

---

# CENTRAL INFORMATION PLATFORM - Web Service Integration Guide

- DOCUMENT VERSION 1 / RELEASE 16

---

23 June 2021

---

Copyright notice

**Copyright © ENTSO-E. All Rights Reserved.**

This document and its whole translations may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, except for literal and whole translation into languages other than English and under all circumstances, the copyright notice or references to ENTSO-E may not be removed.

This document and the information contained herein are provided on an "as is" basis.

**ENTSO-E DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN**

---

**WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF  
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

---

## REVISION HISTORY

Version	Release	Date	Paragraph	Comments
0	1	2014-04-22		First draft
15	1	2021-12-22		Included sections 2.1 and 2.2 steps to create self signed certificate
16	1	2022-07-27		Updated new URL's sec 2.2

---

## REFERENCED DOCUMENTS

- 1 Transparency Regulation 543/2013
- 2 Transparency Platform Manual of Procedures
- 3 ECP Integration Guide for transparency platform
- 4 Web Services Integration Guide for transparency platform

## DRAFTING TEAM MEMBERS

<b>Member</b>	<b>Company</b>	<b>Country</b>	<b>Working Group</b>
Andy Spiceley	ENTSO-E	-	-
TP Team	ENTSO-E		

Table of Contents:

1.	Overview .....	6
1.1	Usage of Web Services .....	6
2.	Web Service Channel Configuration .....	8
2.1	Steps to create self signed certificate using Keytool.....	8
2.2	Configuration of machine user.....	10
3	Data Service .....	12
3.1	Data Submission .....	12
3.2	List Messages.....	12
3.3	Get Messages .....	12
3.4	Data Retrieval .....	13
3.5	Digital Signatures.....	13
4	Guideline for Data Provider's submissions .....	13
4.1	Main Goals of the Guideline.....	13
4.2	Handling of Versions .....	13
4.2.1	Repeating Submission for All Previous Hours.....	14
Submission of XML Files with Lower/Same Version.....		14
4.2.2	Too Frequent Submissions .....	14
4.3	Data Granularity.....	14
4.3.1	Incorrect Submission Resolution.....	14
4.3.2	Too Detailed Data in Curves .....	15
4.4	Master Data Management.....	15
4.4.1	Too Frequent / Regular Updates.....	15
5	Web Service Client Troubleshooting.....	15
6	References.....	16

---

## 1. Overview

Web Services are one of the integration channels, which can be used for communication with ENTSO-E Transparency Platform.

Web service design and message format is based on the REE document *Electronic data interchanges on the Internal Electricity Market*<sup>1</sup> [SPEC], which is based on the *Part 100 of the IEC 61968 standard* [STAND]. Knowledge of these documents is necessary for successful application of this guide.

### 1.1 USAGE OF WEB SERVICES

Data Providers may use Web Services for following purposes:

1. Sending data to ENTSO-E Transparency Platform
2. Receiving Acknowledgement Documents from ENTSO-E Transparency Platform
3. Receiving Notification of missing data in form of Problem statement document
4. Listing and requesting submitted messages
5. Retrieving data (also for Public Users)

---

<sup>1</sup> Document *Electronic data interchanges on the Internal Electricity Market* is to be superseded by the *Technical Specification for the utilization of web services for electronic data interchanges on the European Energy Market for Electricity* when published. These two documents contains the same information.



## 2. Web Service Channel Configuration

### 2.1 STEPS TO CREATE SELF SIGNED CERTIFICATE USING KEYTOOL

**Generating self signed Certificate ( Caution: Keep note of password):**

`keytool -genkeypair -alias "Your key name" -keyalg RSA -keysize 2048 -storetype PKCS12 -keystore "Your certificate name" _Certificate.p12 -validity "No of days of validity"`

```
lpendyala@Laxmikanths-MacBook-Pro Downloads % keytool -genkeypair -alias Test -keyalg RSA -keysize 2048 -storetype PKCS12 -keystore Test_Certificate.p12 -validity 3650
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Laxmikanth Pendyala
What is the name of your organizational unit?
[Unknown]: ENTSOE
What is the name of your organization?
[Unknown]: ENTSOE
What is the name of your City or Locality?
[Unknown]: Bruxelles
What is the name of your State or Province?
[Unknown]: Brissees
What is the two-letter country code for this unit?
[Unknown]: BE
Is CN=Laxmikanth Pendyala, OU=ENTSOE, O=ENTSOE, L=Bruxelles, ST=Brissees, C=BE correct?
[no]: yes
```

```
-rw-r--r--  1 lpendyala  staff   2584 22 Dec 11:39 Test_Certificate.p12
```

**Importing to the Key store (Caution: Keep note of password):**

`keytool -importkeystore -srckeystore "Your certificate name" _Certificate.p12 -srcstoretype pkcs12 -destkeystore "Your certificate name" _Certificate.jks -deststoretype JKS`

```
lpendyala@Laxmikanths-MacBook-Pro Downloads % keytool -importkeystore -srckeystore Test_Certificate.p12 -srcstoretype pkcs12 -destkeystore Test_Certificate.jks -deststoretype JKS
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias test successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
lpendyala@Laxmikanths-MacBook-Pro Downloads %
```

```
-rw-r--r--  1 lpendyala  staff   2584 22 Dec 11:39 Test_Certificate.p12
-rw-r--r--  1 lpendyala  staff   2254 22 Dec 11:43 Test_Certificate.jks
```

**Listing the keying the Key store:**

`keytool -list -v -keystore "Your keystore name".jks`



```
lpendyala@Laxmikanths-MacBook-Pro Downloads % keytool -list -v -keystore Test_Certificate.jks
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: test
Creation date: 22-Dec-2021
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Laxmikanth Pendyala, OU=ENTSOE, O=ENTSOE, L=Brusseles, ST=Brissees, C=BE
Issuer: CN=Laxmikanth Pendyala, OU=ENTSOE, O=ENTSOE, L=Brusseles, ST=Brissees, C=BE
Serial number: 66bc96a6
Valid from: Wed Dec 22 11:39:58 CET 2021 until: Sat Dec 20 11:39:58 CET 2031
Certificate fingerprints:
MD5: 8E:73:2A:D8:7E:82:07:FB:87:C8:59:9C:96:68:B5:12
SHA1: 27:48:F5:67:FF:AA:2A:8F:32:23:C2:7D:03:E3:82:65:09:CD:16:B2
SHA256: 29:F6:81:38:7C:20:E6:5E:4E:28:E9:98:51:95:AB:58:73:23:7C:2F:19:FB:2E:0A:77:1F:3F:A2:1E:EE:A2
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0A C8 9B A8 8E 4D 7A BE C2 32 A2 DE E7 45 65 48 ....Mz..2...EeH
0010: B9 A2 D5 26 ....G
]
]

*****
*****
```

**Open SSL for generating generation public and private keys pair in PEM Format:**

openssl pkcs12 -in "Your certificate name"\_Certificate.p12 -out "Your certificate name"\_Certificate.pem

```
lpendyala@Laxmikanths-MacBook-Pro Downloads %
lpendyala@Laxmikanths-MacBook-Pro Downloads %
lpendyala@Laxmikanths-MacBook-Pro Downloads % openssl pkcs12 -in Test_Certificate.p12 -out Test_Certificate.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
-rw-r--r-- 1 lpendyala staff 3515 22 Dec 11:50 Test_Certificate.pem
```

```

Bag Attributes
  friendlyName: test
  localKeyId: 54 69 6D 65 20 31 36 34 30 31 36 39 35 39 38 35 30 31
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFBjBAGBqkqkiG9w0BBQwMzAbBgkqhkiG9w0BBQwDgQIgcw2LieQGYMCAgGA
MBQGCCqGSIb3DQMHBAgt0pv5Nr++HASCBMCEC0sutBLeHU/vR0e71V2cjXP3Yx0J
hnYJmPncGvYKhh6hqpA4I0D7wktREfV0p35i87j/NlIgle042sx0WCenb6Lq6jH
pDE64QDYh45x0K08AK9mtpfwXByIwHofdqHsAP87LMqv8SxR5A10DbfSn7H0eKz
Viyd4ZuHexH8GCR9u1+TSi80vyEs7E6mZZQglhwtsSS519tKT3KfVfQmZj/Mmrc
MSAQG2CafoJ0FbV251y2Z54++GzhvtCnhckEdSsAvmjY/rjaSX2pX0k/DActbUp
1vWNkjbQz92bjyTTw2iYNHsYRVZ86AV0s4U2af6Kgj6vKPIKjfskTIphrP4yqvm
iu2Us7bc+ovRbT5XPxPaPoicDKH3c+x8ha7MIK6AJyGLGGJJSWCsVp3jPYSpmY
05jusXzmYIQRwRYB/yLZH/gJbx0bVVMzgfGJgph+xkh9zocTwmizHk47GG2EBHdp
jJaKMBR44Mw85ama9RRdjE7Hvjv47pCd8p3YdIFRPrh/7+Ejrzx7dnVa16RmpRmCS
WArigrPM+dwc9fWNT7IIo+rwJM9EBHwRujPI9Cnf+eay7ynBHe7doWlkWkKhcNep
1ft00Ns6akl3BYsxcDzfA9Ufa3E8/ZrDqiCsdvPx3f0vo+wSK9XKRVo9xdhd0Ba
rur0Q50AFdAwBo/W57g+sZaenLwqA4XS3R2zzCJNq97edjMbJTvns5TAJLZ6E60
mqXlRwnnH0P17GzRV0RHmGTtnIGhBCRTIRTzLEr0zuwzKsCWIqhadi+Mt1UuLAm
3F0M/gtjDuEF1FUR6R//ouvhww19i7h1Ildky27GkuVr+0ma9MNGbwPumRBE1+u
L4y20EuF4MznqifwoUjMDMXcWpW8FymTg85cUz+x70v0Z16AqH9iVgtVXS9V1z
wJokeRuroH8BfbmziflvF2r9CHIldsSEo+brmq7dsIIqAZVrdEknoybtDQK+msL
H6E2Sfml6L8Sd3DgrHfWwonWtzrErCg61QFYtJETQ6eLfv9370YExu+KY/80S0
noRAmsv/n530xu8mtfdB0KU/eTFf24uwk8Fot3M+ioZPRGqi83BsGhdYumGkN0
bx6qBPfU56adeWvz3j7Ahp2Yyv/rGpge9VFb9y8D7RTx+0SGT4KLfpyjKVPbVdp
h7xA047Aw/kNgnimfEBx0EG5I0zJRAVfLty/S1P8+Qm0YCRdP+7ox5sRZzH/DXI d
v2yM6EEr1Nxu3MKXrCxjT6Mnt0cCSj9829S5Sg5l3JK3MwKATMe73bXcmCY3VfMFK
GCNK3L0SCYE5AE2IFHLNnSra7aodzjacezGydyk6nEYhKMENGEGXG99wCw4+0
S4RdF8RvGpWJHNLIXN+z5WQAuFD3+4cJKuuJ44NbvkD9fN/2lqooadB0V6tQUK
iWq0BqnLVtY4BK9L6qyA5xv9xgJ1m0ux9EDLAWWnPWK08LkctcQz08Uhm++F3
DyPGzWgG1csP1sdM7r3CB7nGFTFSr0lj7ZMmMHGx73Jp+WTcJMSPLnxzazkYCRj
j0AQQjg1ex7780UzyxkHqeoLZ73m0+Bd64L0sz0FFNoJlQ4jK+cxE5dw
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
  friendlyName: test
  localKeyId: 54 69 6D 65 20 31 36 34 30 31 36 39 35 39 38 35 30 31
  subject=/C=BE/ST=Brisses/L=Brusseles/O=ENTSOE/OU=ENTSOE/CN=Laxmikanth Pendyala
  issuer=/C=BE/ST=Brisses/L=Brusseles/O=ENTSOE/OU=ENTSOE/CN=Laxmikanth Pendyala
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIEZryWpJANBgkqhkiG9w0BAQsFADB0MQswCQYDVOQGEwJc
RTERMA8GA1UECBMIQnJpc3NlZXMxejAQBgNVBAcTCUJydXNzZwZlcZEPMA0GA1UE
ChMGRU5U09FM08wDQYDVQQLZWZFTLRTT0UxHDAaBgNVBAMTE0xheG1pa2FudGgg
UGVuZlhbGwEhcnMjExMjYyMTAzOTU04WncNMzExMjYyMTAzOTU04WjB0MQswCQYD
VQQGEwJCRTERMA8GA1UECBMIQnJpc3NlZXMxejAQBgNVBAcTCUJydXNzZwZlcZEP
MA0GA1UEChMGRU5U09FM08wDQYDVQQLZWZFTLRTT0UxHDAaBgNVBAMTE0xheG1p
a2FudGggUGVuZlhbGwEwggEjMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC
aG6wHBB/yDHSuq13zmtLJsn3BG37IF8nLJcS12aNIUF0n6NQY0B/P0i4ZwiF5HkZ
FHuwjNuvwC95UKYHtrm34Fe1tiVcrIUukSbZL1wnuqhr1zwmQEadaELKDoRzYBTL
tbMGwXb78WTFQsdF9nu0R5sLwBIRdaZsCMsx73o8KH3aZNMoyeZ8ycw7m1Bw1VRT
iiAttoASVo0Ne92uzw3daL6B8osei40dfg/NB1P3Gis2+do4LCW8U83mXLPaDdtE
HVANKg+oaUE4KLHmzdjCJ6Fe9u8r0SU1CvjQLXJycw0X7VP08hUf0xmN02NHGt0P
EQRHNK3kpkP1305Ea8ErAgMBAAGjITAFMB0GA1UdDgQWB8QKyJuojk16vsIyot7n
RWVtUaLVJjANBgkqhkiG9w0BAQsFAA0CAQEAE8wbvK3uuip80eGNTNgK54sshmU
NpL20JoaDWIj7KGh6qpYxVnD86HtU3ZtmhLfyksuh+eqK7eLV+ATU8+/JTzXLU+N
GV4tUfrxgyjmmVeW0JuQ4i3DwZ69nKBsVKBwcVp54cIt7/IUtW4xbB3t3U2MLBkv
E/Zgvd4P551pvP4P8Pfmhf6JtJAHAJq5LJMxgqM2Mw3jhaJEQYXB4TXuRcxibudb
EV0wUp6X9kVmq5EST1/EES/F/8i0oUVU5jThDGK8FwB07ExSPItGGEibG4w1bPd4
UKhC1p7JgiEJ466VoNsamxhcX3Zd77aY2+DLc+7Xd6nKVaVDohLYaaMKA==
-----END CERTIFICATE-----

```

Public Part of the Key pair which should be configured against the machine user configured in Transparency platform

## 2.2 CONFIGURATION OF MACHINE USER

To enable WS support the WS information in your Machine User settings in ENTSO-E Transparency Platform must be appropriately configured as described below.

**New Machine User**

Name \*

Channel Type \*

Please select one (or more) of the data-sending channels.

ECP - ECP Endpoint Code:

FTPS ? FTPS Password:

Web service ? Select strategy:  Pull  Push

Certificate:

```
-----BEGIN CERTIFICATE-----
MIDJTCcAnWgAwBAGIEFrFwDANBqkqkhiG9w0BAQsFADB3MQswCQYDVQQGEwJD
VjEKMAGGA1UECBMBSDkEaMBGGA1UEBwwRSHJhZGVjEtywqBsb3BiqJoxGDVWBgNv
BAoTD1BvcGVsYXkiplHmuc5vLJEHNMAsGA1UECXMELU3ZwejeXMBUGA1UEAMORnJh
bnRlFZvbWVja2EwHhcNMTQwMjM0YyZyNzAyVHcNMTUwMjM0YyZyNzAyVjB3MQsw
CQYDVQQGEwJDVjEKMAGGA1UECBMBSDkEaMBGGA1UEBwwRSHJhZGVjEtywqBsb3Biq
JoxGDVWBgNvBAoTD1BvcGVsYXkiplHmuc5vLJEHNMAsGA1UECXMELU3ZwejeXMBUG
A1UEAMORnJhbnRlFZvbWVja2EwHhcNMTQwMjM0YyZyNzAyVHcNMTUwMjM0YyZyNzAy
AolBAQDSvsspBgCjKDZOmQa3p0p03gD5EiqepvsfdHrq3pNz2zqCkxwhdckk1
eKNC8wVj3Z5w4TU7PKYoNxEkft+MGwsm6MRKJsu1XKsIFOWZ4fkyNcnJh81Pm
DU8BgeVbxJbQrv98sne05QRLHUW1Q0Mw2Uq78wdJdc6Yq2FpMqHFfz+2wZl
BncB5OZYA0s3f8eOITF1Y/OBGqdlDUjCsbXgCwLkEmyMn7RvwKcEtIG3yVHXFQ
/jLirmQsym6nXR/yaRHnUe78ds2Cy24Jzav+u0D0py4V036C6pN5XdcfAhLg9
tzHLk02xmxSqz7FJOMKyfOlqzAgMBAAQJITAMBOGA1UtdDgQWBBTWqLCE7D87
zBtuxKF3Zf6INjM9zANBqkqkhiG9w0BAQsFAOACQAEAxKukZdeP2sEJHgnMTg6Y
MLyGK7nUtalthxORETZdxvec5Hj0zSjRkanG4bHXWEguJdt+dvYEGV0B9n0HFo
JnGW2Wc+AgnlUjU6BpPiqVIsjG0sLTS3xseqGRWlrpab2xEcFaSnuhk1X0b6G
Xgd4TFTQILTQE6p8i3aAM0y9mmfBskGvCCnOpKX087KmGaficGhS1ve8royMym
wIQPQVOpJDGk0vgI54QGAEE0LkYv6P0y6pmmM1omGc7CRBH1wNlufmJ7j
6IF9Ld8ZnbnmRutAGtmL5kgJPPTeKwSUs9iFIEgHBHfwXrOebCUth+nG7vTRp
fw==
-----END CERTIFICATE-----
```

Endpoint:

Organization

Description ?

\* - required field

Create User

Figure 1

Check Web service checkbox, insert your Public part of the PEM certificate and specify the required strategy for messages from the Platform. Pull strategy means that you will request messages by GET request. Push strategy means that the Platform will push message to your WS. For Push strategy provide also your WS endpoint address. Please see informative wireframe (Figure 1).

WS URIs for all environments are provided in the table below. The version of WSDL defined by [SPEC], on which the Data Service WSDL is built on, is available at <https://webstore.iec.ch/publication/22465>.

Environment	WSDL URI	Endpoint URI
PROD	https://ws-submission.tp.entsoe.eu ( 20.71.78.90)	https://ws-submission.tp.entsoe.eu/data-receiver-ws/endpoints/DataService
IOP	https://ws-submission.tp-iop.entsoe.eu ( 20.31.194.118)	https://ws-submission.tp-iop.entsoe.eu/data-receiver-ws/endpoints/DataService
UAT	https://ws-submission.tp-uat.entsoe.eu (51.137.9.102)	https://ws-submission.tp-uat.entsoe.eu/data-receiver-ws/endpoints/DataService

Table 1: WS URIs

WS connection requires client HTTPS authentication. Client certificate is checked against certificate provided in Machine user settings.

### 3 Data Service

Please note that this description addresses only specific aspects of the Platform's Web Service implementation. General concepts with examples can be found in [SPEC].

#### 3.1 DATA SUBMISSION

Data are submitted in XML Payload element. See [SPEC], Chapter 5.3 *Put Messages*. Element with the message shall be the only child of the Payload element. No binary data are currently expected.

Format of submitted messages (data) is defined by ENTSO-E implementation guides and XSDs which are available from the ENTSO-E website.

As a response to submitted data, the acknowledgement document is generated and returned. In the case that submitted data are not processed before timeout configured in the Platform, problem statement document is generated instead of acknowledgement. An Acknowledgement document is then generated after data processing and depending on the selected strategy, is either pushed to data provider's web service or stored in the data provider's message queue from which it may be pulled by GET request.

#### 3.2 LIST MESSAGES

Data provider may list unread messages from the Platform or messages submitted by this data provider. Only messages not older than 30 days may be listed. See [SPEC], Chapter 5.1 *List Messages*.

#### 3.3 GET MESSAGES

Data provider may get messages from his message queue or messages submitted by him. See [SPEC], Chapter 5.2 *Get Message*.

### 3.4 DATA RETRIEVAL

Machine user may retrieve data from the Platform using web services. Refer to our Subscription user guide for the steps to configure data subscription.

[https://transparency.entsoe.eu/content/static\\_content/download?path=/Static%20content/knowledge%20base/Subscription%20Configuration%20User%20Guide%20v0.1.pdf](https://transparency.entsoe.eu/content/static_content/download?path=/Static%20content/knowledge%20base/Subscription%20Configuration%20User%20Guide%20v0.1.pdf)

### 3.5 DIGITAL SIGNATURES

Web service invocations that convey “business” xml messages should be signed. Please see following table for, which defines the services that should be signed. Services not mentioned in the table below are not signed.

Service	Signed
Data Service PUT	Request and Response
Data Service GET	Response
Data Service QueryData	Response
Data Service LIST	Not signed

Table 2: Signatures

Digital signature is described in [SPEC], Chapter 10 Security with example in Annex A. 6 Digital Signature.

For data submissions (PUT) certificate in Signature element is checked against certificate provided in Machine User settings. Data responses from the Platform are signed using Platform’s certificate.

## 4 Guideline for Data Provider’s submissions

### 4.1 MAIN GOALS OF THE GUIDELINE

The main goal of this guideline is to raise awareness about unnecessary submissions of data performed by Data Providers. Descriptions are based on actual experience from the legacy Transparency platform and Release 1 of new Transparency platform. Expectations for Release 2 (extensions to support transparency regulation) are also taken into account.

Data Providers can help to fulfil their performance expectations of the platform by following these guidelines.

The document also provides Data Providers with information that should be used during implementation and maintenance of their systems used for data submissions into the ENTSO-E Transparency Platform.

### 4.2 HANDLING OF VERSIONS

Current issues related to versions of XML files are described in the following sub-chapters.

## 4.2.1 REPEATING SUBMISSION FOR ALL PREVIOUS HOURS

There are cases when data for all previous hours of the day were resent every hour although nothing has changed in those previous hours. This led to a situation when the system had to receive, process, store and publish not only data for one hour (e.g. 13:00-14:00), but also for hours 00:00-01:00, 01:00-02:00, 02:00-03:00 ... 12:00-13:00, etc.

**Recommendation:**

To send XML file with higher version only in cases that values were changed.

### Submission of XML Files with Lower/Same Version

It appears quite often that Transparency platform receives XML file with a lower or the same version than the one which is already stored in the platform.

**Recommendation:**

Increase version of XML file with each change within XML file. Do not submit historical versions of XML file. These are not published anyway.

## 4.2.2 TOO FREQUENT SUBMISSIONS

There are situations when despite data are supposed to be received for each hour (for example the deadline for time interval 13:00-14:00 is at 15:00) the platform had to receive, process, store and publish many XML files (tens of files where one file is sufficient) submitted during that time interval (13:00-14:00).

**Recommendation:**

Meet the deadline requirement, but to submit only the latest data. It is not necessary and even not required by Regulation to submit the complete evolution of data.

Moreover evolution of such a data is not shown on the EMFIP portal – only latest version is displayed and users would need to log in and drill down to see historical values.

## 4.3 DATA GRANULARITY

Issues with amount of data in XML files were identified and described in following sub-chapters.

### 4.3.1 INCORRECT SUBMISSION RESOLUTION

Data are submitted in different resolution than the system expects. This will lead to rejection of data.

**Recommendation:**

To submit data in resolution that is configured in the Transparency platform. The expected resolution is defined in the Configuration Matrix via rule Submission Resolution.

---

Data Provider can update the rule and it can be set differently for different time periods.

### 4.3.2 TOO DETAILED DATA IN CURVES

Release 2 of the transparency platform offers the possibility to display evolution of values during some time period. Data can be delivered as a curve. For example results of a Yearly allocation can be submitted in one hour resolution. This creates 8 760 values that need to be received, processed, stored and published. But the Implementation Guides enable submission in thirty minute (about 17 500 values) or even fifteen-minute (about 35 000 values) resolution.

This requires a lot of processing time and a lot of storage is needed. Moreover transparency platform release 2 has a limit of processing maximally 10 000 position within XML.

Recommendations:

Use the lowest possible resolution. For example, in case that Implementation Guide allows delivery in PT15M, PT30M, PT60M and P1D, please use P1D. Market Time Unit resolution should only be used when transparency regulation requires it.

Use the CurveType "A03" as much as possible. When this curve type is used, only positions with changes are delivered. This leads to a smaller size of XML file and faster processing time. For example submit CurveType "A03" and then only value for first position in case that value does not change during the time interval.

## 4.4 MASTER DATA MANAGEMENT

Potential issues related to Master data are described in following sub-chapters.

### 4.4.1 TOO FREQUENT / REGULAR UPDATES

Modification or Synchronization messages do not contain any changes.

**Recommendation:**

Modification or Synchronization of master data should be done in the very same way as suggested for Data Items. New documents should be submitted only when there is some real change in the data itself.

Recurring submissions without any actual changes would generate unnecessary burden for the system.

## 5 Web Service Client Troubleshooting

In general, a Web Service communication is established through the Transparency platform access point which operates with TLS 1.2 and 1.3 (TLS 1.0. and 1.1 is deprecated and no supported any more). Thus, a used client intended for messaging has to be compliant with the supported TLS standards.



---

In case of a communication failure, please check following in your client:

- > A client in use does not support TLS 1.2 or 1.3,
- > A client in use does not use supported cypher suites,
  - *TP supported SSL Cipher Suites "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384"*,
- > A client certificate in use is not compliant with the supported SSL Cipher Suites,
- > A client in use does not have imported the ENTSO-E certificate in the trust store,
  - The public certificate is available and downloadable for example on <https://transparency.entsoe.eu/> website, certificate export is possible in certificate details.

## 6 References

SPEC	AF_284 Electronic data interchanges on the Internal Electricity Market (Superseded by IEC TS 62325-504)
STAND	IEC 61968-100 Application integration at electric utilities – System interfaces for distribution management –Part 100: Implementation Profiles
QUERY_SPEC	Parameters for query data.