

# ClearstreamXact

## **Security Guide**

## ClearstreamXact Security Guide

December 2017

Document number: 6209

Information in this document is subject to change without notice and does not represent a commitment on the part of Clearstream Banking S.A. (referred to hereinafter as Clearstream Banking or CBL), or any other entity belonging to Clearstream International, S.A. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written consent of Clearstream International, S.A.

© Copyright Clearstream International, S.A., (2017). All rights reserved.

Clearstream and Xact File Transfer are registered trademarks of Clearstream International, S.A. S.W.I.F.T. is a registered trademark of the Society for Worldwide Interbank Financial Telecommunication. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks are the property of their respective owners.

Clearstream International, S.A. is a Deutsche Börse Group company.

## Security Guide

ClearstreamXact is a suite of connectivity products that gives Clearstream customers real-time access to enhanced information, instruction input, transaction and position reporting.

ClearstreamXact offers secure multi-channel connectivity to Clearstream with a choice of connection via web-browser, file transfer and the SWIFT network. Whatever your operating or technical environment, ClearstreamXact provides seamless, direct access, giving you adaptable connectivity for your growing business.

### About this guide

The purpose of this guide is to assist ClearstreamXact customer technical staff to understand the security details with regard to the different options for connectivity.

This guide is organised into chapters dedicated to the individual connectivity channels, as follows:

- [“1. Xact Web Portal”](#) on page 1-1;
- [“2. Xact File Transfer via Internet”](#) on page 2-1.

Each chapter may be further subdivided into areas of general and/or specific subject matter within the respective channel.

**Note:** For details of the SWIFT network, please refer to SWIFT’s proprietary documentation.

## Contact details

For technical assistance with ClearstreamXact, please contact Customer Service Connectivity Support as follows:

	<b>Luxembourg</b>	<b>Frankfurt</b>	<b>London</b>
Tel:	+352-243-38110	+49-(0) 69-2 11-1 15 90	+44-(0)20-786 27100
Fax:	+352-243-638110	+49-(0) 69-2 11-6 1 15 90	+44 (0) 20-786 27254
Email:	connectlux@clearstream.com	connectfrankfurt@clearstream.com	connectlondon@clearstream.com

You can also consult our website [www.clearstream.com](http://www.clearstream.com) under Products and Services/Connectivity for the latest information on ClearstreamXact.

Before contacting Clearstream Banking, please ensure that you have the following information to hand:

- Your organisation name and account number with Clearstream Banking.
- Your telephone number, fax number and email address.
- Details of the problem (please have full details available).
- If you have received an error message, full details of the error, with the error message number.

Customers should note that, as is normal practice within financial organisations, Clearstream Banking has implemented telephone line recording to ensure that the interests of Clearstream Banking and of its customers are protected against misunderstandings or miscommunications.

Areas subject to telephone line recording include Client Services, the Treasury Dealing Room and back office operations. The recorded lines are the subject of an ongoing formal maintenance and quality control programme to ensure their continued effective and appropriate deployment and operation.

<b>Security Guide</b> .....	<b>i</b>
About this guide .....	i
Contact details .....	ii
<b>1. Xact Web Portal</b> .....	<b>1-1</b>
Registration and initial administrator activation .....	1-1
Certificate import and user login .....	1-1
User credentials .....	1-3
Certificate storage in the Windows Keystore .....	1-4
Certificate storage on smartcards .....	1-4
Certificates .....	1-5
Password expiry .....	1-5
Password attempts / blocked .....	1-5
Network .....	1-5
OU security settings .....	1-6
Audit log .....	1-8
Digital signatures .....	1-9
Additional client-side recommended security measures .....	1-9
Penetration test reports .....	1-9
Data encryption .....	1-9
<b>2. Xact File Transfer via Internet</b> .....	<b>2-1</b>
Integrating with firewalls .....	2-1

# Security Guide

This page has intentionally been left blank.

## 1. Xact Web Portal

The Xact Web Portal is the interface for the Clearstream Banking online platform to access instruction input, query, reporting and exception handling services.

The application and all associated data is hosted in Luxembourg, Europe.

It is under the oversight of the Commission de Surveillance du Secteur Financier (CSSF -www.cssf.lu), the Luxembourg financial regulator.

### Registration and initial administrator activation

Please refer to the [Xact Web Portal User Guide](#).

### Certificate import and user login

In order to login to Xact Web Portal, a user must have received the following from the Organisational Unit (OU) administrator:

- p12 file
- p12 password
- user password

Step 1: save the p12 file you have received via email to a drive (local drive, personal drive, USB etc)

Step 2: In Internet Explorer go to <https://xact.clearstream.com>

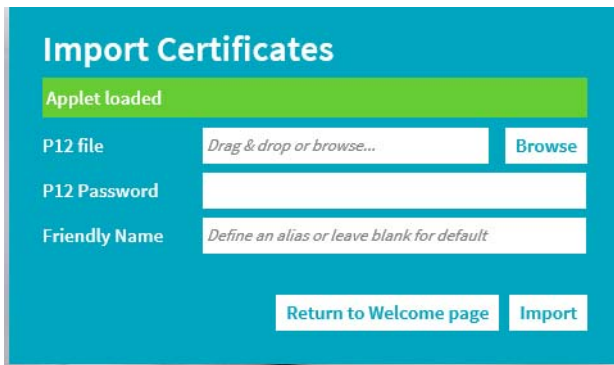
Click on:



Click "Browse" and navigate to the p12 file you have saved in step 1.

Alternatively you can also drag and drop the p12 file from Windows Explorer into the "P12 file" field:

# ClearstreamXact Security Guide



The screenshot shows a web form titled "Import Certificates" with a blue header. Below the header is a green bar that says "Applet loaded". The form contains three input fields: "P12 file" with a "Browse" button, "P12 Password" with a text input field, and "Friendly Name" with a text input field containing the placeholder text "Define an alias or leave blank for default". At the bottom of the form are two buttons: "Return to Welcome page" and "Import".

Step 3: In the password field enter the p12 password you have received from your administrator.

Step 4: (optional) you can enter in the Friendly Name field, an alias which will be shown on each login on the certificate.

Step 5: click Import. You should see the message "certificate imported successfully".

Step 6: click "return to welcome page"

Now you can login:

The home page of Xact Web Portal is <https://xact.clearstream.com>

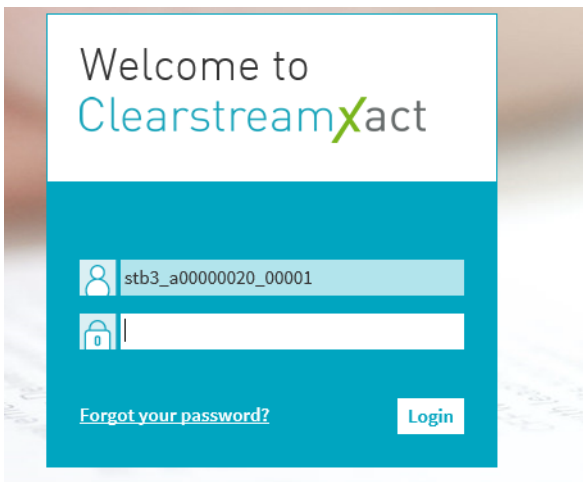
Please double-check that the URL shown in your browser shows the padlock symbol and that there are no warnings or errors that the server certificate could not be verified, which would indicate an unsecure connection.



To proceed to the login page please click on:

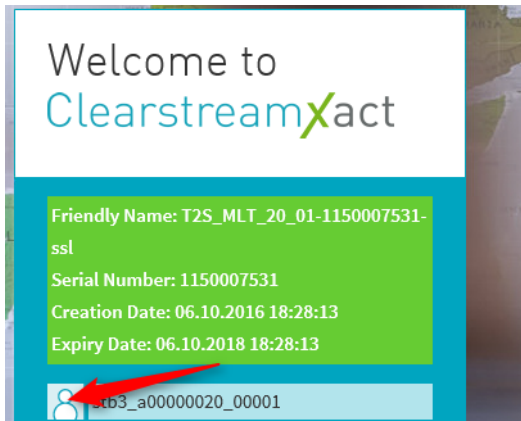


You will be prompted by Windows to select your user certificate (which you previously imported). After selection you can see your user ID on the screen.





To see additional details of the selected user certificate you can click on the user icon.



To continue with the login enter your user password and click 'Login'.

## User credentials

Each Xact Web Portal user has the following personal credentials:

- a user password, as given by the OU Administrator.
- an SSL certificate, to authenticate to the Xact Web Portal web server
- a SIGNING certificate, to digitally sign operations and transactions when working in Xact Web Portal

The two certificates are issued by Clearstream Banking's Certification Authority (CA) and certify the two private keys that users generate on their local PC.

## Certificate storage in the Windows Keystore

The certificates and keys are stored in the user's personal Windows Keystore that is part of the user's Windows profile. In a corporate environment the Windows profile is usually stored on a central server and during the Windows login the profile is copied to the local PC. At logoff the Windows profile is copied back to the central server. Therefore it is important that when you have generated new certificates in the Windows Keystore (using Xact Web Portal) that you logoff your current Windows session properly so that the updated Windows Keystore is properly stored on the central server when logging off.

You can view the content of your Windows Keystore either via:

- Internet Explorer → Tools → Content → Certificates → User certificates
- Microsoft Management Console → Snap-in Certificates
- On the Xact Web Portal support page: <https://xact.clearstream.com/support.html> → Browser certificate list

## Certificate storage on smartcards

If you work with smartcards, the certificates are stored on the smartcard and a copy without the private key is copied by the smartcard middleware to your Windows Keystore. These copies are automatically removed when you unplug the software.

The supported smartcard reader is:

- Athena ASEdrive (IIIe or V3 USB)

If the driver is not installed automatically by Windows you can download it manually from:

[http://www.nxp.com/assets/downloads/data/en/device-drivers/v4101\\_KMDF\\_driver.zip](http://www.nxp.com/assets/downloads/data/en/device-drivers/v4101_KMDF_driver.zip)

The supported smartcard is:

Safenet etoken 4100

The software for the card must be installed on the user's PC

**Note:** Smartcards are mandated by some local regulators.

## Certificates

The certificates received from Clearstream or from the OU Administrator are always temporary certificates, this means they are:

- Only valid for six (6) weeks
- Must be regenerated upon login

When the temporary certificates are regenerated by the user, permanent certificates are received that are valid for two (2) years.

All digital certificates have an expiry date. Before the expiry date is reached the user will be prompted at login to regenerate the certificates, and the new certificates will have an expiry date of two (2) years in the future.

If the certificates are not regenerated before the expiry date the user cannot use the certificates anymore and must contact the OU Administrator to receive new certificates.

## Password expiry

The password of the user expires according to the password rules defined in the Xact Web Portal OU properties of the user. When the password has or is going to expire users are prompted at login to change their user password.

## Password attempts / blocked

After 10 wrong password attempts, the user's password is blocked and the OU Administrator has to reset the password.

## Network

Via Internet the Xact Web Portal is available at <https://xact.clearstream.com>.

The IP address is 194.36.230.129 and the only port used is 443 (the regular SSL port).

The Xact Web Portal web server supports TLS1.1 and TLS 1.2.

The traffic is regular https and you can use a network proxy server however as the traffic is two-way SSL the proxy must not try to terminate or intercept the SSL connection as this will break the connection.

Instead or in addition to Internet you can connect via VPN leased line. For this a Deutsche Börse Router will be installed on your premises which connects you to the Extranet of Deutsche Börse.

Via VPN, Xact Web Portal is available at: <https://xact.clearstream.banking>.

You can request an offer for this service from Clearstream Client Services or your Relationship Manager.

## OU security settings

OU properties					
Service name	Property name	Category	Propagation	Updatable by	Value
User Management					
User Management	Minimum Password Length	Password	OU	Only Support & Entity Admin Users	8 characters
User Management	Minimum Password Complexity	Password	OU	Only Support & Entity Admin Users	3 of 4 constraints
User Management	Maximum Password Validity Period	Password	OU	All Types of Admin Users	3 months
User Management	Minimum Password History Length	Password	OU	All Types of Admin Users	12 passwords
User Management	Maximum Session Time	Re-authentication	OU	All Types of Admin Users	60 minutes
User Management	Risk Based Re-Authentication	Re-authentication	OU	Only Support & Entity Admin Users	OFF
User Management	Smart Card	Credentials Types	User	All Types of Admin Users	Allowed
User Management	Windows Key Store	Credentials Types	User	All Types of Admin Users	Allowed
User Management	User Mgt N-Eyes Principle	N-Eyes	User	All Types of Admin Users	4 eyes

There are a number of configurable security settings on the Organisation Unit level.

1. Minimum Password Length  
the minimum number of characters a user password must have.  
Possible values:
  - 8 characters
  - 10 characters
  - 12 characters
  - 16 characters
  - 24 characters
  - 35 characters
2. Minimum Password Complexity  
The number of character categories from which a user password must be composed, categories are: lower case; upper case; numbers and special characters.  
Allowed values are:
  - 3 of 4 constraints
  - 4 of 4 constraints
3. Maximum Password Validity Period  
This time is used to calculate how long before users have to change their password.  
Allowed values are:
  - 1 month
  - 2 months
  - 3 months
  - 6 months
  - 9 months
  - 12 months

#### 4. Minimum Password History Length

This is the number of previous passwords that users cannot reuse when changing their user password.

Allowed values are:

- 1 password
- 3 passwords
- 5 passwords
- 10 passwords
- 12 passwords
- 15 passwords
- 20 passwords
- 24 passwords

#### 5. Maximum Session Time (screenlock)

This is the time of inactivity after which users are taken back to the login screen to enter their user password to get back into the Xact Web Portal.

Allowed values are:

- 5 minutes
- 10 minutes
- 20 minutes
- 40 minutes
- 60 minutes

#### 6. Risk Based Re-Authentication

If this setting is ON, users must re-enter their user password when performing sensitive operations, for example, releasing an instructions.

- ON
- OFF

#### 7. Smart Card

If this setting is Allowed, users are allowed to store their Xact Web Portal user certificates on a smartcard.

Allowed values are:

- Allowed
- Not Allowed

#### 8. Windows Key Store

If this setting is Allowed, users are allowed to store their Xact Web Portal user certificates in the Windows Keystore (or Firefox keystore). If this setting is Not Allowed users must use a smartcard.

Allowed values are:

- Allowed
- Not Allowed

# ClearstreamXact Security Guide

## 9. User Mgt N-eyes principle

If this setting is 4-eyes then all actions in User Management must be confirmed by a second user before they become active.

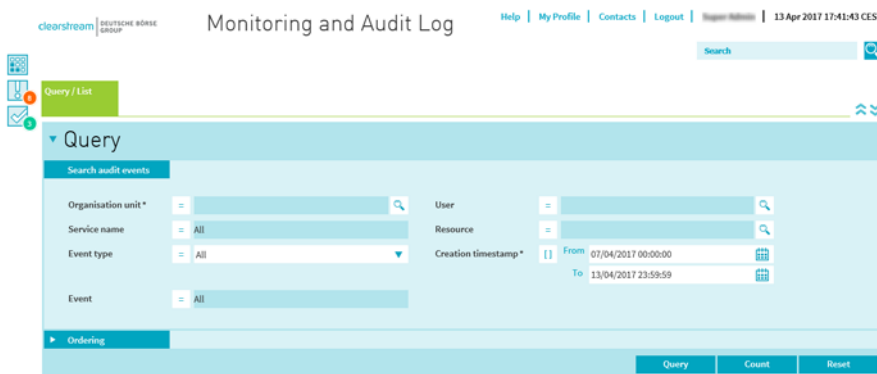
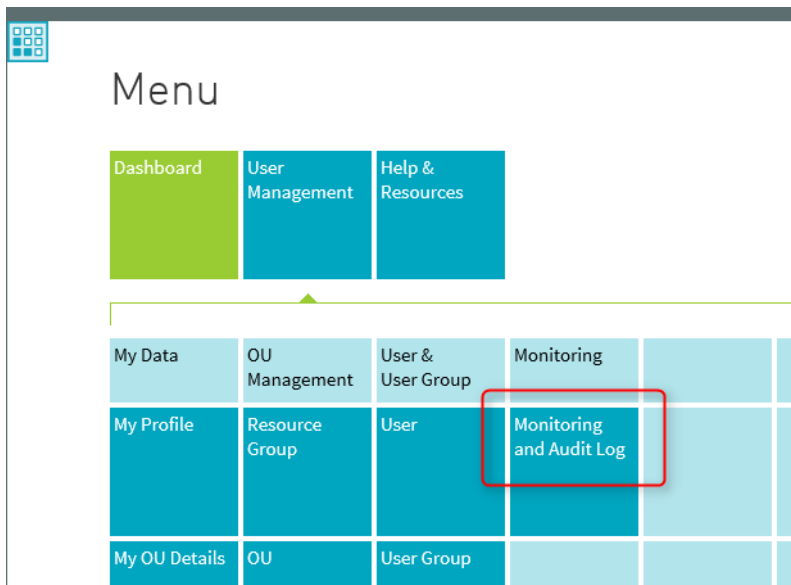
Allowed values are:

- 2-eyes
- 4-eyes

There is a separate N-eyes principle property available for each business service subdomain, for example, Securities Instructions, Cash Instructions, so that you can choose a different eyes level per business service.

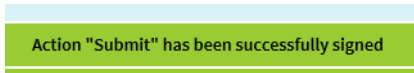
## 1.11. Audit log

All actions taken by users in the OU are audited and stored in the Monitoring and Audit Log of the OU. The OU Administrator can access the Audit Log via Xact Web Portal and query the recorded audit events.



## Digital signatures

When submitting instructions to Clearstream the instruction data is digitally signed (SHA512) with the private key of your user certificate and the signature is submitted to Clearstream. There your signature is verified and if accepted you will see the following message:



The signature is stored with the instruction for audit purposes.

## Additional client-side recommended security measures

It is the users responsibility to ensure that:

- the Operating System and other software installed is up-to-date and receives the regular security updates;
- they are not logged-in with the administrator account;
- an anti-virus scanner is running on the PC and anti-virus signatures are updated regularly;
- no software received from unknown sources or via email is installed.

## Penetration test reports

The security of the Xact Web Portal application is regularly reviewed by an external security company and the resulting penetration test reports are available on request.

## Data encryption

For data in transit a TLS session is established between the browser and web server. All messages pass over this encrypted session. Commercial strength 256-bit keys are used for the encrypted session and no ability to negotiate weak keys is possible.

Data at rest is stored in the application database which is encrypted. In addition it is protected by the highest level of physical security and access to the database is restricted to only a limited number of Clearstream Banking staff who are subject to strict confidentiality agreements.

# ClearstreamXact Security Guide

This page has intentionally been left blank.



## 2. Xact File Transfer via Internet

Xact File Transfer via Internet is a workstation-based file transfer service that provides you with an easy to use and efficient means of sending instructions and retrieving reports.

Instruction files are sent via the dedicated web site [https:// www.cdinternet.com](https://www.cdinternet.com) to Clearstream Banking where they are stored in a customer-specific area (the "filestore"). They are then immediately transferred to the Creation platform for clearing and settlement. Reports generated by the Creation platform are stored in the filestore from where you can browse them or save them locally.

Xact File Transfer via Internet is an efficient, secure and reliable file transfer connectivity solution. When used with CreationOnline or Xact Web Portal, it gives you the benefits of enhanced instruction life cycle monitoring, on-line queries, exception handling and large-volume reporting providing accurate, real-time information on the status of any instruction at any time.

The key objective of the Xact File Transfer via Internet service is to provide a file transfer service to your desktop. By using the Secure Sockets Layer (SSL) over the secure HyperText Transfer Protocol (HTTPS) or secure File Transfer Protocol (FTPs) (RFC 2228), Xact File Transfer via Internet is a highly secure service that is accessible from your desktop, provided that you have access to the public internet from a web browser.

Certificates to access the application are x509v3 128-bit SSL certificates generated by the CreationOnline application and stored on the user's Internet Explorer profile.

### Integrating with firewalls

Xact File Transfer via Internet is implemented using internet technologies. It is therefore highly recommended that customers using Xact File Transfer via Internet protect their interior networks from the outside world using a Firewall architecture.

In order to run Xact File Transfer via Internet through a firewall, the following protocols need to be allowed to traverse the firewall:

If HTTP protocol is used

- HTTPS uses TCP port 443 for the initial web site connection and for the interaction with the application. A 128-bit key size is used in the encryption algorithm.

if FTP protocol is used

- FTP uses TCP port 21 for control;
- FTP uses TCP port 54000 to 55000 for data connection.

if SFTP (SecureSSH) protocol is used

- SFTP uses TCP port 22 for control and data transfer.

# ClearstreamXact Security Guide

This page has intentionally been left blank.



---

**Contact**

[www.clearstream.com](http://www.clearstream.com)

**Published by**

**Clearstream Banking Luxembourg**

**Registered address**

Clearstream Banking SA  
42, Avenue JF Kennedy  
L-1855 Luxembourg

**Postal address**

Clearstream Banking  
L-2967 Luxembourg

December 2017

Document number: 6209

---