Security Policy

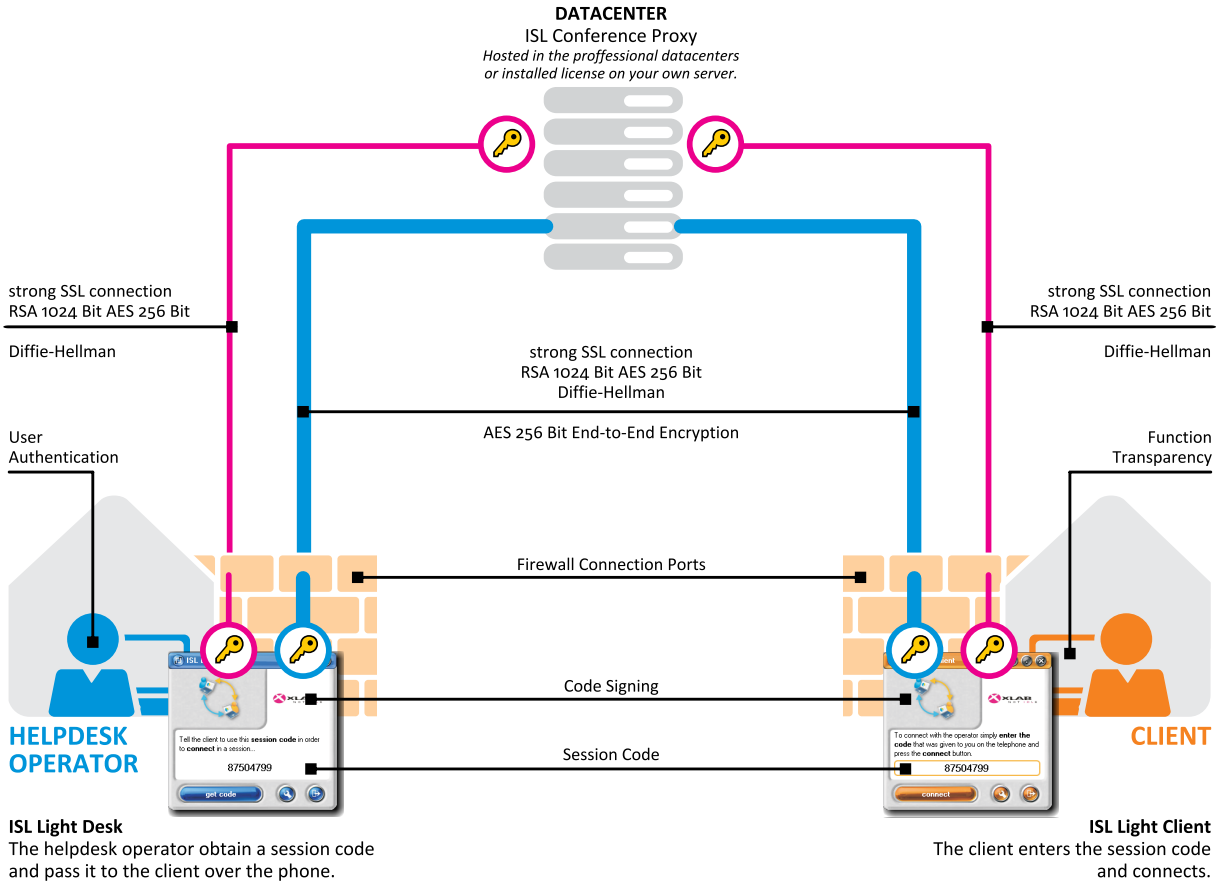
Revision Date: 23 April 2009

Remote Desktop Support

- Version 3.2.1 or later for Windows
- Version 3.1.2 or later for Linux and Mac

ISL Light
Security Policy

This section describes the procedure for establishing the ISL Light session and the implemented security layers.



ISL Light Desk
The helpdesk operator obtain a session code and pass it to the client over the phone.

ISL Light Client
The client enters the session code and connects.

Firewall Connection Ports

No firewall adjustments are needed to start the remote desktop support session, as the ISL Light automatically initiates an outgoing connection. ISL Light tries to connect using ports 7615, 80 and 443 therefore it works with your existing firewall and does not require any additional configuration.

SSL Secured Communication

The Secure Sockets Layer (SSL) cryptographic protocol provides security and data integrity of the communication. For each ISL Light connection an additional SSL layer is established over the HTTP protocol. Widelly tested and used OpenSSL library is used for the SSL implementation.

RSA 1024 Bit Public /Private Key Exchange

To initiate the remote desktop support connection with a client, the helpdesk operator needs to start the ISL Light Desk application which carries an RSA 1024 Bit Public Key of the ISL Conference Proxy server. The initial connection is established when the Public Key of the ISL Light Desk application and the Private Key of the ISL Conference Proxy server are verified and exchanged successully. The industry standard X.509 certificates are used to guarantee authenticity of transmission. This PKI (Public Key Infrastructure) prevents the »Man-in-the-middle-attacks«.

Upon the successful RSA 1024 Bit Public / Private Key Exchange the Diffie-Hellman cryptographic algorithm is used to exchange symmetrical AES 256 Bit keys. After the exchange all subsequent communication between the ISL Light Desk application and the ISL Conference Proxy server is encrypted using a symmetrical AES 256 Bit keys.

User Authentication

The helpdesk operator needs to be a registrated ISL Online user with a valid username and password. To obtain a unique session code, the operator needs to be identified by providing the username and password to the ISL Conference Proxy server. The AES 256 Bit encrypted username and password are sent to the ISL Conference Proxy for the verification. Username and password is checked against ISL Conference Proxy user database. Alternatively, when using the Server License, different types of the authentication schemes can be integrated within the ISL Conference Proxy, like the RADIUS or LDAP authentication.

Session Code

Upon the successful authentication, a unique session code is generated by the ISL Conference Proxy server and returned to the ISL Light Desk application through the AES 256 Bit encrypted channel. The helpdesk operator needs to pass the session code (for example over the phone) to the client, who enters the session code in the ISL Light Client application and initiates the connection with the ISL Conference Proxy server.

The ISL Light Client application carries an RSA 1024 Bit Public Key of the ISL Conference Proxy server. The initial connection is established when the Public Key of the ISL Light Client application and the Private Key of the ISL Conference Proxy server are verified and exchanged successfully. The industry standard X.509 certificates are used to guarantee authenticity of transmission. This PKI (Public Key Infrastructure) prevents the »Man-in-the-middle-attacks«.

RSA 1024 Bit Public / Private Key Exchange with the Diffie-Hellman cryptographic algorithm is used to exchange symmetrical AES 256 Bit keys. After the exchange all subsequent communication between the ISL Light Client application and the ISL Conference Proxy server is encrypted using a symmetrical AES 256 Bit keys.

The unique session code is sent through the AES 256 Bit encrypted channel from the ISL Light Client to the ISL Conference Proxy. Based on the unique session code, the ISL Conference Proxy matches together the ISL Light Desk and the ISL Light Client applications. The session code is invalidated immediately after the connection is established between the ISL Light Client and the ISL Light Desk.

AES 256 Bit End-to-End Encryption

Once the ISL Light Desk and the ISL Light Client applications are matched on the ISL Conference Proxy server by the means of the identical unique session code the new SSL handshake is started.

The ISL Light Client application carries an RSA 1024 Bit Public Key of the ISL Light Desk application. The initial connection is established when the Public Key of the ISL Light Client application and the Private Key of the ISL Light Desk application are verified and exchanged successfully. The industry standard X.509 certificates are used to guarantee authenticity of transmission. This PKI (Public Key Infrastructure) prevents the »Man-in-the-middle-attacks«.

RSA 1024 Bit Public / Private Key Exchange with the Diffie-Hellman cryptographic algorithm is used to exchange symmetrical AES 256 Bit keys. After the exchange all subsequent communication between the ISL Light Client application and the ISL Light Desk application is encrypted using a symmetrical AES 256 Bit keys.

AES 256 Bit encrypted data transfer end-to-end SSL tunnel is established between the ISL Light Desk and the ISL Light Client applications. All the information exchanged between the helpdesk operator and the client is encrypted from end-to-end, meaning that even the ISL Conference Proxy cannot decrypt the content of the session but only transfers the packets from one side to another.

Session data storage

The data transferred between the ISL Light Desk and ISL Light Client during the session (desktop sharing images, files, audio/video communication, etc.) is NOT stored on the ISL Conference Proxy server. Only the basic session parameters (IP addresses of the ISL Light Desk/Client, session length, bytes transferred, end of session dialogs, etc.) are stored on the ISL Conference Proxy server.

The ISL Light sessions can also be recorded. However the ISL Light Desk and the ISL Light Client users are always notified when the session recording starts and stops. Session recording files are stored locally, on the ISL Light Desk or ISL Light Client computer.

Code Signing

ISL Light Desk and ISL Light Client applications are digitally signed by means of a VeriSign Code Signing certificate, which reliably identifies XLAB as the software publisher and guarantees that the code has not been altered or corrupted since it was signed with a time-stamped digital signature.

Datacenters

The ISL Online Network's dedicated servers are hosted by the professional datacenters round the globe. We only choose highly reliable and industry-proven datacenters with modern facilities and equipment, such as redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. We solely control the servers running the ISL Conference Proxy application and have strict administrative password storage policy. Due to the AES 256 Bit end-to-end encryption security policy even the administrators of the network cannot see the content of the sessions.

For most security delicate organizations such as banks, national agencies, corporate environments etc., we offer the Server License model, where the ISL Conference Proxy application is installed on the server within such organization. In this case, all ISL Light connections are established through the ISL Conference Proxy installed on the server running in the organization, completely independent from the ISL Online Network. As the Server License installation is a stand-alone system, the organization is solely responsible for the server's administration.

Function Transparency

ISL Light is designed for providing the remote support to the clients over the internet but only upon the client's explicit request. The client initiates the session and the client can also terminate the session anytime. During the session, the client is asked for permissions to start the desktop sharing, enable the remote keyboard and mouse control, send and receive files, turn on or off the audio and video communication etc. Even when the operator has a full remote desktop control over the client's PC, the client can easily revoke the control from the operator by simply moving the mouse.

The functionality of the software is totally transparent, meaning that the application is never running in the background. The client is always aware of the running session and can follow the actions performed by the helpdesk operator all the time. Once the session is terminated, the helpdesk operator cannot access the client's computer again with the same session code.

Program Executables Integrity

The Quality Assurance policy is implemented in the cycle of the ISL Online product development. All program applications need to go through the following stages:

- Development
- Release Candidate
- Testing
- Official Release
- Distribution
- User Download

We guarantee that the software applications we develop reach the final destination intact. Several mechanisms are implemented to assure that:

- A branch is created in the development source tree for each release. This assures that smaller improvements on the minor release are always implemented on the level of the specific source branch, which is thoroughly tested.
- The release candidate application executables are signed using the proprietary algorithm by the secure key which is accessible to the ISL Online release team only.
- In the testing department a team of experts is responsible for the quality control of each software branch.
- When the release candidate is approved by the testing department, the official release of the application executables are signed using the proprietary algorithm by the secure key which is accessible to the ISL Online release team only.
- When the official release is deployed, the proprietary signature is verified by the ISL Conference Proxy.
- The software applications downloaded by the user are additionally signed by means of a VeriSign Code Signing certificate, which reliably identifies XLAB as the software publisher and guarantees that the code has not been altered or corrupted since it was signed with a time-stamped digital signature.

This process assures the integrity of the ISL Online application executables from the development stage to the user download.