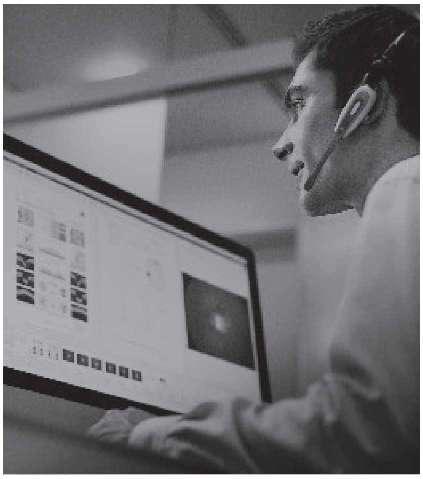
Remote Service from ZEISS

Technical Description

We make it visible.

The moment you realize that
we're there when you need us.
This is the moment we work for.
//CUSTOMER CARE
MADE BY ZEISS

ZEISS Remote Service
What is Remote Service?



The increasing networking of medical equipment and the rising speed of data transfer paths are broadening the opportunities for direct support in the service field. The main purpose of this document is to explain the technical principles and security aspects of ZEISS Remote Service.

With the help of the latest remote support technologies, ZEISS can offer its customers shorter service response times, accompanied by higher system availability in line with current trends. In the past, customers had to wait for a service engineer to call. Today, many issues can be resolved directly by remote means.

However, certain constraints arising from regulatory and statutory conditions for medical products have to be taken into account in the remote servicing of medical equipment. In particular, the confidentiality of patient data, security in the manipulation of medical data and guaranteeing the security and effectiveness of the medical instrument being serviced must be considered.

Essentially, Remote Service offers support for the following aspects:

- Questions regarding the application of the system
- Software updates and upgrades
- Technical support

Our specialists are directly available to you with active support and advice – all online on your display. You always have full control over the applications that you want to make accessible to our support staff.

ZEISS Remote Service

Setting up a session

The setup of a session is shown below:

1 The moderator (ZEISS Service) launches the moderator program which sends the operator server (VMS) an invitation to the session.

2 Once the moderator has been successfully authenticated, the operator server sends a six-digit session number and the address of the communication server (KS) back to the moderator.

3 The moderator program contacts the communication server and waits till the attendees join the session.

4 In the next step, the moderator provides the attendee with the six-digit session number by telephone or invitation e-mail. If required, more than two participants can join a remote session simultaneously (e.g a customer, a ZEISS service engineer and a ZEISS 2nd level service engineer with special product know-how).

5 The attendees launch the attendee program and enter the session number in the appropriate field. The attendee programs then send a request to the operator server.

6 The operator server returns the address of the communication server, for which the moderator program is waiting.

7 The attendee programs contact the communication server.

8 The session is then set up between the moderator program and the attendee program via the communication server.

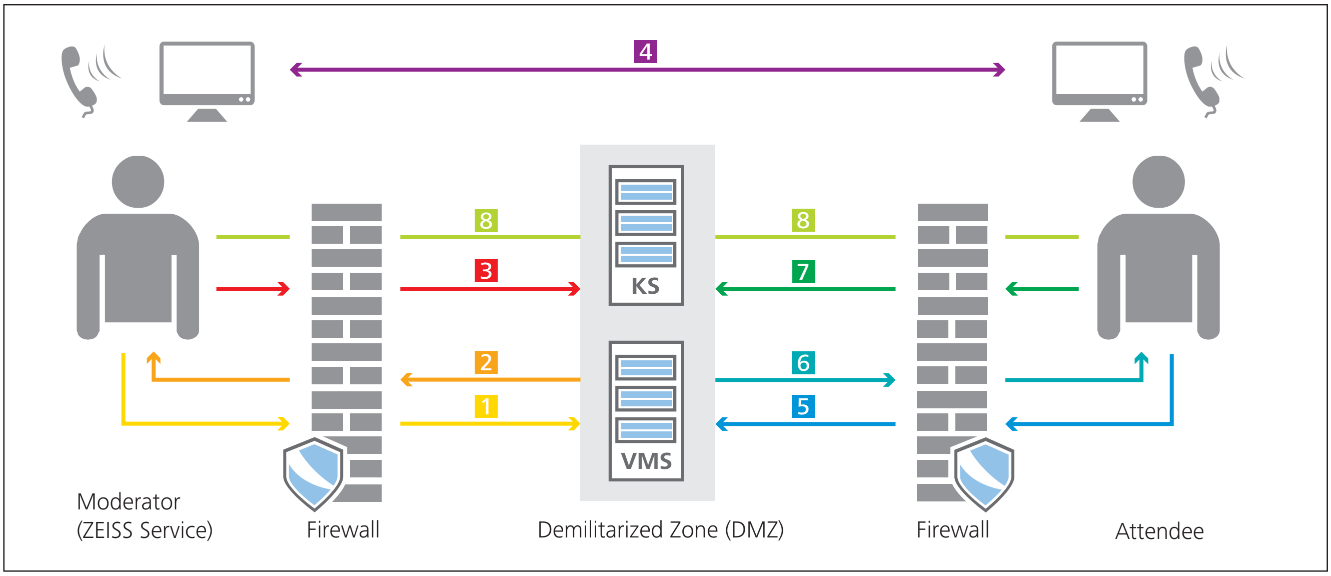


Fig. 1 Setting up a remote service connection

Security

Encryption methods

Mutual authentication between clients and servers is realized using an asymmetric encryption method. The public and private keys are hard-coded into the software.

The moderator program uses the server's public key and its own private key, while the server uses its own private key and the client's public key. Data privacy and integrity are insured by two encryption methods: ECC (Elliptic Curve Cryptography) and Blowfish.

The asymmetric 160-bit ECC keys are used for authentication and for exchanging keys. The symmetric 128-bit Blowfish key secures the integrity and confidentiality of communication between the moderator and attendees.

The encryption certificates are issued by an independent certifying body (Verisign).

Security at the application level

When the moderator program is launched with access to the central ZEISS domain, the moderator is directly authenticated via a dedicated assignment of rights to certain user groups in the ZEISS Active Directory. He can then launch a new session immediately. If the moderator is not connected to the ZEISS domain, he is authenticated using his personal user name and password directly via integrated user management and the security mechanisms of the ZEISS Netviewer platform. Once the moderator program is successfully launched, a unique six-digit session number is generated by the operator server and forwarded to the moderator program. This number is passed on to the attendees by telephone or by e-mail (see Figure 1).

During the session

The privacy of all session participants and any personal data are protected during a Remote Service session by several functions and configurations.

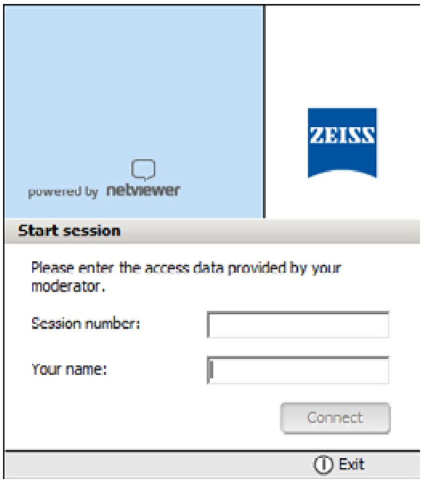
- All Remote Support actions can be observed by the attendees during the session.
- Neither the moderator nor the attendees can obtain remote control of a participant's computer without his or her consent.
- The session participants have to explicitly allow any change in the status of their computer (change of viewing direction, remote control, file transfer). Another participant is only able to remotely control the computer or carry out other actions after permission is given.
- Applications or files that are not intended to be transferred to session participants can be explicitly deselected. It is possible, for example, to hide the desktop or the taskbar. Applications and screen elements which are not released cannot be operated by remote control.
- The participant who is sharing his or her screen can interrupt screen transfer and transmit a still image in order to process confidential data or applications during the session (pause function of the monitor tray).
- The right of remote control can be immediately withdrawn from the session participant using the security key (standard is F11).

- The moderator can remove individual attendees from the session.
- The moderator can block the session to additional attendees.
- The attendee can cancel the session at any time.
- Background file transfers are not possible. The attendee can observe all file transfers and cancel them if appropriate.

Reporting and recording

Reports of every session are created on the ZEISS Remote Service server. The date, time, session moderator, duration of the session, the number of bytes transferred etc. are recorded.

All session data including video and audio data can also be recorded by the attendee concerned on the client side and if necessary saved for subsequent review.



Start session

Please enter the access data provided by your moderator.

Session number:

Your name:

Network security

Network security

The servers of the Remote Service platform are located in a specially secured network segment – the Demilitarized Zone (DMZ) – which is protected by firewalls both from the ZEISS corporate network and externally from the Internet.

The network addresses of the ZEISS Remote Service server are hard-coded into the attendee and moderator programs. This ensures that sessions cannot be redirected via servers other than the ZEISS Remote Service servers.

These measures prevent any unauthorized access to customer systems via the Remote Service platform.

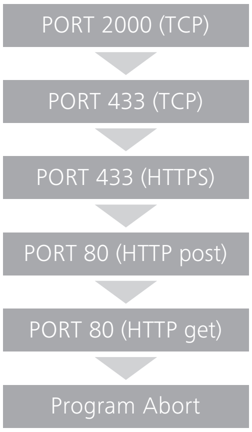
Communication

Communication during a Remote Service session can take place either via the HTTP port 80 or the TCP ports 2000 or 443. The attendee programs will first try to use TCP port 2000 or 443, then HTTPS (SSL) via port 443 and after that port 80.

If the firewall allows communication via one of the TCP ports, the session data will be transferred directly by TCP. If the firewall blocks TCP communication, the connection is set up via HTTPS port 433 or HTTP port 80 and therefore normally via a proxy server.

The use of TCP-based communication can improve the session's performance.

Both TCP-based and HTTPS/HTTP-based communication only require the ZEISS Remote Service server network addresses to be accessible via the port in question – full Internet access from the device is not needed. The network addresses can, if needed, be requested from ZEISS Service at the email address support.datamanagement@zeiss.com.



Data privacy

Organizational measures

- Only trained and certified engineers are assigned to the Remote Service department at ZEISS. They are given special training in Remote Service in addition to their product-specific training courses.
- Every Remote Service engineer is given a special briefing and has to give undertakings relating to data privacy and data security.
- Access to the ZEISS Remote Service platform is gained by additional authentication. Access is only granted to engineers who have successfully completed the required trainings and participated in the briefing mentioned above and have then given written undertakings relating to data privacy and data security.
- Within the framework of the service agreement, an additional Remote Service agreement can be concluded which sets forth precise details of the accountability and responsibility.
- In parallel to the Remote Service session, telephone communication always takes place to keep attendees informed of the actions carried out.

Summary

The security of the ZEISS Remote Service solution and the integrity of the transmitted data is guaranteed by the use of a number of security mechanisms.

- Certification by an independent certifying body (VeriSign).
- 160-bit ECC key for mutual authentication and asymmetric encryption between client and server.
- 128-bit Blowfish key to encrypt session data.
- Operator server and communication server are independent entities.
- Addresses of the ZEISS Remote Service servers hard-coded into attendee program.
- Keys hard-coded into software.
- Exchange of session number takes place by a separate medium (telephone or e-mail).
- Session between client and server with end-to-end encryption.
- Reports on session can be made by the moderator, by attendees or on the server.
- Session data can be recorded for subsequent auditing.
- A new session number is generated for every session.
- No actions can be carried out on a session participant's computer without explicit agreement. That applies to both the moderator and the attendees.
- Optionally, a session password may be used in setting up a connection.
- The moderator can remove individual attendees from the session.
- The moderator can block the session to additional attendees.
- When the moderator leaves the session, the session is ended.
- The attendee can cancel the session at any time.
- Background file transfers are not possible. The attendee can observe all file transfers and cancel them if appropriate.

If you have any further questions about Remote Service, please get in touch with your local ZEISS contact.

Your notes:

EN_30_025_0091OI Printed in Germany CZ-X/2014

The content of this publication may differ from the current licensing of the service in your country. For further information, please contact our regional representatives. Printed on elementary chlorine-free bleached paper.

Carl Zeiss Meditec AG
Göschwitzer Straße 51–52
D-07745 Jena
Germany
www.meditec.zeiss.com/contacts
www.meditec.zeiss.com/customercare