

# Smart Services from ZEISS

Security Concept



## 1. 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:

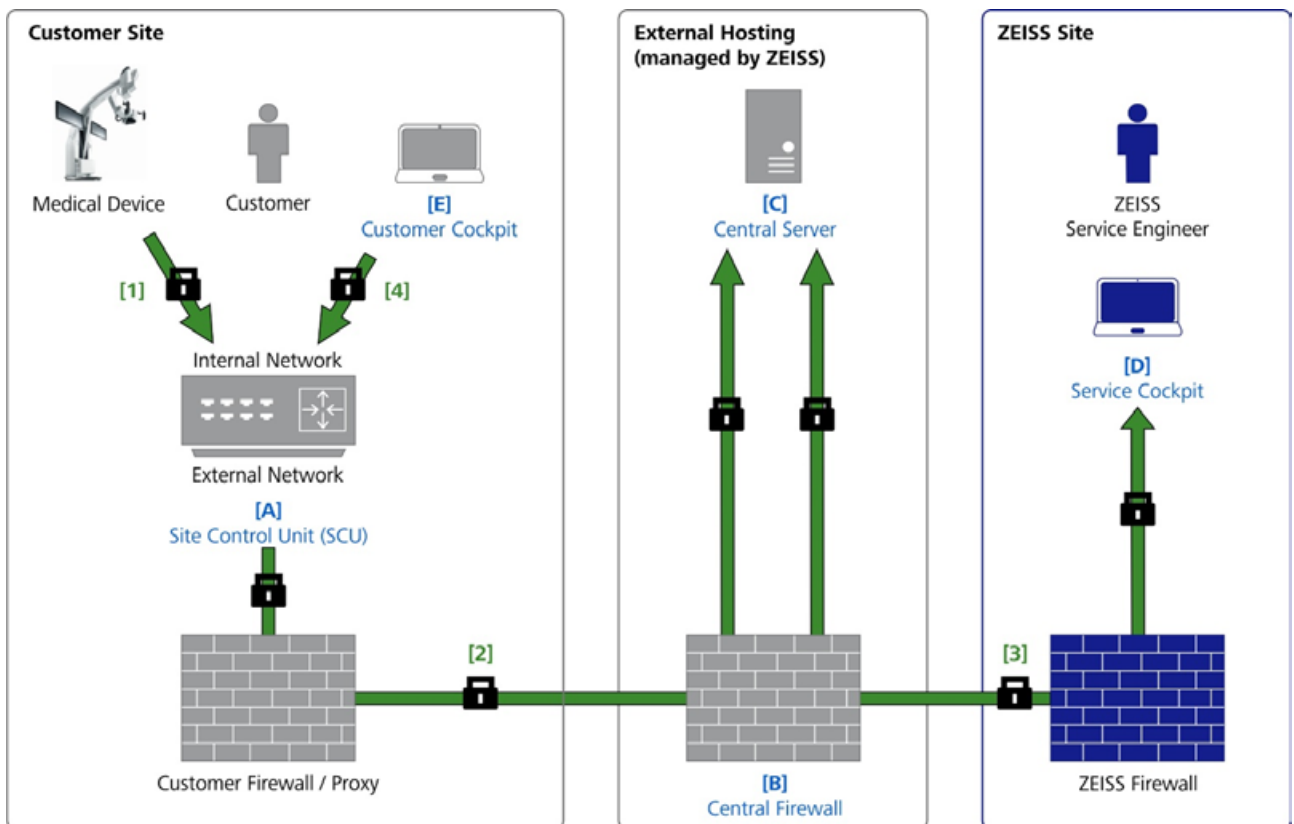
**File Transfer:** Transferring files from defined paths either from or to the medical device.

**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.



## 2. How does ZEISS Smart Services work?

### 2.1. 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 of the customer's ZEISS medical devices prepared for ZEISS Smart Services connect to this SCU via an SSL-encrypted connection. Alternatively, instead of the SCU box a software-only version can be installed on a customer's system.

#### [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.

### 2.2. Connection and meeting setup

#### [1] Connection between medical device and SCU

The ZEISS Smart Services client on the medical device establishes an SSL-encrypted 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 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), 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] Connection between customer and SCU

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

## 3. Security

### 3.1. 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.

### 3.2. 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.

### 3.3. Transport encryption

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

### 3.4. Logs

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. In addition, when using the Remote Desktop function, the entire session is recorded as a screen recording and filed on the customer's SCU. The customer can access these log files and session recordings via the customer cockpit.

### 3.5. 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.

### 3.6. Server security

The central server does not have a public IP address and can only be reached via the services explicitly activated on the central firewall. The only port on the central firewall that can be accessed externally is 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.

### 3.7. 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 currently certified by TÜV in accordance with ISO 27001.

### 3.8. 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.

## 4. 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.

## 5. Prerequisites

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:
    - Ethernet (1000Base-T) to the internal network interface (separate medical device network),
    - Ethernet (1000Base-T) to the external network interface (no network separation)
    - WLAN (requires WLAN-enabled medical device and SCU model with WLAN)
  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 1 Mbit/s (synchronous) is needed, but at least 2 Mbit/s (synchronous) is recommended.
4. Also required when using the software-only SCU solution:
    - PC, server or virtual server designed for 24/7 use,
    - Windows server 2012 R2 operating system (other operating systems on request)

## 6. SCU hardware specifications

<b>Interfaces</b>	Gigabit Ethernet (Intel i211AT) Serial interface, I/O: DB9 serial port Dual USB connection: 2 USB 3.0 connections WLAN antenna sockets: RP-SMA connectors
<b>Single board PC</b>	CPU: AMD Embedded G series GX-412TC, 1 GHz quad Core (Jaguar) with 64-bit and AES-NI support, 32 kB Data + 32 kB Instruction Cache per core, shared 2 MB L2 Cache, fanless Main memory: 2 or 4 GB DDR3-1333 DRAM Secondary storage: 16 or 64 GB SSD OPTIONAL PCIe WLAN card, 2 WLAN antennae (2.4 GHz, to 5 dBi, 2x2 MIMO) <b>or</b> PCIe WLAN card with increased ESD protection, 2 WLAN antennae (2.4 GHz to 5 dBi, 2x2 MIMO)
<b>Power supply</b>	Direct current in control box: 24 V with 0.9 A = max. 20 W With plug-in power supply: 12 V direct current with 2 A = max. 24 W
<b>Dimensions</b> (LxHxW in mm)	Without adapter: 200x203x69 With "thin" top-hat rail adapter: 240x205x77 With "large" top-hat rail adapter: 200x203x73 Packaging: 272x272x120
<b>Weight</b>	SCU box: 1314 g "Thin" top-hat rail adapter: 285 g "Large" top-hat rail adapter: 333 g WLAN set: 56 g

**Carl Zeiss Meditec AG**  
Goeschwitzer Strasse 51–52  
07745 Jena  
Germany  
[www.zeiss.com](http://www.zeiss.com)  
[www.zeiss.com/med/contacts](http://www.zeiss.com/med/contacts)

**EN\_37\_012\_00011 SER.10137** CZ-VII/2018 International edition: Only for sale in selected countries.  
The contents of the brochure may differ from the current status of approval of the product or service offering in your country. Please contact our regional representatives for more information.  
Subject to changes in design and scope of delivery and due to ongoing technical development. KINEVO is a registered trademark of Carl Zeiss Meditec AG.  
© Carl Zeiss Meditec AG, Jena, 2018. All rights reserved.