gt;</td>
</tr>
<tr>
<td></td>
<td>- &lt;Participant ID 2&gt;</td>
</tr>
<tr>
<td></td>
<td>- &lt;Participant ID 3&gt;</td>
</tr>
</tbody>
</table>

4.4 Send the certificate to AEMO

Email the CSR file to AEMO's Support Hub with the following information:

<table>
<thead>
<tr>
<th>To:</th>
<th><a href="mailto:supporthub@aemo.com.au">supporthub@aemo.com.au</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>From:</td>
<td>Participant email</td>
</tr>
<tr>
<td>Subject:</td>
<td>CSR request</td>
</tr>
<tr>
<td>Attachment</td>
<td>CSR file</td>
</tr>
<tr>
<td>Body:</td>
<td>AEMO Support Hub</td>
</tr>
<tr>
<td></td>
<td>Please find attached a Certificate Signing Request (CSR) for signing by the AEMO Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>The following Participant ID’s will use this certificate:</td>
</tr>
<tr>
<td></td>
<td>&lt;Participant ID 1&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Participant ID 2&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Participant ID 3&gt;</td>
</tr>
</tbody>
</table>
4.5 AEMO validates, generates, and issues the certificate

Once received, AEMO:

1. Validates your CSR.
2. Generates the SSL certificate from the CSR.
3. Emails the following SSL certificate details to all involved Participant IDs:
   a. Participants' public certificate
   b. e-Hub (production and pre-production) public certificate
   c. CA certificate

4.6 AEMO and participants install the digital certificate

4.6.1 AEMO API Gateway

AEMO applies the SSL certificate to the requested Participant IDs in the e-Hub API Gateway.

4.6.2 Participant API Gateway or system

Participants apply the SSL certificate to their own API Gateway or system.
5 NEEDING HELP

5.1 FAQs

<table>
<thead>
<tr>
<th>Question</th>
<th>Wholesale APIs</th>
<th>MSATS retail B2B APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I need an API Key to use AEMO’s APIs?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Do I have to gain accreditation from AEMO before I can use APIs?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Do I need a certificate for each API?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>You can have 1 certificate for many APIs.</td>
<td></td>
</tr>
<tr>
<td>Can I have 1 certificate for many Participant IDs?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>The choice is yours, see Decide how to use certificates on page 25.</td>
<td></td>
</tr>
<tr>
<td>Can I have 1 certificate for each Participant ID?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>The choice is yours, see Decide how to use certificates on page 25.</td>
<td></td>
</tr>
</tbody>
</table>

5.2 Related resources

API Portal: API resources and documents, including OAS (Swagger) files.


Connecting to AEMO’s IT Systems: Details and URLs for connecting to AEMO’s IT Systems.

Guide to Electricity Information Systems: Information about AEMO’s participant IT systems.

Guide to User Rights Management: Assisting participant administrators (PAs) to use the user rights management functions available in AEMO’s web portals.

## 5.3 Glossary

<table>
<thead>
<tr>
<th>Abbreviation/Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Gateway</td>
<td>The gateway on AEMO’s side providing participant communication options, accessible over the internet or MarketNet. It uses resources and methods to push messages to Participants’ API Gateways.</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface; a set of clearly defined methods of communication between various software components.</td>
</tr>
<tr>
<td>API Web Portal</td>
<td>Where you can view available APIs, view and manage your API Keys, obtain OAS files.</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request is a block of encoded text given to a Certificate Authority when applying for an SSL Certificate. It also contains the Public Key to include in the certificate. Usually, a Private Key is created at the same time, making a Key Pair.</td>
</tr>
<tr>
<td>e-Hub</td>
<td>Consists of the API Web Portal and the API Gateway for both electricity and gas.</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>Key Pair</td>
<td>SSL uses a technique called public-key cryptography, based on the concept of a Key Pair. The Key Pair consists of encrypted Public and Private Key data. It is only possible to decrypt the Public Key with the corresponding Private Key.</td>
</tr>
<tr>
<td>MarketNet</td>
<td>AEMO’s private data network connection.</td>
</tr>
<tr>
<td>MSATS</td>
<td>Retail Market Settlement and Transfer System</td>
</tr>
<tr>
<td>OAS</td>
<td>OpenAPI Specification</td>
</tr>
<tr>
<td>Participant API Gateway</td>
<td>The interface implemented by participants where AEMO’s API pushes messages.</td>
</tr>
<tr>
<td>Participant ID</td>
<td>Registered participant identifier</td>
</tr>
<tr>
<td>Payload</td>
<td>The data sent by a POST request. The Payload sections sits after the header.</td>
</tr>
<tr>
<td>PID</td>
<td>Participant ID</td>
</tr>
<tr>
<td>Private Key</td>
<td>The secret Private Key is a text file used initially to generate a Certificate Signing Request (CSR), and later to secure and verify connections.</td>
</tr>
</tbody>
</table>
### Abbreviation/Term | Explanation
--- | ---
Public Key | The Public Key is included as part of your SSL certificate, and works together with your Private Key to make sure your data is encrypted, verified, and not tampered with. Anyone with access to the Public Key (i.e. the certificate) can verify the digital signature is authentic without having to know the secret Private Key.

SOAP | Simple Object Access Protocol

SSL | Secure Sockets Layer, cryptographic protocol providing API communication security.

Swagger file | The OpenAPI Specification (OAS) definition of the API.

TLS | Transport Layer Security, cryptographic protocol providing API communication security.

WSDL | Web Services Description Language

XML | Extensible Markup Language
Guide to AEMO’s e-Hub APIs

6 INDEX

2

200, 12

4

400, 12
401, 12
404, 12
405, 12

5

500, 12
503, 12

A

API Gateway, 7
API Web Portal, 7
application/json, 10

B

Basic Authentication, 15
BasicAuth, 10

C

Certificate Signing Request (CSR), 25
Challenge password, 26
CN (common name), 26
Connection timeout, 14
Content-type, 10
CSR file, 27
Custom Ports, 14

D

DELETE, 11

G

GET, 11

H

HTTP, 14

HTTP response code, 12
HTTPS protocol, 9

I

Invalid credentials, 12
IP addresses, 19

K

Key Pair, 14

M

Market, 10

O

one certificate for each participant ID, 25
one certificate for multiple participant IDs, 25
one new certificate for each additional participant ID, 25
OU, 26

P

payloads, 9
PID, 10
POST, 11
Public key algorithm, 26

R

Read timeout, 14
register, 18
response Payload, 12
RESTful, 8

S

Signature algorithm, 26

U

URLs, 18, 19