

Document title

CLEARING CONNECTIVITY

Document type or subject

TECHNICAL OVERVIEW

Revision number

Revision Number: 1.2

Date

March 2023

Number of pages

44

Author

Euronext Clearing

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext's subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext.

Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at euronext.com/terms-use.

©2023, Euronext N.V. - All rights reserved.

Preface

PURPOSE

The purpose of this document is to describe and address the actions that must be undertaken by Euronext Clearing and all participants to establish a communication between Members' infrastructure and the Clearing System through distinct channels and protocols.

This document mainly refers to the testing environment (EUA) of the Clearing System. Details on how to access the production environment will be provided in a future release of this document, to be published in due course.

Dedicated annex for Client Credential UI user guide will be delivered according with external test timeline.

TARGET AUDIENCE

All Euronext clients that will adopt Euronext Clearing as their clearing house.

WHAT'S NEW?

The following lists only the most recent modification made to this revision/version. For the Document History table, see the Appendix.

REVISION NO./ VERSION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
1.2	3 March 2023	Euronext Clearing	EUA FQDN change (removing "uat" preferring "eua"); public IP adjustment

ASSOCIATED DOCUMENTS

The following lists the associated documents that either should be read in conjunction with this document or which provide other relevant information for the user:

- Euronext Clearing Interfaces Technical Specifications v 2.0
- Euronext Clearing Application Programming Interfaces Specifications v 2.0

Contents

1. RESOURCE AND ARCHITECTURE	4
1.1 Definition of acronyms	4
1.1.1 Processes and applications in the perimeter.....	5
2. CLEARING OVER INTERNET	6
2.1.1 Public access security	7
2.1.2 Endpoints EUA	9
3. USER ONBOARDING.....	10
3.1 Client Credentials functionalities	11
3.2 Certificate management and PKI.....	12
4. ACCESS PROCEDURE	13
4.1 Clearing System UI.....	13
4.1.1 Account creation	14
4.1.2 MFA.....	16
4.2 API	20
4.3 SFTP	20
4.3.1 Keys preparation.....	21
4.3.2 Keys sharing methods	24
4.3.3 Technical EUA endpoint.....	25
4.4 FIX	26
4.4.1 FIX resend request.....	28
4.4.2 FIX over TLS	28
4.4.3 FIX SERVER ENGINE Configuration File	29
4.4.4 FIX MEMBER Configuration File	30

1. RESOURCE AND ARCHITECTURE

Euronext Clearing's technological infrastructure is based on enterprise-class systems, which are redundant and provide geographical distribution of the databases, in line with information classification standard methodologies. This is possible through the use of high-performance storage systems, specific tools for the duplication of information and diversified backups. In this way the critical data for core services are always aligned between the two data centres (DCs), both located in Italy.

The two DCs are connected via dedicated lines, which are also redundant.

In the case of a disaster event affecting the Primary Data Centre (PDC), clients' connectivity to Clearing services will not be impacted in terms of endpoint configuration, since all requests are received by a Global Load Balancer that dispatches them internally.

Note that Euronext Clearing's technological infrastructure is not the same as the technological infrastructure of Euronext Exchanges.

Euronext Clearing guarantees a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in line with the European Regulatory directives.

1.1 Definition of acronyms

UI	User Interface
IdP	Identity Provider
SFTP	Secure File Transfer Protocol
FIX	Financial Information eXchange
API	Application Programming Interface
X.509	Digital certificates
PKI	Public key infrastructure
SPA	Single page application
OTP	One-time password
MFA	Multi-factor authentication
CDN	Content delivery network
PDC	Primary Data Centre
SDC	Secondary Data Centre
CSR	Certificate Signing Request

1.1.1 Processes and applications in the perimeter

Find below the list of features grouped by platform and applications:

Function	Platform	Applications	RTO	Process	Criticality
User Interface (U2A)	Containers	SPA	< 2 hours	Data visualisation (referential, clearing, settlement, collateral, risk data) Interaction with clearing system	1
Machine to machine (A2A)	Containers	API server	< 2 hours	Data retrieval (referential, clearing, settlement, collateral, risk data) Interaction with clearing system	1
Reports download	Virtual server	SFTP server	< 4 hours	Data retrieval (referential, clearing, settlement, collateral, risk data)	2
Trades acknowledgement	Containers	FIX engine	< 2 hours	Drop copy sent to members	1

2. CLEARING OVER INTERNET

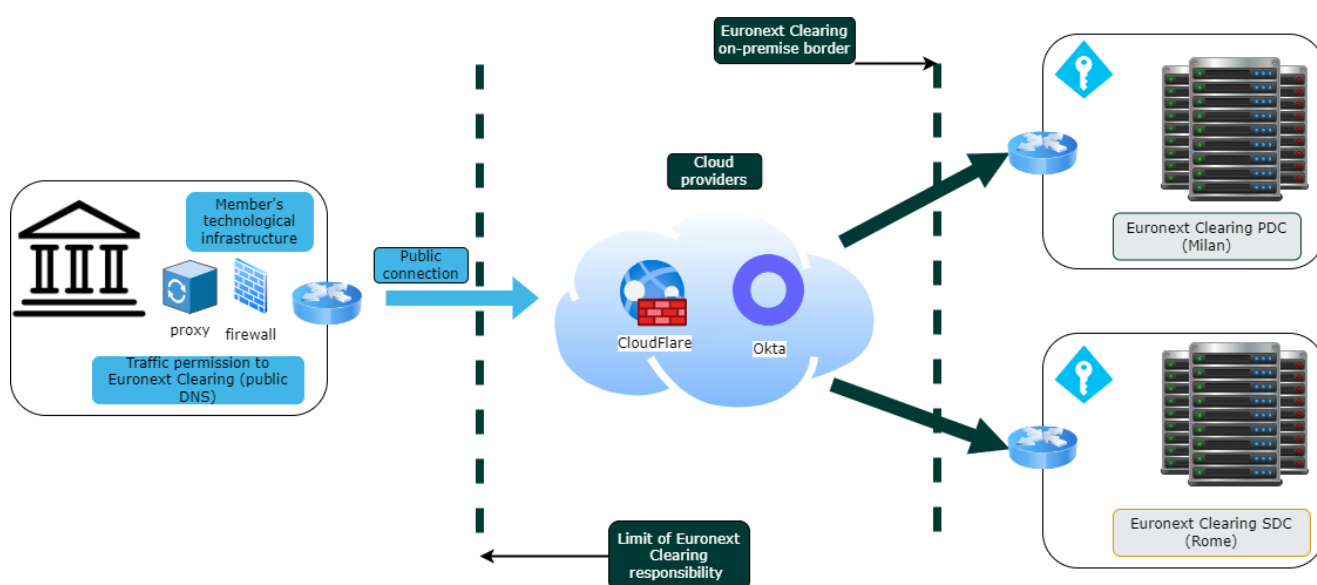
This section aims to explain how public connectivity can facilitate plug-in and onboarding for Members.

The services offered by Euronext Clearing are accessible over the Internet (no leased lines or network service providers are needed) and are deployed on private infrastructure. The connections to Euronext Clearing's own data centres guarantee high and strong levels of protection, integrity and availability of member information, through private leased lines between the CDN cloud provider and the on-premise infrastructure.

Members' choice in terms of bandwidth and throughput is therefore the responsibility of each Member and is not the responsibility of Euronext Clearing. Sizing should be determined according to the Member's internal requirements, constraints, policies and estimated traffic. Since post-trading operations are not affected by latency (typically considered as a critical factor during trading phases), the minimum bandwidth requirement is 4 Mbps.

All solutions provide encrypted data transfers between Members and Euronext Clearing systems in order to guarantee security and confidentiality.

The Member may permit traffic on its own boundary firewalls or proxies in order to reach the public DNS allocated by Euronext Clearing services.



Public connectivity allows access to:

- API solution, access to Clearing System from client applications
 - Clearing System UI solution, access to Clearing System Web Interface
 - Client Credentials UI solution, access to Admin Interface
 - FIX solution, access to Euronext Clearing FIX engine
-
- SFTP solution, access to member folders to download files (Pull) from the Euronext Clearing server
 - Euronext Clearing official website
 - Euronext Clearing Member Portal

Features of Euronext Clearing Internet connectivity

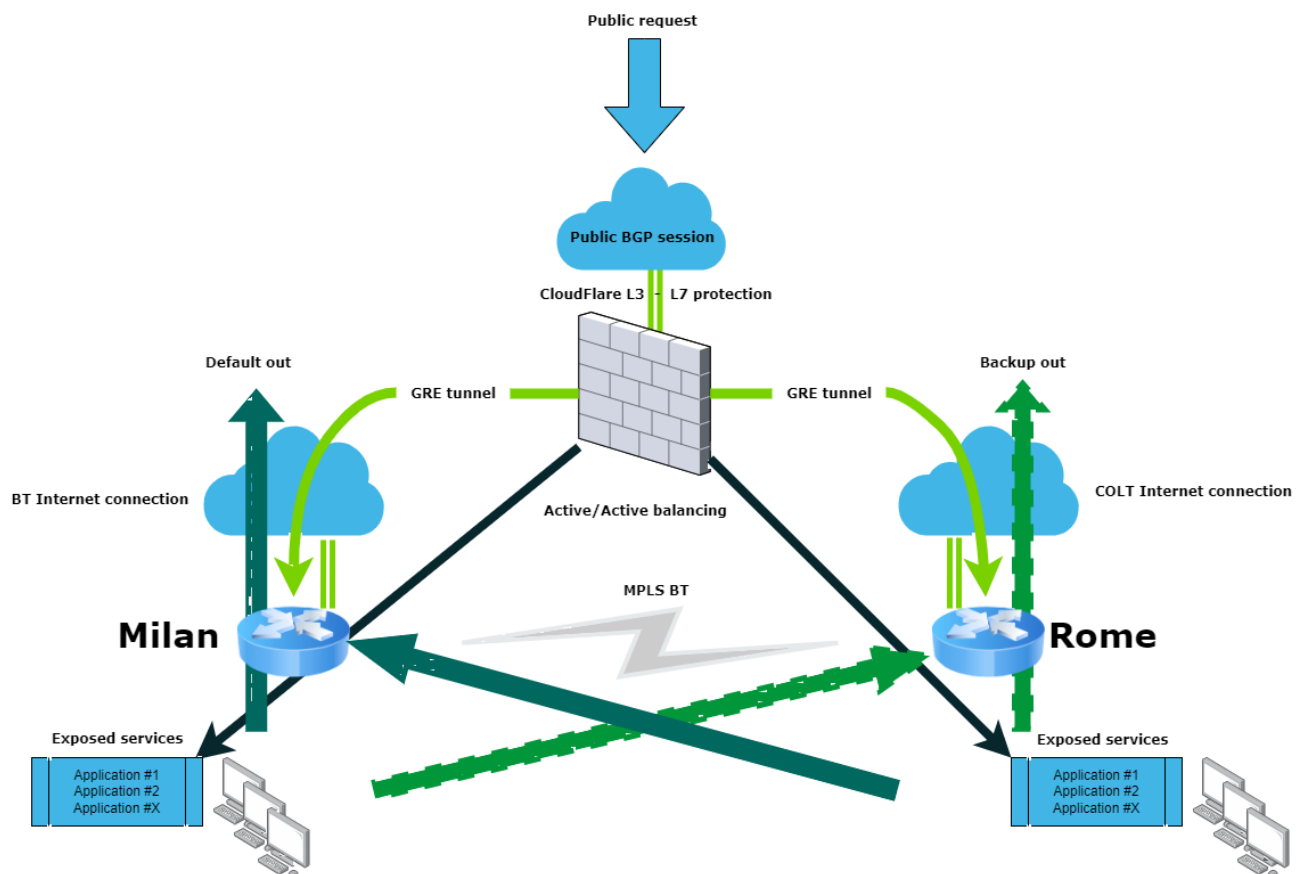
- Allows automation of files downloading and processing
- Easy to implement (Internet)
- Straight Through Processing solution to the Member's information system

Security, integrity and confidentiality are guaranteed by encryption (GRE tunnel) and external IP address filtering.

2.1.1 Public access security

In order to meet Euronext Group security standards, Euronext Clearing has implemented all best practices established in the internal Group's policies and external regulatory entities:

- Multifactor authentication is managed by an Identity Provider in order to facilitate credentials rotation, Secrets protection and prevent violations.
- Zero Trust approach requiring all users, outside and inside the Euronext Clearing network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted access or maintaining access to applications and data.
- Implementation and use of x.509 Digital Certificates to support the new Clearing system through a mutual authentication mechanism, applicable to all four available access points (UI, API, SFTP, FIX).
- Unmetered DDoS protection and Web Application Firewall that stop the most advanced attacks for APIs and Website.
- Throttling that reduces the risk of disruptive events and prevents malicious attacks that aim at overflowing the systems.



Internet connectivity on the Member side is not provided by Euronext Clearing; Members must subscribe to an Internet connection by their own means.

2.1.2 Endpoints EUA

Below the summary of FQDN and IP for services exposure.

Please note that using static IP is not best practice and should be avoided, especially for future production environments (PDC vs SDC).

Channel	FQDN	IP address	IP port
UI	wcsui-eua.clearing.euronext.com	Dynamic*	443
API	wcsapi-eua.clearing.euronext.com	Dynamic*	443
SFTP	data-eua.clearing.euronext.com	212.239.86.13	22
FIX	wcsfixe-eua.clearing.euronext.com	212.239.86.14	7001

*public addresses are managed and proxied by CloudFlare CDN depending on fast delivery of Internet content by geography ([IP Ranges | Cloudflare](#))

3. USER ONBOARDING

In order to be able to connect to the Clearing System, each Member must submit a formal membership request for connectivity, that will be validated and approved by the Euronext Clearing Membership Team. The Euronext Clearing Membership Team is responsible for service activation or deactivation throughout the duration of the contract between the Member and the CCP.

The formal connectivity request must be submitted to the Euronext Clearing Membership team through the Member Portal (<https://memberportal.ccg.it>). Details on how to access the Member Portal and the information to be sent to the CCP will be provided in a dedicated Membership document.

The form can contain request access for the following purposes:

- Clearing System UI access for business users (mandatory).
- Client Credentials access for technical users (optional). This type of user is needed only if the Member wants to include FIX, SFTP and API in post-trade operations. From the Client Credentials UI, the Client's technical user can generate by itself the client credentials for machine-to-machine access.

The following table summarises the actions that Members must perform to obtain access credentials for each desired channel.

	Member Portal	Client Credential UI
Clearing System UI (mandatory)	Request new users: the Member must specify the list of usernames. ID creation is managed by Euronext Clearing IT.	No action required
Client Credentials UI (optional)	Request new users: the Member must specify the list of usernames. ID creation is managed by Euronext Clearing IT.	No action required
SFTP (optional)	Request new users: the Member must specify the number of accounts. ID creation is managed by Euronext Clearing IT.	Upload SSH public keys: technical users can upload public keys for SFTP authentication. Euronext Clearing IT is in charge of moving those keys onto the server side .

API (optional)	Specify number of credentials: the member must specify the desired number of credentials that will be managed autonomously from the Client Credential UI by the technical users.	Manage credentials: the technical users can create or revoke credentials and manage x.509 client digital certificates.
FIX (optional)	Specify number of credentials: the member must specify the desired number of credentials that will be managed autonomously from the Client Credential UI by the technical users.	Manage credentials: the technical users can create or revoke credentials and manage x.509 client digital certificates

3.1 Client Credentials functionalities

Please note that access to this Interface is reserved for technical users from the client's organisation only.

From this User Interface, the technical user can do the following:

- Request and manage Client Credentials for API access and FIX. The user will receive a pair of Client IDs and Secret that will be used for machine-to-machine access. Please refer to the "Euronext Clearing Application Programming Interfaces Specifications v 2.0" document for further details.
- Request x.509 Certificate for Mutual TLS on API and FIX. The certificate must be installed in a trust store file that will be used by the client application.
- Upload the public key generated on Client's side for SFTP. This key will be used by IT Clearing staff and loaded in the SFTP server for authentication purpose.

A quick user guide can be found in a dedicated annex B to this document.

3.2 Certificate management and PKI

Euronext Clearing adopts an Enterprise PKI Manager to protect users, servers and systems.

The certificates' lifecycle can be managed in the Client Credentials UI. The technical user will be able to create, activate, suspend or revoke certificates, along with the client credentials associated with the certificates.

The Client's technical user must be responsible for storing the certificate in a trust store file that will be used by the client application each time the certificate is created or renewed. The complete flow of the certificates' lifecycle will be described in a dedicated annex to this document.

The lifecycle of the certificates comprehends:

- Creation
- Activation
- Revocation
- Suspension
- Renewal

For more details of each of the lifecycle phases, please refer to the Appendix A: Certificate Management and PKI.

4. ACCESS PROCEDURE

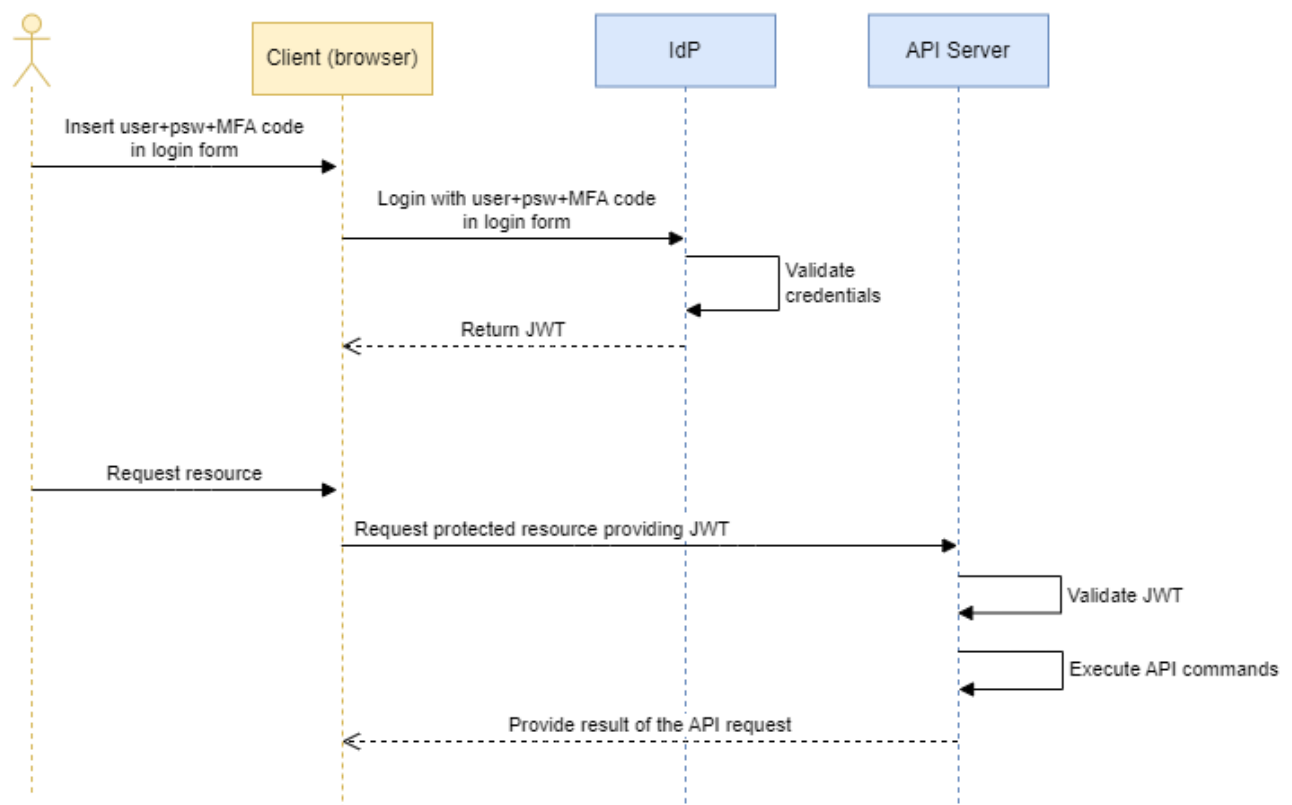
4.1 Clearing System UI

Mandatory channel

The Web Clearing System is a SPA (Single Page Application) written following standard framework and available via the most commonly used internet browsers:

- Firefox >= 96.0.1
- Chrome >= 97.0.4692
- Edge >= 97.0.1072
- Safari >= 15.6.1

The following sections (4.1.1 and 4.1.2) are valid for both the Clearing System UI and the Client Credentials UI and explain how to create accounts for User Interface access. The following diagram represents the overall authentication process executed at each login request.



4.1.1 Account creation

After the Client's Representative has requested the account creation via the Member Portal (please refer to Chapter 3 for more details), the Euronext Clearing IT team will create the accounts.

Once the accounts have been created, the IdP will send an auto-logon form to the email address provided by the Client's Representative.

The user will receive a registration email from [Okta](#), the IdP adopted by Euronext Clearing. The sender will be noreply@okta.com and the body of the message will contain an invitation to complete the registration. Below is an example of the message that the user will receive:

Welcome to Okta!



Okta <noreply@okta.com>
To ●



If there are problems with how this message is displayed, click here to view it in a web browser.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



euronextclearing - Welcome to Okta!

Hi

Your organization is using Okta to manage your web applications. This means you can conveniently access all the applications you normally use, through a single, secure home page. Watch this short video to learn more: <https://www.okta.com/intro-to-okta/>

Your system administrator has created an Okta user account for you.
Click the following link to activate your Okta account:

[Activate Okta Account](#)

This link expires in 7 days.

4.1.2 MFA

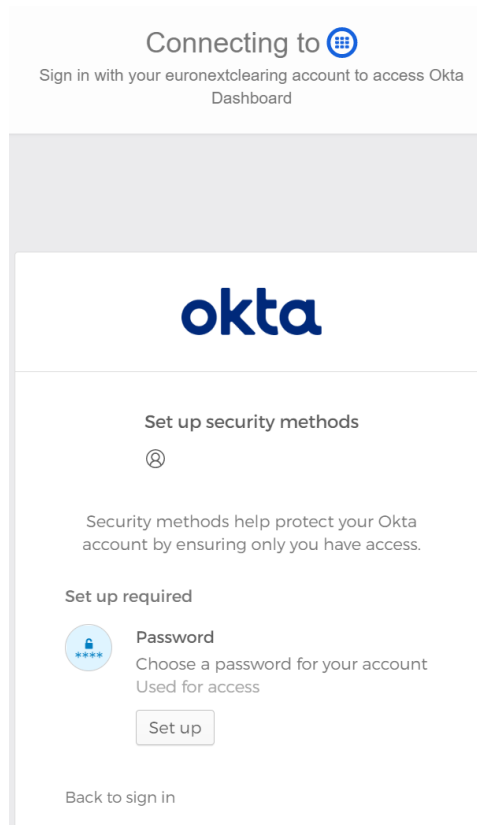
Access to the new Euronext Clearing system web interface is secured not only through the use of basic credentials, but also adopting dual factor authentication.


In order to use dual factor authentication, the user has two options:

1. Install and configure the **Okta Verify** application on the preferred device owned by the user, as explained in the following guide: [Okta Verify | Okta](#)
2. Receive the token via **SMS**. Please note that this option is preferred if the user does not have an available device on which to install the Okta Verify Application.

By clicking the activation link received by email as shown above, the user will be redirected to an online wizard where they must perform the following actions:

- 1) Set a password




Connecting to 

Sign in with your euronextclearing account to access Okta Dashboard


okta

Set up security methods






Security methods help protect your Okta account by ensuring only you have access.

Set up required

 **Password**
Choose a password for your account
Used for access

[Back to sign in](#)



Set up password

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Your password cannot be any of your last 12 passwords
- At least 1 day(s) must have elapsed since you last changed your password


Enter password

Re-enter password


Next
[Return to authenticator list](#)
[Back to sign in](#)

- Please note that the password policies shown above are temporary and will be enhanced and reinforced in the near future before they are implemented.


2) Select **Okta Verify** as a security method:

Connecting to 

Sign in with your euronextclearing account to access Okta Dashboard




Set up security methods




Security methods help protect your Okta account by ensuring only you have access.

Set up optional



Okta Verify
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Used for access

Set up



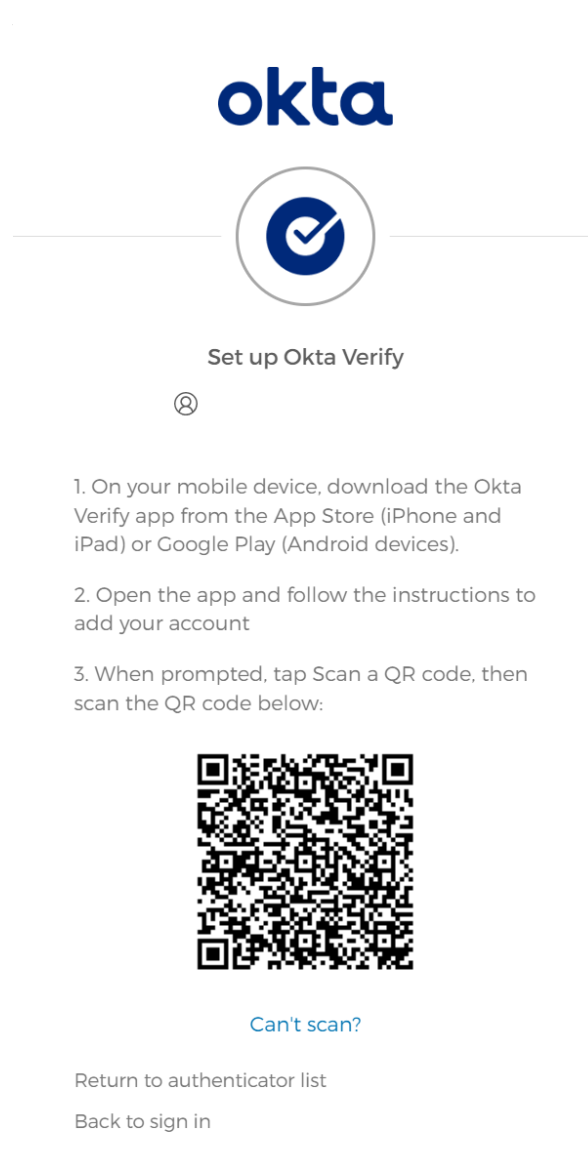
Phone
Verify with a code sent to your phone
Used for access

Set up

Set up later

[Back to sign in](#)

3) Scan QR code displayed



After scanning the code, the Okta Verify Application will display a short-lived token associated to Euronext Clearing. The OTP token will be required at each login to the Euronext Clearing System UI or Client Credentials UI.

The user can now log into the Euronext Clearing System UI or Client Credentials UI simply by typing the provided URL into a browser:

<https://wcsui-eua.clearing.euronext.com>

Testing can now start.

4.2 API

Optional channel

API is a method to interact with Euronext Clearing using machine-to-machine interfaces. For this specific area, Euronext Clearing strengthened authentication by adding mutual TLS constraints. Hosts that need to consume APIs can do this using a temporary JWT token in addition to the client x.509 digital certificate installed in a trust store repository.

Access to the new Euronext Clearing via API is permitted only using a JWT token requested via authentication to the IdP with the client credentials. Additionally, the IdP will require a client certificate installed into the advised host or machine. It is assumed that the participant has downloaded and installed the certificate, as explained in section A.1.1.

No direct interaction between member and IdP is required: the authentication phases will be managed through specific API supplied by Euronext Clearing.

Please refer to the document "Euronext Clearing Application Programming Interfaces Specifications v 2.0" for further details on how to interact with the APIs.

4.3 SFTP

Optional channel

In order to automatically fetch clearing reports, an SFTP server is available at Euronext Clearing. The member must generate a set of private/public keys following a standard procedure.

SFTP (which stands for FTP over SSH) is a secure FTP protocol that transmits files over secure shell (SSH). SSH gives SFTP extra security because it provides organisations with a high level of protection for their file transfers. SFTP also implements AES, Triple DES, and similar algorithms to encrypt the files that transfer between systems.

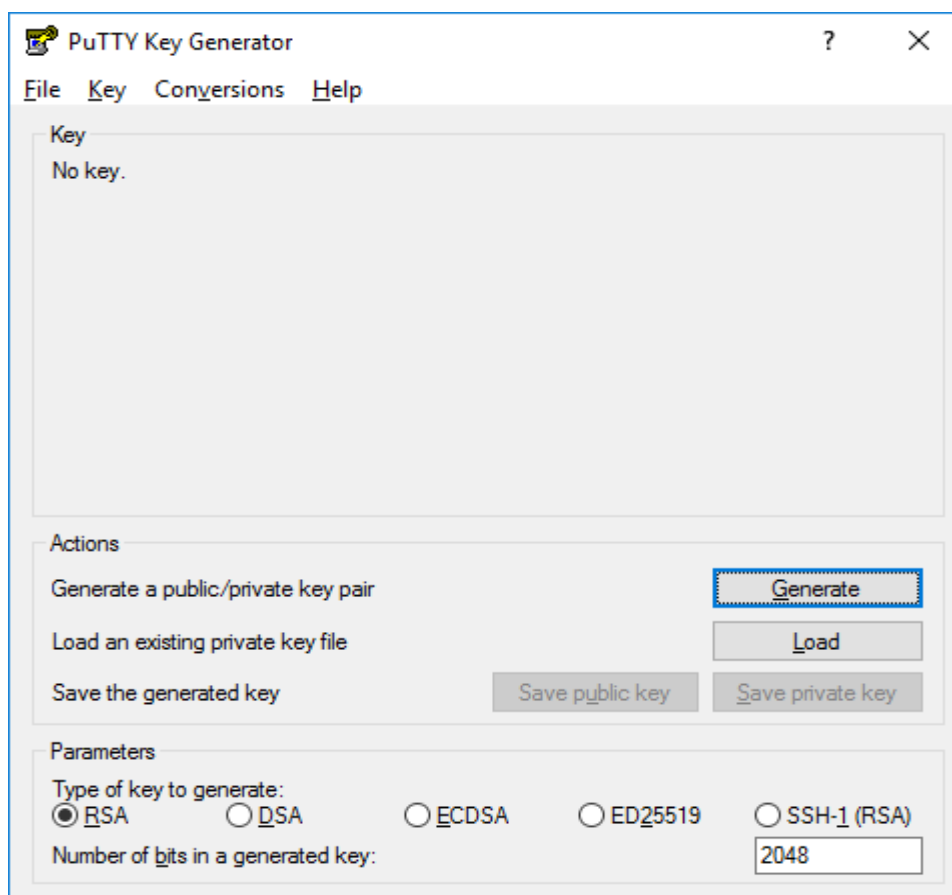
For authentication, SFTP users have several choices. They can test a connection with a user ID and password, an SSH key, or a combination of a password and SSH key. This is highly beneficial for organisations that need to implement stronger security measures around their file transfer processes and user access.

4.3.1 Keys preparation

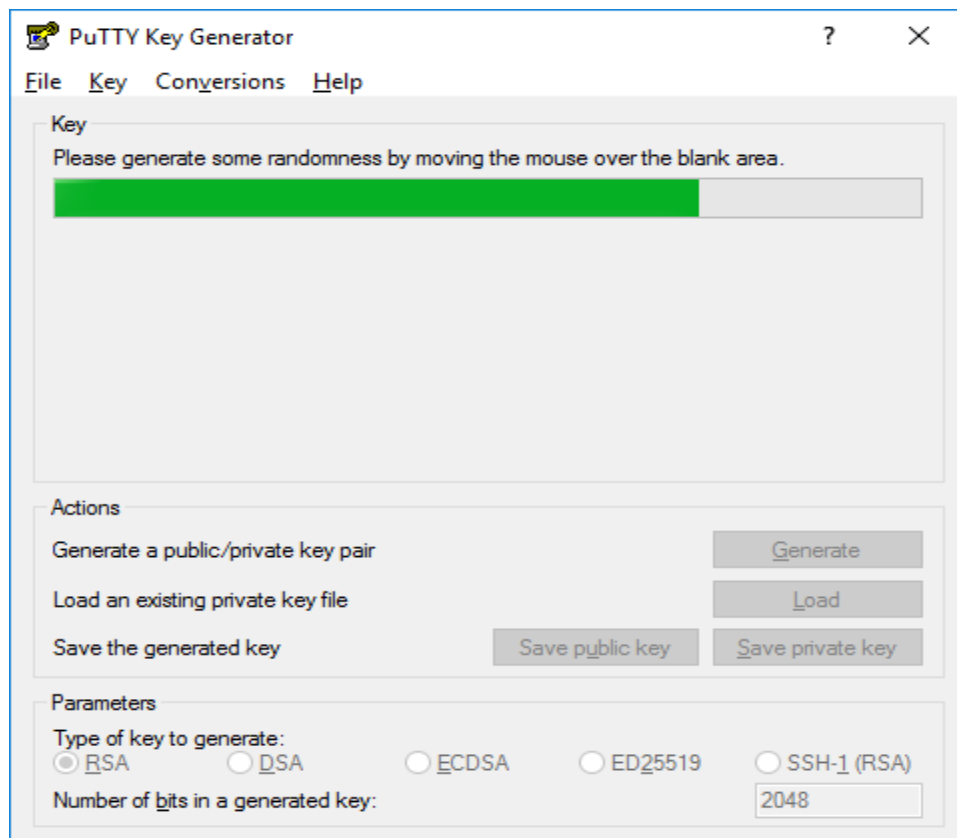
To generate public/private key pairs for SFTP, please follow the steps detailed in the sections below.

4.3.1.1 GUI

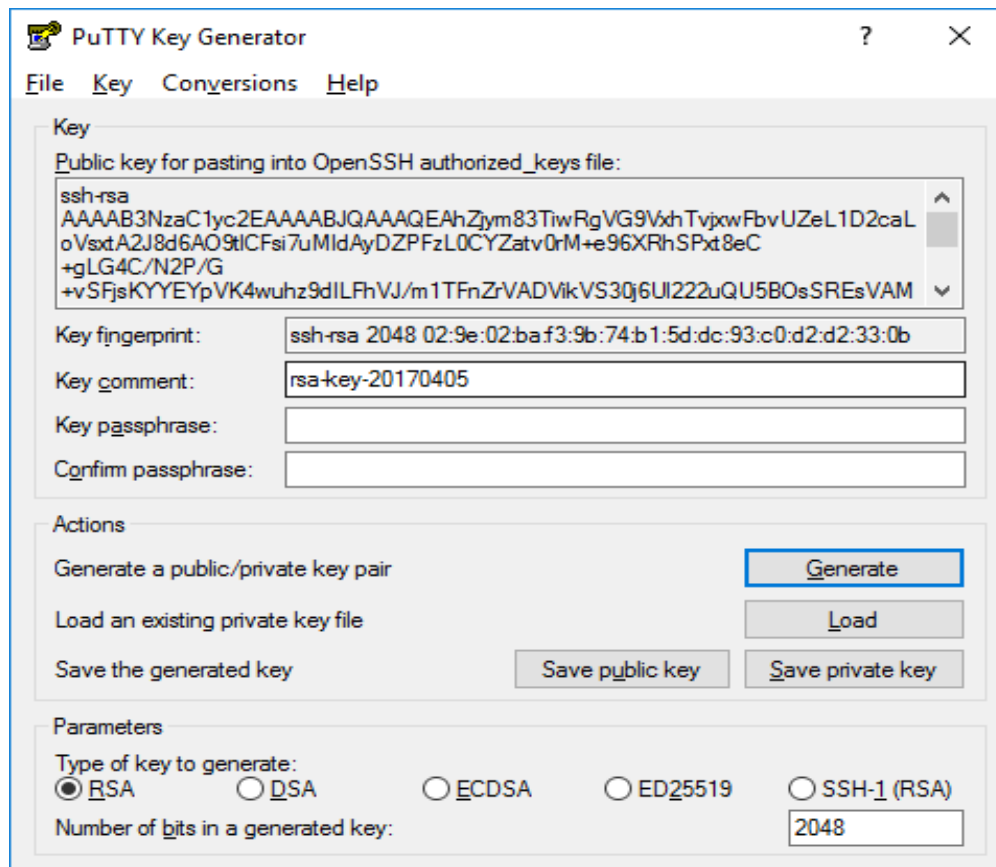
The user should install the PuTTY Key Generator, navigate to the PuTTYgen directory, and launch it. The default directory path is C:\Program Files (x86)\PuTTY\puttygen.exe.



1. To create a new key pair, select the type of key to generate from the bottom of the screen.
(Note: using SSH-2 RSA with 2048 bit key size works well for most users; another well-known alternative is ECDSA).
2. Click **Generate**, and begin to move the mouse within the Window. Putty uses mouse movements to collect randomness, as the exact way that the user moves their mouse cannot be predicted by an external attacker.
The user may need to move the mouse for some time, depending on the size of the key. As the mouse is moved, the green progress bar should advance, as shown in the image below:



3. Once the progress bar is full, the key generation computation takes place. This may take from several seconds to several minutes. When complete, the public key should appear in the Window. The user can now specify a passphrase for the key.
4. The user should save at least the private key by clicking **Save private key**. It may be advisable to also save the public key, though this can be regenerated later by loading the private key (by clicking **Load**). The outcome of the procedure should be as shown in the image below:



4.3.1.2 Command line

Ssh-keygen is a tool for creating new authentication key pairs for SSH.

The simplest way to generate a key pair is to run ssh-keygen without arguments. In this case, it will prompt for the file in which to store keys. See an example below:

```
klar (11:39) ~>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ylo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): Enter same passphrase again:
Your identification has been saved in /home/ylo/.ssh/id_rsa.
Your public key has been saved in /home/ylo/.ssh/id_rsa.pub.
The key fingerprint is: SHA256:Up6KjbnEV4Hgfo75YM393QdQsK3Z0aTNBz0DoirrW+c
ylo@klar
```

First, the tool asks where to save the file. SSH keys for user authentication are usually stored in the user's .ssh directory under the home directory. However, in enterprise environments, the location is often different.

Then, it asks the user to enter a passphrase. The passphrase is used for encrypting the key, so that it cannot be used even if someone obtains the private key file. The passphrase should be cryptographically strong.

Choosing an Algorithm and Key Size

SSH supports several public key algorithms for authentication keys. These include:

- `rsa` – an established algorithm based on the difficulty of factoring large numbers. A key size of at least 2048 bits is recommended for RSA; 4096 bits is better. However, note that RSA is aging and significant advances are being made in factoring. Choosing a different algorithm may be advisable.
- `ecdsa` – a new Digital Signature Algorithm standardised by the US government, using elliptic curves. This is probably a good algorithm for the current applications. Only three key sizes are supported: 256, 384, and 521 (sic) bits. 521 bits is the most widely recommended key size, since this is probably more secure than the smaller keys.

The algorithm is selected using the `-t` option and key size using the `-b` option. The following commands illustrate:

```
ssh-keygen -t rsa -b 4096
ssh-keygen -t ecdsa -b 521
```

Specifying the File Name

Normally, the tool prompts for the file in which to store the key. However, it can also be specified on the command line using the `-f <filename>` option.

```
ssh-keygen -f ~/tatu-key-ecdsa -t ecdsa -b 521
```

4.3.2 Keys sharing methods

The client should send the public key only to Euronext Clearing using one of the suggested methods:

- `https`: through the dedicated area in the Client Credentials UI. This is the preferred solution for the Production environment.
- `email`: less secure and hence suggested for the test environment only.

4.3.3 Technical EUA endpoint

- Server EUA IP: **212.239.86.13**
- URL: **sftp://data-eua.clearing.euronext.com**
- Prod/EUA environments are distinguished by userid and by IP
- The EUA service is provided via FQDN **data-eua.clearing.euronext.com**
- The service is hosted on two servers: primary and secondary. The IP of the FQDN may change accordingly on DNS
- Test the connection to both the IP addresses to be ready in case of IP change on DNS
- Verify that the IP change does not block your procedure (ie: IP spoofing error)
- Accept the keys from both the Primary and Secondary server to avoid "key warning" in case of a switch (mandatory for PROD service)
- Only authorised IPs can connect to the SFTP service (IPs should be provided by the Member)
- The connection is secured by ssh key. The member should provide the public part (name+password login method is not supported)
- Only the userid "owner" can request source IP or key updates
- Files are available in the directory called "data".
- Report name will contain a prefix to distinguish files (test vs prod)

An example of command to manually connect is:

```
sftp USERID@data-eua.clearing.euronext.com -i /path/private_key
```

The USERID will be communicated after member onboarding phase.

4.4 FIX

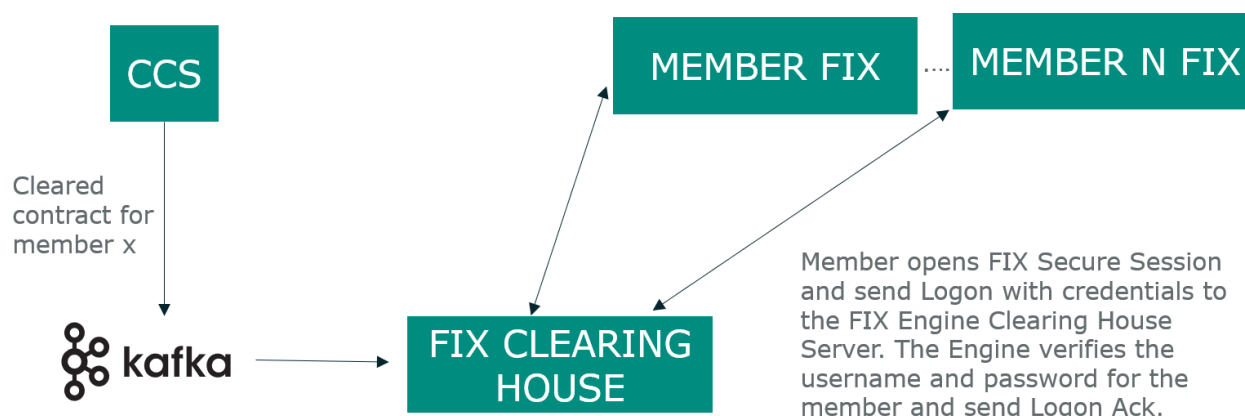
Euronext Clearing will also make FIX connectivity available to its participants in order to receive trade confirmations. An internal FIX Engine has been implemented and is reachable via public Internet like the other channels.

FIX-over-TLS (FIXS) is a technical standard adopted to enforce data exchange, especially in case of further development or additional requirements.

Euronext Clearing allows Clearing Members to use FIX protocol to receive a real time notification for each trade being captured in the clearing system. The FIX "Execution report" will be used for that purpose.

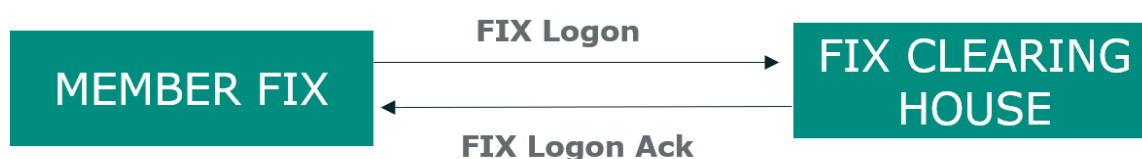
However, the Fix Engine / protocol also requires the implementation of a set of administration messages to guarantee reliability and resilience.

The FIX Engine on Client side must be configured accordingly to the technology used to implement it (e.g. Java, C++, etc.).

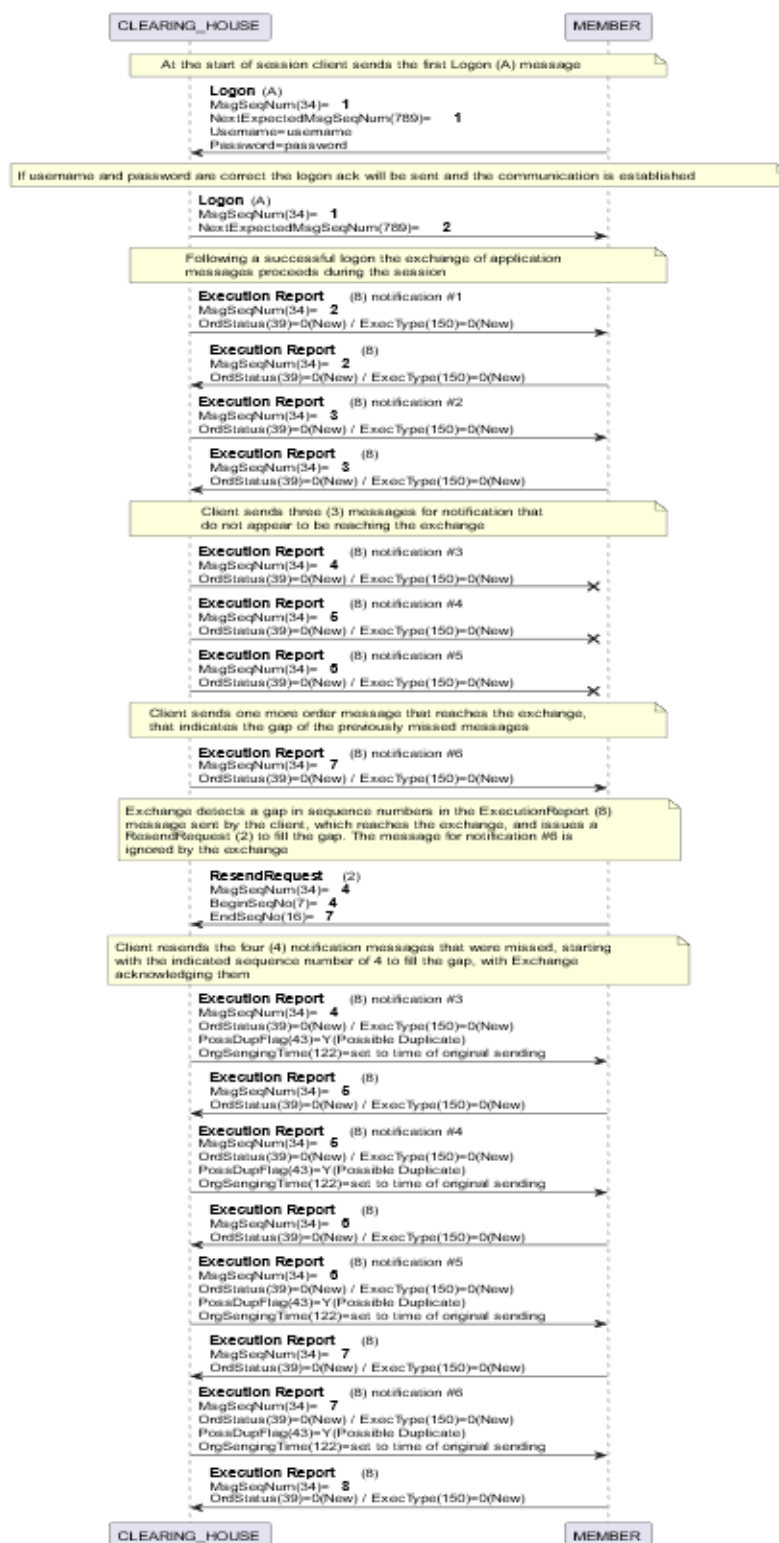


Within the Logon member will enter the username and password fields, in the username the unique customer identifier and the password generated via Client Credentials UI.

The Fix CCP verifies that the credentials are correct and sends Logon Ack to the member establishing the FIX communication, as shown in the sequence diagram below. After successful logon, once received the Kafka topic that notify a cleared contract, the server will be able to send an ExecutionReport with customized fields to notify this event.



The chart below represents the authentication and the data exchange flows between the Member and Euronext Clearing:



4.4.1 FIX resend request

The receiving application initiates the retransmission of messages by sending a resend request when:

- A sequence number gap is detected
- A message is lost by the receiving application
- Is a function of the initialization process

The sending application may wish to consider the message type when resending messages, anyway this kind of behaviour is managed by FIX protocol itself.

Addition info can be found [here](#).

4.4.2 FIX over TLS

A certificate pair will be issued for each member to implement security in FIX communication. The Fix Engine Server at CCP side will have a session configuration as acceptor for each member.

BeginString is the version of FIX this session should use, FIXT.1.1 in our case.

DefaultApplVerID required only for FIXT 1.1, in our case FIX.5.0.

SenderCompID is your ID as associated with this FIX session, a case-sensitive alpha-numeric string.

TargetCompID is counterparty's ID as associated with this FIX session, a case-sensitive alpha-numeric string.

SocketConnectHost is the endpoint domain name wcsfixe-eua.clearing.euronext.com

SocketConnectPort is the endpoint port 7001

4.4.3 FIX SERVER ENGINE Configuration File

This part is related to Euronext Clearing perimeter and should be considered just as an example:

```
[default]
UseJmx=Y
FileStorePath=store
FileLogPath=log
HeartBtInt=120
# SSL properties
SocketUseSSL=Y
EnabledProtocols=TLSv1.2
SocketKeyStore=./data/p12/keystore.p12
SocketKeyStorePassword=password
KeyStoreType=PKCS12
NeedClientAuth=Y
TimeStampPrecision=MICROS
```

Acceptor Session part, repeated for each member

```
[session]
ConnectionType=acceptor
BeginString=FIXT.1.1
DefaultAppVerID=FIX.5.0
SenderCompID=CCEGITRRXXX
TargetCompID=MEMBER #this is the CM code registered during onboarding
SocketAcceptPort=7001
AppDataDictionary=./spec/FIX50.xml
SSL properties
SocketTrustStore=./data/p12/truststore.p12
SocketTrustStorePassword=password
TrustStoreType=PKCS12
```

4.4.4 FIX MEMBER Configuration File

The keystore and truststore showed in this example are PKCS12 but the participant can select also JKS, or any other format compatible with the client application.

Into keystore must be places client digital certificate generated via Client Credential UI.

The truststore must be populated with public Certificate Authority that Euronext Clearing uses to sign its own server certificate, and it can be retrieved by Client Credential UI section.

```
[default]
UseJmx=Y
FileStorePath=store
FileLogPath=log
HeartBtInt=120
# SSL properties
SocketUseSSL=Y
EnabledProtocols=TLSv1.2
SocketKeyStore=./data/p12/keystore.p12
SocketKeyStorePassword=password
KeyStoreType=PKCS12
TimeStampPrecision=MICROS
SocketTrustStore=./data/p12/truststore.p12
SocketTrustStorePassword=password
TrustStoreType=PKCS12

[session]
ConnectionType=initiator
BeginString=FIXT.1.1
DefaultAppVerID=FIX.5.0
AppDataDictionary=./spec/FIX50.xml
SenderCompID=MEMBER #this is the CM code registered during onboarding
TargetCompID=CCEGITRRXXX
SocketConnectPort=7001
SocketConnectHost=wcsfixe-eua.clearing.euronext.com
```

APPENDIX A: CERTIFICATE MANAGEMENT AND PKI

A.1.1 Certificate request

The certificate request process is triggered automatically the moment after the generation of the client credentials to be used for FIX and API access. In particular, once the client credentials have been generated, it will be placed in status Off, waiting for the user to download the generated digital certificate transparently from the IdP, via the PKI platform.

Below is a description of the certificate request process.

1. Technical User will request via Client Credential UI function the activation of the credential entering a CSR previously generated (openssl or any other tool available at member side). Addition info can be found [here](#).
2. Client Credential UI will executes a certificate request via API exposed by PKI;
3. PKI platform replies to that request with a certificate and the relative serial number;
4. Client Credential UI makes the certificate available to the Technical User

A.1.2 Certificate revocation

The certificate revocation process fits into the current user revocation process. For example, this operation can be performed by the Client Credential UI, which, once the revocation request action has been performed, will automatically generate a revocation request to the PKI.

Below is a description of the certificate revocation process that arises from the request for revocation of the Client credentials.

1. Revocation of the user is requested by operating from the Client Credential UI;
2. PKI revokes the certificate and:
 - a. Confirm the correctness of the operation to the IdP;
 - b. Sends an email to the email address given in step 2 of paragraph A.1.1 to inform the user that the certificate has been revoked;

A.1.3 Certificate suspension

The certificate suspension process plugs into the current IdP suspension process, triggered by the Client Credential User Portal. In particular, as an extension of the current IdP suspension process, once the request for suspension action has been performed, the Client Credential User Portal will automatically generate the user's certificate suspension request to the IdP, which it will send via hook vs PKI.

Below is a description of the certificate suspension process that begins with the Client credential suspension request.

1. The suspension of the Client credential is requested, which engages the suspension on the IdP;
2. IdP performs a certificate suspension request for that specific Client ID vs PKI;
3. PKI suspends the certificate and:
 - a. Confirm the correctness of the operation to IdP;
 - b. Sends an email to the email address given in step 2 of paragraph A.1.1 to inform the user that the certificate has been suspended;
4. The IdP consequently updates the user's status to Pending and informs the user about suspension.

A.1.4 Certificate activation

The certificate activation process plugs into the current IdP activation process, in the case of the API triggered by the Client Credential User Portal. In particular, as an extension of the current IdP activation process, once the activation request action has been performed, the Client Credential User Portal will automatically generate the user activation request to the IdP, which it will send via hook vs PKI.

Below is a description of the certificate activation process that starts from Client credential activation request.

1. The activation of the Client credential is requested, which engages the activation on the IdP;
2. IdP performs a certificate activation request for that specific Client ID vs PKI;
3. PKI activates the certificate and:
 - a. Confirm the correctness of the operation to IdP;
 - b. Sends an email to the email address given in step 2 of paragraph A.1.1 to inform that the certificate has been activated;
4. The IdP consequently updates the status to Active for the user and informs the user of the variation.

A.1.5 Certificate renewal

The IdP periodically checks the expiration date of valid certificates on PKI;

As soon as the expiration date of the certificate enters the renewal time window (typically 30 days before the deadline, but the period can be modified according to need), the IdP performs the following steps:

1. Verify that the user associated with the certificate is valid and active Send an expiration notice email to the Technical User inviting him to access the Client Credential UI;
2. Technical User accesses the Client Credential UI and requests renewal for the user by entering the new previously generated CSR

3. Client Credential UI performs a renewal request via APIs exposed by PKI passing the serial number of the certificate and the CSR
4. PKI responds to the request with the certificate and its serial number
5. Client Credential UI makes the certificate available to the Technical User

A.1.6 User cancellation

It is assumed that the existing process for revoking the certificate also triggers the cancellation of the relative user on the IdP. In this case the proposed flow is as follows.

1. Technical User accesses the Client Credential UI and requests revocation/cancellation of the user
2. Client Credential UI executes a Seat ID deletion request via APIs exposed by PKI
3. PKI:
 - a. Revokes all active certificates associated with the Seat ID
 - b. Delete Seat ID
 - c. Confirm the correctness of the operation to Client Credential User Interface
4. Client Credential UI informs Technical User of the conclusion of the operation

APPENDIX B: CLIENT CREDENTIAL USER GUIDE

This annex aims at providing a complete guide to the usage of Client Credentials UI.

It describes the application offered by Euronext Clearing through which users can generate credentials and certificates in order to connect to clearing applications.

This application must be used only in a machine to machine scenario. Credentials for Clearing System UI application cannot be generated using this application.

B.1.1 Login

Users arrive at the log in page with the access link:

<https://wcsccred-eua.clearing.euronext.com>

On this page, users will have to enter the member credentials provided by the Euronext Clearing, an username and an associated password. The user can choose to remain logged in the platform by flagging a specific field below the password bar.

By clicking on the "Sign In" button, after entering user's credentials correctly, users access the home page of the WCS.

Connecting to

Euronext CLEARING

Sign In

Username

Password

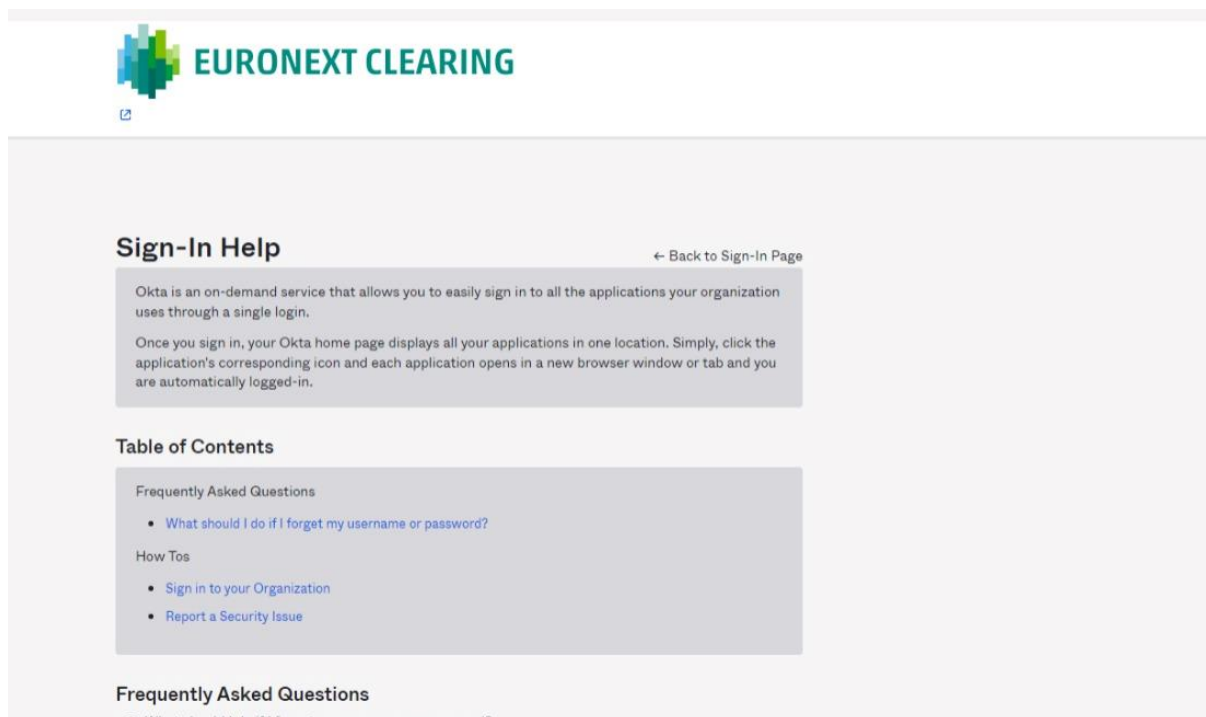
☐ Keep me signed in

[Forgot password?](#)
[Help](#)

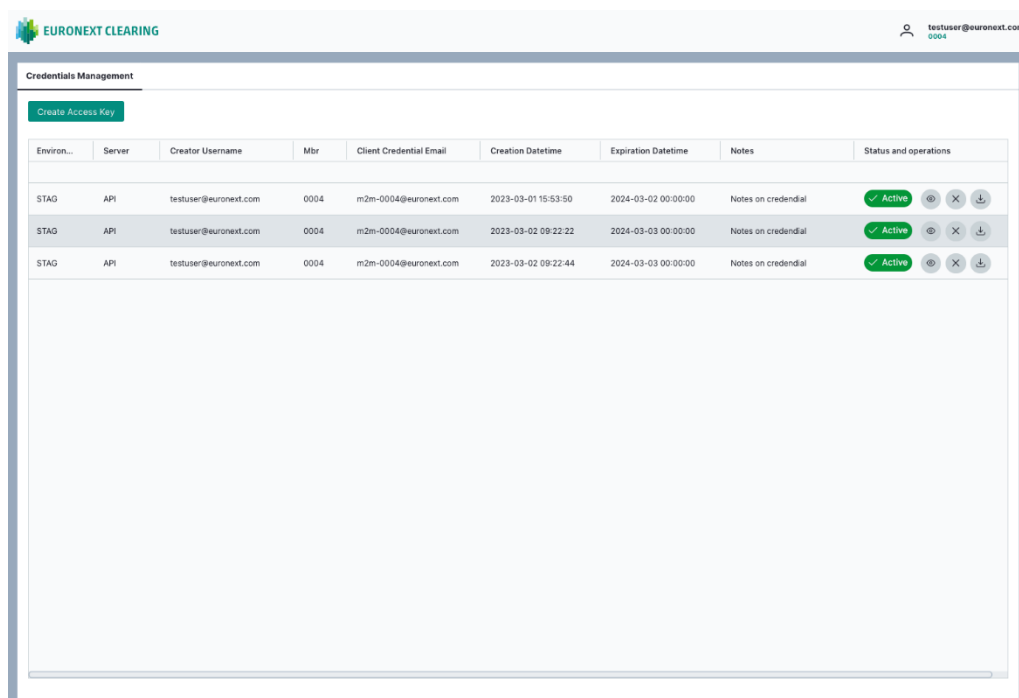
Powered by Okta Privacy Policy

If the user has forgotten the password, it should click on "[Forgot password?](#)" below the "Sign in" button. On a new screen view, the user enters the log in email and receive instructions on how to reset the password directly in the mailbox.

However, for any other helps, the user can click on the “[Help](#)” option below the “[Forgot password?](#)” option. A page with several FAQs will open and will help finding the answer.



After logging in, the Home Page is shown on the screen.



B.1.2 Credentials generation

In order to create a new set of credentials the user must:

- **Create Access Key:** clicking on this button the user will be able to create a new set of credentials.

EURONEXT CLEARING testuser@euronext.com 0004

Credentials Management

Create Access Key

Access Key Creation

Application*

Environment*

Groups*

Public Key*

Note

Mbr	Client Credential Email	Creation Datetime	Expiration Datetime	Notes	Status and operations
0004	m2m-0004@euronext.com	2023-03-01 15:53:50	2024-03-02 00:00:00	Notes on credential	✓ Active <input type="button" value="🔍"/> <input type="button" value="✕"/> <input type="button" value="📄"/>
0004	m2m-0004@euronext.com	2023-03-02 09:22:22	2024-03-03 00:00:00	Notes on credential	✓ Active <input type="button" value="🔍"/> <input type="button" value="✕"/> <input type="button" value="📄"/>
0004	m2m-0004@euronext.com	2023-03-02 09:22:44	2024-03-03 00:00:00	Notes on credential	✓ Active <input type="button" value="🔍"/> <input type="button" value="✕"/> <input type="button" value="📄"/>

- **Application:** select from the box the system for which you need to generate the credentials:

EURONEXT CLEARING testuser@euronext.com 0004

Credentials Management

Create Access Key

Access Key Creation

Application*

API
FIX

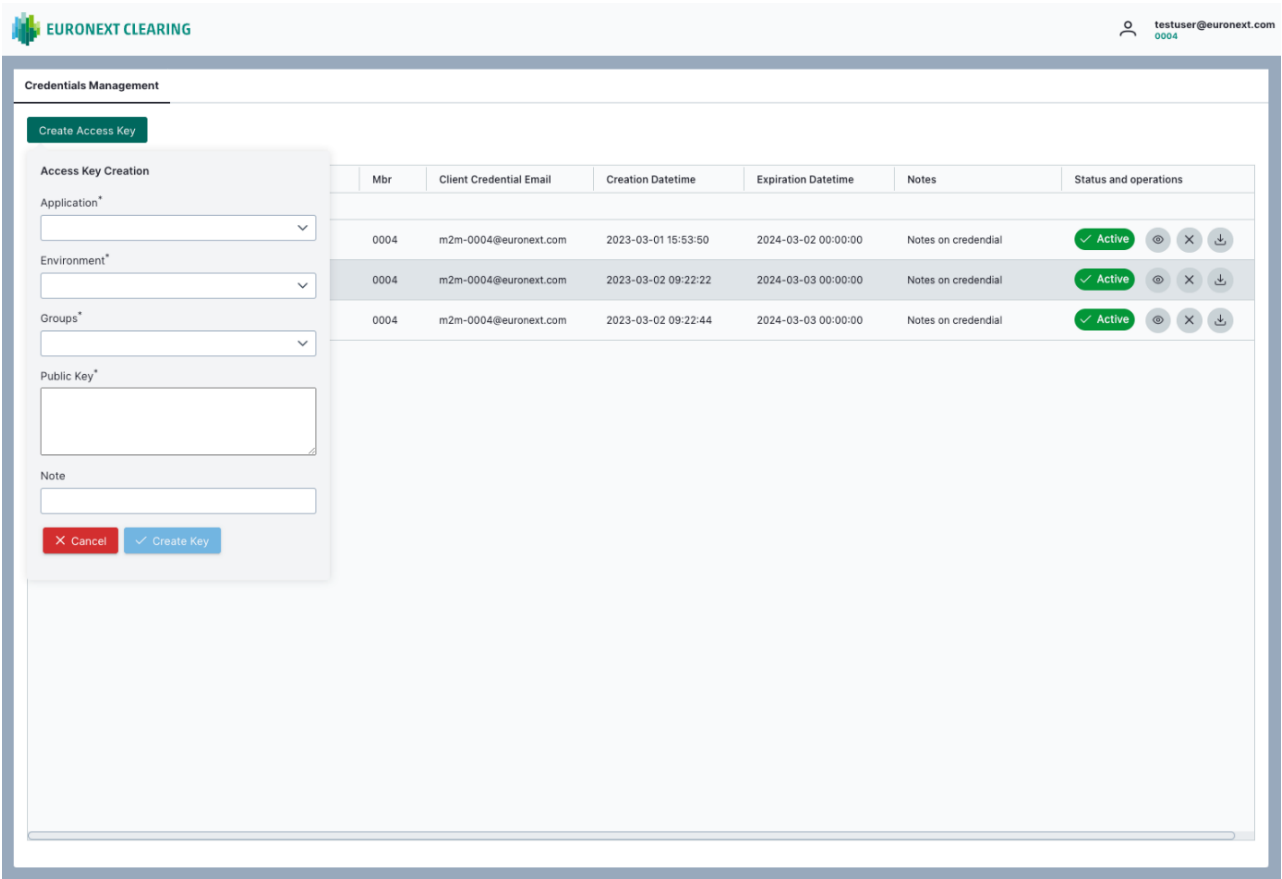
Groups*

Public Key*

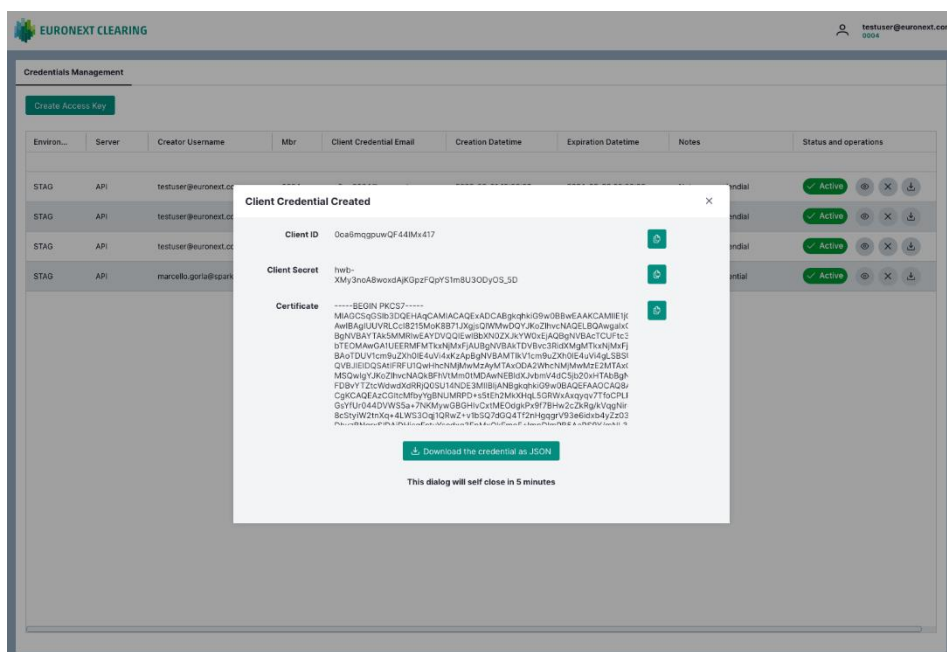
Note

Mbr	Client Credential Email	Creation Datetime	Expiration Datetime	Notes	Status and operations
0004	m2m-0004@euronext.com	2023-03-01 15:53:50	2024-03-02 00:00:00	Notes on credential	<input checked="" type="checkbox"/> Active <input type="button" value="eye"/> <input type="button" value="X"/> <input type="button" value="download"/>
0004	m2m-0004@euronext.com	2023-03-02 09:22:22	2024-03-03 00:00:00	Notes on credential	<input checked="" type="checkbox"/> Active <input type="button" value="eye"/> <input type="button" value="X"/> <input type="button" value="download"/>
0004	m2m-0004@euronext.com	2023-03-02 09:22:44	2024-03-03 00:00:00	Notes on credential	<input checked="" type="checkbox"/> Active <input type="button" value="eye"/> <input type="button" value="X"/> <input type="button" value="download"/>
0004	m2m-0004@euronext.com	2023-03-02 10:18:03	2024-03-03 00:00:00	Notes on credential	<input checked="" type="checkbox"/> Active <input type="button" value="eye"/> <input type="button" value="X"/> <input type="button" value="download"/>

- **Create:** clicking on Create button the user will be able to create a new set of credentials.

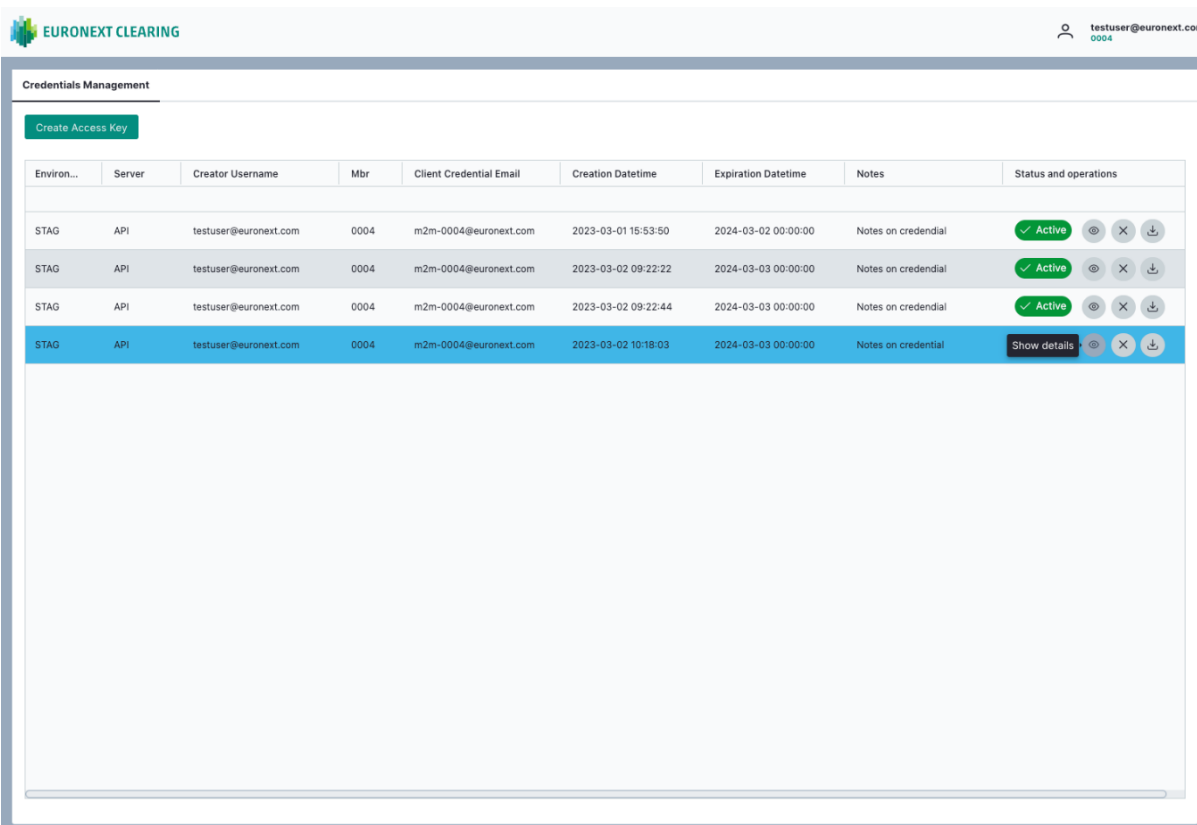














- In the popup the user is able to view the credentials created in terms of Client ID, Secret and Certificate



B.1.3 Credentials control

In the Home Page the user is able to check all the credentials available

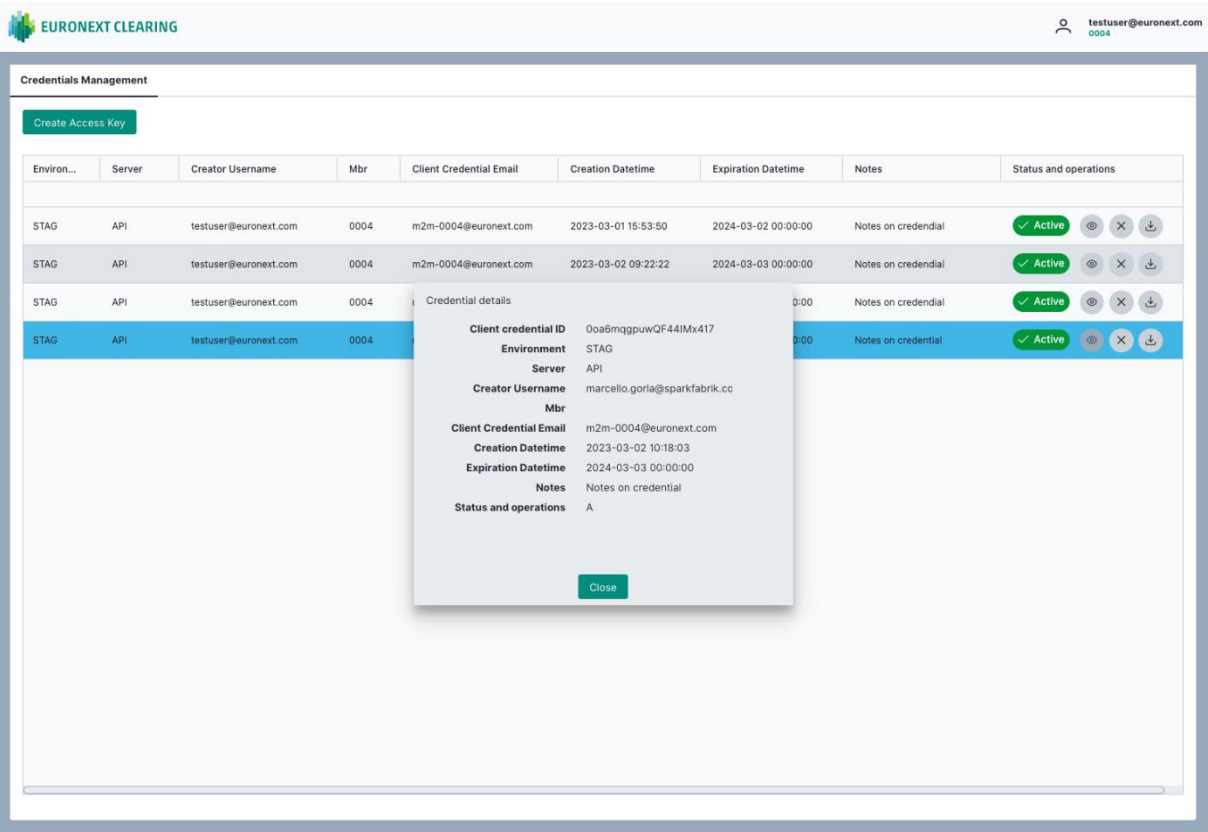


Environ...	Server	Creator Username	Mbr	Client Credential Email	Creation Datetime	Expiration Datetime	Notes	Status and operations
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-01 15:53:50	2024-03-02 00:00:00	Notes on credential	✓ Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 09:22:22	2024-03-03 00:00:00	Notes on credential	✓ Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 09:22:44	2024-03-03 00:00:00	Notes on credential	✓ Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 10:18:03	2024-03-03 00:00:00	Notes on credential	Show details   

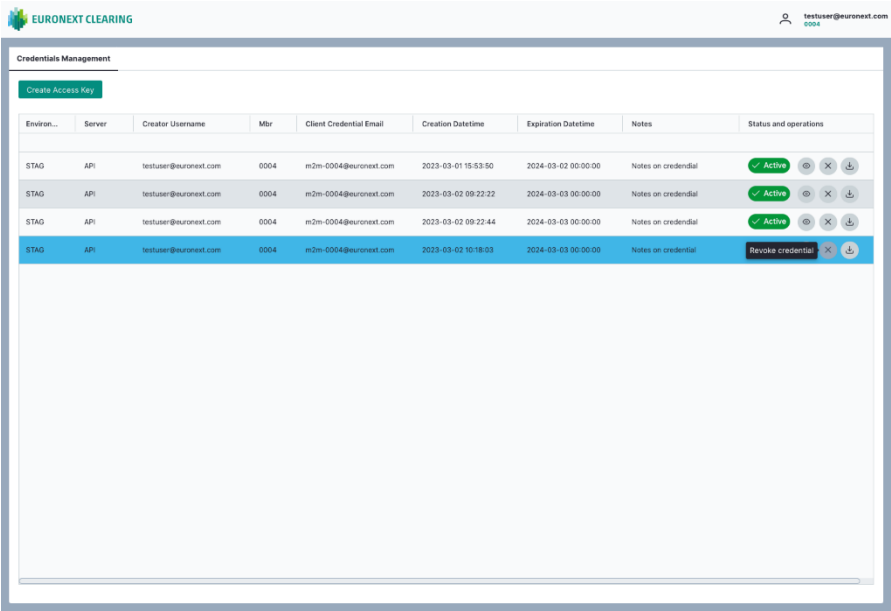
Clicking on the single row the user is able to check all the information related to the set of credentials selected.

The popup that appears provide useful information on the credentials like:

- Client Id
- Application
- Expiration Date
- Creation Date



Clicking on the cancellation symbol the user is able to revoke the set of credentials selected















This operation is irreversible and needs further confirmation from the user that must click on the confirmation popup

testuser@euronext.com
0004

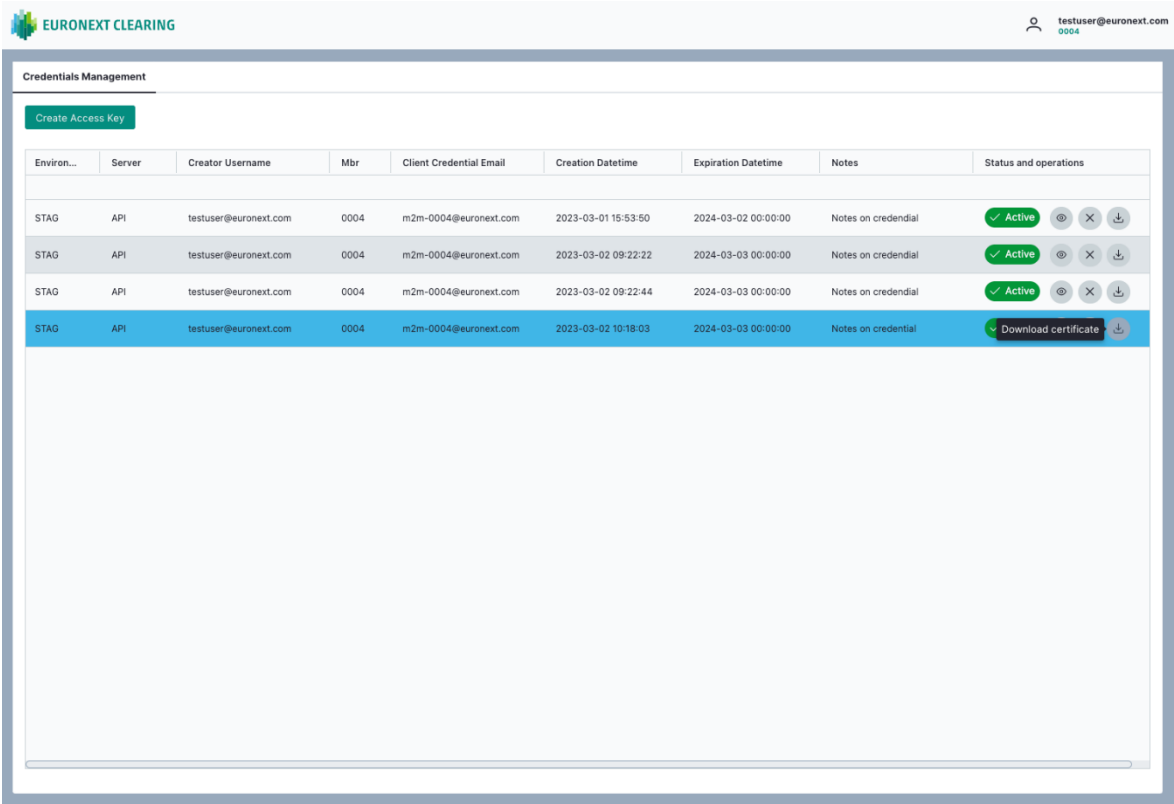
Credentials Management

Create Access Key

Environ...	Server	Creator Username	Mbr	Client Credential Email	Creation Datetime	Expiration Datetime	Notes	Status and operations
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-01 15:53:50	2024-03-02 00:00:00	Notes on credential	Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 09:22:22	2024-03-03 00:00:00	Notes on credential	Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 09:22:44	2024-03-03 00:00:00	Notes on credential	Active   
STAG	API	testuser@euronext.com	0004	m2m-0004@euronext.com	2023-03-02 10:18:03	2024-03-03 00:00:00	Notes on credential	Active   

Are you sure you want to revoke this credential key?
No Yes

Clicking on the download symbol the user is able to download the certificate associated to the selected set of credential



APPENDIX C: DOCUMENT HISTORY

REVISION NO./ VERSION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
1.0	3 January 2023	Euronext Clearing	First Draft
1.1	3 February 2023	Euronext Clearing	FQDN specification; public IP definition; FIX session examples
1.2	3 March 2023	Euronext Clearing	EUA FQDN change (removing "uat" preferring "eua"); public IP adjustment