

Whitepaper Security: one2one.

This whitepaper describes the security mechanism within the Netviewer one2one product. In the first part we focus on security aspects at the network transport layer. In the second part we describe the application layer related security mechanisms.

Security at the Network Transport Layer

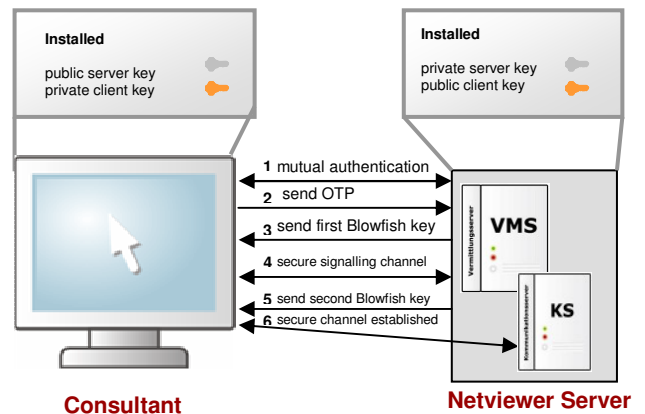
The security at the network transport layer is the basis for a secure communication. This section describes how Netviewer assures that the communication channel is secured in terms of mutual authentication and encryption.

Encryption methods

The mutual authentication between the Netviewer clients and the Netviewer servers is done by using asymmetric keys. The Netviewer software uses the VeriSign certificate to proof its authenticity. Both public and private keys are included in the Netviewer software as part of the software generation stage.

The consultant program uses the public key of the server and its own private key. The server uses the private server key and the public key of the client.

The privacy and the integrity of data are secured by two encryption methods called ECC (Elliptic Curve Cryptography) and Blowfish. The asymmetric 160-bit ECC key is used for the authentication between the clients and the connection server, the symmetric 128-bit blowfish key is used for the communication between consultant and participant. The following chart shows how the network session is setup in detail.

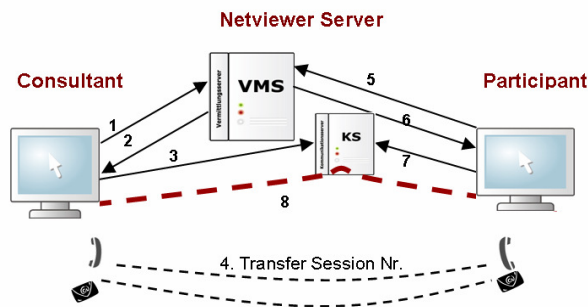


In the first step the client and the server authenticate each other by using the ECC asymmetric keys and random numbers (1). The client then generates an OTP (one time pad) and sends it to the server encryptedly (2). The server generates the symmetric Blowfish key and transfers the key to the client (3). From that point all signalling traffic will be encrypted by using the Blowfish key in combination with the OTP (by an XOR combination of OTP and Blowfish) (4). The connection server then generates a second Blowfish key that is transferred to the client via the secured channel (5). This second Blowfish key will be used for the data traffic communication via the communication server (6). Within Netviewer one2one, this second Blowfish key is not communicated to the communication server at any time.

Session setup

This session setup section explains how a session gets established by using the encryption methods explained above.

The consultant starts the consultant program and the program contacts the connection server (VMS) to request a session (1). After the consultant has been authenticated successfully (user name and password, Active Directory,...) the connection server sends back a 6-digit session number and the address of the communication server to the consultant (2). Then the consultant will contact the communication server and wait for the participant to join the session (3).



In the next step the 6-digit session number is given to the participant via telephone or e-mail (4). The participant starts the program and enters the session number in the assigned field. The participant program then sends a request to the connection server (5). The connection server sends back the address of the communication server where the consultant is waiting (6). The participant program contacts the communication server (7) and the session is established end-to-end between the consultant and the participant through the communication server (8).

The integrity of the data during the session is secured by the Blowfish key. For the Netviewer one2one product an end-to-end encryption is used and therefore the communication server is not able to decrypt any traffic content. In addition, no other party can join this session as it is limited to two parties.

The connection server and the communication server are independent entities. It's not possible for the communication server to encrypt the data of the session as it has no information about the Blowfish key used during the session.

Security at the Application Layer

At the application layer Netviewer supports a variety of security methods that enable additional levels of security. These concepts are technology and process based.

The consultant needs a user name and password to start the consultant program. After a successful authentication, a one-time 6-digit session number, generated by the connection server, will be transferred to the consultant program. This number will be forwarded by phone or email to the participant. A session password and a second confirmation PIN sent

from the participant to the consultant can be used in addition.

During a Session

The privacy of each participant and his data during a Netviewer one2one session are protected by different methods and settings.

Neither the consultant nor the participant are able to get the right to control the PC of the other party without their approval.

The participants will always be asked to allow any change of the status of their PC (change of direction of view, remote control, file transfer, information about the configuration of the PC). Only after the approval the second party will be able to remotely control the PC.

It's possible to select applications or files which shall not be shown to the second party. For example it is possible to hide the desktop or the task bar. In this case, these applications can't be used by remote control either.

The shower can freeze the screen to secure the secret use of the own PC while working with another program (monitor pause function).

Pushing the F11 key immediately stops the remote control.

The session is immediately stopped if one of the participants closes the communication panel. It can't be continued without repeating the standard log-in procedure.

Logging

The consultant program can create a .txt file at the end of a session to log the duration of a session and the number of transferred bytes.

The session data can also be stored as a .csv file on the consultant and/or participant side for further use, i.e. for billing. In addition, all session data can be logged on the server side.

All parts of the session, including video and audio, can be recorded and stored in a Netviewer proprietary .nvl file format, which can't be manipulated afterwards. It is possible to change this file to an .avi file format manually.

Summary

The security of Netviewer one2one and the integrity of the data are guaranteed by using different levels of protection:

- The Netviewer software is signed by an independent Certification Authority (VeriSign).
- A 160-bit ECC key is used for the mutual authentication and the asymmetric encryption between client and server.
- A 128-bit symmetrical Blowfish key is used to encrypt the data of the session.
- The connection and communication server are independent entities.
- The exchange of the session key is handled by different media (phone or e-mail).
- After the start of the session, no third party can join. The session is end-to-end encrypted.
- All sessions can be logged on consultant, participant and server side.
- All data can be recorded for later review.