ZEISS Smart Services

Security Concept

What is ZEISS Smart Services?

The increased networking of medical technology instruments and the growing speed of transmission routes are expanding the opportunities for direct support in the service sector. This document explains the technical principles and security aspects of ZEISS Smart Services.

Via remote support, ZEISS is able to offer its customers shorter response times in service as well as a higher degree of system availability. Problems that previously required a technician to be present on-site can now be diagnosed remotely by the ZEISS Service employees and then be prepared for on-site support if necessary, or even be resolved directly.

Depending on the type of device, the ZEISS Smart Services platform offers the following core functions:

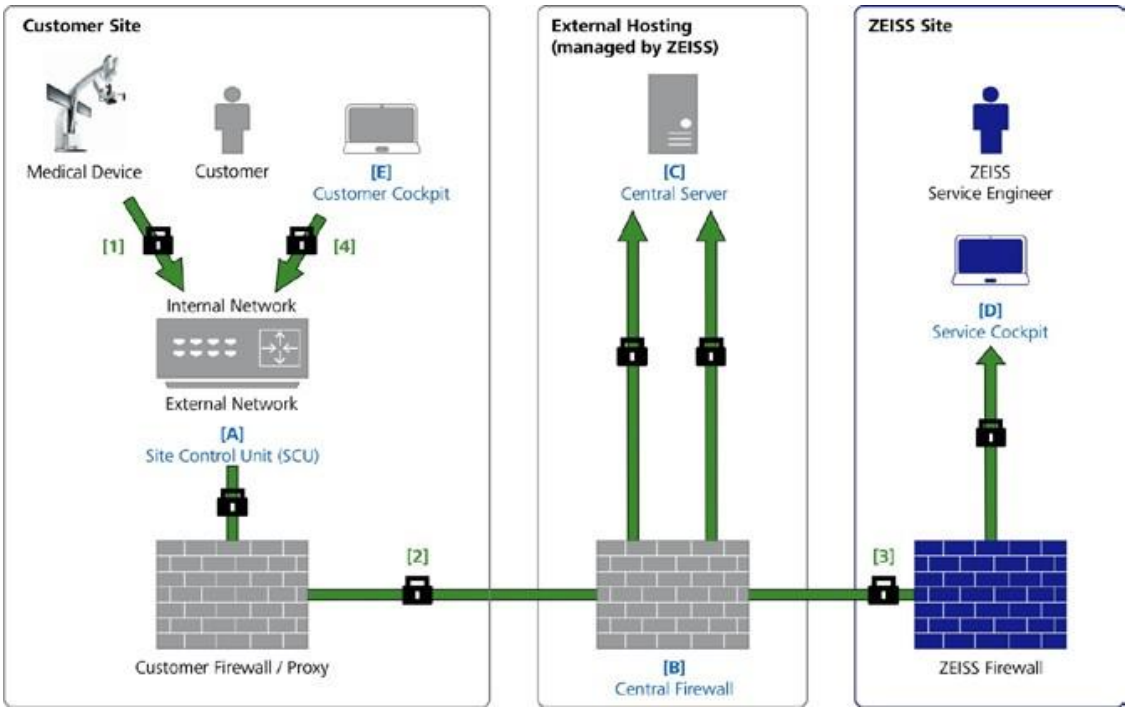
File Transfer: Transferring files from defined paths either from or to the medical device.

Diagnostic Package: Creating a diagnosis package with log files and system status information to prepare for the ZEISS Service technician.

Monitoring: Monitoring the parameters of the medical device and its evaluation and presentation.

Remote Desktop: Viewing or controlling the medical device user interface remotely. To use this function, the user of the device must explicitly allow remote access to the device as standard.

In the case of the remote servicing of medical devices, some constraints resulting from regulatory and legal requirements for medical devices must be taken into consideration. In particular, the confidentiality of patient data, the protection of medical data from manipulation and the guaranteeing of the safety and effectiveness of the serviced medical device must be ensured.



How does ZEISS Smart Services work?

Components of the ZEISS Smart Services platform

[A] Site Control Unit (SCU)
Hardware box with hardened Linux and integrated firewall, which is installed on-site. This provides the configurations and logic for the connected medical devices, serves as a storage location for log files and diagnosis packages and, through two separate network interfaces, offers a separation between the medical device network and the network used to connect to the central server. This ensures that the medical devices themselves cannot establish a network to the external network or the internet. All the customer's ZEISS medical devices prepared for ZEISS Smart Services connect to this SCU via an SSL-encrypted connection.

As an alternative solution, we also offer a software-only solution: This can be installed on a customer server. The requirements for it are described below. It offers the same functionality and number of services as the hardware version.

[B] Central Firewall
Firewall through which the central server is shielded from the internet.

[C] Central Server
Central service to which the SCUs and service cockpit connections are established using SSL encryption. This is where authentication and authorization of the ZEISS Smart Services users takes place.

[D] Service Cockpit
Software used to authenticate ZEISS technicians on the central server and grant them access to the relevant SCUs and medical devices depending on the authorization levels assigned.

[E] Customer Cockpit
Software used to authenticate the customer directly on their local SCU and grant them access to the SCU.

Connection and Establishing Session

[1] Connection between Medical Device and SCU
The ZEISS Smart Services client on the medical device establishes an SSL-encrypted (TSL v1.2) connection to the SCU via port 7778/ TCP. Depending on the local network environment, the SCU is recognized by the medical device either via a lookup mechanism (7700-7703/UDP outgoing and 7716-7719/UDP incoming) or a static configuration of the IP address or the FQDN of the SCU.

[2] Connection between SCU and Central Server
The SCU establishes an SSL-encrypted (TSLv1.2) connection to the central server via port 443/ TCP. This can occur via activation of the source/target IP address combination on the customer's in-house firewall or via an HTTPS proxy server. Only an outgoing connection via this port is required.

[3] Technician's Connection to the Medical Device
In the service cockpit, the ZEISS technician connects to the central server via port 443/ TCP (using SSL encryption via TSLv1.2), and can then connect to the desired SCU or the customer's medical device via the communication channels set up under (1) and (2), subject to successful authentication and authorization.

[4] Customer Connection to SCU
In the Customer Cockpit, the customer can connect to the SCU via port 7778/ TCP (using SSL encryption via TSLv1.2), and from there can view any access logs, session recordings and diagnosis packages created; this is subject to successful authentication and authorization.

Security

Establishing a Connection
The connection will be established from the customer's internal network. No ports need to be opened to gain external access via the internet. The only connection to the outside is the one from the SCU, which is the SSL-encrypted channel initiated from within the local network, via port 443/ TCP, to the central server. All communication occurs via this channel.

Authentication and Authorization
Authentication takes place via role-specific SSL certificates. Each user of the ZEISS Smart Services platform receives a personal username and password. The ZEISS Smart Services platform offers a role-based user concept, which ensures that ZEISS Service employees only have access to functions activated for them.

Transport Encryption
For transport encryption between the medical device, SCU, central server, and the cockpit, the ZEISS Smart Services platform uses TSL v1.2 with public key RSA 2048 bit and symmetrical AES 256-bit encryption.

Logs and Auditing
All actions by ZEISS Service employees on the SCU and the medical device are logged with a date and time stamp as well as a user ID. Furthermore, when using our remote desktop tool (VNC), the entire session is recorded as a screen recording and stored locally on the customer's SCU. The customer has access to these log files and session recordings via the Customer Cockpit.

Blacklisting
On the central server and the SCU, after 10 failed authentication attempts, the corresponding IP address is placed on a blacklist to counteract potential brute-force attacks. It will not be possible for any more logins to take place from this IP address, until no login attempt has been made via this IP address for a period of 30 minutes.

Server Security
Our central server system can be only reached passing our central firewall system via port 443/ TCP, via which the SCUs and cockpits establish encrypted connections to the central server. For additional security against unauthorized access, the data storage media on the server instances are encrypted with BitLocker.

TÜViT and ISO 27001 certifications
The ZEISS Smart Services software meets the requirements of Security Qualification (SQ), Version 10.0 Security Assurance Level SEAL-3 of TÜV Informationstechnik GmbH. The operation of the ZEISS Smart Services platform is certified by TÜV in accordance with ISO 27001.

Optional Connection via IPsec VPN
In scenarios with security regulations that allow outbound connections to be established only via IPsec VPN, the connection between the SCU and the central server can be established using IPsec VPN. The endpoint for the VPN in such cases is the central firewall, via which all standard IPsec configurations are possible.

Data Protection

In the ZEISS Smart Services area, ZEISS only employs qualified and certified technicians. They receive training on specific devices and on ZEISS Smart Services.

Each ZEISS Smart Services technician receives training and is obliged to observe data protection and data security regulations.

Access to the ZEISS Smart Services platform requires additional authentication. Only ZEISS technicians who have successfully completed the required training as specified above are granted access.

Access to the relevant medical device is controlled by a role concept. This ensures that only authorized technicians can connect to the relevant device.

Pre-requisites

The following is required to connect to ZEISS Smart Services:

1. One or more medical devices made by Carl Zeiss Meditec and intended for ZEISS Smart Services.

2. A network connection between the medical device and the SCU. The connection to the SCU can be established via:

   - LAN-Interface: Ethernet (1000Base-T) to the internal network interface
   - WAN-Interface: Ethernet (1000Base-T) to the external network interface

3. Accessibility of the central server from the SCU with port 443/TCP. This can take place (if necessary restricted to the IP address of the SCU and IP address of the central server) via:

   - Direct activation on the customer's firewall
   - Configuration of a customer proxy on the SCU without proxy authentication
   - Configuration of a customer proxy on the SCU with proxy authentication (machine account without password change guideline recommended)

   *A bandwidth of at least 2 Mbit/s synchronous is required. A 10 Mbit/s synchronous is recommended (no reserved bandwidth is needed).

4. Also required when using the Software-only SCU:

   - PC, server or virtual server designed for 24/7 use, Windows server 2012 R2 operating system
   - 20 Gig Storage space
   - Server +0,5 Gig RAM (for the application

SCU Hardware Specification

Specifications

General

Certification	CE, FCC, UL, CCC, BSMI
Dimensions (W x D x H)	100 x 70 x 30 mm (3.9" x 2.8" x 1.2"), UNO-2271G-E21AE 100 x 70 x 65 mm (3.9" x 2.8" x 2.6"), UNO-2271G-E22AE and E23AE
Form Factor	Pocket Size, same dimension as standard 2.5" SSD/ HDD
Enclosure	Aluminum Housing
Mounting	Stand, Wall, VESA (Optional), DIN-rail (Optional), Pole (Optional)
Weight (Net)	0.5 kg (1.1lbs) for UNO-2271G-E21AE 0.6 kg (1.2lbs) for UNO-2271G-E22AE and E23AE
Power Requirement	10 ~ 30V_{DC}
Power Consumption	12W (Typical), 20W (Max)
Operating System	Linux

System Hardware

BIOS	AMI EFI64 Mbit
Watchdog Timer	Programmable 256 levels timer interval, from 1 to 255 sec
Processor	Intel Atom E3815 1.46GHz (E3825 support by project)
System Chip	Intel Atom SoC integrated
Memory	Onboard 4GB DDR3L 1066 MHz
Graphics Engine	Intel® HD Graphics
Ethernet	Realtek RTL8111E GbE, 802.10av
LED Indicators	LEDs for Power, HDD, LAN (Active, Status)
Storage	Onboard 32G eMMC (Option mSATA)
Expansion	1 x Full-size mPCIe slot

I/O Interfaces

Serial Ports	2 x RS 232/422/485 by extension mini card for UNO-2271G-E23AE
LAN Ports	2 x RJ45, 10/100/1000 Mbps IEEE 802.3u 1000Base-T Fast Ethernet
USB Ports	1 x USB 3.0 for UNO-2271G-E21AE 3 x USB 2.0 and 1 x USB 3.0 for UNO-2271G-E22AE 1 x USB 3.0 for UNO-2271G-E23AE
Displays	1 x HDMI, supports 1920 x 1080 @ 60Hz
Power Connector	1 x 2 Pins, Terminal Block
Grounding Protection	Chassis Grounding

Environment

Operating Temperature	0 ~ 50°C (32 ~ 122°F) @ 5 ~ 85% RH with 0.7 m/s airflow
Storage Temperature	- 20 ~ 70°C (-4 ~ 158°F)
Relative Humidity	10 ~ 95% RH @ 40°C, non-condensing
Shock Protection	Operating, IEC 60068-2-27, 50G, half sine, 11 ms
Vibration Protection	Operating, IEC 60068-2-64, 2 Grms, random, 5 ~ 500 Hz, 1hr/axis (mSATA)
Ingress Protection	IP30