clearstream | DEUTSCHE BÖRSE GROUP

CreationOnline

Security Guide

March 2017

CreationOnline Security Guide

March 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, CreationOnline and CreationDirect 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 s a registered trademark of Microsoft Corporation in the United States and other countries. Connect:Direct® is a registered trademark of IBM International Group B.V., an IBM Company. All other trademarks are the property of their respective owners.

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

Security Guide

CreationOnline gives Clearstream customers real-time access to enhanced information, instruction input, transaction and position reporting.

About this guide

The purpose of this guide is to assist CreationOnline customer technical staff to understand the security details of CreationOnline.

Contact details

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

	Luxembourg	**Frankfurt**	**London**
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	connectfranfurt@clearstream.com	connectlondon@clearstream.com

You can also consult our website www.clearstream.com under Products and Services/Connectivity for the latest information on CreationOnline.

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.

This page has intentionally been left blank.

This page has intentionally been left blank.

1. CreationOnline

CreationOnline is a web-browser connectivity solution that allows customers to connect to the Creation platform. CreationOnline allows Clearstream Banking customers to manage instructions and holdings from a standard workstation equipped with a web browser.

CreationOnline is designed to operate over insecure networks. In order to achieve this, the application incorporates an integrated security subsystem, based on state-of-the art security software and deploying standard cryptographic algorithms and commercial-grade key lengths. This subsystem integrates into the Clearstream Banking Public Key Infrastructure (PKI).

It is assumed that the reader has an elementary knowledge of modern cryptographic techniques. For hardware and software details, please refer to the CreationOnline Technical Requirements document.

For information and support for CreationOnline, please contact **Connectivity Support** (see "Contact details" on page i).

This chapter contains the following sections:

Architectural overview of CreationOnline security

Architectural principles relating to security

The architectural principles underlying the CreationOnline security subsystem are as follows:

Scope

- The security is designed as an end-to-end solution.
- All server-side components are required to be compatible with current security baselines as defined by the IT Security unit of Clearstream Services.
- The CreationOnline workstation can be configured to be compliant with the security policy of the local site.

Standards

- Wherever possible, security services and mechanisms are based on commonly accepted standards. These standards are referenced as appropriate throughout this document.
- Cryptographic mechanisms are implemented using standard algorithms and commercial grade key lengths.
- The core network security services are implemented using standard cryptographic techniques and protocols.

Implementation

- Security mechanisms have been integrated into the application to reduce the dependence of these mechanisms on third party software, such as browsers.
- The chosen solution allows centralised updates to security software on end-users' workstations.
- Users can choose between a highly secure key storage mechanism, based on smart card technology, and a software storage mechanism.

Cryptography

- End-users generate their own cryptographic keys and send the public key for certification to Clearstream Services. This approach minimises the risk of key compromise and is a prerequisite for the non-repudiation services.
- The delay in publishing revocation information to end-users has been minimised by the use of an OCSP server, tightly integrated with the Clearstream Banking Signing Certificate Authority.

Integration with security architecture

- CreationOnline has been designed to take advantage of the Clearstream Banking security architecture.

Performance

- The security subsystem has been designed to offer a high level of performance. In particular, cryptographic accelerators are used at the server side.

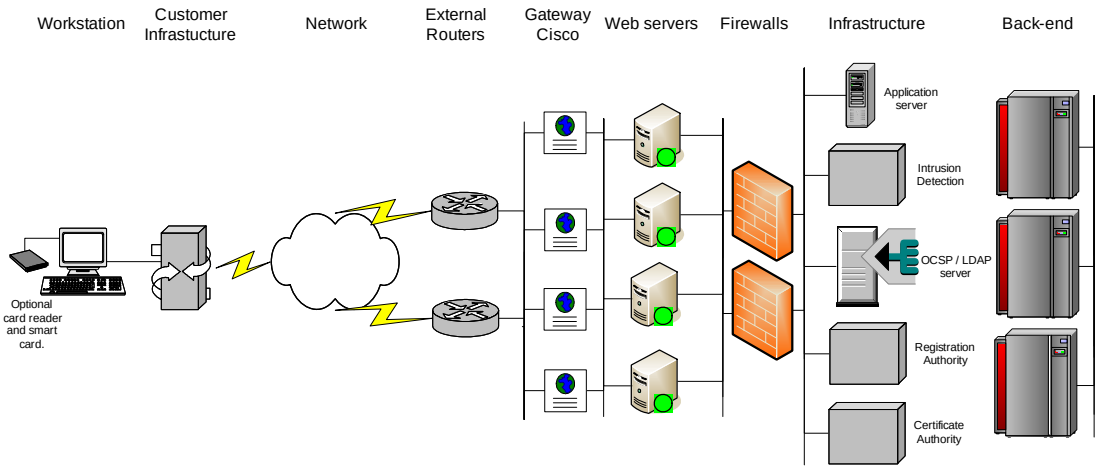
Scalability

- The security subsystem has been designed to be scalable.
- The CreationOnline system uses public key cryptography. For public key cryptosystems the number of keys required varies linearly with the number of users, whereas for symmetric key cryptosystems the number of keys required is ${}^{n}C_{2}$ where n is the number of users.

Usability

- The security subsystem has been designed to be user-friendly.
- Installation tasks are almost exclusively menu driven.
- In as far as it is possible, security functionality is transparent to the end-user.

Architectural diagram



Security components

The CreationOnline security architecture is composed of the following high-level components.

- **Server-side components:**
  - PKI core components – Certification Authority (CA), Registration Authority (RA) and LDAP database
  - On-line Certificate Status Protocol (OCSP) Server
  - nCipher cryptographic accelerators and plug-ins
  - Firewalls
  - Network intrusion detection engines
  - Other Clearstream Banking Security architecture components.

Our Network Security Infrastructure is based on a variety of equipment (routers, Firewalls, IDPS, etc.) combined with a tight integration with ISP services and application design to offer defence in depth.

- **Client-side components:**
  - Security toolkits
  - Smart cards / PKCS#12 files.

These components are briefly discussed in the following text. A full description of each component is presented in "Implementation" on page 1-15.

High-level description of components

PKI core components

The Clearstream Banking Public Key Infrastructure (PKI) is a standard PKI deployment, comprising of a Root Certificate Authority (CA), a "Signing" Certificate Authority (CA), a Registration Authority (RA) and a LDAP (Lightweight Directory Access Protocol) Directory.

The function of the root CA is to sign the certificates attributed to the signing CA(s). As this is an infrequent operation, the root CA is rarely used and is kept off-line.

The functions of the signing CA are as follows:

- Receive PKIX certification requests from the RA
- Sign a certificate based on the information received from the RA in the PKIX message.
- Return this certificate to the RA in another PKIX message.
- Publish this certificate to LDAP
- Allow revocation of certificates, either manually or from PKIX messages from the RA.
- Maintain a Certification Revocation List (CRL) and periodically publish this to the LDAP directory.

The PKIX standards referred to are published as IETF Request For Comments (RFC) documents. For details, see references. [2], [3], [4], [5] in "References" on page 1-33.

The functions of the RA are:

- To establish and verify the relationship between an end-user and his/her public key, whilst ensuring possession of the corresponding private key.
- To act as an intermediary between the CA and the end-user for all information flows relating to certificate management.

  The function of the LDAP directory is to publish information about X.509 certificates. This includes both the certificates themselves and the associated revocation information.

Software versions

- The PKI infrastructure supporting CreationOnline uses the following software packages:
  - Verizon Business Unicert
  - Sun ONE Directory Server

OCSP server

The On-line Certificate Status Protocol is documented by RFC 2560 [1]. The OCSP server is tightly integrated with the signing CA allowing pseudo real-time revocation.

Software

- Tumbleweed Enterprise Validation Authority

nCipher cryptographic accelerators

nCipher cryptographic accelerators are used at the server side to provide a secure key storage mechanism and to perform cryptographic acceleration. The nCipher cryptographic accelerators are certified FIPS 140-1 Level 2 (6). Higher security levels are not required as this material is stored in a highly secure data centre.

Both the Sun ONE web server and the WebLogic application server use plug-ins to communicate with the nCipher devices.

Hardware/Software versions

- nCipher netHSM

Firewalls

CreationOnline server-side components are protected at the network level by a layered Firewall architecture. This architecture is composed of PIX Firewalls in the first layer and Checkpoint firewalls in the second layer. The firewalls are fully meshed and load-balancing technologies are used to ensure optimal performance.

By deploying two different firewall technologies in series, the risk of a critical security breach due to firewall vulnerabilities is minimised (as both types of firewall would have to exhibit the vulnerability for penetration to occur).

Firewall versions

Outer Layer: Cisco 4 x firewalls load-balancing using Cisco switches

Inner Layer: Checkpoint Firewalls , load balanced using Stonebeat Full Cluster load balancing software.

Network intrusion detection engines

The network perimeter segments are protected by RealSecure intrusion detection engines. These engines are configured to recognise and respond to known attack signatures.

Software

- ISS RealSecure Engines and sensors.

Smart cards

The use of smart cards as a key storage mechanism at the client side is optional. Smart cards are the recommended key storage medium as they provide a higher level of physical security. In the CreationOnline deployment, cryptographic keys never leave the card. The end-user unlocks the keys by supplying a Personal Identification Number (Passcode).

For those customers who do not wish to use smart card technology, keys are stored either in a password-protected file on the hard disk of the CreationOnline workstation or on a USB drive. This environment is compliant with the PKCS#12 standard [7].

Smart card Hardware/Software versions

- Datakey DKR 731 USB smart card reader
- Athena ASEDrive 3e USB smart card reader
- Safenet eToken 4100/5100 smart cards

Other Clearstream Banking Security architecture components

The CreationOnline server-side components have been integrated into the Clearstream Banking IT Security Architecture. In this configuration, these components are protected by a number of additional security services delivered by this architecture, including:

- Operating system and database integrity checking using defined security baselines and host-based security scanners
- A three-tiered malicious virus framework
- Restricted privileged access using privilege managers
- Structured management of cryptographic keys within the context of the Public Key Infrastructure (PKI).

Summary of CreationOnline security

The CreationOnline security subsystem has been designed with true end-to-end (E2E) security in mind and is based on sound architectural principles. This subsystem is deployed as a series of components, designed to work together to deliver a number of security services.

The security services and example scenarios of how they are used are presented in the following section.

Deployed security services

The term security service is used to refer to the provision of specific security functionality without defining how this functionality is implemented. Security services are implemented using security mechanisms and/or procedures.

The following security services are deployed by CreationOnline:

- Authentication
- Protection of confidentiality
- Protection of integrity (both session and data integrity)
- Non-repudiation
- Logging and audit trail.

These services are described in the following sub-sections.

Authentication

Authentication is the process by which one principal (which may be an end-user or a software process) proves its identity to another.

In the case of CreationOnline, each end-user is a principal and needs to authenticate him/herself to the CreationOnline web server before any further communication is allowed. Similarly, the CreationOnline web server must also authenticate itself to the end-user. CreationOnline therefore deploys mutual authentication.

Detailed description of deployment

Authentication during the set-up phase

Prior to the initial configuration of CreationOnline at the customer site, it is assumed that there is no cryptographically secured channel between the customer and Clearstream Banking.

In order to configure the system and establish such a channel, a special procedure has been developed, using "out-of-band" authentication techniques. This procedure is described in "Certificate management services" on page 1-12.

CreationOnline authentication mechanisms

CreationOnline uses standard cryptographic challenge-response protocols to perform mutual authentication at logon time. This mutual authentication is carried out as part of an application-level SSL session and is based on the use of X.509v3 certificates.

The CreationOnline server certificate is generated at the time the system is launched and is signed by the Clearstream Banking signing Certificate Authority (CA) that can be verified by clicking on the "Padlock" icon in the browser window. For the procedure, see section "Verifying the signed applet" on page 1-18.

At the customer site, local security administrators supply end-users with X.509 certificates (see "Registration" on page 1-12). These certificates can be stored on smart-cards or in PKCS#12 formatted files – this is a choice made by the local site administrator.

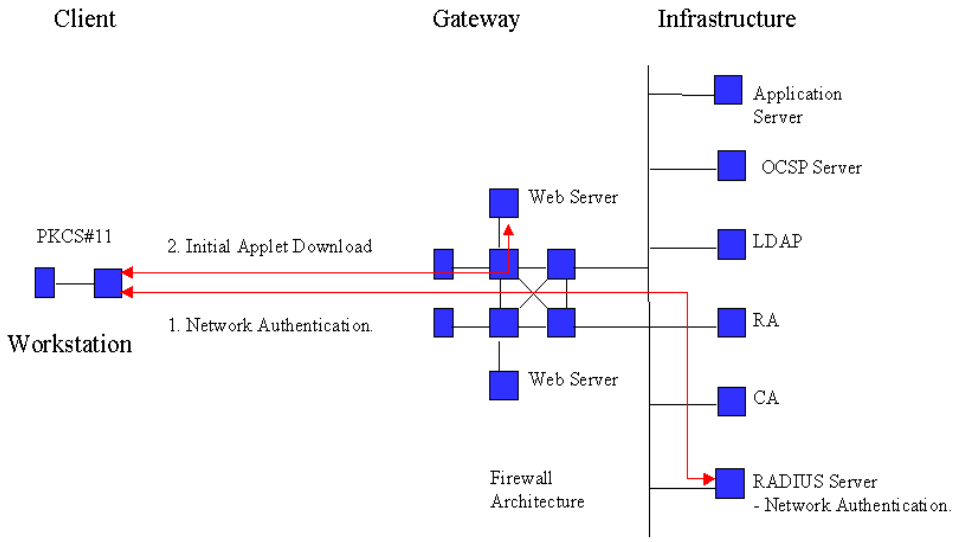
The SSL protocol uses the end-user certificates and the server certificate, together with standard public-key cryptography techniques, to authenticate the customer to the CreationOnline web server and to authenticate the CreationOnline web server to the customer. This is known as mutual authentication.

The **RSA** algorithm and **2048-bit key length** are used by the authentication protocol of the SSL session.

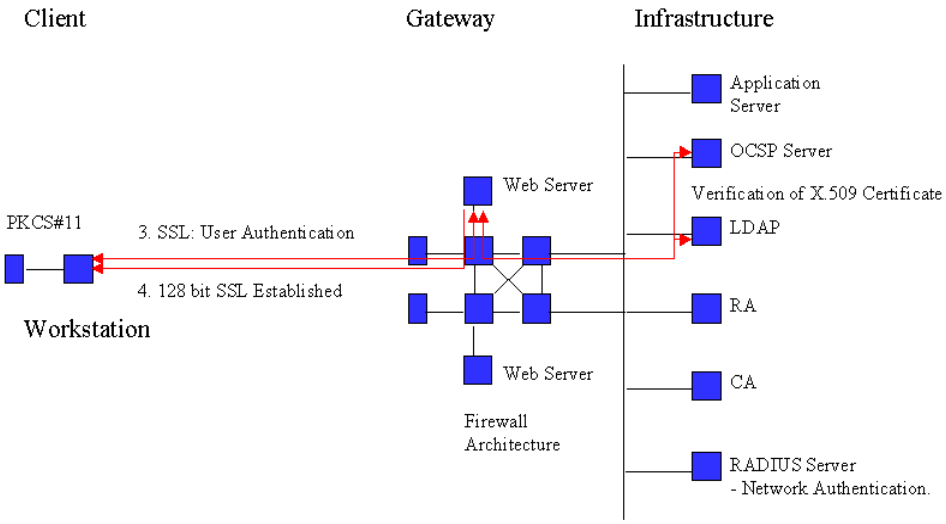
CreationOnline scenarios

The following steps are performed at logon time:

1. If VPN is used, the end-user authenticates himself/herself to the network using a static password. This is not a security mechanism and is used purely for billing purposes. This password is verified by a RADIUS server (Remote Access Dial-In User Service), at the Clearstream Banking site. For details of the RADIUS protocol see reference [8] in "References" on page 1-33.
2. The end-user starts a CreationOnline session by clicking on appropriate URL on the Clearstream Banking CreationOnline web server.
3. This triggers the establishment of a browser to browser 128-bit SSL session. The applets implementing the business and security functionality are downloaded over an HTTP session. These applets are digitally signed.



4. The applet initiates an application-level SSL session to the CreationOnline application server using 128-bit cryptographic keys. The mutual authentication is performed as part of this SSL session. Certificate revocation information is checked at this time using the On-line Certificate Status Protocol (OCSP). In order to achieve this, the web server sends an OCSP request to the OCSP server as part of this process.



5. The net result of this process is the establishment of an authenticated, application-level SSL session.

Protection of confidentiality

The confidentiality of data is said to be preserved if the data can only be read by a pre-defined target group. The data is said to be confidential with respect to this target group.

For CreationOnline, the target group for all network flows is restricted to the sender and the receiver. For information stored on systems belonging to Clearstream Banking, the target group is restricted to authorised Clearstream Banking staff (authorisation is provided on a "need to know" basis).

Detailed description of deployment

Confidentiality of data exchanged between the end-user workstation and the Clearstream Banking CreationOnline web server is ensured by the SSL protocol.

The **AES or 3DES** algorithm and **128-bit key length** are used to encrypt data within the SSL session.

CreationOnline Scenarios

Initial signed applet download

CreationOnline uses an application-level SSL session to protect data exchanged between the end-user workstation and the web server. By implementing the SSL session within the application, the security mechanisms are as independent as possible of the underlying browser and operating system software.

However, the application-layer SSL session is initiated by the applet resident on the end-users workstation and therefore cannot be used to protect the download of the applet itself.

As there are no requirements to protect the confidentiality of the applet (which contains no sensitive business data), initial applet download over an insecure session is not an issue.

Other information exchange

Following the successful download of the applet, all exchange of information between the end-user's workstation and the CreationOnline web server is protected by the application layer SSL session.

Protection of integrity

Data integrity is said to be preserved if the data received over a network connection by the receiver is identical to that sent by the sender.

Session integrity is said to be preserved for a network connection if all packets sent by the sender are received by the receiver in the correct sequence with no losses or additions. In addition, there must be no possibility of replaying either the session itself or individual packets at a later time.

Detailed description of deployment

Network integrity protection is implemented at two distinct levels by CreationOnline:

- Integrity protection mechanisms integrated by SSL.
- End-to-End (E2E) Digital Signatures.

SSL integrity protection mechanisms

The SSL protocol incorporates mechanisms for protecting the integrity of the session and the data transported over the session. For the CreationOnline implementation, this is achieved using Message Authentication Codes (MACs) generated using the MD5 and SHA message digest algorithms.

E2E Digital Signatures

CreationOnline protects the following types of communication using an end-to-end digital signature.

- Setting the default predefined security parameters.
- Updates to predefined security parameters.
- Deletion of predefined security parameters.
- Performing a life cycle step of any cash instruction (release, verify, ...).
- Performing a life cycle step of any Triparty Repo instruction (release, verify, ...).
- Performing a life cycle step of the securities instruction (release, verify, ...).
- Performing a life cycle step of the custody instruction (release, verify, ...).
- Performing a life cycle step of the message exchange instruction (release, verify, ...).
- Performing a life cycle step of the Business special service instruction (release, verify, ...).
- Sending a broadcast notification.
- Adding a distribution list to the system.
- Updating a distribution list.
- Managing the life cycle of a scheduled report (create, approve, ...).
- Managing the life cycle of a user, user group or OU (create, approve, ...) including CreationDirect.
- Generating credentials.

Depending on the context, this signature is either (a) generated on the end-user workstation and verified on the CreationOnline application server or (b) generated on the CreationOnline application server and verified on the end-user workstation.

CreationOnline Scenarios

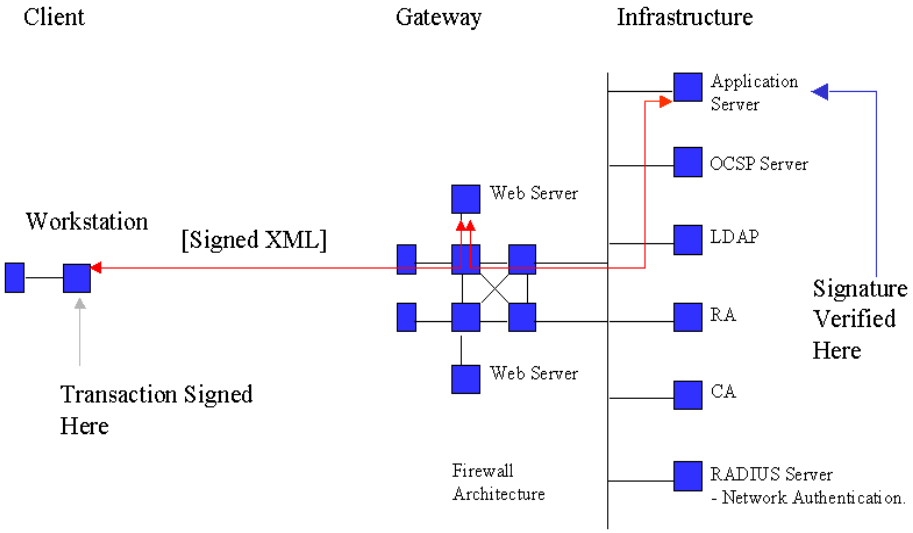
Signed messages client to server

The following steps are performed when generating a signed message:

1. The end-user uses the CreationOnline interface to generate a business message. The fact that the message is signed is transparent to the user – there are therefore no special actions required.
2. The CreationOnline software detects that this message should be signed. This software generates the digital signature and appends it to the message.
3. The message is then sent in the usual way.

The following steps are performed when verifying a signed message:

1. The message is received by the Clearstream Banking CreationOnline web server.
2. The CreationOnline web server transmits the message, together with the appended digital signature, to the CreationOnline application server.
3. The CreationOnline application server checks the validity of the signing key by looking up and verifying the X.509v3 certificate corresponding to this user and subsequently verifying the signature.
4. A record of the verification is stored in a local database.



Non-repudiation

Repudiation is the process by which a party denies having performed some action (such as sending or receiving a particular message) during the course of a communications session. A non-repudiation service is a set of technical and procedural controls aimed at preventing the repudiation of actions, which occur during a communications session.

Detailed description of deployment

CreationOnline uses digital signatures in combination with logging and audit trail services to deploy non-repudiation.

The client software and server software use application-level private keys to sign messages and signatures are verified using the information in the corresponding X.509 certificates.

The **RSA** algorithm and **1024-bit key length** are used by the application to create digital signatures.

CreationOnline Scenarios

Signed messages

This scenario is as described in "CreationOnline Scenarios" on page 1-10.

Logging and audit trail

For security purposes logging is performed to provide non-repudiation. This requires the message and corresponding signature to be copied to a database in order that the user's signature on the message can be verified at any time in the future.

The audit types listed below are those deemed to provide a full audit trail for any message flow between client and server. The Audit log is kept online for the previous 12 months, plus the current month. Older logs are archived for 15 years.

Vestima+ logs are kept on the Vestima+ application.

Detailed description of deployment

The following services are logged. Each service is actually a heading for a list of detailed actions performed by the user which are logged.

- Balances
- Predefined Parameters
- Cash Instructions
- Securities Instructions
- Custody instructions
- Repo instructions
- Tax instructions
- Message exchange instructions
- Business special service instructions
- Notification
- Reporting
- User Management.

The following audit event type families are audited:

- Alerts
- Reporting

- User management
- OU management
- Securities C&S
- Cash
- Queries.

Where applicable, the date and time of the generation of the audit event, the organisation unit to which the audit event refers, the account number, and the user id are logged.

CreationOnline Scenarios

Signed messages client to server

This scenario is as described in section "CreationOnline Scenarios" on page 1-10.

Certificate management services

The network security services deployed by CreationOnline are implemented using standard cryptographic techniques and protocols. As such, CreationOnline uses both symmetric cryptography and asymmetric (or "public-key") cryptography.

The procedures and mechanisms used to manage public and private key pairs are collectively referred to in this document as certificate management services, as they are largely synonymous with management of the associated X.509v3 certificates.

This section provides the details of how such services are implemented for CreationOnline.

Registration

For the purposes of this document, the term registration covers all activities leading up to, but not including, the signing of a X.509 certificate.

Administrator and end-user certificates

CreationOnline defines two distinct user roles:

- Local security administrators
- End-users.

Local security administrators are responsible for configuring the CreationOnline security subsystem at the customer site (see "Troubleshooting" on page 1-27 and "Glossary" on page 1-30) and for all local aspects of certificate management. This includes generating keys for end-users and registering the resulting certificates with Clearstream Banking.

End-users are business users of CreationOnline and have no specific security-related responsibilities other than due care in protecting their security credentials.

Overview of the registration process

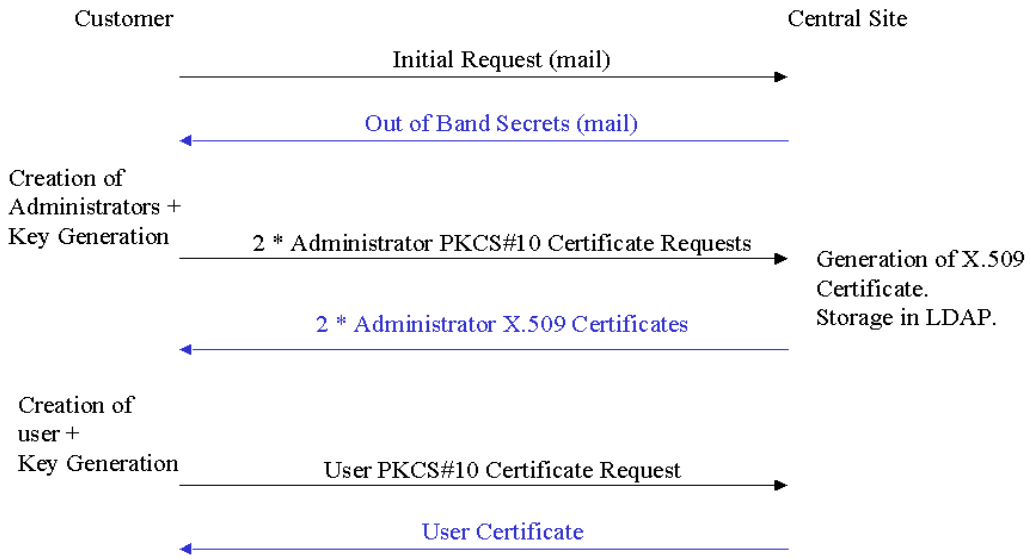
This section provides an overview of the certificate management activities performed as part of this activity.

1. Following the application by a customer to use CreationOnline, Clearstream Banking generates two random authentication codes and splits each code into two parts. The first part of each of these codes is sent by secured mail to the customer security contact.
2. The customer carries out the local software installation. This process involves installing a key file that contains the certificate of the Clearstream Banking CreationOnline web server and verifying

this certificate. This in turn enables the local security administrator to authenticate the Clearstream Banking CreationOnline web server.

3. The business information sent by the customer as part of the application process is used to initialise CreationOnline. Once this has been done, the second parts of the authentication codes are sent to the customer's security contact.
4. The customer's security contact generates key pairs for two administrators (see "Key generation" on page 1-13 and "Glossary" on page 1-30) and uses the two random authentication codes to register the corresponding public keys with the Clearstream Banking PKI. Although the details of this process are transparent to the users, CreationOnline generates a PKCS#10 message for each of the two key pairs that are to be registered.

   The authentication codes referred to above are used to authenticate these requests to the Clearstream Banking Registration Authority (RA). This authentication relies on the generation of a HMAC [11], where the out-of-band authentication code is used to generate the key.
5. Upon successful verification of authenticity, the administrator certificates are signed by the Clearstream Banking signing CA and published in the LDAP directory. The signed certificates are then sent back to the local administrators.
6. Once the administrator certificates have been registered, the local security administrators are able to create new users. Creation of a new user normally requires two local administrators (principle of dual control), but this can be overridden by the local site administrators if local policy allows for this.
7. Administrators register certificates for end users by signing the corresponding PKCS#10 messages with their signing keys.



Key generation

Clearstream Banking central site components

All public/private key pairs generated within Clearstream Banking for CreationOnline components are generated within FIPS 140-1 Level 1 Hardware Security Modules. Random seeding entropy is provided from system data as specified in the Level 1 requirements and no user seeding data is required. Miller-Rabin testing is used by nCipher and Verizon Business Hardware security modules.

Client-side component

All public/private key pairs used by customers are generated at the customer site through the CreationOnline user management interface.

As part of the RSA key generation process, administrators are asked to provide randomised input by moving the mouse and/or typing on the keyboard. The application uses 20 bytes of this random data to seed the pseudo random number generator (prng). This prng is always a Blum-Blum-Shub generator with a 512 bit modulus.

The public exponent is always set to 65537 (the 5th Fermat number, 2^(2^5)+1). The prng is then used by a probable prime generator that generates a random odd number p of the required size, such that the gcd of p-1 and the public exp is 1.

The function then tests p for primality by performing trial division by the 995 smallest primes and running 5 iterations of the Miller-Rabin test. If the number is not a prime, 2 is added to the number and the test is run again. 2 suitable primes are generated and the secret exponent is generated. The private key is always stored in CRT format.

Certificate registration

Once generated, public keys are sent to the Clearstream Banking Registration Authority using PKCS#10 messages signed by the administrator who created the CreationOnline account (see "Authentication" on page 1-6 for details of how administrator certificates are authenticated).

Revocation

The term revocation refers to the operation of rendering a X.509 certificate permanently invalid.

Revocation of user certificates can be performed remotely by a customer administrator, or centrally by Clearstream Banking administrators. Revocation of a user's certificates results in the following actions:

- The Clearstream Banking Certification Authority publishes and signs an updated Certificate Revocation List (CRL).
- The CRL is published to the LDAP directory master and slave instances.
- A "stop" flag is entered in the user account profile database.
- The users certificate serial number entry in the user database is set to a null value.

The above revocation actions are performed within 10 seconds of the Certification Authority receiving the revocation request.

In the event that a customer needs to revoke a certificate and is not able to connect and perform the revocation via the application GUI, certificates can be revoked by contacting the Clearstream Banking Connectivity Support Help Desk (see "Contact details" on page i) and providing a separate confirmation of the request via an authenticated channel such as SWIFT.

Revocation scenarios

Revocation of certificates is performed automatically under the following circumstances:

- When a user generates new credentials via the CreationOnline GUI. The old certificates are revoked.
- When a user moves to smart card key storage. New keys are generated by the smart card and the old keys are revoked.
- When the Customer OU administrator removes a user.

Manual revocation of certificates may be required in the following situations:

- When an OU administrator suspects their keys may have been compromised for any reason.
- When Clearstream Banking staff need to suspend the operation of an account for any reason.
- When a revocation request, authenticated by a SWIFT message or other authenticated medium, is received and confirmed by Clearstream Banking.

Implementation

An architectural overview of the design model will be presented. This describes the main components in the design of the system that define the key behavioural and structural mechanisms.

The implementation is completely in Java, except the only native component (C, C++) being the native smart card DLL supplied by Safenet.

Architecture of client workstation

The implementation of the client is such as to provide all the security services necessary to communicate securely with the server. This necessarily includes credentials handling and secured I/O streams for signing and verifying over SSL to provide confidentiality, integrity, authentication and non-repudiation.

Identification of security components

The following components comprise a grouping of model elements constituting a specification of the behaviour offered in that component.

- Client SecuredTransport
- Client HTTPS
- Client HMAC
- Client PKI libraries
- Client Entropy

Client SecuredTransport

The client SecuredTransport component is used directly by the applet to transport securely business commands to the business logic hosted by the application server. This component uses an I/O stream model in that it provides seamless secure input and output streams between the client and server. All the security functionality is hidden by the stream abstraction. Secure input and output streams between client and server are provided in the form of standard InputStream and OutputStream interfaces which present Java I/O interfaces and hide the details required to sign and verify the data buffers.

UserCredential and UserCredentialAccessor classes provide an abstract interface to the user's physical security credentials regardless of the physical storage medium (smart cards or file).

Client HTTPS

The client HTTPS component provides the necessary extension of a URL over SSL to communicate with the web server using the SSL protocol.

Client HMAC

The client HMAC component provides all the HMAC functionality required by the client. For OU administration HMACs are used to sign I/O streams to the server. Behaviour includes generating the HMAC key and encrypting the client authentication code.

Client PKI libraries

The client PKI component provides the abstraction of dual key and certificate request generation for any key medium.

Client Entropy

The client Entropy component provides the required functionality for processing and generating sufficient randomness to seed a strong random number generator for key generation.

Server-side security implementation

All requests from the client are processed through a servlet which accesses security components implemented as distributed Enterprise Java Beans running in a Weblogic application server container. All business messages must be processed by the security layer and only on successful completion of the security checks are the messages forwarded to the business beans.

Identification of security components

The following components comprise a grouping of model elements, which constitute a specification of the behaviour offered in that component.

- Server SecuredTransport
- Server HMAC
- Server MessageLog
- Server nCipher
- Server OCSP
- Server Registration
- Server PKI
- Server UserAccessor

Detailed description of each component

Server SecuredTransport

The CreationOnline servlet processes secure messages using a server SecuredTransport component, which supplies an authenticated stream provider exposing VerifyingInput, and SigningOutput streams that hide verifying, logging and signing components behind an I/O stream abstraction. Responses back to the client are signed using a SigningOutputStream, which delegates the signing process to the nCipher server component.

Server HMAC

The server HMAC component provides all the HMAC functionality required for the server. For OU administration, the server verifies HMACs coming from the client. Encrypted authentication codes are copied to the database and decrypted by the nCipher component during HMAC verification.

Server MessageLog

The server MessageLog component abstracts all the interaction with the database required by the security layer to provide non-repudiation.

Server nCipher

The server nCipher component abstracts all the interaction with PKCS#11 hardware, which implements signing, verifying, decryption, session and key management functions.

Server OCSP

The server OCSP component abstracts all the interaction with the OCSP server to validate a user's signing certificate.

Server Registration

The server Registration component abstracts all of the registration and revocation process and provides the implementation of high level interfaces to user management functions such as registerNewUser, changeCredentials and stopUser.

Server PKI

The server PKI component is the CreationOnline RA, which implements all the PKIX certification and revocation request handling to the Clearstream Banking CA. A policy is applied to each certificate registration and revocation request being processed.

Server UserAccessor

The server UserAccessor component implements user certificate validation against the CreationOnline database.

Guidelines for client-side implementations

Security policy

CreationOnline has been designed to be as flexible as possible with respect to the requirements of the local site security policy. In particular:

- The security of the underlying operating system can be configured in accordance with local security baselines.
- Although the recommended configuration implements the principle of "dual control" for local security administrators (that is, two administrators are required to create an end-user), this can be deactivated if required.
- The customer has the choice of deploying smart cards or PKCS#12 files as a key storage mechanism.
- Implementing CreationOnline has a minimal impact on local system and security administration procedures. Those security administration procedures that are required by the application are carried out using the CreationOnline user interface.

Integrating with firewalls

CreationOnline is implemented using internet technologies. It is therefore highly recommended that customers using CreationOnline protect their interior networks from the outside world using Firewall architecture.

In order to run CreationOnline through a firewall, the following protocols need to be allowed to traverse the firewall to www.creationconnect.com (or creationonline.clearstream.banking in case of VPN):

- HTTPS uses port 443 for the initial website connection and for the interaction with the application. A 128-bit key size is used in the encryption algorithm
- HTTP uses port 80 for the download of the Java applet, that can therefore be cached.

Only outbound sessions are required to be enabled for these ports.

Storing Authentication Code Letters for future use

Local security administrators are requested to securely store the initial "out of band" authentication codes used to initialise the system. In a situation where one or both of the customer administrators accounts have been blocked through incorrect password entry or certificate expiration. The only alternative is to re-send new codes by registered mail or express courier, incurring a delay of several days.

These codes can also be used to authenticate the administrators in the event that the initial registration of keys fails and replacement credentials must be sent out. The procedure for this is as follows:

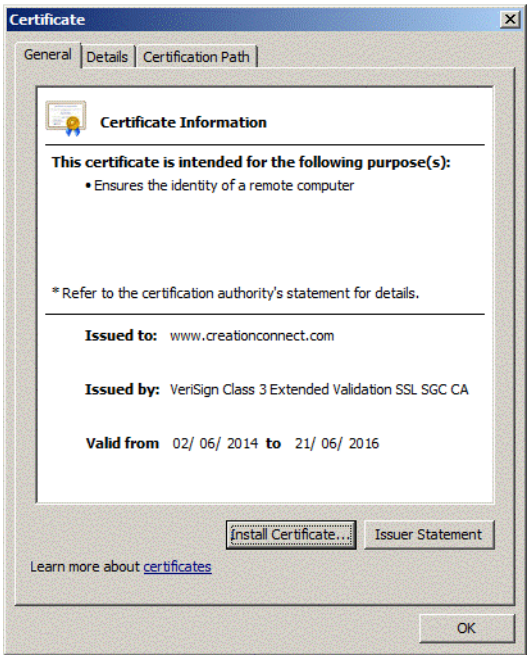
- The customer should contact Clearstream Banking Connectivity Support Help Desk (see "Contact details" on page i).
- New credential files created with the original Authentication code as the password will be sent to the customer via e-mail.

Verifying the signed applet

The Application JAR files that make up the application are all digitally signed by the Clearstream Banking code signing certificate issued by Verisign. This signature is verified automatically upon download of the JAR files by the Java Runtime Environment against the Verisign Root CA certificate stored in the JRE keystore.In case there are verification errors the user is alerted by a pop-up from the JRE.

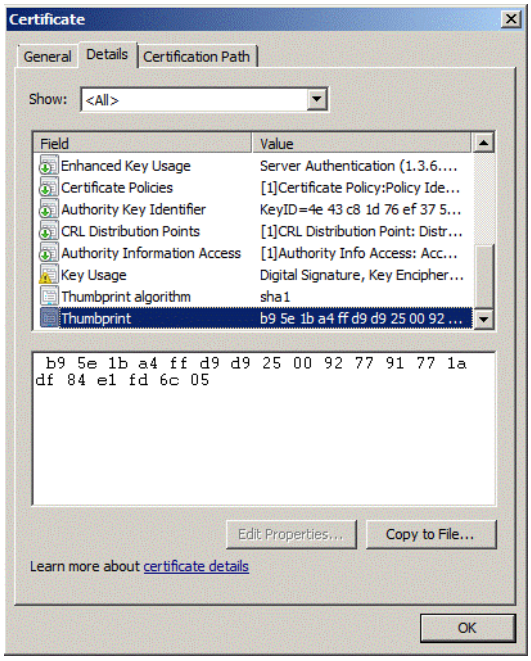
Verifying the server certification

The validity of the Clearstream Banking web server hosting the CreationOnline Java applet can be verified by clicking on the "Padlock" icon in the bottom right-hand side of the browser window.



In this window, select "Details".

The thumbprint value b9 5e 1b a4 ff d9 d9 25 00 92 77 91 77 1a df 84 e1 fd 6c 05 can be found in the screen shot below:



Use of Java cache

CreationOnline consists of multiple signed Java JAR files. During the initial connection to the CreationOnline web server, these signed JAR files are downloaded, the signature is verified, and they are stored in the Java Virtual Machine JAR cache. On subsequent connections, if no newer versions of the JAR files exist on the Web server, the cached JAR files are used.

To refresh the JAR files and ensure a new download of all files, the JAR cache can be suppressed manually using the Sun Java console on the control panel of the client PC.

JAR files are downloaded using the HTTP protocol, this allows customers to cache JAVA files in their proxy servers. When JAR files are updated, the proxy server does not always recognise the new JAR file. When this happens, it is necessary to clean the proxy JAR files.

Use of a proxy server

CreationOnline involves **two** distinct SSL sessions, as follows:

- A 128-bit SSL connection (TCP port 443) handled by the browser or Java Web Start to download the application HTML page.
  - If you are connecting via the Orange VPN, connect to:

    https://www.creationonline.clearstream.banking IP: 194.235.205.65
  - If you are connecting via the public internet, connect to:

    https://www.creationconnect.com IP: 194.36.230.101
- An HTTP connection (TCP port 80) handled by the Java Runtime Environment to download the Java applet.
  - If you are connecting via the Orange VPN, connect to:

    https://www.creationonline.clearstream.banking IP: 194.235.205.65

- If you are connecting via the public internet, connect to:

  https://www.creationconnect.com IP: 194.36.230.101

  By default, the Java runtime is configured to use the browser's proxy settings.

  Once the applet has been downloaded the connection to CreationOnline is cut.

- A second 128 bit SSL connection handled by the Java applet.
  - If you are connecting via the Orange VPN, connect to:

    https://www.creationonline.clearstream.banking IP: 194.235.205.65

  - If you are connecting via the public internet, connect to:

    https://www.creationconnect.com IP: 194.36.230.101

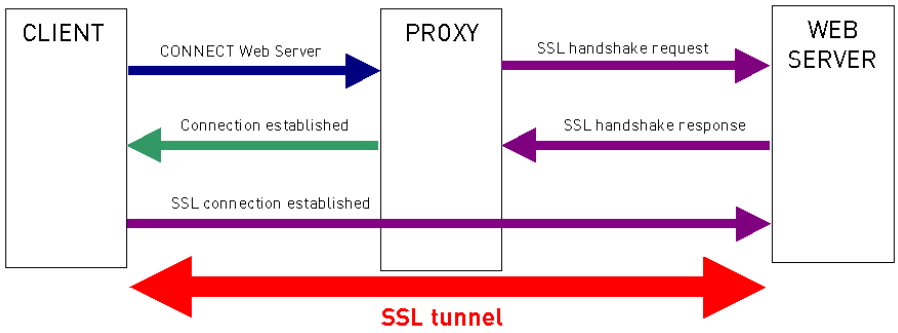
You must specify the details of your proxy server, for example host and port on the login page of CreationOnline

You can tick the HTTP 1.1 option to use the http keep-alive feature.

Proxy servers and SSL tunnelling

SSL employs a security **handshake** that is used to initiate the TCP/IP connection. This handshake results in an agreement between the client and the server as to the level of security to be used. After the handshake, SSL encrypts and decrypts the bytestream of the application protocol being used (that is, HTTP).

When a client requests an SSL connection to a secure web server through a proxy server, the proxy opens a connection to the web server and then simply copies data in both directions without intervening in the secure transaction.



In order to do this, the client has to send a **CONNECT** SSL packet to the proxy server, instead of trying to initiate the SSL handshake directly with the web server.

Authentication on proxy servers

Proxy servers can authenticate users to access internet resources in any of the following ways:

- **Anonymous** (that is, no authentication): any user can use the proxy.
- **Basic** (standard authentication): on connection, the user is prompted for user ID and password.
- **NTLM**: NT user account is used for authentication on the proxy server.
- **Digest**: Not common but a very secure standard.

Proxy servers directly supported by CreationOnline

CreationOnline natively supports and has been tested with the following proxy servers:

- SQUID

- Microsoft ISA server
- Blue coat
- Netscape proxy

The authentication algorithms supported are **Anonymous** and **Basic**.

The use of these proxy servers and the supported algorithms can be configured by an initial administrator through CreationOnline itself, as described in the section on accessing CreationOnline in the CreationOnline Installation notes and the CreationOnline Installer Guide.

For details of how to configure CreationOnline for use with proxy servers that employ NTLM or Digest authentication, see "Configuring CreationOnline to support a proxy server that uses NTLM or Digest authentication" below.

Configuring CreationOnline to support a proxy server that uses NTLM or Digest authentication

CreationOnline supports the Anonymous and Basic authentication algorithms. If NTLM or Digest authentication is used on the proxy server, you can do one of the following:

- Modify the authentication protocol for all or (if possible) for specific workstations;
- Allow direct connection to CreationOnline through the company firewall, without using NTLM authentication;
- (for Microsoft proxies only) Install a proxy/firewall client on the workstation.

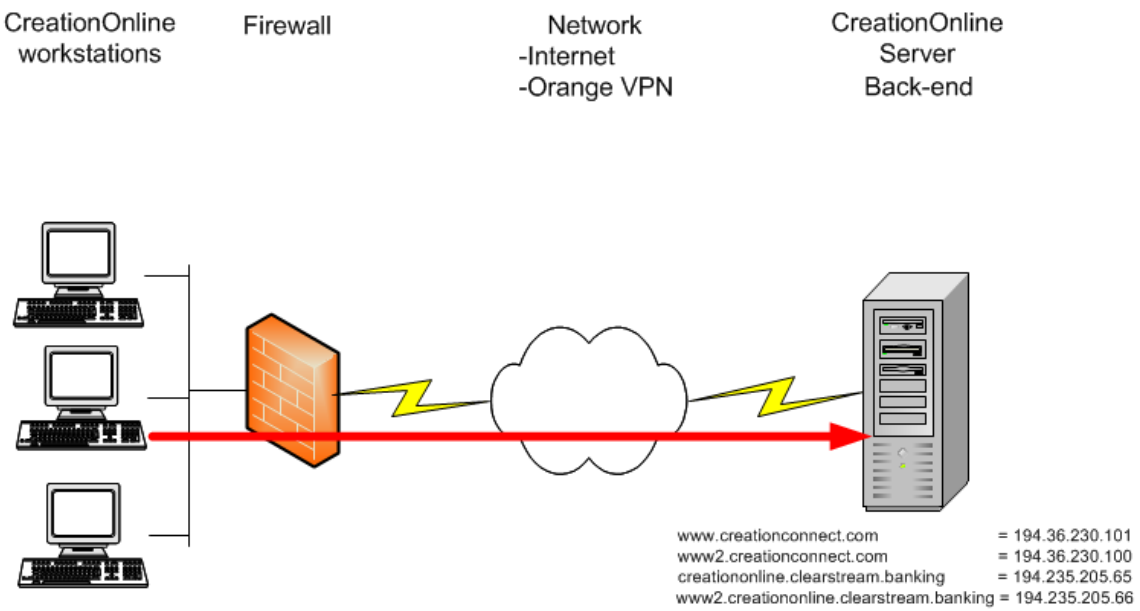
Modifying the authentication protocol

You can change the authentication protocol of the proxy server to Anonymous or Basic and then configure CreationOnline accordingly (see the section on accessing CreationOnline in the CreationOnline Installation notes or the CreationOnline Installer Guide).

Note: Some proxy servers (for example, SQUID) can be configured for different workstations to use different protocols. This means that, of the workstations connected to a proxy server, you may be able to configure some to use CreationOnline while others are used for other applications requiring a different authentication protocol.

Allowing direct connection

The connection type is as shown in the following illustration:



Note: The illustration above shows either an internet connection or a VPN connection.

The connection must be configured at two levels: on the workstation (Internet Explorer settings) and on the company firewall level.

Note: In most cases, to interact with the firewall, the workstation's IP address must be fixed and reserved on the network. DHCP services cannot be used.

Internet Explorer settings

Internet Explorer must know that CreationOnline requires direct connection instead of the proxy connection.

This can be done in either of the following ways:

- manually, by configuring the exceptions list

  In Internet Explorer, Tools menu: Internet Options, Connections tab, LAN Settings button, Advanced button, add the following CreationOnline host URLs to the Exceptions list:

- If you are connecting via the Orange VPN:

  https://creationonline.clearstream.banking

- If you are connecting via the public internet:

  https://www.creationconnect.com

- automatic, if Internet Explorer is configured to use an automatic configuration script

  The script must be configured to enable DIRECT connections. The network administrator will be responsible for this. The following is an example of an automatic proxy configuration file for an internet connection:

```
function FindProxyForURL(url, host)
{
if (isInNet(host,"194.36.230.101","255.255.255.255"))
return "DIRECT";
}
```

Company firewall settings

The company firewall must be configured to allow HTTPS traffic from the CreationOnline workstations to the CreationOnline servers. This can be configured very easily on a Checkpoint Firewall as follows:

Source	Destination	Service	Action	Track	Install On	Time	Comment
Creationonline_workstations	www.creationconnect.com www2.creationconnect.com	https	accept	Long	Gateways	Any	CreationOnline workstations: Direct connection allowed

The firewall must also be configured to allow HTTP.

Security considerations

Most companies use proxy servers to connect to the internet in order to filter content, restrict sites and add an additional level of protection for their users' workstations.

Opening the company firewall as described above does not increase the level of risk:

- The traffic is only open from the internal network to the external world.
- The Source and Destination IP addresses are clearly restricted.
- The Service is restricted to the minimum requirement
- Mutual authentication is used in CreationOnline, which means that neither the Source nor the Destination addresses could be "spoofed" without the user noticing it.
- All communication is still encrypted and message integrity is verified.

Installing a proxy/firewall client on the workstation

Note: This option is valid for Microsoft proxy servers only.

With Microsoft ISA server, Microsoft supplies a Firewall client.

The software can be installed at the administrator's discretion. The software should be installed on all client workstations that will be using CreationOnline. This client intercepts the network traffic on the PC at the socket layer and redirects it to the proxy server.

Also, the software handles the entire communication and redirects all traffic to the proxy server. There is no need for the user to configure CreationOnline for proxy settings via the logon screen as described in the section on accessing CreationOnline, in the CreationOnline Installation notes, or in the CreationOnline Installer Guide.

Microsoft ISA server: Firewall client

This client software handles Microsoft authentication in a way that is transparent not only to the user but also, in the case of CreationOnline, to the Java applet. As a result, the applet performs the authentication without causing problems to Microsoft ISA server. Please refer to Microsoft ISA server documentation for a correct setup. Microsoft ISA server client is provided with Microsoft ISA server installation.

Proxy dialog box auto-detect option

Each time the user starts CreationOnline, the auto-detect feature will automatically read the proxy details from the user's Java™ settings and populate the Host Name and Port parameters as appropriate.

Note: Java proxy settings can be set to the user's browser settings in the Java Control Panel.

If your proxy requires user identification, you will have to enter the details in the respective Proxy User Id and Proxy User Password fields. These values will not be auto-detected but will be saved for later use.

If proxy settings are not found during auto-detection, the user will have to select Manual and enter the details manually. Where a proxy server is not used, the default "Direct Connection" must be specified.

Use of HTTP 1.1

If your network, proxy, firewall(s), router(s), ISP and/or internet route to Clearstream supports HTTP 1.1, you will be able to use the new checkbox to specify this. This feature will contribute significantly to improved performance because, under HTTP 1.1, the TCP connection will not be closed and re-created for each request, thus saving network time and reducing network traffic in general, resulting in shorter application response times.

By default (checkbox not ticked), HTTP 1.0 will be used.

Performance considerations

An additional setting is required for performance reasons.

The Java plug-in performs DNS reverse lookup queries on the host to which it is trying to connect. In the case of a connection via a proxy server, the reverse lookup is done on the IP address of the proxy server (and not on the IP address of the web server as with direct SSL connections).

This means that the customer's DNS server (or local hosts table) must be configured with an entry for the proxy server as well as the reverse entry.

Smart cards versus PKCS#12

Customer sites can opt for software key storage (PKCS#12 files) or hardware key storage (smart cards). The recommended configuration is to use hardware key storage.

Integration with other Java applications

With the exception of the fact that CreationOnline requires a particular version of the Java Runtime Environment (JRE) to run correctly, there are no other restrictions affecting the ability of the local site to run other Java applications.

Use of ActiveX within CreationOnline

The application does not use any ActiveX controls in any part of the applet/application and no ActiveX controls are downloaded by the application at any stage. Any customer site that blocks ActiveX technology at their network gateway will be able to run CreationOnline.

However, the entire Java Runtime Environment interfaces to Internet Explorer by appearing as an ActiveX control. When the JRE is installed locally via CD, it is installed as an ActiveX component and the browser sees it at such. This is a feature of Sun and Microsoft's installation approach and cannot be changed. All Java applets work in this way and this is standard industry practice.

For customers who utilise a policy of disabling all ActiveX controls at the browser, use of CreationOnline can be enabled by specifying "Administrator Approved" for the JRE. All other ActiveX controls remain disabled. This configuration can be distributed using the usual distribution mechanisms available in Windows systems.

The <OBJECT> tag is used to load an ActiveX control within a web page. When Internet Explorer parses this HTML it will first check the registry to see if the object is already installed by searching for the classid listed. If the object is installed, then the registry entry will list the program file to run. This is the case for the JRE and CreationOnline.

Within each IE security zone there is an option to only run controls that have been "Administrator Approved". The "Administrator Approved" setting can enforce security policy after a control has already been installed. This applies to the JRE which has already been installed and which is identified by its classid within the CreationOnline HTML download page.

The JRE control can be configured to execute, within the context of an ActiveX disabled policy, in the following steps:

1. Within IE, set: Internet Options > Security > Custom Level > Run ActiveX controls and plug-ins > Adminstrator approved.
2. Then apply the registry settings corresponding to your JRE.

```
2. 2) [HKEY_CURRENT_USER \SOFTWARE \Policies \Microsoft \Windows
\CurrentVersion \Internet Settings\AllowedControls]
"{CAFEEFAC-CLSID version}"=dword:00000000
```

The above classid uniquely references the JRE and only this control is permitted to execute.

Internet versus intranet risks

In general, intranets are regarded as being associated with less risk than the Internet. This is because such environments are assumed to be accessible by a restricted number of users, often under the control of the organisation implementing the intranet. The public Internet is essentially a federation of independent networks and is therefore deemed to be associated with greater risk.

In assessing the risks associated with specific intranets, it is important to have a clear view of the connectivity within the intranet. If a participant in the intranet is also connected to the Internet, there may also be a route from the Internet to the intranet and vice versa. In this case, the intranet becomes a part of the Internet.

The usual way of dealing with this situation is to adopt a defensive stance with respect to an intranet whose connectivity scheme is not known. This typically involves deploying a Firewall architecture at the gateway between the internal network and the intranet access point and possibly deploying other network security services such as intrusion detection.

Java mobile code security risks and mitigations

Java presents a multi-tiered approach to security. At a general level, the tiers include:

- Restricted access to file systems and the network;
- Restricted access to browser internals;
- A set of load time and runtime checks to verify that byte code is following the rules;
- A system for signing code and assigning it some level of capability.

In addition to a number of advanced language features like array bounds checking and byte code validation, Java provides:

- A set of cryptographic APIs for standard algorithms;
- A strong, stack-based security system.

Potential risks

The following introduces some of the types of risk that web-browser based applications may be subject to:

- System Modification: the most severe class of attacks. Applets that implement such attacks are attack applets. Consequences of these attacks: severe. Java defence is strong.
- Invasion of Privacy: these are implemented by malicious applets. Include mail forging. Consequences of these attacks: moderate. Java defence is strong.
- Denial of Service: these attacks can bring a machine to a standstill. Also implemented by malicious applets. May require re-boot. Consequences of these attacks: moderate. Java defence is weak.
- Antagonism: merely annoying, this attack class is the most commonly encountered. Implemented by malicious applets. May require restart of browser. Consequences of these attacks: light to moderate. Java defence is weak.

Mitigations

With the major changes in the Java 2 security architecture come a number of important responsibilities, the most important of which is mobile code policy creation and management. Essential to any mobile code system that makes use of code signing is the use of a solid key management capability, that is, a PKI.

- **Malicious applets:** the best alternative is to set a security policy that allows only applets signed by trusted parties to run. But if the requirement is to surf with a Java-enabled browser and run every Java applet on the Web, the safest thing to do is to avoid unknown and untrusted Web sites unless Java is disabled.
- **Annoying applets:** (for example, Business Assassin applet) Java has attracted its share of bad programmers and bad Java code can be annoying. To be counted as a hostile applet, some malicious intent on the part of the author is usually required, but a poorly written Java applet may aid a real cracker in breaking a Java security system. The best guidance is to avoid running bad code, and to make sure that code being run has adhered to sound software engineering practices.
- **Denial of service applets:** guidance is to use resource allocation limitations. For example, placing upper limits on CPU usage, on the number of instructions that can run, or on the number of windows allowed is one line of defence.
- **Attack applets:** each has been implemented by either the Secure Internet Programming team (SIP) at Princeton University (see, for example, www.cs.princeton.edu/sip/java-faq.html) or other researchers. To date, 16 serious security problems have been discovered in implementations of Java. Some of these flaws allow full system penetration.

The CERT Co-ordination Centre (an organisation that keeps track of computer security violations on the Internet), have stated that there have been no confirmed reports of loss due to attacks exploiting these security holes.

While most of these problems have been fixed in all Java-enabled versions of Microsoft Internet Explorer, it my still be possible for the some of the above weaknesses to be exploited in different ways. Other problems have not been fixed at all. General guidance in this area is to keep the operating system of the PC fully patched, including all up to date security patches, along with security patches for any browser being used on the PC. This is particularly relevant for any new operating system, such as XP.

Credential and Password handling

Credentials and passwords should not be shared and should never be transmitted via the same channel.

Additional client-side recommended security measures (as per market practice)

- Install anti-virus, anti-spyware and firewall software on personal computers and update them on a regular basis.
- Remove file and printer sharing if connected to unsecure internet.
- Make regular backups of critical data.
- Log off from the online session.
- Consider the use of encryption technology to protect highly sensitive or confidential information.
- Clear browser cache after each online session.
- Do not install software or run programs of unknown origin.
- Delete junk or chain mails.
- Do not open attachments of unknown origin.
- Do not disclose personal or financial data to unknown websites.
- Do not use a computer or device that cannot be trusted.
- Do not use public computers to access online services or perform financial transactions.

Troubleshooting

In this section, it is assumed that the JRE client is installed.

Smartcard reader and smart card troubleshooting

- Supported readers are the Datakey DKR 731 (USB) and Athena ASEDrive 3e(USB). The supported smart card is the eToken 4100 and the eToken 5100 USB dongle.
- Supported smart card software is SafeNet Authentication Client 8.1 SP1 or higher. This information can be determined by right-clicking the Safenet icon in the Windows taskbar and select→About.
- Check the smart card is correctly inserted and firmly grasped by the reader. Check the green light on the reader illuminates when an application (for example, CreationOnline or Token Utilities) accesses the smart card.
- If the driver for the eToken is correctly installed you will find the etpkcs11.dll in the \system32 folder.This version can be checked by right- clicking on the file, then select Properties. Select the Version tab.
- Check for the presence of the Safenet service. This Windows service must be enabled for proper operation of the card and reader with CreationOnline. This can be checked by selecting Start→Settings→Control Panel→Services. Check that the service has Startup as Automatic and Status as Started.

Note: There are tools on the plug-in.html for initialising or resetting the smart card.

Credentials troubleshooting

- Check size of P12. The correct size of a P12 file is about 9KB or 10KB. A P12 file contains 2 keypairs and a certificate chain for each keypair (3 certificates in each chain). Given that a certificate is about 1KB in size, we therefore expect a P12 of size 1KB to be corrupt.
- Change credentials. Do not overwrite any existing P12 with the new P12. The security model of a P12 is that of a "Vault", whereby a new Vault must be created for new keys and certificates.
- Both certificates and passwords have an expiry. The validity period of a CreationOnline certificate is 2 years, whereas the validity period of a password is much shorter. End-users are presented with warnings when either their certificate or password are due to expire. Certificate expiry requires end-users to change their credentials, whereas password expiry does not.

Passcode/password troubleshooting

P12 passwords are managed differently to smart card PINs in the application.

- The PIN length should be a minimum of 6 digits.
- The CreationOnline applet does not manage PIN expiration.
- The CreationOnline applet does not manage PIN or PUK history.
- The CreationOnline applet does not force a change in the passcode at first logon.
- The Safenet operating system contains functionality to "lock" after a certain number of consecutive unsuccessful PIN entry attempts. The maximum value of attempts is set when the card is formatted.
- If PIN/PUK codes are lost/forgotten the course of action is to re-initialise the card, which destroys any objects on the card.
- The smart card PIN can be changed through the tools available on the plug-in.html.

Authentication code troubleshooting

Authentication code entry

An authentication code is typically 20 characters long, and therefore must be entered carefully. A restricted character set is used for legibility. If an error is made on entry, the client will not be able to generate new credentials.

Code expiry

An authentication code is valid for only 60 days after which it is unusable. This is not configurable. Contact the Connectivity Support Help Desk (see "Contact details" on page i).

Code entered too many times

A client can make only three attempts to enter the correct code, after which the code becomes unusable. This is not configurable. Contact the Connectivity Support Help Desk (see "Contact details" on page i).

Confirmation receipt of code has not been communicated to Clearstream Banking

The OU Administrator authentication code entry has been attempted prior to the confirmation of receipt to Clearstream Banking. The authentication code has become invalid and a new authentication code must be requested from Clearstream Banking.

Java troubleshooting

Enabling applet debugging environment variables

Customer Support may request end-users to enable simple applet debugging by connecting to https://www.creationconnect.com/plug-in.html, and select Alternative: Login to CreationOnline with debug output enabled.

A more detailed debug may be requested by Customer Support. This is done through the java plug-in on Windows Control Panel

Enter the following parameter to debug:

```
-Djavaplugin.trace=true -Djavaplugin.trace.option=basic|net|security|ext|liveconnect -Djavax.net.debug=all
```

The Java log trace file should be sent to Customer Support for further analysis.

Clearing JAR cache

Sometimes Customer Support may request end-users to clear their Java cache if there is a local contention of JARs on their PC. This is done through the java plug-in on Windows Control Panel. Sometimes it may be necessary to clean the company network proxy cache. This is normally done by the network proxy administrator.

Check JRE version used

Check the installed java and Internet Explorer versions against the CreationOnline Technical Requirements document.

Miscellaneous troubleshooting

Time out of synchronisation between CA and web server does not allow new user to log in. If the CA time is in front of the web server machine, when a user changes credentials and tries to log in, the web server will reject the certificates as not yet valid, so the user cannot log on.

HTTP error codes returned to client from servlet

HTTP error codes will be visible in the client Java Console, and are used in CreationOnline as below.

- SC_INTERNAL_SERVER_ERROR (HTTP 500 return code). This error code denotes a serious server side error. It can be caused, for example, by a failure in communication between servers.
- SC_FORBIDDEN (HTTP 403 return code). This error code denotes that the user is not authorised to access the system, for example if the user is trying to connect with revoked or expired credentials.

Glossary

Concept	Definition
Asymmetric cryptography	See: Public Key Cryptography
Authentication	The process by which a user or a process proves its identity to a process offering a service in order to use the facilities of the latter.
Certificate	See X.509 certificate
Certification Authority (CA)	That component of the Public Key Infrastructure (PKI), which is responsible for signing certificates and revocation information.
Certificate management	The generic term covering all activities relating to the creation, distribution and deletion of X.509 certificates.
CreationOnline security subsystem	The components and mechanisms deployed to ensure that CreationOnline delivers the security services described in this document.
Confidentiality protection	The security service, which aims to ensure that information exchanged between and end-user and Clearstream Banking using CreationOnline is not available to third parties.
Cryptographic accelerator	A device used to accelerate cryptographic operations. Such devices are typically also used for secure key storage.
Cryptography	The means of rendering plain information unintelligible and of restoring encrypted information to intelligible form.
Cryptographic key	A piece of data used together with a cryptographic algorithm in order to produce a result (for example, encryption). In modern cryptographic systems, the design of the algorithm can be made public, but at least one of the cryptographic keys with which it is used must remain secret. In this sense, the security of the cryptosystem depends on the key.
Data integrity protection	Data integrity is said to be preserved if the data received over a network connection by the receiver is identical to that sent by the originator.
Digital Signature	A code created from data to be signed using the private key of the signer. This code is unique for each new piece of data and may be used to support authentication, integrity and non-repudiation services.
End-user	A business user of CreationOnline situated at a customer site.
FIPS 140-1	Federal Information Processing Standards Publications (FIPS PUBS) 140-1 is a US government standard for implementations of cryptographic modules.
Firewall	A combination of devices used to enforce an access control policy at the network perimeter. Typically, this policy will be expressed in terms of rules applying to protocols in the TCP/IP protocol stack.
gcd	Given two positive integers a and b, the gcd is the largest number that divides both evenly.
HTTPS	HyperText Transmission Protocol Secure of HTTP for secure transactions.

Concept	Definition
Integrity protection	The security service, which aims to ensure that information exchanged between and end-user and Clearstream Banking using CreationOnline is not tampered with whilst in transit. Integrity protection can be sub-divided into data integrity protection and session integrity protection.
Internet	The largest example of the wide area network (WAN).
Intranet	Internal network. Companies use intranets to share files, utilise web sites and collaborate. Usually cannot be accessed from the internet
Intrusion Detection System	An intrusion detection system inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
JAR	Java Archive is a file that contains the image and sound files for a Java applet gathered into a single file and compressed for further loading to your web browser.
JRE	Java Runtime Environment - The Java Runtime Environment consists of the Java virtual machine (JVM), the Java platform core classes, and supporting files. It is the runtime part of the Java Development Kit -- no compiler, no debugger, no tools. The JRE is the smallest set of executables and files that constitute the standard Java platform.
JVM	Java Virtual Machine. Computer software that interprets and executes the byte code in java class files much as a microprocessor executes machine code. There are many virtual machines available from different vendors and for different purposes.
Lightweight Directory Access Protocol (LDAP)	A protocol for accessing directory services across multiple platforms. LDAP is a simplified version of Directory Access Protocol (DAP), used to access X.500 directories.
Local security administrator	CreationOnline requires the customer site to configure at least two local security administrator accounts on CreationOnline. These accounts are used to perform local administration, including the generation of security credentials for end-users.
Non-repudiation	A non-repudiation service is a set of technical and procedural controls aimed at preventing the repudiation of actions that occur during a communications session. Non-repudiation is the inability to disavow transactions.
Online Certificate Status Protocol (OCSP)	OCSP is a request-response protocol for verifying the status of certificates online. The protocol is specified by RFC 2560.
PKCS	An abbreviation for “Public Key Cryptography Standards”, a set of standards written and maintained by RSA Security Incorporated.
PKCS#12	A key storage format specified within the PKCS framework.
Public key cryptography	Refers to the use of algorithms, which employ both a public key and a private key. These algorithms are based on hard problems in mathematics.
Public Key Infrastructure (PKI)	A set of components used to manage public/private key pairs. This is usually equivalent to managing X.509v3 certificates. The core components of a PKI are the certification Authority (CA), the Registration Authority (RA) and the LDAP (or alternatively X.500) Directory.

Concept	Definition
Public/private key pair	A pair of cryptographic keys used together with asymmetric (or "public key") algorithms. One key (the public key) is rendered public, and the other (the private key) is kept secret. There exists a mathematical relationship between the two keys, such that operations performed with one key can be "undone" by the other.
Registration Authority (RA)	That component of a public-key infrastructure (PKI) involved in verifying, enrolling and revoking X.509 certificates.
Request For Comment (RFC)	Internet Request For Comment (RFC) documents are produced by the Internet Engineering Task Force (IETF). Many of these documents have become de facto standards.
RSA	Internet encryption, which is the most commonly used encryption algorithm and is included as part of the web browser.
Secure Sockets Layer (SSL)	A protocol developed for use in the transmission of private documents via the internet.
Security architecture	A collection of components designed to deliver a defined set of security services.
Security component	A component of a security architecture.
Security credentials	Something a user or a process possesses in order to prove its identity and rights. In the case of CreationOnline, this is synonymous with the public key pair and X.509v3 certificate.
Security service	The term security service is used to refer to the provision of specific security functionality without defining how this functionality is implemented.
Session integrity protection	Session integrity is said to be preserved for a network connection if all packets sent by the originator are received by the receiver in the correct sequence and there is no possibility of replaying either the session itself or individual packets at a later time.
SSL	See Secure Sockets Layer.
Symmetric cryptography	The use of cryptographic algorithms that employ a single key. The term symmetric is used to indicate that the key held by the receiver is identical to that held by the sender (strictly speaking, the key used by the receiver is derivable from that of the sender). CreationOnline uses the most advanced cryptographic keys.
Thin client	A system that runs a lightweight operating system and executes applications delivered over the network.
Trojan Horse	Sometimes abbreviated to a Trojan. A program that provides some functionality but hides its true intent from the user. The true intent, for instance, may be to allow a malicious hacker to take control of the user's PC. A Trojan does not modify and infect other files.
URL	Universal (or Uniform) Resource Locator. The address of a web site on the world wide web.
Validation Authority (VA)	A VA system facilitates checking of revocation information.
X.509 Certificate	The X.509 certificate can be considered as an "electronic passport". It is a signed electronic data structure, which binds a public key to a name (and hence an entity) by means of a digital signature.

References

(1) Request For Comment (RFC) 2560 – X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol (OCSP). See http://www.faqs.org/rfcs/rfc2560.html

(2) Request For Comment (RFC) 2459 – X.509 Internet Public Key Infrastructure, Certificate and CRL Profile. See http://www.faqs.org/rfcs/rfc2459.html

(3) Request For Comment (RFC) 2510 – X.509 Internet Public Key Infrastructure, Certificate Management Protocols. See http://www.faqs.org/rfcs/rfc2510.html

(4) Request For Comment (RFC) 2511 – X.509 Internet Public Key Infrastructure, Certificate Request Message Format. See http://www.faqs.org/rfcs/rfc2511.html

(5) Request For Comment (RFC) 2527 – X.509 Internet Public Key Infrastructure, Certificate Policy and Certificate Practices Framework. See http://www.faqs.org/rfcs/rfc2527.html

(6) Federal Information Processing Standards (FIPS) publication 140-1, Security Requirements For Cryptographic Modules. See http://www.itl.nist.gov/fipspubs/fip140-1.htm

(7) Request For Comment (RFC) 2865 – Remote Access Dial In User Service (RADIUS). See http://www.faqs.org/rfcs/rfc2865.html

(8) For information on the HMAC function, see the article "The HMAC Papers", published at the following address: http://www-cse.ucsd.edu/users/mihir/papers/hmac.html

Error messages

Error message	Action to be taken
A certificate could not be found in the LDAP directory. The nCipher HSM could not be opened.	Contact your administrator with the full debug stack trace which will contain the certificate serial numbers you are connecting with. The server HSM is down or not responding. Contact your administrator with the full debug stack trace.
A certificate could not be verified. The LDAP directory could not be accessed.	The certificate you are connecting with does not match the serial number on the server. Make sure you are using a valid credentials. Contact your administrator with the full debug stack trace. The LDAP server is down or not responding. Contact your administrator with the full debug stack trace.
A CreationOnline certificate could not be found on the smart card.	Please check contents of the card for the correct CreationOnline labels. Contact your administrator with the full debug stack trace.
A CreationOnline certificate could not be found on the smart card. The call to the OSCP libraries failed.	Please check contents of the card for the correct CreationOnline labels. Contact your administrator with the full debug stack trace. There was an error during the call to the OCSP server. Contact your administrator with the full debug stack trace.
A malformed URL was encountered.	The URL was incorrect. In IE check the HTML with View→Source. Contact your administrator with the full HTML source.
A revoked certificate was encountered. Could not initialise the SSL support libraries.	The certificate you are connecting with is revoked. Check your credentials are current. Contact your administrator with the full debug stack trace. There is a problem with the smart card/P12 concerning the SSL session. Contact your administrator with the full debug stack trace.
An error occurred in trying to sign a message.	This is a rare occurrence, but could happen if there is a lack of client system resources. Contact your administrator with the full debug stack trace.
An unverified message was received.	This is a server error. Check the P12 used is current. Contact your administrator with the full debug stack trace which will contain your certificate serial numbers.
Authentication code could not be registered.	Upon successful use of the code, the certificates could not be issued. Contact your administrator with the full debug stack trace.
Authentication code could not be registered. General error in security.	Upon successful use of the code, the certificates could not be issued. Contact your administrator with the full debug stack trace. A catch all security error message. Contact your administrator with the full debug stack trace.
Authentication code is inactive. Please contact an administrator. Invalid password format. Please refer to help.	The code is activated only upon confirmation of receipt. Please check you have confirmed receipt of the code. Please contact your administrator. When specifying a new password, validation rules are applied. Please refer to help. If problem persists, contact your administrator with the full debug stack trace.
Authentication code is invalid. Please re-enter it. An error occurred in trying to sign a message.	The code entered is invalid. Please carefully re-enter the code. This is a rare occurrence, but could happen if there is a lack of client system resources. Contact your administrator with the full debug stack trace.

Error message	Action to be taken
Connection with CreationOnline could not be established. Please contact your administrator.	There is a general connectivity problem. Contact your administrator with the full debug stack trace.
Could not create WLEC pool initial context.	The application server hosting registration and revocation is down. Contact your administrator with the full debug stack trace.
Could not create WLEC pool initial context. Your authentication code has expired. Please contact Clearstream Banking Customer Services.	The application server hosting registration and revocation is down. Contact your administrator with the full debug stack trace. The code expires after 30 days. Please contact your administrator. For customer service, contact the Connectivity Support Help Desk (see "Contact details" on page i).
Could not initialise the SSL support libraries.	There is a problem with the smart card/P12 concerning the SSL session. Contact your administrator with the full debug stack trace.
Error in revoking the user. Problem sending/receiving CreationOnline signing certificate.	A server PKI component failed or did not respond. Contact your administrator with the full debug stack trace. One or more of the connectivity components between client and server is down or not responding. Contact your administrator with the full debug stack trace.
Failure in generating HMAC. Connection with CreationOnline could not be established. Please contact your administrator.	An error occurred when generating the HMAC. Contact your administrator with the full debug stack trace. There is a general connectivity problem. Contact your administrator with the full debug stack trace.
General error in security. Unknown security error encountered. Please contact administrator.	A catch all security error message. Contact your administrator with the full debug stack trace. An unknown error occurred. Contact your administrator with the full stack trace and debug enabled.
HMAC did not verify. A malformed URL was encountered.	The authentication code you are connecting does not correspond with that on the server. Contact your administrator with the full debug stack trace. The URL was incorrect. In IE check the HTML with View→Source. Contact your administrator with the full HTML source.
Identifier does not exist. Please re-enter it.	Please double-check that you have entered the Identifier value from the authentication letter correctly.
Authentication code is invalid. Please re-enter it.	The code entered is invalid. Please carefully re-enter the code.
Invalid password format. Please refer to help.	When specifying a new password, validation rules are applied. Please refer to help. If problem persists, contact your administrator with the full debug stack trace.
It was not possible to generate the key pair. Your password cannot repeat any of your previous {0} passwords. Type a password which meets this requirement in both text boxes.	There is a problem with generating keys on the smart card/P12. For a smart card check with token utilities. Contact your administrator with the full debug stack trace. Choose a password not already in the password history of the P12.

Error message	Action to be taken
It was not possible to generate the user credentials. The passwords you typed do not match. Type the new passwords in both text boxes.	There was a general problem in generating the user credentials, for example, media not present or comms error. Contact your administrator with the full debug stack trace. Make sure the passwords match. If in doubt use copy and paste.
No token was found in the smart card slot. HMAC did not verify.	Please check there is a smart card correctly inserted in the smart card reader. Contact your administrator with the full debug stack trace. The authentication code you are connecting does not correspond with that on the server. Contact your administrator with the full debug stack trace.
Problem sending/receiving CreationOnline signing certificate.	One or more of the connectivity components between client and server is down or not responding. Contact your administrator with the full debug stack trace.
The call to the OSCP libraries failed. The message log could not be accessed.	There was an error during the call to the OCSP server. Contact your administrator with the full debug stack trace. The server message log table is unavailable. Contact your administrator with the full debug stack trace.
The LDAP directory could not be accessed.	The LDAP server is down or not responding. Contact your administrator with the full debug stack trace.
The message log could not be accessed.	The server message log table is unavailable. Contact your administrator with the full debug stack trace.
The nCipher HSM could not be opened.	The server HSM is down or not responding. Contact your administrator with the full debug stack trace.
The pass phrase is too long.	The passphrase must be <= 24 characters long.
The pass phrase is too long. The passphrase is invalid.	The passphrase must be <= 24 characters long. The password entered does not match the password used to encrypt the P12. If you have forgotten your password, please ask your administrator to generate you a new P12.
The pass phrase is too short.	The passphrase must be >= 8 characters long.
The pass phrase is too short. A certificate could not be verified.	The passphrase must be >= 8 characters long. The certificate you are connecting with does not match the serial number on the server. Make sure you are using a valid credentials. Contact your administrator with the full debug stack trace.
The passphrase is invalid. The user's PKCS 12 credentials file could not be opened.	The password entered does not match the password used to encrypt the P12. If you have forgotten your password, please ask your administrator to generate you a new P12. There is a problem with the P12 (for example, corrupt file). Contact your administrator with the full debug stack trace.
The passwords you typed do not match. Type the new passwords in both text boxes.	Make sure the passwords match. If in doubt use copy and paste.
The permitted number of Registration attempts have been exceeded. Your authentication code is now invalid. Please contact Clearstream Banking Customer Services. It was not possible to generate the user credentials.	The authentication code is locked out. This occurs on 3 incorrect attempts. Please contact your administrator. There was a general problem in generating the user credentials, for example, media not present or comms error. Contact your administrator with the full debug stack trace. For customer service, contact the Connectivity Support Help Desk (see "Contact details" on page i).

Error message	Action to be taken
The smart card has been blocked.	The smart card blocks on the 10th incorrect attempt. Use a passcode unblocking code or re-initialise your card. If the latter ask your administrator to generate you a new P12. You will then change credentials from a P12 to smart card.
The smart card has been blocked. Error in revoking the user.	The smart card blocks on the 10th incorrect attempt. Use a passcode unblocking code or re-initialise your card. If the latter ask your administrator to generate you a new P12. You will then change credentials from a P12 to smart card. A server PKI component failed or did not respond. Contact your administrator with the full debug stack trace.
The smart card PIN is either blocked or not initialised.	There is a problem with the smart card. Check the card has been initialised or is not blocked. Contact your administrator with the full debug stack trace.
The smart card PIN is either blocked or not initialised. The system could not logon. Please check that you specified a valid credentials file and a valid password.	There is a problem with the smart card. Check the card has been initialised or is not blocked. Contact your administrator with the full debug stack trace. The P12 is invalid, for example, user names in SSL and signing certificate do not match. Please contact your administrator with the full debug stack trace. If necessary, please ask your administrator to generate you a new P12.
The system could not logon. Please check that you specified a valid credentials file and a valid password. An unverified message was received.	The P12 is invalid, for example, user names in SSL and signing certificate do not match. Please contact your administrator with the full debug stack trace. If necessary, please ask your administrator to generate you a new P12. This is a server error. Check the P12 used is current. Contact your administrator with the full debug stack trace which will contain your certificate serial numbers.
The user's PKCS 12 credentials file could not be opened.	There is a problem with the P12 (for example, corrupt file). Contact your administrator with the full debug stack trace.
There is a problem with the credential handling. Please contact your administrator.	This is a catch all registration error. Contact your administrator with the full debug stack trace.
There is a problem with the credential handling. Please contact your administrator. Authentication code is inactive. Please contact an administrator.	This is a catch all registration error. Contact your administrator with the full debug stack trace. The code is activated only upon confirmation of receipt. Please check you have confirmed receipt of the code. Please contact your administrator.
There is not enough free capacity on the card.	The free memory of the card is limited. Please check contents of the card. Contact your administrator with the full debug stack trace.
There is not enough free capacity on the card. A revoked certificate was encountered.	The free memory of the card is limited. Please check contents of the card. Contact your administrator with the full debug stack trace.The certificate you are connecting with is revoked. Check your credentials are current. Contact your administrator with the full debug stack trace.
There is not enough total capacity on the card.	The total memory of the card (public and private) is limited. Please check contents of the card. Contact your administrator with the full debug stack trace.

Error message	Action to be taken
There is not enough total capacity on the card.A certificate could not be found in the LDAP directory.	The total memory of the card (public and private) is limited. Please check contents of the card. Contact your administrator with the full debug stack trace. Contact your administrator with the full debug stack trace which will contain the certificate serial numbers you are connecting with.
Unknown security error encountered. Please contact administrator.	An unknown error occurred. Contact your administrator with the full stack trace and debug enabled.
Your authentication code has expired. Please contact Clearstream Banking Customer Services. It was not possible to generate the key pair.	The code expires after 30 days. Please contact your administrator. There is a problem with generating keys on the smart card/P12. For a smart card check with token utilities. Contact your administrator with the full debug stack trace. For customer service, contact the Connectivity Support Help Desk (see "Contact details" on page i).
Your password cannot repeat any of your previous {0} passwords. Type a password that meets this requirement in both text boxes.	Choose a password not already in the password history of the P12.
Your user credential file has expired. Please contact your administrator.	The user certificate has expired. Certificates are valid for 2 years. Contact your administrator with the full debug stack trace.
Your user credential file has expired. Please contact your administrator. The permitted number of Registration attempts have been exceeded. Your authentication code is now invalid. Please contact Clearstream Banking Customer Services.	The user certificate has expired. Certificates are valid for 2 years. Contact your administrator with the full debug stack trace. The authentication code is locked out. This occurs on 3 incorrect attempts. Please contact your administrator. For customer service, contact the Connectivity Support Help Desk (see "Contact details" on page i).

Contact

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

March 2017

Document number: 6209