

White Paper Security: Netviewer one2one.

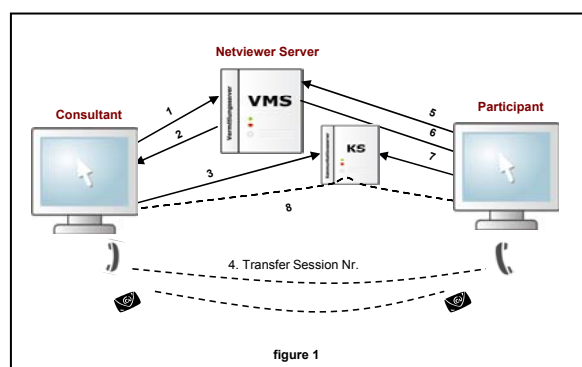
This White Paper describes the security mechanism within the Netviewer one2one product. In the first part we focus on security aspects at the network transport layer. In the second part we describe the application layer related security mechanisms.

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.

Session setup

The session setup is shown in figure 1 and will be explained in detail in this section. 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 consultant gives the 6-digit session number 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). The session is then 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 an 128-bit Blowfish encryption. Netviewer uses an end-to-end encryption 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. Signalling data (e.g. authentication, keys) and session data are therefore logically separated. The connection server uses the Netviewer httpRPC protocol, the communication server uses the Netviewer ping-pong protocol.

Encryption methods

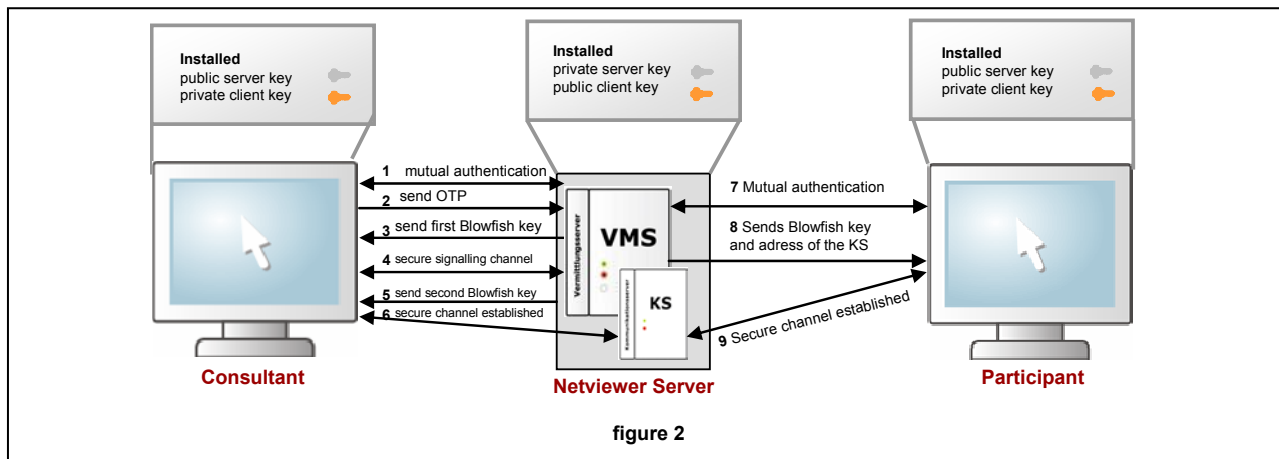
The mutual authentication between the Netviewer clients and the Netviewer servers is done by using asymmetric keys. Both public and private keys are included in the Netviewer software as part of the software generation stage.

The consultant program uses the public key of the server and its own private key. The server uses its own private 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 keys are used for authentication and key exchange. The symmetric 128-bit Blowfish key secures the integrity and the privacy of the communication between consultant and participant.

Figure 2 shows how the network session is setup in detail.

In the first step the client and the connection 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 connection server encryptedly (2). The connection server generates the symmetric Blowfish key and transfers the key using an XOR combination of OTP and Blowfish to the client (3). From that



point all signalling traffic will be encrypted by using the Blowfish key (4). The connection server then generates a second Blowfish key that is transferred to the client via the secured channel (5). The connection server destroys the key immediately after it was delivered to the participant program. This second Blowfish key will be used for the session data traffic via the communication server (6). The second Blowfish key is not communicated to the communication server at any time.

Security at the Application Layer

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

Session setup

Consultant and participant are able to verify the authenticity of the Netviewer software. The software is signed with a certificate from the independent Certification Authority VeriSign.

To start the consultant program the consultant needs a user name and a password. 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 (see figure 1). 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 is 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 e.g. to remotely control the PC.

Applications or files which shall not be shown to the second party can be selected. For example it is possible to hide the desktop or the task bar. In this case, these applications can not 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 security key (default F11) immediately stops the remote control.

The session is immediately stopped if one of the participants ends the Netviewer session, e.g. by closing the panel. The session can not be continued without establishing a new Netviewer session.

Logging

The consultant program creates 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. 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 with a certificate from 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 session data.
- The connection and communication server are independent entities.
- The exchange of the session number is transferred through a different medium (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.
- For every session a new session number will be generated
- No action on the 2nd party computer is possible without permission. This is valid for both consultant and participant.
- It is possible to use a session password and a second PIN before the session is established.