

Contents

1. Introduction.....	3
2. Participants' obligations.....	4
2.1. Mandatory values.....	4
2.2. PII Data Submission.....	5
2.2.1. PII Data Post Brexit Submission (UK national persons).....	7
3. Process Overview.....	7
3.1 NUF Admin Set-Up and Initial Upload.....	7
3.2 Preparing an Upload File.....	9
3.3 Daily Schedule.....	10
4. Connectivity and Authentication options.....	10
4.1 Supported protocols.....	10
4.1.1 Key Authentication.....	11
4.1.2 Password Authentication.....	11
4.1.3 IP Addresses for Firewall Rules.....	11
4.2 HTTPS Connectivity Via An Internet Browser.....	12
4.2.1 Logging In.....	12
4.2.2 Uploading a file.....	13
4.2.2 File validation.....	14
4.3 Using SFTP to Connect.....	16
4.3.1 Configuring Filezilla.....	16
4.3.2 Uploading a File.....	18
4.3.3 SFTP Error Messages.....	18
4.3.4 Sample Commands for Scripting.....	20
5. Data Flow and Security.....	20
5.1 Submission and Verification.....	20
5.1.1 NUF Over SFTP.....	20
5.1.2 NUF Over HTTPS.....	21
5.1.3 NUF IP Blocking.....	21
5.1.4 Verification (Automatic).....	21
5.1.5 Verification (Manual).....	21
5.2 Database.....	21
5.2.1 Participant Database.....	21
5.2.2 Operating System Patching.....	22
5.2.3 General Security Protocols.....	22
5.2 Backup Storage and Destruction.....	22
5.5 Participant Data Handling Disclaimer.....	22
6. Contact Us.....	23

1. Introduction

Pursuant to Directive 2014/65/EU (“MiFID II”)¹ and Regulation (EU) No 600/2014 (“MIFIR”)¹, the trading venue operators are required to identify participant firms, their natural person users and their trading algorithms for regulatory reporting and record keeping purposes.

Under MIFIR and the supplementing Regulatory Technical Standards for the reporting of transactions to competent authorities (“RTS 22”)¹ and for the maintenance of relevant data relating to orders in financial instruments (“RTS 24”), the trading venues are required to report details of transactions which are executed through its systems by a firm which is not itself subject to the MiFIR transaction reporting regime (non-EEA for EEA trading venues / non-UK for UK trading venues) and to maintain the relevant data relating to all orders in financial instruments which are advertised through its systems. The regulatory requirements apply to CME Group’s EU and UK regulated entities which operate the trading venues (jointly, the “Trading Venues”) listed below:

Market	Legal Entity	Trading Venue and MIC code	Country of Incorporation	Regulatory documents
BrokerTec	CME Amsterdam BV	BrokerTec EU RM - CLOB EU (BTAM) and Quote EU (BTQE)	The Netherlands	https://www.cmegroup.com/markets/brokertec/regulatory-documents.html
	BrokerTec Europe Limited	BrokerTec UK MTF - CLOB (BTEE)	United Kingdom	
EBS	BrokerTec Europe Limited	EBS UK MTF (XEBS)	United Kingdom	https://www.cmegroup.com/markets/ebs/regulatory-documents.html#documentation

To comply with these regulations, the Trading Venues must collect and retain the following participant information for trading on their systems:

- Legal Entity Identifier (LEI)- ISO 17442 (<https://www.gleif.org/en>)
- Natural Person Identification Information (“PII”)
- Designation for identifying the algorithm trading systems

Trading Venue participants are required to supply and maintain updated records of this data in order to satisfy the eligibility criteria for trading on the Trading Venues, as set out in the relevant Trading Venue rulebooks.

¹ and the UK onshored version of the same as amended and transposed into the laws of the United Kingdom pursuant to the European Union (Withdrawal) Act 2018 and the European Union (Withdrawal Agreement) Act 2020.



The NEX Upload Facility ("NUF") is a secure channel available for MiFID II participant customer data submission, whereby each participant can upload to their own folder and download back any Error Record files (as explained below). CSV template submissions are accepted via either Secure File Transfer Protocol ("SFTP") or Hyper Text Transfer Protocol Secure ("HTTPS").

The purpose of this guide is to describe the required PII data, the participants' obligations to provide the required data and format for submission, the process to access the NUF, mechanisms for initial upload and daily updates (if required), data flow and security, plus troubleshooting and support contact details.

2. Participants' obligations

Trading Venue participants, to be allowed to trade, must complete the initial upload of PII data for manual traders and individuals operating algorithm trading systems, as well as provide the designation for identifying the algorithm trading systems trading products offered by the Trading Venues. The upload of PII data must be completed using the NUF (<https://sftp.nex.com>), following the participant's successful registration (as explained in section 3. Process Overview). The designation for identifying the algorithm trading system can be uploaded either via the Algorithm Trading Annual Certification Form at CME Customer Center (please refer to [CME Customer Center - User Help System](#)) or using the NUF, as explained below. Failure to pre-register active traders will result in traders not being allowed to trade.

For manual traders and operators of algorithm trading systems, the PII data provided by the participant is linked to the short code associated with the Globex User Signature ("GUS") ID (trader ID) and for algorithm trading systems the algo identifiers are linked to the algo short code associated with the GUS ID. Please review the mandatory values outlined in section 2.1 for further information.

2.1. Mandatory values

When submitting PII data or algo identifiers on the NUF, participants must ensure the submitting files contains the following required values:

Column	Attribute	Mandatory	Value Restrictions	Details
A	LEI	Yes	Alphanumeric (20 characters)	LEI of the submitting Firm. N.B. where users are required to upload for multiple LEIs, one file must be submitted per LEI.
B	GFID	Yes	Alphanumeric	Globex Firm ID ("GFID") under which Trader will execute (corresponds to legacy Bank Code) Note: EBS GFIDs (unique 4-characters ID) / BrokerTec EU GFIDs (up to 5 characters ID)
C	ALGO / PERSON	Yes	A, P	A = Algo / P = Person
D	SHORT CODE	Yes	Numeric only (10-digit)	Shortcodes containing alpha or special characters will be

			max, initial digit must not be zero)	rejected by NUF.
E	(GUS) TRADER ID	No	N/A	Do not populate this field. Rows with Trader ID populated may be rejected by NUF.
F	LOCATION	Yes	ISO 3166-1 alpha-2	Trading entity location. See ISO Country Codes ; select Country Codes then Search.
G	ALGO NAME	<u>ALGO</u> only	Alphanumeric (50-character max)	Only the following characters may be used: capital Latin letters (A-Z), numbers (0-9). Value must correspond to an Algo Name specified in Algo Self-Certification Form.
H	FIRST NAME	<u>Person</u> only		
I	SURNAME	<u>Person</u> only		
J	DOB	No	N/A	Do not populate.
K	NATIONALITY	<u>Person</u> only	ISO 3166-1 alpha-2	Natural person nationality. See ISO Country Codes ; select Country Codes then Search.
L	IDENTIFICATION TYPE	<u>Person</u> only	CCPT, NIDN, CONCAT	Must correspond to ESMA directions according to the country specified in NATIONALITY - refer to section 2.2 for ESMA guidelines on accepted type and format.
M	IDENTIFICATION VALUE	<u>Person</u> only		The unique CCPT, NIDN or CONCAT value for the person.
N	STATUS	Yes	ACTIVE, INACTIVE	If you wish to indicate that a Trader or Algo is no longer active on the venue, flag as inactive.

2.2. PII and Algo Data Submission

To be allowed to trade on the Trading Venues, participants are required to upload:

- For natural persons, the designation resulting from the concatenation of the ISO 3166-1 alpha-2 (2 letter country code) of the nationality of the person, followed by the national client identifier of the person.
- For computer algorithms, the designation for identifying the computer algorithm, which shall be unique for each set of code or trading strategy that constitutes the algorithm, used consistently when referring to the algorithm or version of the algorithm once assigned to it, and unique over time.

The national client identifier for natural persons shall be assigned in accordance with the priority levels provided in the table below, which can be found at RTS 22, Annex II (https://www.esma.europa.eu/sites/default/files/library/2016-1064_rts_22_annex_ii.pdf.pdf), using the highest priority identifier for that given nationality.

For information on how different national identifiers are specified in the above table (Annex II of RTS 22) are represented, refer to: ESMA UPDATES Q&A ON MIFIR DATA REPORTING (page 47) link: <https://www.esma.europa.eu/press-news/esma-news/esma-updates-qa-mifir-data-reporting-8>.

ISO 3166-1 alpha 2	Country Name	1st priority identifier	2nd priority identifier	3rd priority identifier
AT	Austria	CONCAT		
BE	Belgium	Belgian National Number (Numéro de registre national – Rijksregisternummer)	CONCAT	
BG	Bulgaria	Bulgarian Personal Number	CONCAT	CONCAT
CY	Cyprus	National Passport Number	Passport Number	
CZ	Czech Republic	National identification number (Rodné číslo)	CONCAT	
DE	Germany	CONCAT		
DK	Denmark	Personal identity code 10 digits alphanumerical: DDMMYYXXXX	CONCAT	
EE	Estonia	Estonian Personal Identification Code (Isikukood)		
ES	Spain	Tax identification number (Código de identificación fiscal)		
FI	Finland	Personal identity code	CONCAT	
FR	France	CONCAT		
GB	United Kingdom	UK National Insurance number*	CONCAT	
GR	Greece	10 DSS digit investor share	CONCAT	
HR	Croatia	Personal Identification Number (OIB – Osobni identifikacijski broj)	CONCAT	
HU	Hungary	CONCAT		
IE	Ireland	CONCAT		
IS	Iceland	Personal Identity Code (Kennitala)		
IT	Italy	Fiscal code (Codice fiscale)		
LI	Liechtenstein	National Passport Number	National Identity Card Number	CONCAT
LT	Lithuania	Personal code (Asmens kodas)	National Number Passport	CONCAT
LU	Luxembourg	CONCAT		
LV	Latvia	Personal code (Personas kods)	CONCAT	
MT	Malta	National Identification Number	National Number Passport	
NL	Netherlands	National Passport Number	National identity card number	
NO	Norway	11 digit personal id (Foedselsnummer)	CONCAT	
PL	Poland	National Identification Number (PESEL)	Tax Number (Numer	CONCAT

			identyfikacji podatkowej)	
PT	Portugal	Tax number (Número de Identificação Fiscal)	National Number	Passport CONCAT
RO	Romania	National Identification Number (Cod Numeric Personal)	National Number	Passport
SE	Sweden	Personal identity number	CONCAT	
SI	Slovenia	Personal Identification Number (EMŠO: Enotna Matična Številka Občana)	CONCAT	
SK	Slovakia	Personal number (Rodné číslo)	National Number	Passport CONCAT
All other countries		National Passport Number	CONCAT	

2.2.1. PII Data Post Brexit Submission (UK national persons)

As a result of Brexit, the **highest priority designation to identify UK natural persons trading on EEA trading venues** (such as, BrokerTec EU RM) **shall be National Passport Number**. If not available, the second priority identifier shall be CONCAT.

For UK natural persons trading on UK trading venues (such as, BrokerTec EU MTF and EBS UK MTF), the requirements for reporting remain the same as pre-Brexit. The **highest priority identifier shall be the UK National Insurance Number**, and if not available, the second priority identifier shall be CONCAT.

In case a UK natural person trades on both EEA and UK trading venues, participants shall be required to upload the highest priority identifier for each jurisdiction (National Passport Number and UK National Insurance Number), and if not available, CONCAT.

Where the identifier assigned refers to CONCAT, the natural person shall be identified by the participant using the concatenation of the following elements in the following order:

- (a) the date of birth of the person in the format YYYYMMDD;
- (b) the five first characters of the first name;
- (c) the five first characters of the surname.

Please note, for (b) and (c) forenames and surnames of less than five characters must be completed with "#" symbols so that the forenames and surnames shown contain five characters. The use of name prefixes, apostrophes, accents, hyphens, punctuation marks or spaces shall be excluded.

Participants shall have responsibility for the completeness, accuracy and timely submission of the PII Data of its natural persons, having special consideration to the priority levels of the national client identifier. Except where explicitly requested as highest priority identifier (i.e. Germany, France, etc.), CONCAT shall not be used as an option if the correct PII data is available to be supplied.

For information on how different national identifiers are specified in the above table (Annex II of RTS 22) are represented, please refer to <https://www.esma.europa.eu/press-news/esma-news/esma-updates-ga-mifir-data-reporting-8> (page 58)

3. Process Overview

In order to comply with the obligations set out in section 2 of this guide, participants must ensure they complete the following steps:

3.1 NUF Admin Set-Up and Initial Upload

- 1) Complete the [NUF Registration Form](https://www.cmegroup.com/files/download/nuf-registration-form.pdf) – see link: <https://www.cmegroup.com/files/download/nuf-registration-form.pdf>.

Upload Facility Registration Form

Customer Entities		Trading Venue Access	MiFID Administrative Contacts			NUF Prod System	Host (Optional)	Set-up Request		
Firm Name	LEI	Products Traded	First Name	Last Name	E-Mail	User Name	Key IP Address	Upload Authenticate	Upload Automation	Encryption
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Legal Entity Identifier
ISO 17442 (can be found at <https://search.gleif.org/#/search/>)

Trading Venue Access
Please complete a row for each Product group per LEI. This is because we offer the following:
BrokerTec EU RM (CABV) - **EGBs & EU Repos**
BrokerTec UK MTF (BEL) - **UK Repo**
EBS UK MTF (BEL) - **FX ON MTF/OFF SEF NDFs**

MiFID Administrative Contacts
Please supply at least 2 contacts who are authorised by the participant, to request key/password changes.

NUF Prod System
Please insert preferred Prod User Name.
NB Must be > 6 characters and <20, only upper or lower case alphanumeric. i.e. no special characters. e.g. janedoe

Set-up Request
Please request either Key Authentication (select **Yes**) or password (select **No**) for NUF access. **If Yes**, please send NEX your firm's Public key with this form.

Please select whether you intend to automate data upload (select **Yes**)

Please select whether you intend to encrypt and if so, by which method of encryption (GPG2, PGP). **If Yes**, we will send you the NEX Public key after registration.

- 2) Please populate the fields as follows:
- a) Firm name – Full legal entity name
 - b) Legal Entity Identifier (LEI) - ISO 17442
 - c) Venue Access – Choose the relevant trading venue for the Products Traded. If you are trading multiple product types from the same LEI, please complete a row for each one, as each has a related trading venue mapping.
 - d) MiFID Administrative contact(s) – please supply at least 2 contacts who are authorised by the firm, to request key/password changes.
 - e) NUF Prod(uction) System User Name – participantCustomers must suggest a Prod Username, which must be more than 6 and less than 20 characters with no special characters, so only a-z, A-Z, 0-9 e.g. "username123".
 - f) Optionally, IP addresses of the connecting systems.
 - g) Request for Key Authentication (or Password).
 - h) Whether the intention is to automate uploads to NUF.
 - i) Whether the intention is to encrypt upload files using GPG2/PGP.

- 3) Return completed NUF Registration Form to Enterprise Application & System Entitlements ("EASE") at EASE@cmegroup.com.
- 4) Participants should instruct their own technical support teams to open firewalls to allow access to the NUF production IP addresses – see section 4.1.3 below.
- 5) Participants shall opt for their preferred supported protocol, SFTP or HTTPS, and send their Public encryption key for SFTP or HTTPS authentication to EASE at EASE@cmegroup.com. For more information on the available supported protocols, connectivity and authentication options, please refer to section 4.
- 6) Participants shall complete initial SFTP or HTTPS authorisations for <https://sftp.nex.com>.
- 7) Participants shall submit initial production files using the file template provided in section 3.2 - Preparing an Upload File, which provides further details.
- 8) Please contact GCC at gcc@cmegroup.com for any troubleshooting on file upload or data verification.
- 9) Participants receiving Error Record email notifications should access the secure folder to download Error Record files.

3.2 Preparing an Upload File

To facilitate the submission of a file, participants required to upload PII Data for manual and algo traders can utilise the Upload Template CSV file, by completing the following steps:

- 1) Download the [Upload Template CSV File](https://www.cmegroup.com/files/download/natural-persons-upload.csv) - link <https://www.cmegroup.com/files/download/natural-persons-upload.csv>.
- 2) Replace the sample entries with the relevant manual and/or algo traders PII data in the required format (please see below table).

Example Row Types

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	TEST1234567890123456	TSNY	P	160554671		US		ANNA	GARCIA		US	CONCAT	19821201ANNA#GARCIA	ACTIVE
2	TEST1234567890123456	TSLN	A	3322657		GB	MY ALGO 657							ACTIVE
3	TEST1234567890123456	TSLN	P	160555783		GB		JOE	BLOGGS		GB	NIDN	AB123456C	ACTIVE
4	TEST1234567890123456	TSNY	P	160555783		US		JOE	BLOGGS		GB	NIDN	AB123456C	ACTIVE
5	TEST1234567890123456	TSLN	P	160553216		DE		MICHAEL	MULLER		DE	CONCAT	19760416MICHAMULLE	INACTIVE

- Row 1: Natural Person
 - Row 2: Algo
 - Rows 3 and 4: Natural Person (GB nationality) that will execute under two different GFIDs in different operating locations (TSLN-GB and TSNY-NY)
 - Row 5: Natural Person being deactivated
- 3) Save the file in Comma Separated Values (CSV) format in the following naming convention:
Filename key

- {LEI} - Legal Entity Identifier - ISO 17442 - of the submitting firm
- {LOCATION} – ISO 3166-1 alpha 2 standard country code for the submitting firm location. Search country codes.
- {YYYYMMDDHHMMSS} – Year, month, date, time of the file submission where the hours are expressed in 24-hour format based on UTC.

Filename structure

- {LEI}_{LOCATION}_{YYYYMMDDHHMMSS}.csv

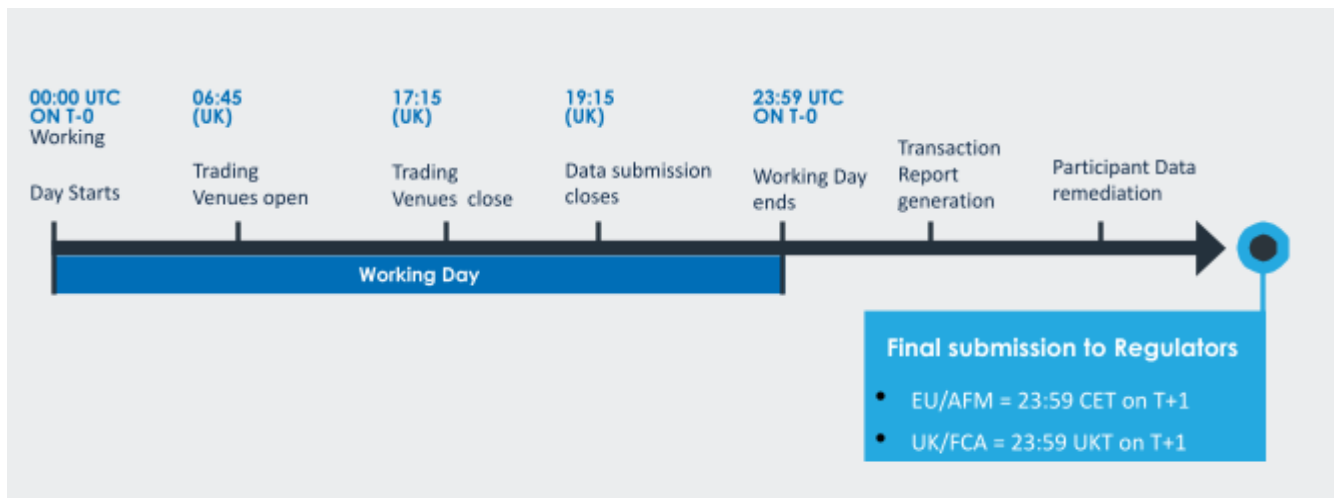
Filename Example

- 2138008LPQ92DIHKHY20_GB_20171022175400.csv

4. Log in to the NUF UI, then upload the file following the steps detailed in sections 4.2 for participants using HTTPS and 4.3 for participants using SFTP to connect to the NUF.

3.3 Daily Schedule

Please see the following representation of the schedule for a “Working Day”, submission of any changes to participants’ data and BrokerTec’s submission to the relevant National Competent Authority (“NCA”):



4. Connectivity and Authentication options

4.1 Supported protocols

There are two available supported protocols for connecting to the NUF, although the Trading Venues operators recommend the use of SFTP in almost all cases:

- SFTP Tools/Commands
 - Commands are normally used in scripts for automation e.g. in batch mode.

- SFTP client software such as WINSCP/FileZilla
- HTTPS
 - Normally interactive via an internet browser.
 - Alternatively using command line tools such as “wget” and “curl”.

There are 2 methods of authentication when connecting to the NUF. NEX Markets recommends Key Authentication from both a security and efficiency perspective.

4.1.1 Key Authentication

- The participant supplies a “SSH Public Key” from a pair of keys their IT team creates on their servers. The participant's IT team keeps the Private Key from this pair of keys.
- This guarantees the authenticity of the incoming traffic from a specific server or set of servers (provided the participant protects the Private Key from unauthorised access or copying).
- Keys lend themselves to better scripting and automation of file transfers, so that they can be more easily scheduled and controlled.
- No hard-coded passwords in scripts or credential type files.

4.1.2 Password Authentication

- Participants are able to request a personalised User Name on the NUF Registration Form for production accounts
- NUF User Names must be in the following format:
 - More than 6 and less than 20 characters
 - Only combinations of a-z, A-Z and 0-9 (so no special characters)
- N.B. NUF User Names must be unique across the service and so EASE may need to modify a suggested User Name.
- Upon receipt of a NUF login request, Username will be confirmed and then a password will be issued by email.
- Passwords are more commonly used if the participant wants to connect manually or ad-hoc via an Internet Browser. Any requests to reset password must be made by contacting EASE at EASE@cmegroup.com.

4.1.3 IP Addresses for Firewall Rules

Participants need to allow access from their organisation to the following IP addresses in order to connect to the NUF service via the internet: <https://sftp.nex.com>

	NEX EXTERNAL IP	NEX SFTP FQDN (PORT 22)	HTTPS CONNECTION (PORT 443)
Primary	185.186.5.16	sftp.nex.com	https://sftp.nex.com (Select the Production domain)
Secondary	185.186.5.144		

Secondary sites are available only in the event of a failure in the primary site.

4.2 HTTPS Connectivity Via An Internet Browser

To connect to the NUF using https, use the following URL: <https://sftp.nex.com>. If you're unable to access this page, check with your IT Team to ensure the necessary firewall permissions are in place.

4.2.1 Logging In

You will be prompted for a domain, username and password (See section 3.1 for more information).

- Select the correct **Domain** from the drop down list: *Production*.
- Enter the chosen **Username** from the welcome email.
- Enter the **Password**. (Usernames and Passwords are case sensitive)

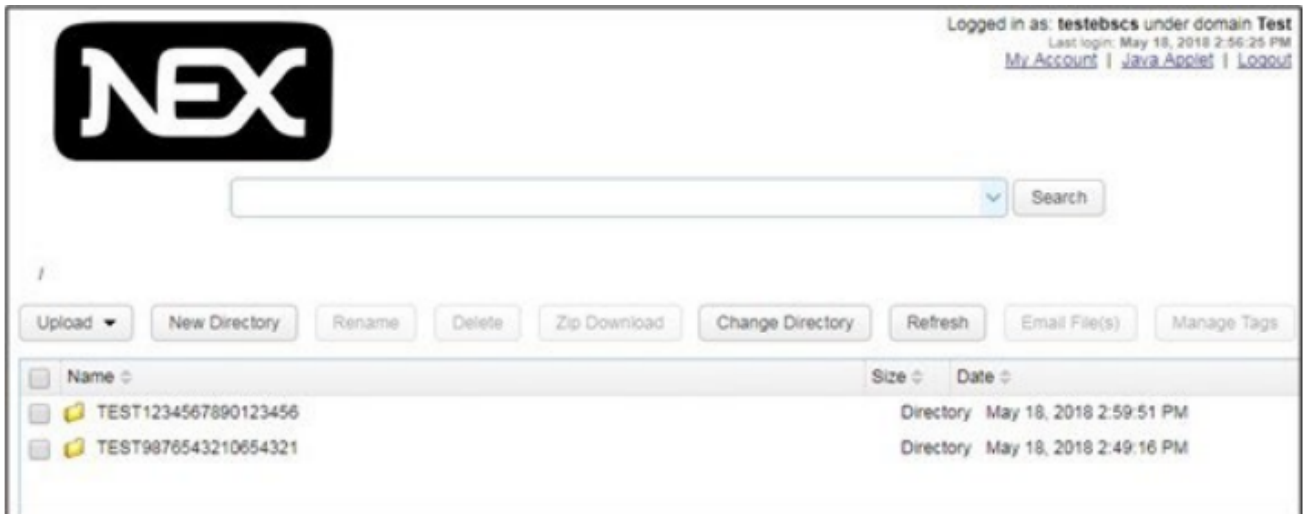


The screenshot shows a web browser window with the address bar containing 'sftp.nex.com/login'. Below the browser is the NEX logo. The main heading is 'JSCAPE MFT Server - Web' with a sub-instruction: 'Enter domain, username and password and click Login.' The login form includes three input fields: 'Domain:*' with a dropdown menu showing 'Production', 'Username:*', and 'Password:'. A 'LOGIN' button is positioned at the bottom right of the form.

Note: Ensure the correct login credentials are used.

After a successful login, the NUF user interface appears, and the secure file transfer process is enabled. If you have issues logging in, please contact EASE at EASE@cmegroup.com.

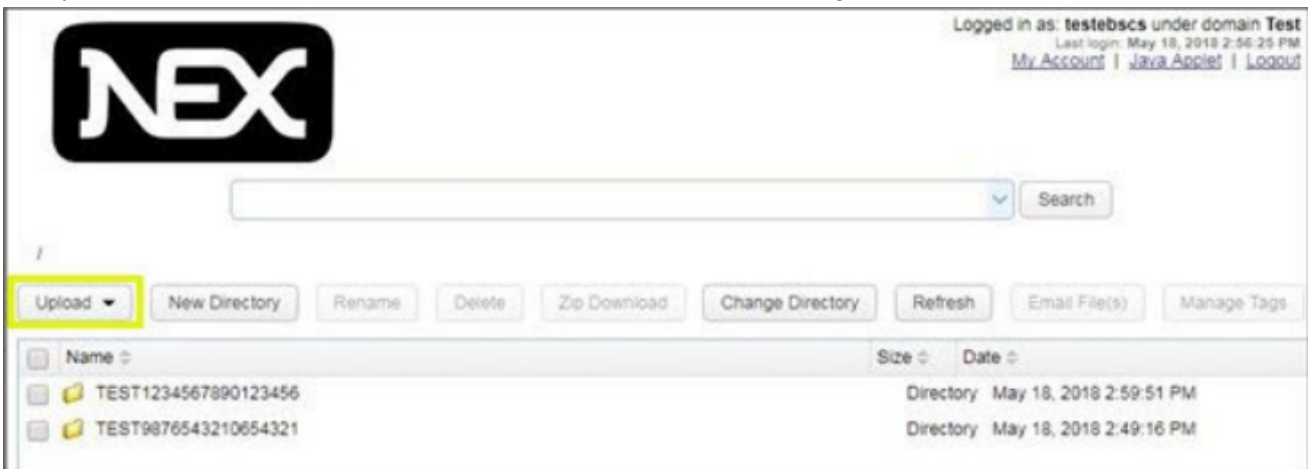
After logging in, the screen shows the contents of the directory to upload trader data files. If you have access to multiple Legal Entities, this directory will contain separate folders for each LEI, identified by the 20-character LEI.



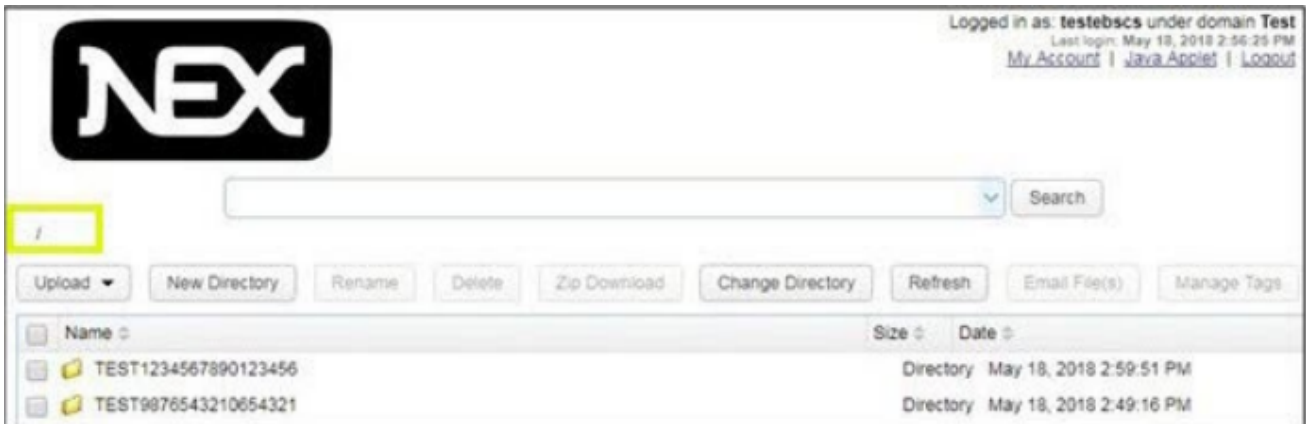
4.2.2 Uploading a file

To upload the EBS Natural Persons / Algo Data trader data file:

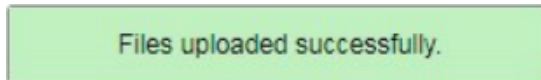
- 1) On the NUF UI screen, select the **Upload** button then navigate to the file.



- 2) If there are multiple folders, ensure the upload of the file to the folder with the LEI corresponding to **Column A (LEI)** of the file; rows with conflicting LEIs will be rejected.
- 3) Select the **backslash** (/, above the upload button), return to the parent folder.



After the file has been uploaded and accepted to the NUF, a confirmation dialog appears.



Note: This dialog does not indicate that all rows have been consumed without errors.

Renaming of files/directories can be done via the **Rename** button after selecting the file. Deleting files can be done via the **Delete** button after selecting the file.

4.2.2 File validation

Submitted files are initially validated syntactically to ensure all mandatory attributes are provided and meet relevant data standards.

Users are notified of the validation results via a response file in the upload directory and an automated email.

NUF Response File: After successfully uploading the .csv file, a response file will be written to the LEI directory in the NUF Portal. Review the results of each submission to ensure no further action is required.



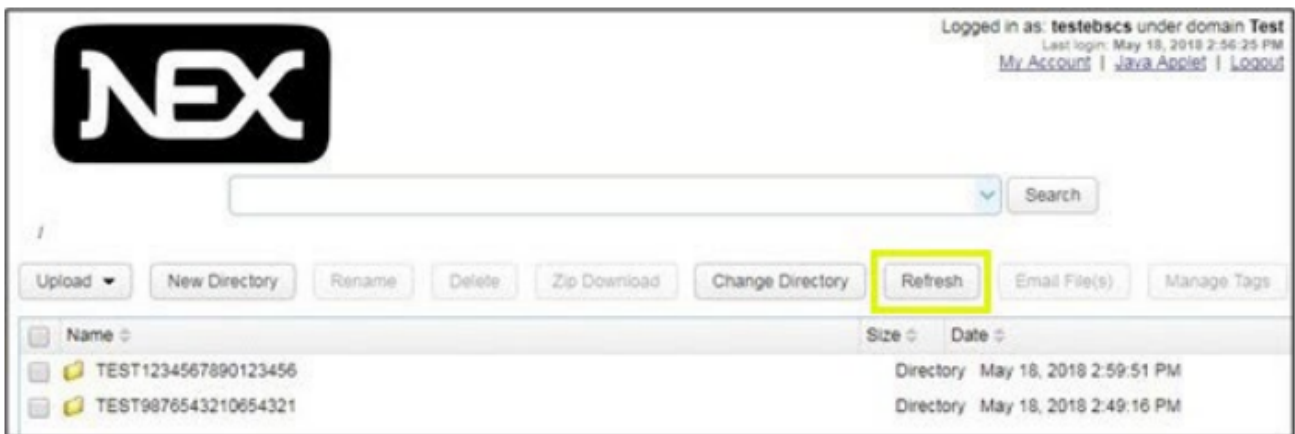
NUF Error Responses:

Error Response	Description
success_[original filename].csv	All rows have been successfully submitted without errors.
error_[original filename].csv	One or more rows contain errors, or the file format is incorrect. Details of the invalid records will be returned in the

	Error Response files with basic troubleshooting guidance. Rows that successfully pass validation will be committed to the NUF data repository.
validation_[original filename].csv	One or more rows require manual validation. Rows that successfully pass validation will be committed to the NUF data repository.

Note: If the response file does not appear after a successful upload, click the **Refresh** button above the upload pane.

Please be informed that files are not actively monitored. In case of "error" or "validation" messages, please contact GCC at gcc@cmegroup.com for any troubleshooting.



NUF Submission Results Email: In addition to the NUF response file, an email communicating the result will be sent to the NUF Admin users at the submitting firm. Where rows have failed validation, a reason will be provided (see example below).

Dear NUF Admin User,

The NUF portal has either partially or fully rejected a Natural Persons/Algo data upload file.

Please see below for results of each submitted record. To view details of the errors in this file, please log into the NUF portal at <https://sftp.nex.com> using your usual credentials.

Submitted details:

Short Code	Accepted/Rejected	Rejection Reason
NGHL123	Rejected	Invalid data in field[NationalIdType] for short code [NGHL123].
NGHL456	Rejected	Please confirm the CONCAT ID value meets ESMA guidelines EXCLUDING the country code from the start. YYYYMMDDXXXXXXXXXX for short code [NGHL456]
NGHL789	Accepted	
15860001	Accepted	

Completion: After the files have been successfully uploaded and appear in the target folder, Click the **Logout** hyperlink on top right of screen to exit the application.



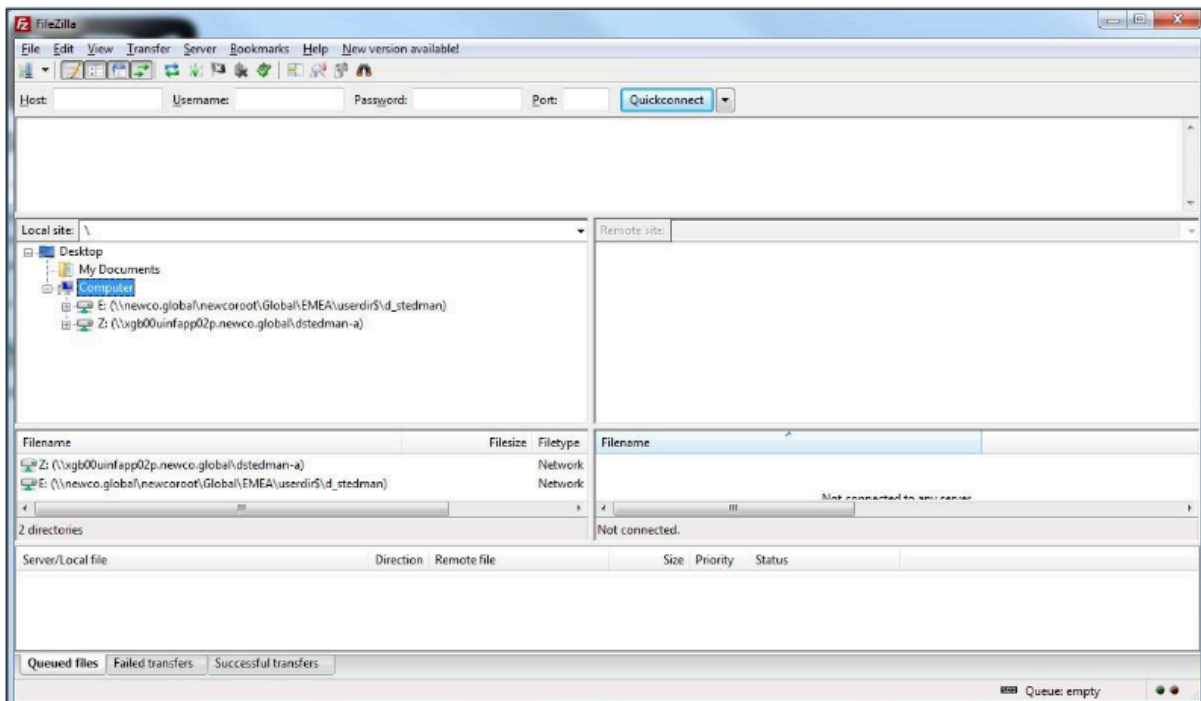
For upload issues or to confirm upload status, contact the **GCC** at gcc@cmegroup.com. If possible, please provide screenshots of any error message.

4.3 Using SFTP to Connect

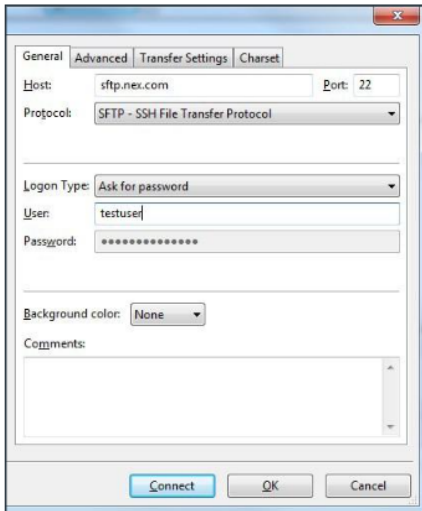
Participants can connect to the NEX SFTP services using client software such as **WinSCP**, or **Filezilla**. These are free SFTP GUI applications which work from the PC and will perform File Transfers using the SFTP protocol.

4.3.1 Configuring Filezilla

Once a participant has installed Filezilla onto its system, the next step is to configure this application to connect to file transfer services.



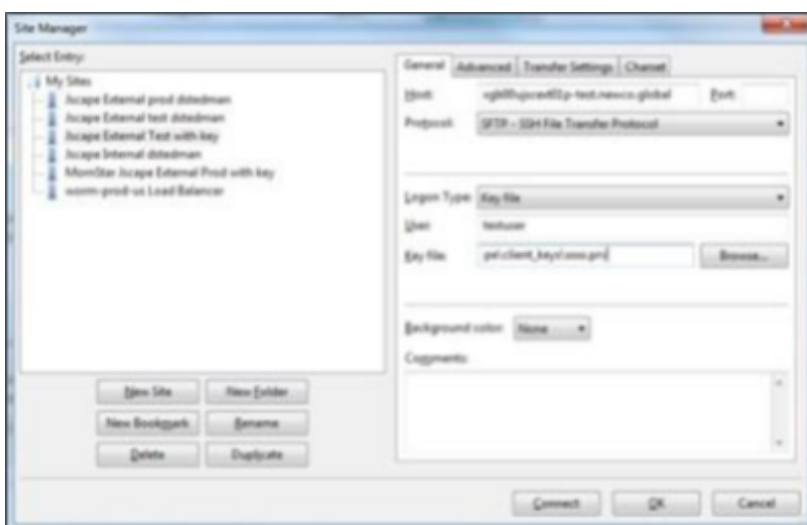
Use File → Site Manager and add the details for the file transfer service that you need to access. Use the “**New Site**” button and fill in the relevant connection details.



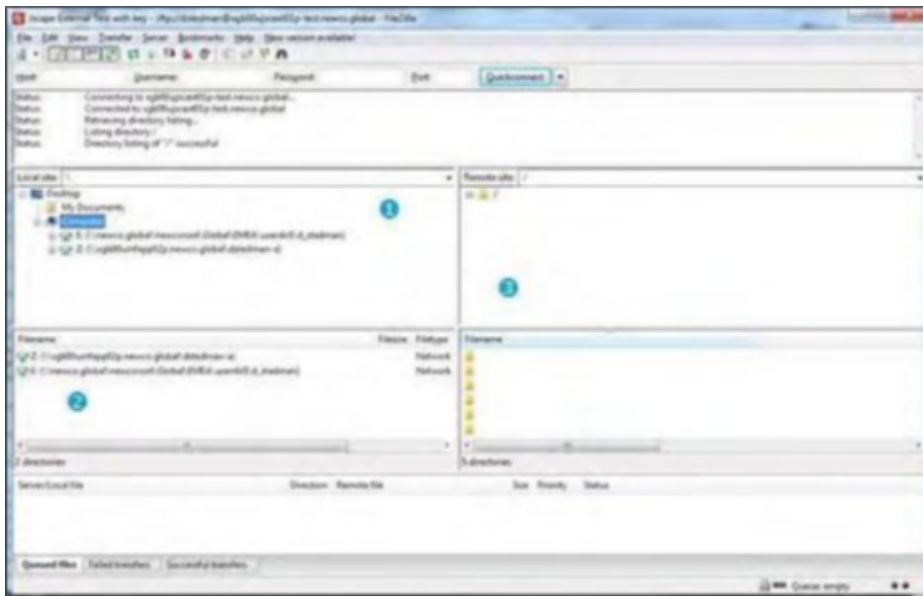
Host:

Source	Product Domain
Internet	http://sftp.nex.com/

- **Username:** Enter the chosen **Username** from the welcome email..
- **Password:** If using Key authentication, you should select “Key file” as the “Logon Type” and supply the “Key file” location. If using Password, input the password from the welcome email. If you do not wish the password to be stored by Filezilla, use “Logon Type” “Ask for password”.
- **Connect:** Then click the “Connect” button to test the connection.
- When the connection has been tested successfully, click the “OK” button to save it. The “Rename” button in the left-hand pane can be used to give the connection a memorable name.
- Once saved in the Site Manager, the “Connect” button can be used to launch the connection when needed again.



Once connected, participants are presented with a split window. The right-hand side of the window displays directories on the SFTP repository, and the left-hand side displays local machine and mount points.



4.3.2 Uploading a File

- Identify the local source directory for MTF/RM participant data.
- Click to highlight the chosen file and then drag it across to the remote destination directory.
- File upload will execute.

SFTP Scripts and Key Authentication

Participants can login and upload files using SFTP/SCP scripting to automate the file upload process. SFTP commands are similar to the older FTP commands.

It is recommended that participants add Key authentication instead of Password authentication to ease connectivity and remove the risks around hard coded passwords within scripts.

Example connection from Linux command line (bold items are typed-in):

Other file transfer clients are available for Linux, such as "lftp", which can also be used for automation and troubleshooting.

4.3.3 SFTP Error Messages

There are several error messages which may be encountered when attempting a file upload using a SFTP/SCP. When reporting any upload issues to GCC, please include screenshots of any error messages that you experience in order to assist with troubleshooting.

Public SSH Key Not Provided/Invalid: If the participant's public SSH key has not been provided to CME and stored in the NUF, then it is only possible to connect using a password. This is an example of

```
<server>:> !sftp <userid>@testsftp.nex.com
Connecting to testsftp.nex.com...
Warning: the RSA host key for 'testsecurefiletransfer.icap.com' differs from the key for the IP address 'xx.xx.xx.xx'
Offending key for IP in /root/.ssh/known_hosts:2044
Matching host key in /root/.ssh/known_hosts:2163
Are you sure you want to continue connecting (yes/no)? yes
<userid>@testsftp.nex.com's password: <password entered>
sftp> dir
Archive external test  sftp>
cd test
sftp> put SQU1664349.pdf
Uploading SQU1664349.pdf to /test/SQU1664349.pdf
SQU1664349.pdf                               100% 16KB 16.4KB/s 00:00  sftp>
dir
91025451.pdf  SQU1664349.pdf
sftp> bye
```

a participant failing to connect in such a case:

```
curl -v -x <PROXY> -U <PROXYLOGIN> --proxytunnel --insecure -u <LOGIN>
sftp://sftp.nex.com/PATH/FILE-2017-09-04.txt.gz
...
MD5 fingerprint: 13ef552196bc87d45180887595186dfb
* SSH authentication methods available: password,publickey
* Using SSH private key file '/opt/eta/.ssh/id_rsa'
0 0 0 0 0 0 0 0 0 --:--:-- 0:00:01 --:--:-- 0* SSH
public key authentication failed: Waiting for publickey USERAUTH response
* Failure connecting to agent * Authentication failure curl: (67) Authentication
failure
```

Attempting to use a Public Key when only password access is enabled (or vice versa): This kind of event can result in messages such as:

```
$ sftp <USER>@sftp.nex.com
Connecting to sftp.nex.com...
Received disconnect from 193.130.196.28: 11: Internal server error.
Couldn't read packet: Connection reset by peer
```

or,

```
"No more authentication methods available"
```

Failure to negotiate Cipher: It is possible that the connecting system and the NUF could not negotiate a mutual encryption cipher for the file transfer, but this is unusual. This will result in messages such as:

```
com.btrade.mft.exception.BtMftRtException: Unable to logon[user: <user>] into target
server [sftp.nex.com:22] via SOCKS proxy [nnn.nnn.nnn.nnn:7,702] because of error:
Failed to negotiate a transport component [hmac-sha2-256,hmac-
sha256,hmacsha256@ssh.com] [hmac-sha1,hmac-md5] [Unknown cause]

Supported ciphers;
Encryption: aes256-cbc
DH key exchange: diffie-hellman-group-exchange-sha256
MAC: hmac-sha2-256
```

or,

```
[deploy@HOST ~]$ sftp -P 22 <USER>@sftp.nex.com
no matching cipher found: client aes256-ctr,aes192-
ctr,aes128ctr,arcfour256,arcfour128 server blowfish-cbc,3des-cbc
Couldn't read packet: Connection reset by peer
```

4.3.4 Sample Commands for Scripting

SCP

```
scp -q -o IdentityFile=$IDFILE -o LogLevel=QUIET $file $USER@$JSC:/
```

Example:

```
scp -o IdentityFile=/admin/test-key.pem -o LogLevel=QUIET file.zip
testuser@sftp.nex.com
```

SFTP batch mode

```
sftp -b $BATCH_FILE $USR@$IP >> $TMPLOG 2>>$TMPLOG
```

Example:

```
sftp -b /admin/batchfile testuser@172.29.1.1 >> /tmp/log 2>> /tmp/log
```

SFTP batchfile

```
cd IN/
! echo "listing remote directory pre file upload"
ls -l
mput NEXFile1* mput NEXFile2*
! echo "listing remote directory post file upload"
ls -l
bye
```

5. Data Flow and Security

Participant data has 3 main lifecycle stages following Connectivity and Authentication:

- Submission and verification
- Database and reporting
- Backup storage and destruction

5.1 Submission and Verification

5.1.1 NUF Over SFTP

Participants can automate submissions to the NUF using the authentication procedure described in section 4.1.1 and may upload files which have been encrypted using PGP/GPG2. These files will be decrypted on receipt at the NUF. The Trading Venues provide a public key in the NUF Admin set-up and we store our equivalent private key in a Key Manager.

The NUF operates on the following PGP Participant compatibility matrix:

Participant	Key Algorithm	Encrypt	Decrypt
-------------	---------------	---------	---------

PGP Desktop 9.x (and above)	DSA ElGamal	Yes	Yes
PGP Desktop 9.x (and above)	RSA	Yes	Yes
GPG 1.4.x (and above)	DSA ElGamal	Yes	Yes
GPG 1.4.x (and above)	RSA	Yes	Yes

Participants will be provided with a dedicated folder to upload their data. The NUF has a file and directory permissioning capability, which is used to ensure that participants can only write to their own data folders. Whilst you cannot access current or past file submissions in your NUF folder, you may access Error Records (see below). Participants may not create additional folders in their NUF data area.

5.1.2 NUF Over HTTPS

Participant Customer administration staff can also access the NUF website at <https://sftp.nex.com> by either following the account opening and key authentication or the password generation procedures described in section 5.1 below. Data transmission to the Trading Venues BrokerTec is encrypted via HTTPS.

5.1.3 NUF IP Blocking

The NUF has been configured to block all connections from an IP address when more than 5 invalid login attempts are detected from that address within 5 minutes.

All IP blocking events are logged so that they can be reviewed by EASE.

5.1.4 Verification (Automatic)

The Trading Venues conduct a basic verification check of the NUF entries, as required under RTS 22, before they are written to any databases. This check takes place in on-premises CME systems and verified records are then added to the participant database (see below). If there are any issues, then the exceptions are returned to the participant's NUF secure folder as an Error Response file along with an email to the participant's Administrator contact.

5.1.5 Verification (Manual)

In some cases, automatic NUF verification may require additional manual intervention from our participant Onboarding team. They have controlled, role-based access to relevant systems and will contact participants to remedy any issues.

5.2 Database

5.2.1 Participant Database

As stated above, verified participant's data is written to the participant database in on-premises CME systems. Access to our systems is penetration tested by a CHECK accredited third party on an

at least annual basis. We commit to remediate any resultant issues within 60 days and inform any affected parties of potential risk exposures. Additionally, CME runs a “test the testers” protocol and rotates penetration test providers. Data storage complies with ISO 27001 standards.

5.2.2 Operating System Patching

The NUF will be subject to regular operating system patching. The minimum requirement is to patch “Urgent” and “Critical” security vulnerabilities, as identified by the security scanning tool operated by CME.

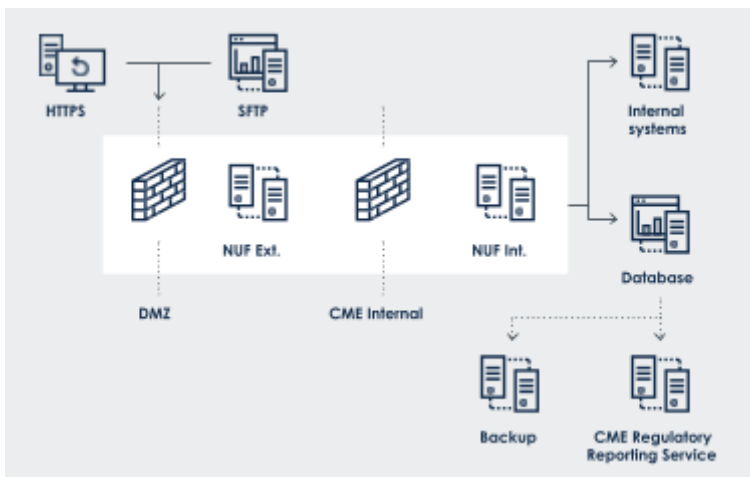
5.2.3 General Security Protocols

CME is a FS-ISAC member and subscribes to other specialist bodies for Advanced Threat warnings. CME also regularly runs internal and external scans against their services to determine if there are known exploits or vulnerabilities. Remedial action is taken as necessary based upon the results of the scans.

5.2 Backup Storage and Destruction

Transactions and participant’s data is encrypted and stored for backup purposes in an encrypted state (to the FIPS US government security standard). We store this data for five years, as per RTS 24 record maintenance and local NCA regulatory obligations, after which time the data auto-expires.

5.4 NUF Network Topography



5.5 Participant Data Handling Disclaimer

The following applies to the use by the Trading Venues of the PII data provided in the NUF relating to the individuals named in it.

The Trading Venues collect and use the PII data for the purposes of compliance with its legal obligations, including under MiFID II and MiFIR.



The legal basis for the Trading Venues's collection and use of the personal information is that it is necessary for compliance with legal obligations. Provision of the information is, therefore, mandatory, and the Trading Venues may not be able to treat an individual as authorised to represent the participant if the information is not provided. The Trading Venues also also have a legitimate interest in collecting and using the personal information for legal compliance purposes and in order to provide and manage services for its participants.

All personal information provided under this process will be used, distributed, and maintained in accordance with **CME Group's Privacy Notice** (<http://www.cmegroup.com/privacy-policy.html>). If completing this process on behalf of another individual, you will ensure that you have the required consent from those individuals to whom the personal information relates, or you satisfy an applicable legal basis for doing so, in compliance with all applicable laws, to enable CME Group to process such personal information.

The Trading Venues may share the information provided in the NUF with other members of its group of companies, with NCAs and other regulatory and governmental authorities and with its service providers holding and processing the information on its behalf. Some of these disclosures may involve transfers of PII data to countries outside the European Economic Area, including countries which are not regarded as ensuring an adequate level of protection for information under applicable laws (such as those in the European Union). We put in place appropriate procedures and safeguards in accordance with applicable legal requirements when conducting such transfers. If you have any comments, questions or concerns about how we process your data, please contact **Privacy Compliance** at Privacy@cmegroup.com.

The PII data provided in the NUF will be retained for as long as the relevant individual remains authorised to represent the participant before the Trading Venues or where required, in accordance with the internal records management and retention policies, as well as regulatory requirements such as MiFID II and MIFIR that may be applicable to us.

6. Contact Us

Please use one of the following methods to contact Global Command Center:

Email: gcc@cmegroup.com	Telephone: USA: +1 800 438 8616 Europe: +44 20 7623 4747 Asia: +65 6532 5010
--	---

