

part of eex group



MiFID II EUREX Reporting Description

17.03.2022
Leipzig

Ref. 0001A

Table of Contents

1.	Introduction	4
1.1	Aims of this Document	4
1.2	Target Group of this Document	4
1.3	Contact Details and Availability	4
1.4	Glossary	4
2.	Preconditions	5
2.1	Provision of Master Data	5
2.2	Account Set-up & Access	5
3.	Workflow	6
3.1	Provision of the MiFID EUREX Instrument File	6
3.2	Upload of Participant Report	6
4.	Technical Details	8
4.1	Certificates	8
4.1.1	Accessing the PKI Platform	8
4.1.2	Requesting a New Certificate	9
4.2	FTP Server	11
4.2.1	Access to the FTP Server	11
4.2.2	Folder Structure	11
5.	Functional Details	12
5.1	Position Report Schema	12
5.2	Report Structure	12
5.3	File Naming Convention	12
5.4	Report Reference Number	12
6.	Decryption of Acknowledgement Files	13
6.1	PFX Conversion	13
6.2	XML Decryption	14
6.3	XML Signature Removal	14
7.	Encryption of Participant Reports	15
7.1	XML Signing	15

7.2	XML Encryption	16
8.	Acknowledgements Files	17
8.1	File Details	17
8.2	Content validation	18
8.2.1	Error Codes	18
8.2.2	Warning Codes	19
8.3	Technical Validation	19
8.4	Contents and Validation	20

1. Introduction

1.1 Aims of this Document

This document aims at describing the preconditions, steps, and knowledge for the use of the MiFID II EUREX Reporting by EUREX Participants. In this context the following aspects will be presented:

- Preconditions for customers of the **MiFID II EUREX Reporting**
- Possibilities for communication between the **EUREX Participant** and **EEX AG**
- Description of the steps related to the reporting of the **Participant Reports**

Please note: EEX AG cannot and does not provide legal advice in the context of these Data Description and any document related hereto. Therefore, all statements or descriptions made in this document shall not be considered as being legal advice. Please be aware, that further regulatory requirements than those outlined in this document, could apply to your firm.

1.2 Target Group of this Document

This document is addressed to EUREX Participants that have concluded the MiFID II EUREX Reporting Agreement.

1.3 Contact Details and Availability

In case of any questions related to the MiFID II EUREX Reporting please contact our Reporting Services department under the following contact details:

- Phone: +49 341 2156 380
- E-Mail: reporting-services@eex.com

1.4 Glossary

Term	Definition
GUI	Graphical User Interface
PKI	Public Key Infrastructure
MIC	Market Identification Code
MiFID II	Markets in Financial Instruments Directive (2014/65/EU)
NCA	National Competent Authority
XML	Extensible Markup Language
XSD	XML Schema Definition

2. Preconditions

2.1 Provision of Master Data

The master data is necessary for the identification and setup of the EUREX Participant's reporting account and its access to EEX AG's sFTP server.

The master data must be provided to EEX AG's Reporting Services department in the context of the conclusion of the MiFID II EUREX Reporting Agreement via the Participation Form. This includes the public IP address(es) of the EUREX Participant's devices/network to access EEX AG's sFTP server and PKI GUI.

EUREX Participants that hold an active "Agreement on the Technical Connection to the Regulatory Reporting Hub" should clarify whether this contract needs to be terminated accordingly.

2.2 Account Set-up & Access

After EEX AG has received a duly filled and signed MiFID II EUREX Reporting Agreement by the EUREX Participant the following steps apply:

- EEX AG will send out a notification of acceptance by email to the contact person named in the Participation Form.
- The public IP address(es) provided in the Participation Form will be whitelisted. EEX AG will inform the IT representative named in the Participation Form after the whitelisting has been completed. **Please note:** The whitelisting process may take up to 20 calendar days.
- EEX AG will send out the URL and login credentials to get access to the PKI platform for creating a certificate to sign the Participant Report before uploading. Please see 4.1 for information about how to create and use a certificate.
- EEX AG will send out the login credentials of the sFTP server to the IT representative named in the Participation Form after the folder has been created. The EUREX Participant will be prompted to change the password after the first login.

It is not possible to use self-signed or third-party certificates. Only certificates generated via the PKI platform are accepted in the context of this data contribution. Although several certificates may be requested, only one certificate may be actively used for an entity. In case several people or external service providers require the same certificate, please provide them with the requested certificate and the respective password.

After the necessary preconditions are fulfilled, the MiFID II EUREX Reporting will be activated by EEX AG on the date the EUREX Participant is assigned to the capacity "Commodity MiFID2" at EUREX. Details related to the reporting and data provision workflow and further technical details can be found in the following chapters.

3. Workflow

- 1 **EEX:** Provision of the **MiFID EUREX Instrument File** on the sFTP server until 10 a.m. CE(S)T
- 2 **EUREX Participant:** Upload of a valid **Participant Report** until 2 p.m. CE(S)T
- 3 **EEX:** Submission and provision of the latest **Participant Report** to BaFIN after 2 p.m. CE(S)T

3.1 Provision of the MiFID EUREX Instrument File

The MiFID EUREX Instrument File contains a complete list of all instruments that are, on the exchange day of the publication of the respective file (generation date and time), subject to reporting obligations for end of day positions on the preceding exchange day (Business Day) under MiFID II Article 58 and including instrument reference data for position reporting purposes in valid format.

The file will be provided daily until 10 a.m. CE(S)T on the sFTP server in the folder "MIFID_Instrument_File_EUREX_BACKUP" for the EUREX Participant's individual download. The purpose of the MiFID EUREX Instrument File is to give the relevant information to create the **Participant Report** based on EUREX Participant's internal data considering the relevant instrument details provided by EUREX.

The file will be provided on a daily basis only for EUREX Participants that fulfilled the necessary preconditions, see chapter 2.2. Please note that only instrument files for the last 5 business days are available on the sFTP server. Additionally, the instrument file is also provided for download via <https://www.eurex.com/ex-en/data/trading-files/com-instruments>.

3.2 Upload of Participant Report

EUREX Participants should provide their complete, signed, and encrypted Participant Report until 2 p.m. CE(S)T on the sFTP server, see chapter 4.2.2. All submitted Participant Reports must be provided according to the functional details (see chapter 5) and must include all applicable positions. Please note that partial deliveries or reports with a reduced set of attributes are not supported. In case a EUREX Participant submits several reports for one business day, EEX AG will submit the latest report to BaFin.

The Participant Report shall only contain positions that are subject to reporting obligations for end of day positions on the preceding exchange day (Business Day). In case a EUREX Participant provides an invalid report or does not submit a report until 2 p.m. CE(S)T, the latest validated Participant Report of a previous Business Day will be submitted.

The Participant Report will be validated against the MiFID EUREX Instrument File. That means position records that refer to instruments that are not included in the MiFID EUREX Instrument File will not be considered for submission to BaFIN.

Please note: The Participant Report provided under the MiFID II EUREX Reporting Agreement must only contain positions of EUREX. Customers that also use EEX AG's MiFIDII/MiFIR Data Services shall not submit data of EEX in this context but use the dedicated infrastructure.

After the contribution of the Participant Report by the EUREX Participant the file will be validated and prepared for further submission to BaFin. In case of rejections EEX AG will inform the EUREX Participant and request a corrected report. The validation status of uploaded Participant Report is shown in the acknowledgement file that is created instantly after the Participant Report could be processed. For further details please see chapter 8.

4. Technical Details

4.1 Certificates

Every EUREX Participant is required to create a certificate by using EEX AG's PKI platform (public key infrastructure). The certificate will be used to sign the Participant Report and decrypt acknowledgement files via OpenSSL. Please use Windows as operating system. Other operating systems (e.g. Linux and MacOS) have not been tested and are not supported as the commands differ. Should your infrastructure be built on operating systems other than Windows we recommend using an emulated Windows version. Minimum standard of your OpenSSL version is 1.0.2. Older versions have not been tested and might lead to an erroneous behavior.

4.1.1 Accessing the PKI Platform

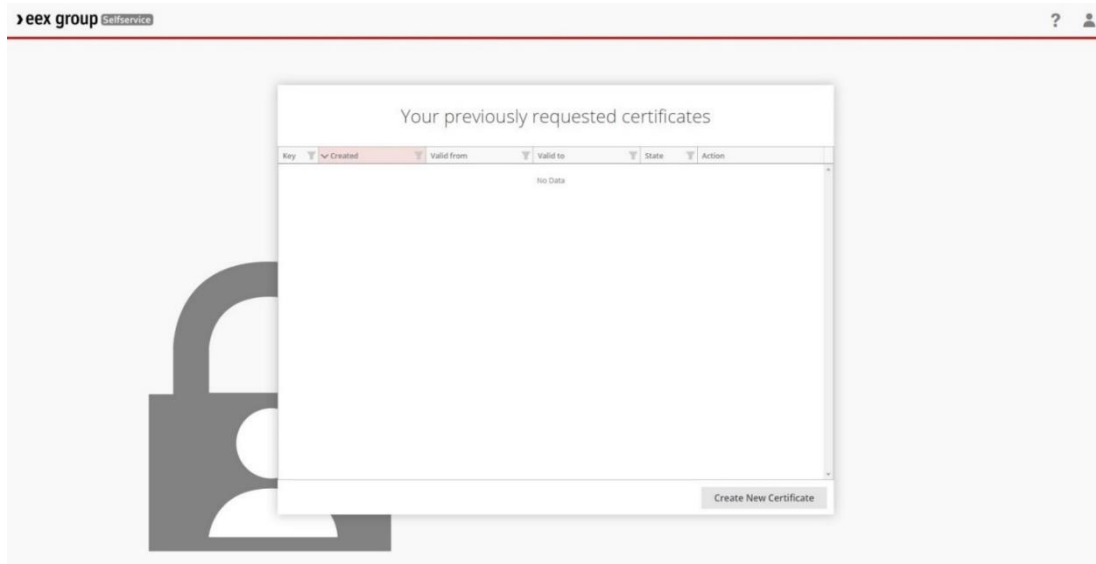
Please open our PKI platform by typing <https://rcr.eex.com/selfservice/> into your browser. We recommend using Internet Explorer as other browsers might lead to an unexpected behavior. Should you not see the below landing page your public IP might not be whitelisted. If this is the case, please send your public IP to reporting-services@eex.com.

› eex group

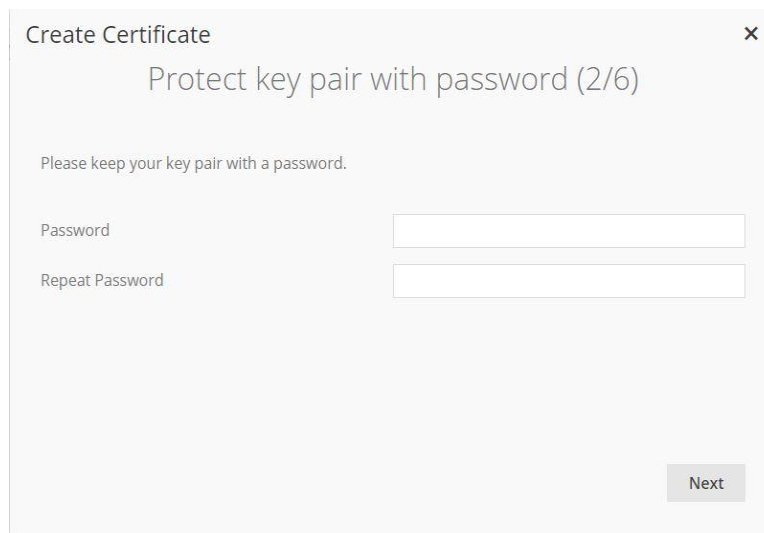
Your password of the PKI platform will be sent by email to the email address of your IT representative or authorised contact person according to your signed MiFID II EUREX Reporting Agreement. Please call +49 (0)341 2156 380 to receive the username. After typing in your correct login credentials, you are asked for an activation code. This 6-digit-code will be given to you by phone as well. Once you have logged in for the first time, you are required to create a new password. For all further login attempts a second-factor authentication code will be sent to the email address of your IT representative or authorised contact person right after you have typed in the correct username and self-created password. Please be aware that your account will be temporarily locked for multiple seconds after entering wrong credentials three times in a row. Every failed login attempt will reset and multiply the counter of remaining seconds.

4.1.2 Requesting a New Certificate

If the login was successful, the EUREX Participant will be forwarded to the welcome page of the PKI platform.

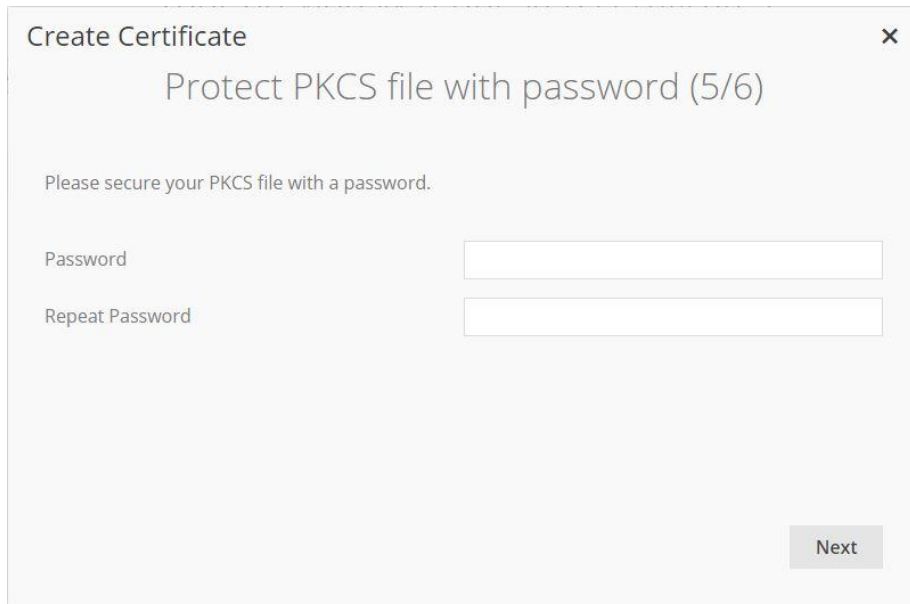


Click on “Create New Certificate” and a separate window will appear to create a new private key. You will be prompted to define a password to protect your private key. Afterwards, you will be asked to save it on your local drive.



Please note: This private key will not serve the function of signing your Participant Report or decrypting the acknowledgement files but provides an additional security. Your certificate will be available to download in the last step of this process. Should your certificate be lost, the download can be triggered again, if you upload your private key and insert the respective password. Please make sure to store both your private key and your password safely.

Once your certificate has been issued, please insert a password to secure the PKCS#12 file. Please store your chosen password safely.



Create Certificate

Protect PKCS file with password (5/6)

Please secure your PKCS file with a password.

Password

Repeat Password

Next

As a last step, you must save your certificate **as PFX format** on your local drive. The PFX file will be used for the OpenSSL application. For more details, please visit openssl.org. Once you have saved the certificate, click on “Finish” and you will be forwarded to the welcome page which will now display your recently created certificate.



Create Certificate

Save Certificate (6/6)

Save the certificate with the private key.

Save as pfx Save as p12 and cer

Finish

Please note: You will have the option to revoke your certificate. We strictly recommend to only revoke certificates in consultation with our Reporting Services experts as the revocation is an irreversible process. Once a certificate is revoked, the state of the certificate will change, and it can no longer be used.

4.2 FTP Server

4.2.1 Access to the FTP Server

EEX AG provides an sFTP server for the provision of the MiFID EUREX Instrument File and the import of Participant Reports by the EUREX Participant. Please use an FTP client like WinSCP to access the sFTP server. Operating systems other than Windows (e.g. Linux and MacOS) have not been tested and are not supported. Should your infrastructure be built on operating systems other than Windows, we recommend using an emulated Windows version.

Please find the connectivity details below. Due to our security policy, username and password are communicated through two different means. You will receive the FTP password per mail. Afterwards, please call +49 (0)341 2156 380 to receive your username.

- **Username:** will be communicated by telephone
- **Password:** will be communicated by mail
- **Port:** 22 (sFTP)
- **URL:** rcr.eex.com
- **IP:** 193.29.70.14

4.2.2 Folder Structure

The 1st level of the FTP server contains five folders. Relevant for MiFID II EUREX Reporting are the folders **MiFID**, **MIFID_Instrument_File_EUREX_BACKUP** and **EEX_Public_Key**.

1st Level	2nd Level	3rd Level
MIFID	ACKNOWLEDGEMENT	<i>Acknowledgement files as encrypted XML files.</i>
	ARCHIVE	<i>Successfully uploaded XML files from folder MIFID\IN.</i>
	ERROR	<i>Unsuccessfully uploaded XML files from folder MIFID\In.</i>
	IN	<i>Encrypted Participant Reports as XML files supposed to be uploaded.</i>
	OUT	<i>Not relevant</i>
	ORDERREPORT	<i>Not relevant</i>
INSTRUMENTFILE	<i>MiFID EUREX Instrument Files</i>	-
EEX_Public_Key	<i>Public Key for encryption of Participant Reports.</i>	-

5. Functional Details

5.1 Position Report Schema

EEX AG uses the “Extended FCA” schema for data exchange with EUREX Participants. Participant Reports must be valid with regard to this schema definition.

5.2 Report Structure

The XML document of the “Extended FCA” schema covers a single FinInstrmRptgTradgComPosRpt element containing one header element for general report attributes and multiple CPR elements for the report data. The CPR element must only contain the report status **NEWT** for newly submitted records.

Please note: EEX AG does not accept Participant Reports with report status CANC or AMND. If a EUREX Participant must correct a formerly sent Participant Report, the previous Participant Report must not be amended or cancelled. EEX AG only accepts a new and complete Participant Report with report status NEWT that will replace the formerly sent Participant Report.

5.3 File Naming Convention

File naming convention for **MiFID EUREX Instrument Files**:

Pattern: com_instruments_<GenerationDate>.csv

Sample: com_instruments_20220401.csv

File naming convention for **Participant Reports**:

Pattern: PRO_<LEI>_NCADE_<GenerationTimestamp>.xml.enc

Sample: PRO_529900J0JGLSFDWNFC20_NCADE_20220302T120020734.xml.enc

The file naming convention for **acknowledgement files** is based on the file name of the corresponding Participant Report:

Pattern: PRO_<LEI>_NCADE_<GenerationTimestamp>_ACK.xml.enc

Sample: PRO_529900J0JGLSFDWNFC20_NCADE_20220302T120020734_ACK.xml.enc

GenerationTimestamp format: YYYYMMDDT000000000

GenerationDate format: YYYYMMDD

5.4 Report Reference Number

The report reference number of each record of the respective Participant Report must be unique to avoid duplicates.

6. Decryption of Acknowledgement Files

Once the Participant Reports has been uploaded and processed, the corresponding acknowledgement file will be created. As this file is encrypted the EUREX Participant must decrypt it and remove the signature.

Preconditions for decrypting acknowledgement files:

- The EUREX Participant has downloaded the encrypted and signed acknowledgement file from the sFTP server.
- The EUREX Participant has access to the PFX file available on the PKI platform.
- The EUREX Participant has installed OpenSSL.

6.1 PFX Conversion

Please follow the below steps to convert your PFX certificate into a PEM coded PKCS#12 format.

1. Open OpenSSL.
2. Ensure to have no spaces in your folder and file names.
3. Use the below command to convert the PFX file.
4. Insert the password that was specified for the PKCS file during the certificate creation.

pkcs12 -in *Filename.pfx* -out *Filename.pem* -nodes

Parameter	Description
-in <i>Filename.pfx</i>	The filename and path of the PFX file that was created during the certificate creation.
-out <i>Filename.pem</i>	The filename and path of the converted PEM coded file, which is about to be created.
Enter Import Password	The password of the PFX (PKCS) file specified during the certificate creation.

```
OpenSSL> pkcs12 -in C:\PKI\CustomerPKCS12.pfx -out C:\PKI\CustomerPKCS122.pem -n
odes
Enter Import Password:
MAC verified OK
OpenSSL>
```

You will receive a certificate as PEM coded PKCS#12 format that is used to decrypt acknowledgement files and to sign the Participant Report with OpenSSL.

6.2 XML Decryption

Please follow the below steps to decrypt the XML file.

1. Open OpenSSL.
2. Ensure to have no spaces in your folder and file names.
3. Use the below command to decrypt the draft report.

smime -decrypt -inform PEM -in *Filename.xml.enc* -out *Filename.xml.sig* -inkey *PKCS12_file.pem*

Parameter	Description
-in <i>Filename.xml.enc</i>	The filename and path of the encrypted XML file, that is about to be decrypted.
-out <i>Filename.xml.sig</i>	The filename and path of the decrypted, but signed XML file, which is about to be created.
-inkey <i>PKCS12_file.pem</i>	The filename and path of the PEM coded file.

```
OpenSSL> smime -decrypt -inform PEM -in C:\PKI\PositionReportOriginal.xml.enc -o
ut C:\PKI\PositionReportOriginal.xml.sig -inkey C:\PKI\CustomerPKCS12.pem
OpenSSL>
```

You will receive a decrypted but signed acknowledgement file. This file is not readable and must be further processed.

6.3 XML Signature Removal

Please follow the below steps to remove the signature and create a readable file.

1. Open OpenSSL.
2. Ensure to have no spaces in your folder and file names.
3. Insert the below command to remove the signature.

openssl smime -verify -noverify -in *Filename.xml.sig* -inform PEM -out *Filename.xml*

Parameter	Description
-in <i>Filename.xml.sig</i>	The filename and path of the decrypted but signed XML file (see chapter 4.2).
-out <i>Filename.xml</i>	The filename and path of the decrypted and unsigned XML-file.

```
OpenSSL> smime -verify -noverify -in C:\PKI\PositionReportOriginal.xml.sig -info
rm PEM -out C:\PKI\PositionReportOriginal.xml
Verification successful
```

You will receive an XML file which is neither encrypted, nor signed.

7. Encryption of Participant Reports

Prior to the upload of a Participant Report the XML file needs to be signed and encrypted.

Preconditions for signing and encrypting reports:

- Customer has successfully applied for a new certificate.
- Customer has access to the PFX file and to the EEX public key, that is stored in the folder “EEX_Public_Key” on the sFTP server.
- Customer has installed OpenSSL.
- Customer has converted the PFX certificate into a PEM coded PKCS#12 format (see 4.1).

7.1 XML Signing

Please follow the below steps to add a signature to your XML file.

1. Open OpenSSL.
2. Ensure to have no spaces in your folder and file names.
3. Use the below command to sign the amended XML file.

```
smime -sign -md SHA256 -nodetach -outform PEM -out Filename.xml.sig -in Filename.xml -signer PKCS12_file.pem
```

Parameter	Description
-in Filename.xml	The filename and path of the decrypted XML file that is about to be signed.
-out Filename.xml.sig	The filename and path of the signed XML file.
-signer PKCS12_file.pem	The filename and path of the PEM coded file.

```
OpenSSL> smime -sign -md SHA256 -nodetach -outform PEM -out C:\PKI\PositionReportAmended.xml.sig -in C:\PKI\PositionReportAmended.xml -signer C:\PKI\CustomerPKCS12.pem
OpenSSL>
```

You will receive a signed XML file, which is not readable anymore. In addition, the signature ensures that all data is authentic and unchanged.

7.2 XML Encryption

Please follow the below steps to encrypt your signed XML file.

1. Open OpenSSL.
2. Ensure to have no spaces in your folder and file names.
3. Insert the below command to encrypt the signed XML file.

smime -encrypt -aes256 -outform PEM -out `Filename.xml.enc` -in `Filename.xml.sig` `EEX_Public_Key.pem`

Parameter	Description
-in <code>Filename.xml.sig</code>	The filename and path of the signed XML file, which is about to be encrypted.
-out <code>Filename.xml.enc</code>	The filename and path of the encrypted XML file, which is about to be created.
<code>EEX_Public_Key.pem</code>	The filename and path of the EEX public key.

```
OpenSSL> smime -encrypt -aes256 -outform PEM -out C:\PKI\PositionReportAmended.xml.enc -in C:\PKI\PositionReportAmended.xml.sig C:\PKI\EEX_Public_Cert.pem
OpenSSL>
```

You will receive an encrypted XML file that can only be decrypted by EEX AG. Please upload the encrypted XML file to the folder “MFID\IN” of EEX AG’s sFTP server.

8. Acknowledgements Files

Once a Participant Report has been uploaded to the sFTP server, a content validation of every record is executed. The following table lists existing error codes and consequent actions if they occur.

Please note: An uploaded Participant Report is rejected if it contains erroneous records. As a result, the whole file must be corrected and re-uploaded if one of the error codes below occurs.

8.1 File Details

Section	Field name	Description
Header	Environment	Identifier of the reporting environment. Usually PRO for production.
Header	Timestamp	Date and time at which the response file was created.
Header	SubmitterID	Indicates the LEI of the response provider.
Header	CustomerID	Indicates the LEI of the response receiver.
Header	InboundFileReference	Identifier of the inbound file the response was created for.
Header	UltimateReceivingNCA	Identifier of the receiving authority.
Header	FileType	Indicates the report type.
Header	ValidationResult	Indicates the validation result for the uploaded file, either Accepted or Rejected.
Header	AcknowledgmentStatus	Indicates the status of the acknowledgement, either Accepted or Rejected.
Header	TotalRecords	Indicates the total number of records within the uploaded file.
Header	ValidRecords	Indicates the number of valid records within the uploaded file.
Header	WarningRecords	Indicates the number of warning records within the uploaded file.
Header	ErrorRecords	Indicates the number of error records within the uploaded file.
Header	RejectedRecords	Indicates the number of rejected records within the uploaded file.
Body	ReportRefNo	Only listed if the validation results in error or warning. Indicates the reference id of the validated record.
Body	Busdt	Only listed if the validation results in error or warning. Indicates the reported trading day of the validated record.
Body	TrdngVenID	Only listed if the validation results in error or warning. Indicates the MIC Code of the validated record.
Body	RecordNumber	Only listed if the validation results in error or warning. Indicates the dataset number of the validated record.
Body	Sequence	Only listed if the validation results in error or warning. Indicates the sequence number of acknowledgment records.
Body	FieldID	Only listed if the validation results in error or warning. Indicates the field Id of the validated record.
Body	FieldName	Only listed if the validation results in error or warning. Indicates the field name of the validated record.

Body	Severity	Only listed if the validation results in error or warning. Indicates the severity of the validated, either error or warning.
Body	ErrorCode	Only listed if the validation results in error or warning. Indicates the error code of the validated record.
Body	ErrorDescription	Only listed if the validation results in error or warning. Indicates the error reason for the validated record.

8.2 Content validation

8.2.1 Error Codes

Once a Participant Report has been uploaded to the sFTP server, a content validation of every record is executed. The following table lists existing error codes and consequent actions if they occur.

Please note: An uploaded file is rejected if it contains erroneous records. As a result, the whole file must be corrected and re-uploaded again including all records if one of the error codes below occurs.

Error Code	Error description	Required action
E001	The specified LEI code is not valid according to the GLEIF database.	Please ensure to only specify LEI codes that are valid and active according to the GLEIF database (gleif.org) for the reported business day.
E002	The specified instrument is not a reportable instrument on the respective business day.	<ol style="list-style-type: none"> 1. Please ensure that the specified instrument is reportable on the respective business day, i.e. included in the MiFID EUREX Instrument File. 2. Please ensure that the specified ISIN is an instrument ISIN and not a product ISIN.
E003	The specified Report Reference Number is not unique and has been used multiple times within the uploaded file.	Please ensure that the uploaded file does not contain duplicate Reference IDs, i.e. Report Reference Numbers. This may be avoided by amending the 'counter' part within the Reference Number.
E004	The country code of the specified National ID is not valid according to ISO 3166.	Please ensure that the specified National ID starts with a valid country code according to ISO 3166.
E006	The uploaded file contained too many elements.	Please ensure that the file was properly created according to the following rules: <ul style="list-style-type: none"> • The file contains only records for one business day, and • The file contains only records for one NCA.
E007	The specified date has an invalid format.	Please specify a valid date.
E008	The specified text is longer than allowed.	Please specify a value with less than 255 digits.

8.2.2 Warning Codes

Once a Participant Report has been uploaded to the sFTP server, a content validation of every record is executed. The following table lists existing warning codes.

Please note: An uploaded file is not rejected, if validated records only cause warning codes. The Participant Report will still be considered for submission to BaFin.

Warning Code	Warning description	Required action
W002	The specified reference instrument master data is incorrect according to the instrument file.	No further action required. The incorrect value will be corrected automatically.

8.3 Technical Validation

Once a Participant Report has been uploaded to the sFTP server, a technical validation of the file is executed. **Please note:** The technical validation is executed on file level and not on record level, hence there are no explicit error codes available, but the error reason is included within the validation result. In addition, if one of the errors below occurred, the submitted file has been rejected.

Error reason	Error description	Required action
Decryption or verification of Member signature failed. Error message: [...]	The submitted file was not correctly signed and/or encrypted.	Please ensure that: <ul style="list-style-type: none"> A file is signed by a valid certificate from EEX AG's PKI platform. A file is encrypted with the public key of EEX AG. The signing and encryption process was executed according to chapter 7.
XML validation of file <FilenameWithPath> failed: [...]	The uploaded file is not valid according to the XSD schema.	Please ensure that the submitted file contains only values and elements according to the XSD schema.
Report contains items for multiple business days: <ListOfBusinessDaysinXMLFile>	The submitted file contains data for more than one reportable trading day.	Please ensure that an uploaded file contains only reportable records for one Business Day.
Multiple NCAs in upload: <ListOfNCAs>	The submitted file contains reportable data for more than one authority.	Please ensure that an uploaded file contains only reportable data for one NCA.
CPR element <Number> with reference number	The identified position element refers to an	Please ensure that an uploaded file contains only instruments that are

<ReferenceNumber> has invalid NCA: [...]	instrument that is not reportable.	included in the respective MiFID EUREX Instrument File. Please note: This error does currently not occur, since datasets that refer to an invalid instrument are automatically ignored.
NCA in header <NCAName> is different from NCA <NCAFromInstrument> of instrument <ISIN>	The identified position element refers to an instrument that must not be reported to the specified authority.	Please ensure that an uploaded file contains only reportable data for the NCA that was specified in the field UltimateReceivingNCA.
Data for Business Day <businessday> and NCA <NCA> already reported to regulatory authority.	The submitted file contains data for a business day that had already been reported.	Please ensure that amendments are submitted to EEX AG on D+1 between 10 a.m. CE(S)T and 2 p.m. CE(S)T.

8.4 Contents and Validation

Field name	Schema Path	Field ID	Code
Report reference number	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/ReportRefNo	RD001	E003
Date and time of report submission	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/RptDt	RD006	E007
Date of the trading day of the reported position	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/BusDt	RD007	E007
Reporting entity ID	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/RptEnt/LEI	PA002	E001
Position holder ID	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnHldr/LEI	PH001	E001 E004
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnHldr/NationalID/Othr/Id	PH001	
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnHldr/NationalID/Othr/SchmeNm/Cd	PH001	
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnHldr/NationalID/Othr/SchmeNm/Prtry	PH001	
Email address of position holder	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstinHldrCntctEml	PH002	E008
Category of position holder	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstinHldrCategory	PH004	n/a

Ultimate parent entity ID	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PrntEnt/LEI	PH005	E001 E004
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PrntEnt/NationalID/Othr/Id	PH005	
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/RptEnt/NationalID/Othr/SchmeNm/Code/	PH005	
	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/RptEnt/NationalID/Othr/SchmeNm/Prtry/	PH005	
Email address of ultimate parent entity	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/ParentPstinHldrCntctEml	PH006	E008
Identification code of contract traded on trading venues	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/ISIN	RD003	E002
Venue product code	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/VenProdCde	RD004	W002
Trading venue identifier	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/TrdngVenID	RD005	W002
Position type	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnTyp	PD001	W002
Position maturity	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnMtrty	PD002	W002
Position quantity	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnQty	PD003	W002
Notation of the position quantity	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnQtyUoM	PD004	W002
Notation of the position quantity (description)	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/PstnQtyUoMDesc	PD007	W002
Delta equivalent position quantity	/FinInstrmRptgTradgComPosRpt/CPR/<Report Status>/CPRBody/DeltaPstnQty	PD005	W002