Declaration about encryption and data security when using FastViewer

The master module receives **from several redundant servers** a list of active, available FastViewer communication servers via **port 80** (HTTP).

The master module connects automatically to the fastest communication server. Thereby, a **hundred per cent system stability** is guaranteed. With your FastViewer customer portal you´ve got the possibility to select the communication server you´d like to use - Worldwide, European or exclusively server that are located in Germany.

The master module tries to use primary **port 5000** (TCP), then **port 443** (HTTPS) and finally **port 80** (HTTP) for connecting the communication server. The connection is also guaranteed if there is a **proxy server**. The master module receives a 6 **digit session number** from the communication server. This number is then relayed to your customer or colleague by phone or e-mail.

The client module connects to the server based on the 6 digit session number entered. The server then receives a list of active, available FastViewer communication servers initially trying to use **port 5000** (TCP), then **port 443** (HTTPS) and finally **port 80** (HTTP) for connecting the communication server. The connection is guaranteed even if there is a **proxy server**.

In the next part of the process, the Master Module generates a **256 Bit AES Key (Rjindael Algorithm)** that is used for the encryption of all following data packets. The client module generates a 2048 Bit RSA Key Pair to make sure that the Server cannot read the Master's 256 Bit AES Key.

FastViewer will then display the screen in the desired direction. The partner that shares his screen is able to lock the remote control by using the **F11 key**. It is also possible to stop the session directly by click on the close button.

Security features of the FastViewer Secure Advisor

Security is absolutely essential for this product and is guaranteed by **ternary security**:

- The installed Secure Advisor client needs only an outgoing port. This means, there is no way to **hack into the program**.
- FastViewer works like a Bank card with pin code. It is only possible to logon the remote client, if you got the appropriate **FastViewer EXE file** and the **correct password**.
- There is additional protection when using the windows login

Authentication by short message enables additional protection

Beyond the already mentioned safety functions a short message authentication is available. In order to access to the remote devices, you need to enter a Login code, which is send to the deposited phone number. Thus only authorized persons are able to connect to the remote clients.

Take control by using your own FastViewer server

Another possibility is running your own FastViewer server. This solution can be used completely **independently from our IT infrastructure**. All sessions will run by your own FastViewer server with the same security features as described above. The system stability is guaranteed by using **several redundant servers**.

About the Rijndael Algorithm

In cryptography, the **Advanced Encryption Standard (AES)**, also known as **Rijndael**, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) on November 26, 2001 after a 5-year standardization. It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages. This marks the first time that the public has had access to a cipher approved by NSA for top secret information. (en.wikipedia.org)

Steffen Fürsch
CEO – managing director