Security
Concept
White paper
Version
12.0

# Smart Remote Services

Your smart connection to digital services

**siemens-healthineers.com/srs**

SIEMENS Healthineers

# Contents

*"The support we receive through SRS provides us with a fast and personalized answer to questions or issues [...]. By having remote access to our server, the syngo supporters (Remote Service Engineers) are really efficient, and can access our workstations, take the control, in order to guide us step by step, for every demand that we have, so we never feel abandoned."*

**Nullam Jeremy Brachet**
MRI Technician, IRM Lyon Nord, Lyon, France

# Smart Remote Services (SRS)

## Your smart connection to digital services

High-quality availability, diagnostic confidence, and smooth operations are essential to meet your performance requirements. At the same time, protecting your equipment and patient data with the right security measures remains one of our top priorities.

With these needs in mind, we focus proactively on keeping you on the path to success. Smart Remote Services (SRS) is a fast, secure, and powerful data link that connects your medical equipment with our experts. They provide proactive and interactive support that helps you in your daily routine and accelerates your operations.

Through the SRS connection, you gain access to our extensive portfolio of Remote Services, enabling you to:

- **Improve diagnostic and clinical outcomes** through context-specific interaction and immediate remote application support.
- **Enhance performance and functionality** through regular remote software updates, keeping your system up to date at all times.
- **Increase system uptime** with real-time remote system monitoring and proactive scheduling of service events.

This Security Concept White paper outlines the measures Siemens Healthineers has implemented – across both technical support and clinical application areas – to help support secure data transfer and protect patient information when performing SRS-based services on your medical devices. The concept applies to all products for which SRS is offered.


Siemens Healthineers has been one of the first manufacturers of medical devices worldwide to implement an internationally valid Information Security Management System (ISMS) for the remote service of medical devices and software systems. The system has been certified by TÜV Süd in Germany according to the international standard ISO/IEC 27001:2022.

The ISO/IEC 27001:2022 certificate and the associated Statement of Applicability (list of controls) is valid and available to all customers, with the exception of customers in China. For China an independent certification according to CPCS Level 3 is available.

# Security measures in our remote service delivery process

SRS is our channel for remotely responding to your requests for reactive and interactive services – such as technical and application support – and for delivering data-driven proactive services. Given the diverse range of services provided through SRS, we apply tailored protection measures to safeguard your business, whether these services are delivered directly by Siemens Healthineers employees or by authorized Business Partners.

## Remote technical support

Our incident-handling process follows a three-step escalation model. Using Smart Remote Services as a direct connection, we provide remote troubleshooting and expert support for our products.

Our engineers at the Customer Care Center respond to your support requests and access your system remotely to perform early diagnosis and troubleshooting. In addition, specialists from our Remote Services Center may access your system to address issues that require second-level attention. For IT systems – such as PACS or advanced post-processing solutions – first-level support is provided directly by our Remote Services Center specialists.

Our products running *syngo*[1] application software include mechanisms to mask patient data before it is transferred to the Customer Care Center for remote troubleshooting. The latest software versions[2] also enable you to define which users have access to specific data within the device (see section "SRS security measures in our applications software"). With this approach, the decision to grant access – whether to a Siemens Healthineers Service Engineer or to your own staff – remains entirely in your control.

For in-vitro products, the Atellica Connectivity Manager (ACM) enables customers to manage system access, including remote control, file transfer, and monitoring.

For products that do not run *syngo* software, granular access control to data is not implemented. In these cases, we rely on our organizational measures and the Smart Remote Services (SRS) infrastructure (see section "Security measures in our Smart Remote Services infrastructure") to protect your data.

## Remote application support

To assist your clinical staff with application-related questions, our Customer Care Center or Remote Services Center application specialists can use SRS to mirror your system display and provide real-time guidance through remote desktop management tools.

Our products are designed to require your explicit authorization before establishing any remote access and allow you to monitor and terminate the connection at any time during the support session.

Many in-vitro products add an additional layer of protection by masking any Protected Health Information (PHI) when a remote session is detected, minimizing the risk of PHI being visible outside your institution. Further details can be found in the Security White paper of the respective medical device.

[1] *syngo is a registered trademark of Siemens Healthineers AG.*
[2] *Information regarding the software version on your system may be obtained from your representative of Siemens Healthineers*

## Proactive monitoring services

Certain proactive services require your device to regularly send a predefined set of data to our Remote Service Centers. This includes system logs, as well as statistical and reliability data, such as the number of scans performed, system events or configuration data, and how often the system has restarted.

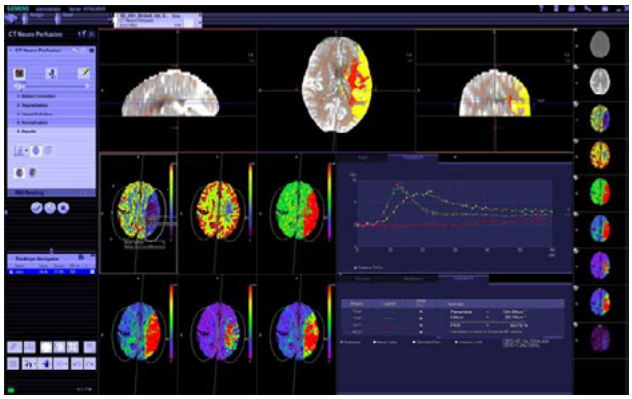

**Figure 1:** *syngo* user interface, anonymizing patient data

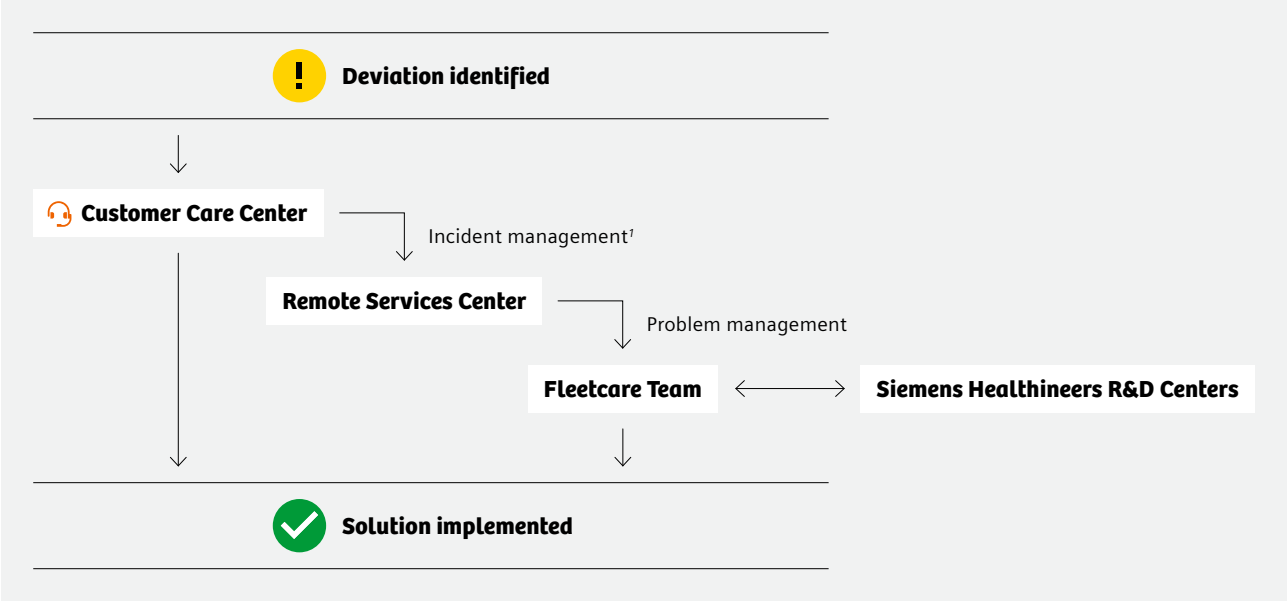


**Figure 2:** Siemens Healthineers escalation process for handling service calls

[1] *Depending on the product line, incident management can be directly handled at our Remote Services Center.*

# Security measures in our applications software

## In-vivo products based on *syngo*

Our products that run *syngo* applications software[1] can be configured with the following features to support data security throughout the whole remote interaction.

**Access control**
You can define the level of access granted to systems operating with our *syngo* application software.

After a predefined period of inactivity, the SRS session on your system is automatically terminated.

When establishing a remote service connection, you can select from four access levels:

- **No access**
  Access is granted only on a case-by-case basis to perform the approved task. Patient examinations on the system can continue uninterrupted.
- **Limited/Restricted access**
  For a predefined time period, the authorized Service Engineer is granted access to a subset of service functionalities that do not interfere with ongoing examinations.
- **Permanent limited access**
  The authorized Service Engineer has access to a subset of service functionalities that do not interfere with ongoing examinations. This access is not time limited.
- **Full access**
  The authorized Service Engineer has full access to all service functionalities. Patient examinations cannot be performed while remote service is in progress.

These access levels define both the duration for which you grant service access to your system and the extent of that access. During each session, you maintain full control and can grant or revoke access rights at any time.

While permanent limited access is the most selected level, you can always choose no access if preferred. Figure 3 illustrates the workflow of a remote service task at this access level.

**Session control**
Every application support session requires a one-time session password. This allows you to decide on a case-by-case basis whether to share your monitor with our expert. Once the issue is resolved, the connection is terminated. Accessing your systems without your authorization is not possible.

**Note:**

The access control described above does not apply to server-based IT systems, such as PACS or advanced post-processing workstations. Remote access to these systems can be established without direct interaction with end users, as such access does not necessarily affect a dedicated workplace.

**Password protection**
When you grant access to your system, the Service Engineer or Application Expert must authenticate using a valid, time-dependent password before being allowed to log in. For IT systems integrated into your IT domain, it is possible to align system password policies and security measures with your environment, provided that system functionality is not affected.

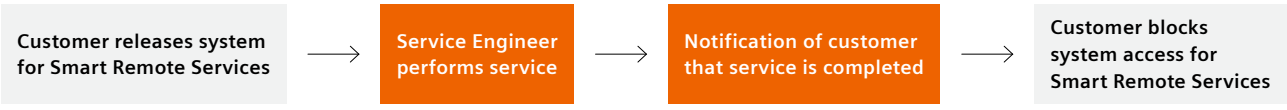


**Figure 3:** Workflow of SRS activities at “no access” level

[1] *Generally includes our diagnostics imaging modalities, and excludes server-based systems such as syngo.via and syngo.plaza*

**Four-eye principle**
During every remote session, your system screen displays an indicator (bottom right-hand corner) showing that remote service activities are in progress. Simultaneously, our Service Engineers or Application Experts explain via voice call the actions they are performing. If you choose to terminate the session, all service programs currently running are immediately and safely shut down, without impacting the continued safe operation of the system.

**Email notification of remote connections**
Upon your request, we can enable an email service providing the connection details of each remote connection to an email address of your choice. This email can be followed up after each session with a second message containing further information on the activities performed. These emails are sent from the SRS DMZ (see section "Security measures in our Smart Remote Services infrastructure"), and not from the medical systems themselves.

## Laboratory diagnostics (in-vitro) equipment and software

Our laboratory diagnostics instruments are enabled for remote monitoring and support through Smart Remote Services by the following three elements:

- Proprietary software protocol on the instrument to facilitate communication with the ACM.
- The ACM connects the SRS infrastructure through a secure and encrypted Internet Based Connection (IBC). For information on IBC, please refer to section "Security measures for internet-based connectivity".
- Smart Remote Services provides both ongoing remote monitoring of connected devices from Siemens Healthineers and as-needed remote desktop support.

**Access control**
Remote access is limited to authorized service staff with appropriate authentication credentials. Both the instruments and the Atellica Connectivity Manager (ACM) require service user accounts to ensure proper management of the product's functionalities.

When issues arise, authorized service staff may need to access the instrument desktop. These staff log into the SRS infrastructure to request a live connection to the instrument or product. All interactions between service staff and the hospital or laboratory's connected instruments are routed through the SRS application and managed by the ACM, preventing your devices from being directly exposed to external networks. All user and system interactions performed by Siemens Healthineers are recorded and available for audit purposes.

**Session control**
You can define the level of access available to remote users through the ACM GUI. This control extends to all connected instruments and allows full management of file uploads, downloads, and remote desktop access. You can grant or deny access to remote sessions, software updates, applications, and monitoring functions.

If a computer issue arises, you can request a remote session with authorized service staff only. Additional service user accounts required to manage product functions may not be removed or modified.

SRS remote desktop sessions are initiated on an ad hoc basis, typically for investigating equipment issues. Authorized service staff logged into the SRS application can request remote access to an instrument or the ACM. Once the request is initiated, you must accept it at the instrument within 30 seconds, or the request will time out. If access is granted, all remote activities are visible on the instrument monitor. The SRS infrastructure logs all remote connections and file transfers. In every case, the local system operator must accept the remote session to allow the remote user to proceed.

**Network control**
SRS supports:

- Static IP addressing and DHCP assignment
- NTLM authentication when using an ISA server as a proxy communication channel, via standard and authenticating proxy servers as required

**Data transfer**
All communication between the SRS infrastructure and the local Atellica Connectivity Manager (ACM) is encrypted by design. Communication between the local ACM and connected instruments can also be encrypted for certain instruments; for specific details, please refer to the Security White paper of your Siemens Healthineers medical device.

Remote monitoring is facilitated by transferring data from the instrument to the SRS infrastructure via the ACM. Depending on the instrument and the type of data involved, this transfer may be initiated either automatically by the instrument itself or by authorized service staff logged into the SRS application.

# Security measures for information in transit

To securely transport data between your facility and the SRS infrastructure we employ a secured, encrypted connection. If you also opt to route all network traffic through your own firewall you will obtain full control over your communication.

The in-vitro medical devices, offer an Internet-Based Connectivity (IBC) technology to create a virtual private connection (VPN). The in-vivo medical devices offer, in addition to IBC, the IPSec and the WebSocket/TLS connectivity technologies to create the VPN connection. Please note that Internet-Based Connectivity (IBC) or WebSocket/TLS may not be available or officially released for all in-vivo modalities.

Depending on the medical device, the consumed services may be deployed on premise or in the cloud-based deployment of SRS.

# Supported protocols

## Security measures for IPsec connectivity

Our Smart Remote Services use an IPSec solution to connect your environment with the SRS infrastructure.

If you do not have a VPN endpoint, Siemens Healthineers can provide a VPN endpoint device required for the SRS connection. We regularly monitor security advisories and remotely update the software on these VPN endpoints as needed. All configuration changes are tracked in our configuration management database and applied to field devices accordingly.

If you already have your own solution, our technicians can assist with implementing the necessary connection parameters. These parameters must then be protected against unauthorized changes.

We have implemented several security measures to protect the connection:

- **Access Control Lists**
  Access Control Lists (ACLs) on your service router function similarly to firewalls: They allow data traffic only to and from known IP addresses. ACLs prevent Siemens Healthineers from accessing other parts of your network and block access by unauthorized parties.
- **IP Security Protocol Suite**
  To prevent network sniffing and data tampering, Siemens Healthineers uses the established IP security (IPsec) protocol (suite) with pre-shared secret keys for encrypted and authenticated data transmission. Pre-shared secret keys consist of arbitrary strings of random characters. The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange encryption key information. For backward compatibility with some legacy connections, we continue to support parameters such as SHA1, MD5, and 3DES in consultation with affected customers. We are actively working with these customers to migrate their connections to the newly recommended parameters.

For new connections, we recommend the following minimum configuration parameters:

| | |
|---|---|
| • Authentication/Integrity | SHA-256 |
| • Encryption | AES-256 / AES-GCM-256 |
| • Key-Exchange | DH-group-16 (4096 bit) |

To further enhance data privacy while maintaining data integrity, we also support higher levels of encryption and authentication, such as SHA-384, SHA-512, and stronger Diffie-Hellman groups (e.g., Group 19–256-bit EC, Group 20–384-bit EC, Group 21–521-bit EC, Group 24–2048/256-bit) for key-exchange security.

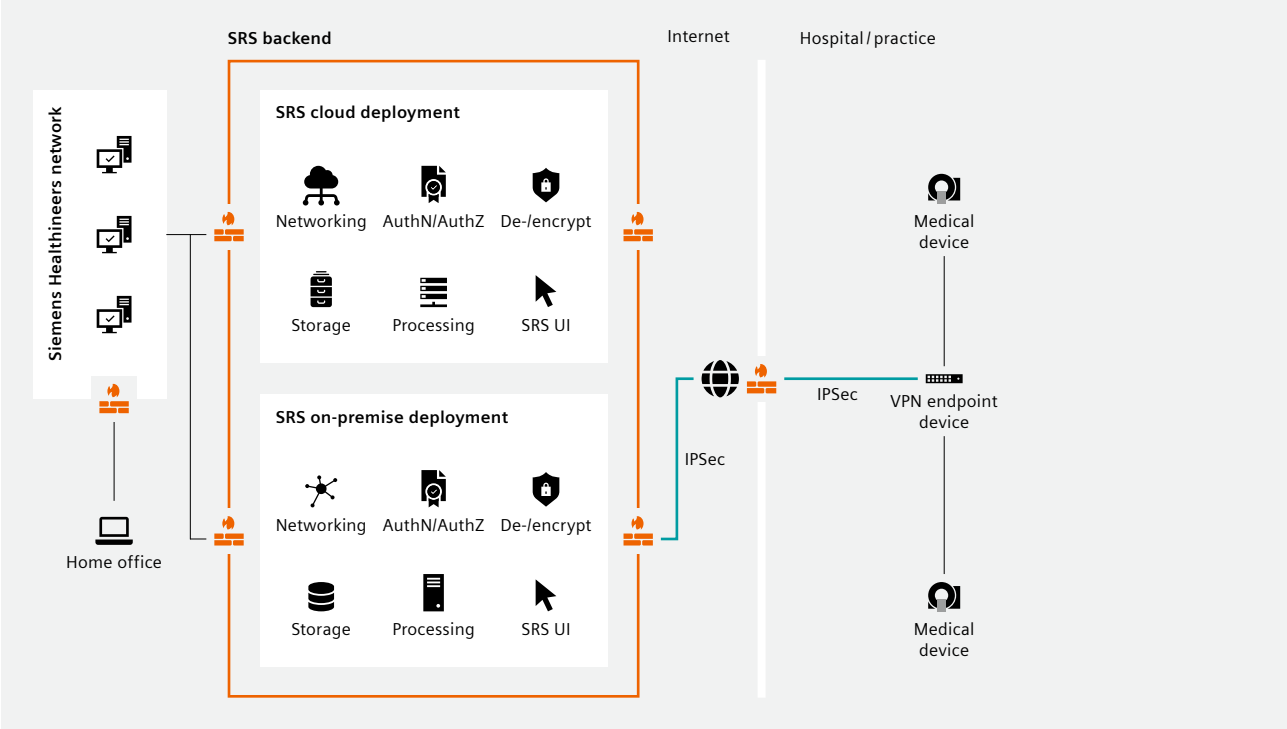


**Figure 4:** IP security protocol suite

## Security measures for internet-based connectivity

Internet-based connectivity (IBC) relies on Transport Layer Security (TLS) and communicates via outbound HTTPS requests on port 443. This technology establishes a secure and private communication channel for data exchange between the system and the SRS DMZ by creating a direct, encrypted network tunnel. It supports data protection and reduces the risk of virus infection from unauthorized third parties during an SRS connection.

IBC with TLS is increasingly recognized across the industry as a highly effective and economical solution for remote access. It enables your medical devices (in-vivo) or ACM (in-vitro) to connect to the Smart Remote Services infrastructure using a standard internet connection, without the need for additional hardware or network modifications, while safeguarding your data and providing greater system mobility.

The TLS certificate is issued by the SRS private Certificate Authority located in the SRS backend and is delivered and installed in the IBC client during setup. For further details, please refer to the Security White paper of the respective medical device (in-vivo) or ACM (in-vitro), or contact your local Siemens Healthineers representative.

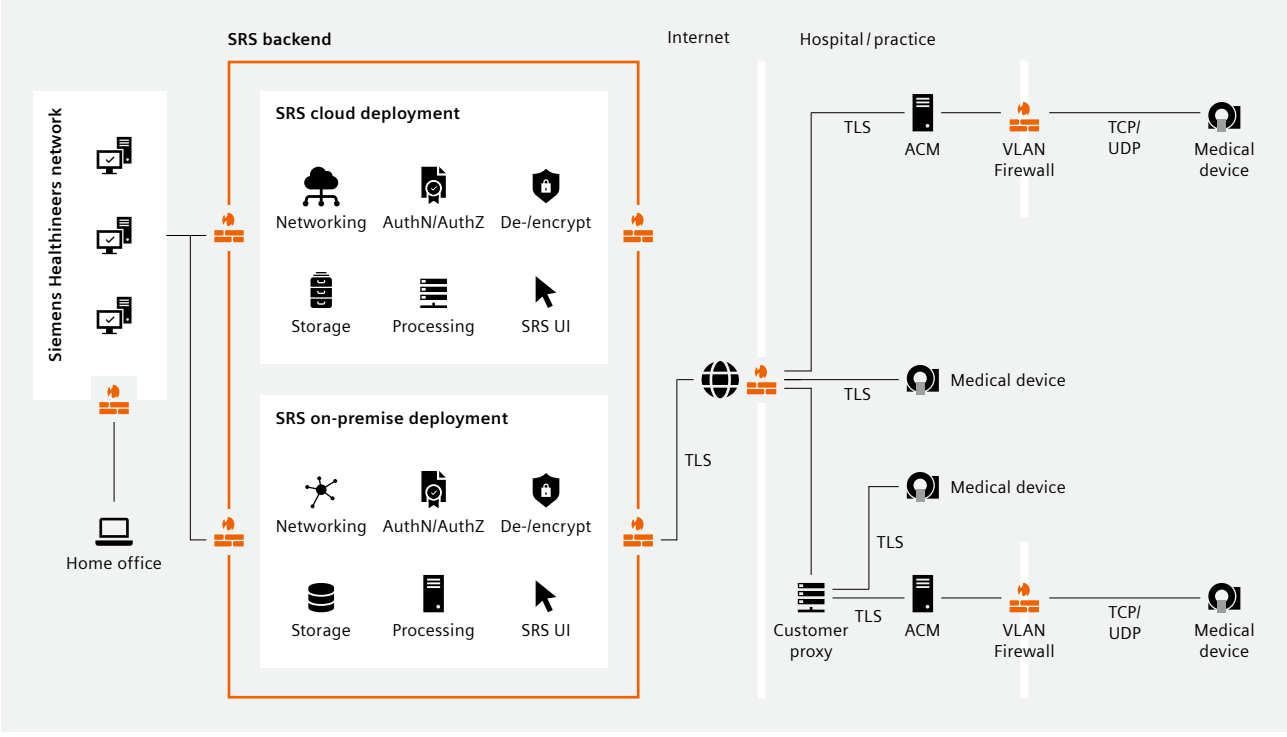


**Figure 5:** IBC connectivity

## Security measures for WebSocket/ TLS connectivity

WebSocket is a connection technology that provides a secure, encrypted communication channel over a single TCP connection on port 443. Similar to IPSec and IBC, it enables bidirectional communication between the medical device and the SRS DMZ, with the client on the device initiating the connection to the Smart Remote Services infrastructure.

Connectivity options for WebSocket/TLS connectivity

1. **Direct connectivity via customer Internet access**
   Medical devices connect directly through the customer's Internet access to dedicated SRS endpoints.

2. **Centralized connectivity via customer proxy**
   Medical devices connect through the customer's proxy server to dedicated SRS endpoints.

3. **Centralized connectivity via IPSec VPN endpoint**
   Medical devices connect through an IPSec VPN endpoint to dedicated SRS endpoints.

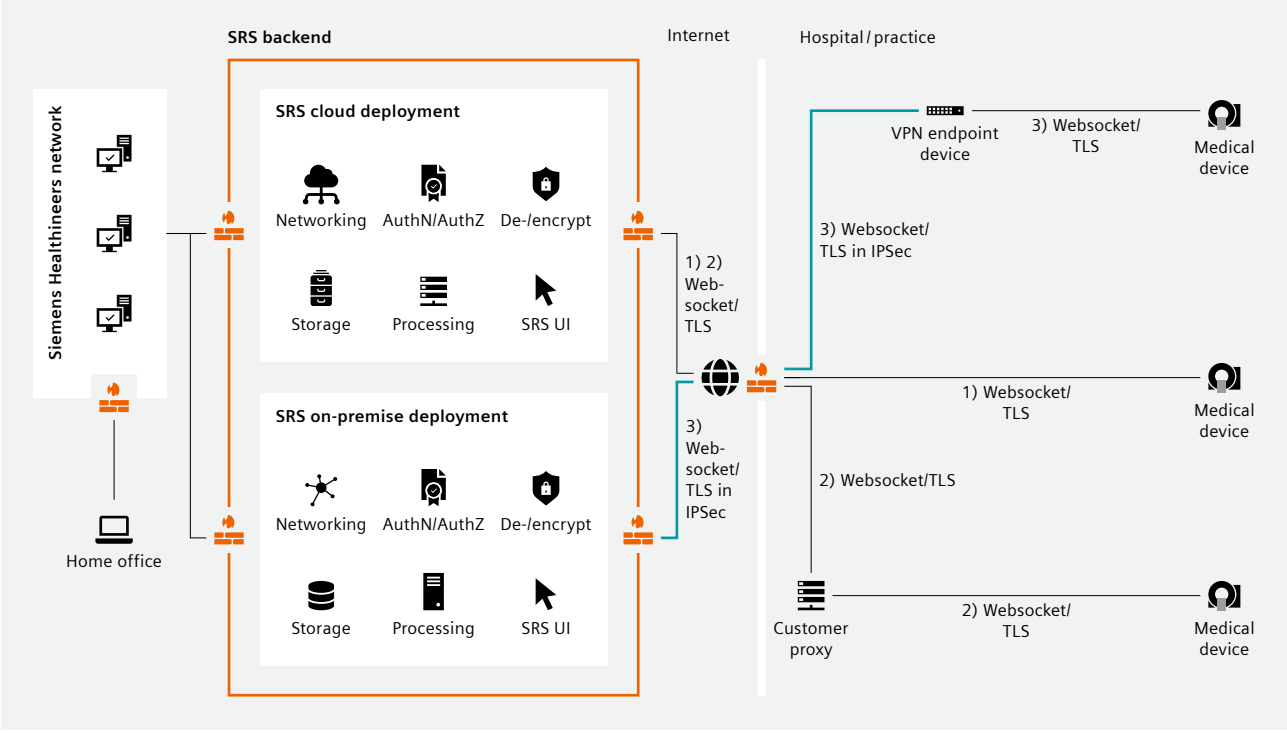


**Figure 6:** WebSocket/TLS connectivity

# Transmission from your systems to the Smart Remote Services infrastructure

Data exchange through the SRS connection is triggered by two different mechanisms. Please note that the data volume transferred depends heavily on the product type, its life cycle phase, and therefore cannot generally be quantified.

- **User-initiated transfers**
  Data transfer is remotely "pulled" from the system by an authorized Service Engineer, or a data "push" is scheduled to resolve a specific issue on the system.

  Data pulls are performed when Customer Care Center service staff first attempt to troubleshoot a reported issue using log data stored locally on the medical device. If further expert support is required, the Remote Service Engineer can initiate a data transfer to the SRS backend. This data is accessible to specialists at the Customer Care Center, Remote Service Center, and the Fleetcare Team, as well as other authorized support units, including the product R&D team. In specific error cases, the transferred data may include PHI/PII (e.g., body height and weight of a patient in MRT studies) in addition to technical data. Such data is accessed only to resolve the reported issue. Service staff are trained annually and reminded of data privacy measures and proper handling of data that may contain PHI/PII.

- **System-initiated transfers**
  Automatic data "push" transfers occur at regular, predefined intervals. For in-vivo devices, transfers are performed via file transfer, and in a limited number of systems, via email from the device to the SRS backend. For in-vitro devices, transfers are performed using a proprietary protocol. Further details regarding the technical data transmitted and its intended use are described in the respective Terms and Conditions, which must be agreed upon in advance.

- **Added value transfers**
  Certain value-added services require that devices access a forwarding service that provides connectivity to dedicated Siemens Healthineers network and/or internet resources. The resources accessible by specific devices are closely monitored within the SRS backend. This access is necessary, for example, to allow mobile devices shipped with the medical device can be updated, or to enable the "Fast Contact" button without granting the medical device direct Internet access.

# Security measures in our Smart Remote Services infrastructure

Our SRS rely on the secure operation of the SRS connection and the SRS Demilitarized Zone (SRS DMZ) (see section "SRS Demilitarized Zone"), which sits between the Siemens Healthineers intranet and the internet. The following measures are implemented to ensure data protection within our SRS infrastructure:

## Authentication and authorization

Access to the SRS infrastructure is restricted through single sign-on (SSO) with two-factor authentication. The first factor combines PKI and username/password, and the second factor is a one-time password (OTP) delivered via mobile app, SMS, or email.

Our granular authorization concept allows us to define which users can access which systems based on a need-to-know principle. In practice, this means that only authorized service staff who require access to a system to perform their support tasks – and who are not explicitly restricted – can access the system.

## Remote access logging

We record every instance of direct access to your system in every instance of direct access to your system via the SRS infrastructure is recorded with a timestamp and a unique user identification of the responsible Service Engineer or Application Expert. This information is retained for up to three years, unless applicable laws or regulations mandate a different retention period. Access to this information, to the extent available, can be provided upon request.

## SRS Demilitarized Zone

Between your network and the Siemens Healthineers intranet, we have established an SRS Demilitarized Zone (SRS DMZ). Multiple SRS DMZ locations worldwide provide a reliable connection while minimizing latency for remote communication.

Access to your medical equipment is only permitted for authorized users via the SRS DMZ, and all sessions are tracked for auditing purposes. This architecture is designed to mitigate the risk of unauthorized network access to customer systems.

## Protected Smart Remote Services infrastructure

Smart Remote Services operates using either an on-premises or cloud-based infrastructure in accordance with the Information Security guidelines of Siemens Healthineers. The effectiveness of these protection measures is regularly audited to verify that the SRS infrastructure operates with up-to-date technology.

## Organizational measures

Siemens Healthineers was among the first medical device manufacturers worldwide to implement an Information Security Management System (ISMS) specifically for the remote service of medical devices and software systems.

This ISMS system has been certified by TÜV Süd in Germany in accordance with the international standard ISO/IEC 27001:2022 (3rd Edition).

In addition, Siemens Healthineers operates a Privacy Information Management System (PIMS) based on ISO/IEC 27701:2019.

Our Service Engineers and Application Experts are trained in, and committed to, both data privacy and security. Siemens Healthineers maintains an electronic record of these service employees along with their corresponding access rights.

Further details on data privacy can be found in the Smart Remote Services Data Privacy White paper.

# Protection against malicious attacks

All measures described in this Security Concept White paper are designed to provide holistic, end-to-end protection for your systems and environment, with a particular focus on minimizing risks from the following specific threats.

### Malware infections

The continuous monitoring and maintenance of the SRS backend contributes to keep the connection between your medical devices and the SRS backend secured. As long as internet access is used for SRS purposes only and the product is operated according to its Security White paper, virus infections are unlikely.

### Malicious email traffic

Certain in-vivo medical devices send emails to the SRS infrastructure. These emails are transmitted from your system to the SRS DMZ.

Emails sent to the SRS DMZ are then forwarded to the appropriate Siemens Healthineers email server and subsequently relayed to the intended recipient. Recipients may include a Siemens Healthineers email address or your own IT department/internal email address. Each recipient address must be whitelisted before an email can be relayed. Importantly, no emails are sent from the SRS DMZ back to the medical device.

In-vitro medical devices do not send emails to the SRS DMZ.

### Cross-system infections

The risk of cross-infection between the Service Engineer's workplace and your system is minimal, as the Service Engineers' workstations are equipped with robust malware protection measures.

# How to support your equipment further

Despite our strong commitment to cybersecurity, the nature of our products may require your active involvement to maintain their secure operation. While we strive to achieve a high level of cyber security the measures for protection within your network are not in our responsibility and thus limited. We rely on your cooperation to complement our measures and jointly achieve adequate protection, e.g. when it comes to access controls or encryption of data.

You are responsible for the security, integrity, and proper configuration of your IT systems, networks, and components. This includes all measures necessary to prevent, detect, and mitigate cybersecurity risks within your environment in line with applicable laws, regulations, and industry standards.

All our equipment and software-only products are released with a Security White paper and/or a Manufacturer Disclosure Statement for Medical Product Security (MDS2). These documents provide detailed information on the security controls implemented on the device, as well as additional considerations for setting up your IT infrastructure in line with the principle of security. This includes implementing strict security policies across all IT layers: network devices, operating systems, application software, and both office and clinical IT devices must have appropriate security measures to protect against potential vulnerabilities. For device-specific guidance, please contact your Siemens Healthineers Customer Services representative to obtain the Security White paper for your medical device.

Additionally, SRS serves as our fast channel for delivering third-party security patches when required. Unless otherwise stated, it is strongly recommended that you maintain an active SRS connection whenever new vulnerabilities affecting your medical devices are disclosed.

At Siemens Healthineers, we pioneer breakthroughs in healthcare. For everyone. Everywhere. Sustainably. As a leader in medical technology, we want to advance a world in which breakthroughs in healthcare create new possibilities with a minimal impact on our planet. By consistently bringing innovations to the market, we enable healthcare professionals to innovate personalized care, achieve operational excellence, and transform the system of care.

Our portfolio, spanning in vitro and in vivo diagnostics to image-guided therapy and cancer care, is crucial for clinical decision-making and treatment pathways. With the unique combination of our strengths in patient twinning[1], precision therapy, as well as digital, data, and artificial intelligence (AI), we are well positioned to take on the greatest challenges in healthcare. We will continue to build on these strengths to help overcome the world's most threatening diseases, enable efficient operations, and expand access to care.

We are a team of more than 73,000 Healthineers in over 70 countries passionately pushing the boundaries of what is possible in healthcare to help improve the lives of people around the world.

The product/features and/or service offerings (here mentioned) are not commercially available in all countries and/or for all modalities.

If the services are not marketed in countries due to regulatory or other reasons, the service offering cannot be guaranteed.

Please contact your local Siemens Healthineers organization for further details (including technical prerequisites that apply to certain service offerings).

Connection to Smart Remote Services (SRS) infrastructure is required. SRS has advanced security measures in place and is compliant with the ISO 27001:2022 Standard for Information Security.

The results of customers of Siemens Healthineers are unique to each setting. Similar outcomes for other customers cannot be guaranteed due to varying factors.

[1] *Personalization of diagnosis, therapy selection and monitoring, after care and managing health.*

**Siemens Healthineers Headquarters**
Siemens Healthineers AG
Siemensstr. 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
siemens-healthineers.com

*Published by Siemens Healthineers AG · QR700029595 · online only · 17213 1125 ·* 