Security Concept
Version 7.0

Smart Remote Services

System support.
Whenever you need us.

siemens-healthineers.com

SIEMENS Healthineers

Contents

General operational concept

Introduction 4

Purpose, scope, and usage 4

Data security as the fundamental prerequisite 4

Service for medical systems 4

Using a standard solution 4

Remote access in the Siemens Healthineers service process 5

Application support 6

Technical capabilities of Siemens Healthineers products 6

Security and privacy of data are our goals 6

syngo applications software 6

Product classes that do not use *syngo* 6

Features of online support (application support) 6

Proactive service activities 6

Technical and organizational security concept

Overview 7

Establishing the connection 7

Access control 8

Four eyes principle 8

Remote access logging 8

Pre-Connect e-mail notification 8

Privacy along the transmission route 8

Organizational measures 8

Security infrastructure of SRS 9

Authentication and authorization of our Service Engineers and optional Business Partners 9

Demilitarized zone 9

Securing the transmission route 10

Security measures for Internet-based connectivity 11

Security measures in the customer network 11

Protection against malicious attacks 11

Protected SRS servers 11

Protecting customer systems 11

Smart Remote Services

System support.

Whenever you need us.

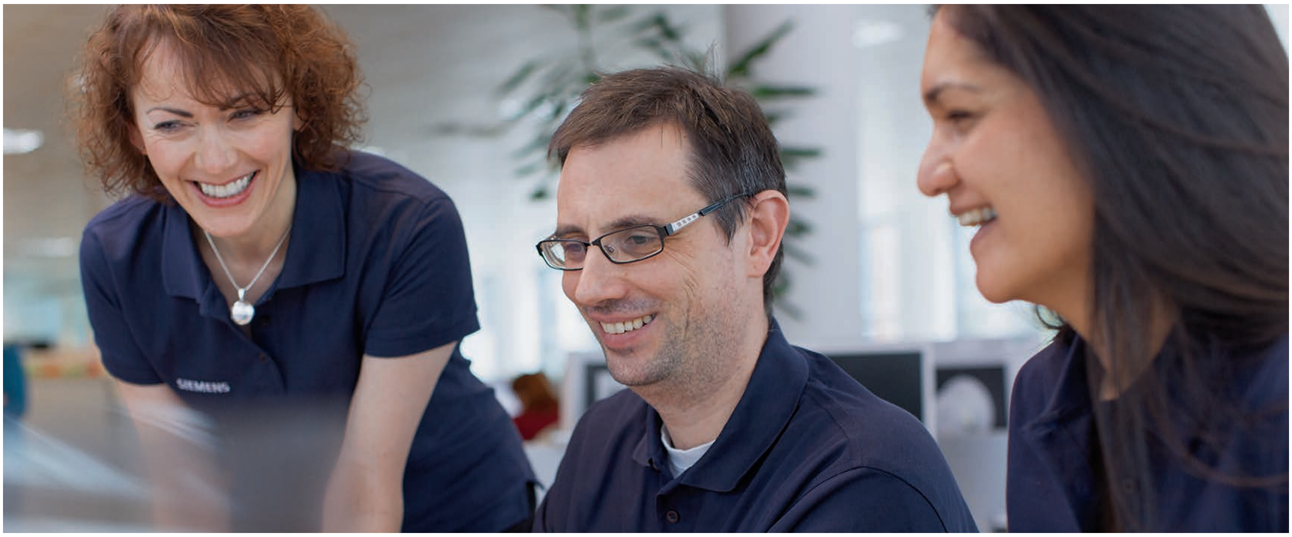
Better service. Peace of mind.
Allowing you to concentrate on what is most important – patient care.

High system availability, diagnostic confidence, optimized workflow – to meet your performance expectations at any time, we systematically focus on being proactive, based on individual contracts. On real-time remote monitoring, fast user support in case of application issues, and preventive maintenance of medical devices. On proactive analysis and anticipatory logistics when it comes to planning and performing service assignments. And on intelligent processes that continuously help us improve.

That's how we help to prevent system failures or quality inconsistencies before they even occur. To keep you on the path to success – for greater system utilization, process efficiency, and productivity. Proactively.

From the very beginning, we have assigned the highest priority to data security and access protection. Our security concept is divided into two main elements. Starting with the general operational component, we will explain the basic concept of Smart Remote Services (SRS), our service process, application support, and the technical capabilities of our products. This first element is aimed primarily at radiologists, hospital administrators, and technical managers who are interested in obtaining a basic understanding of how SRS works and what we do to secure and maintain data privacy.

The second part, the technical and organizational concept, is aimed at IT specialists and data security experts who need to know in detail what technical and organizational security measures we are taking to achieve a high level of security and privacy of patient data. This part explains how a connection to SRS is established, what our security infrastructure looks like, and what we do to prevent malicious attacks.



Introduction

Purpose, scope, and usage

This security concept describes the measures we at Siemens Healthineers undertake to protect patient data when performing SRS-based services, in both technical support and clinical application areas, on our medical devices. It is used in conjunction with all products for which SRS is offered.

Data security as the fundamental prerequisite

When visiting a physician, a patient expects that regulations regarding the protection of personal data will be upheld. This especially includes all requirements regarding security and privacy of data. In the case of security for remote service and application support, both the Healthcare Provider and Siemens Healthineers have an obligation to protect this data. The technical and organizational measures Siemens Healthineers utilizes to protect patient-related data, as well as the infrastructure used to secure SRS, are the subject of this security concept.

Service for medical devices

Given the growing complexity of modern medical devices and their maintenance and care, SRS has responded to the challenge by providing additional support to the on-site Siemens Healthineers Service Engineer for optimally servicing the system. In some cases, it is often simply more efficient and faster to first determine the causes of system problems via remote diagnosis and, where possible, correct the problem through remote repair. However, in those cases where remote repair is not possible, the information obtained via remote diagnosis can support the Siemens Healthineers Service Engineer on-site.

But that's not all. With our proactive services, we act in a preventive manner rather than reacting after a problem occurs. Our software independently monitors specific important parameters within your system. The incoming message is then analyzed and, if necessary, preventive remote repair is initiated. If values exceed or fall below the previously defined limits, the system automatically sends a message to our Customer Care Center. Patients are not affected. We may also correct the problem indicated in the message on-site and within the scope of the particular service agreement.

Whether on-site or remotely: Many problems can be detected and corrected based on technical data from the system. Access to patient data is, in most cases, unnecessary. Should access to data sets or images containing patient data become necessary in individual cases, wherever possible patient-related data is automatically and reliably removed before transmission. In the case of product classes where this is technically impossible, or where the task prohibits it (for example when accessing databases), we limit access to patient data to the extent possible, and implement specialized technical and organizational security measures.

Using a standard solution

A growing number of manufacturers offer remote services for their products in various configurations. This results in an increased number and variety of remote connections between the customer and product manufacturers, as well as increased administrative costs for the customer. However, added administrative complexity can also increase the probability of security gaps. We want to avoid this situation. We offer a solution created and agreed upon by manufacturers from the US, Europe, and Japan within the Joint NEMA/COCIR/JIRA Security and Privacy Committee (www.nema.org/medical/spc).

The solution takes into account the technical feasibility of customer organizations of differing complexities, as well as the basic legal requirements in the US (HIPAA), Europe, and Japan. This makes it much easier for our customers to adhere to the applicable legal requirements.

TÜV SÜD ISO 27001

ISO 27001

Zertifiziertes Informationssicherheits-Managementsystem

www.tuev-sued.de/ms-zert

Siemens Healthineers is 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. This has been certified by TÜV Süd in Germany according to the international standard ISO 27001.

Remote access in the Siemens Healthineers service process

Figure 1 provides a schematic overview of the entire escalation process for service calls, including the work steps normally performed on-site. After receiving the incident, the Customer Care Center uses SRS remote diagnosis to clarify the type of problem and possible cause. If possible, the error is corrected remotely. Otherwise, we send a Service Engineer or an Application Expert who corrects the problem on-site using the information obtained from the remote diagnosis (escalation stage 1).

If this is not successful, we escalate the problem to the Regional Support Center (escalation stage 2) where experts specializing in a system or system group have more in-depth technical knowledge. If the problem still cannot be corrected, it is forwarded (in escalation stage 3) to the Headquarters Support Center or alternatively to the product-specific development department, where the experts will be working on your problem.

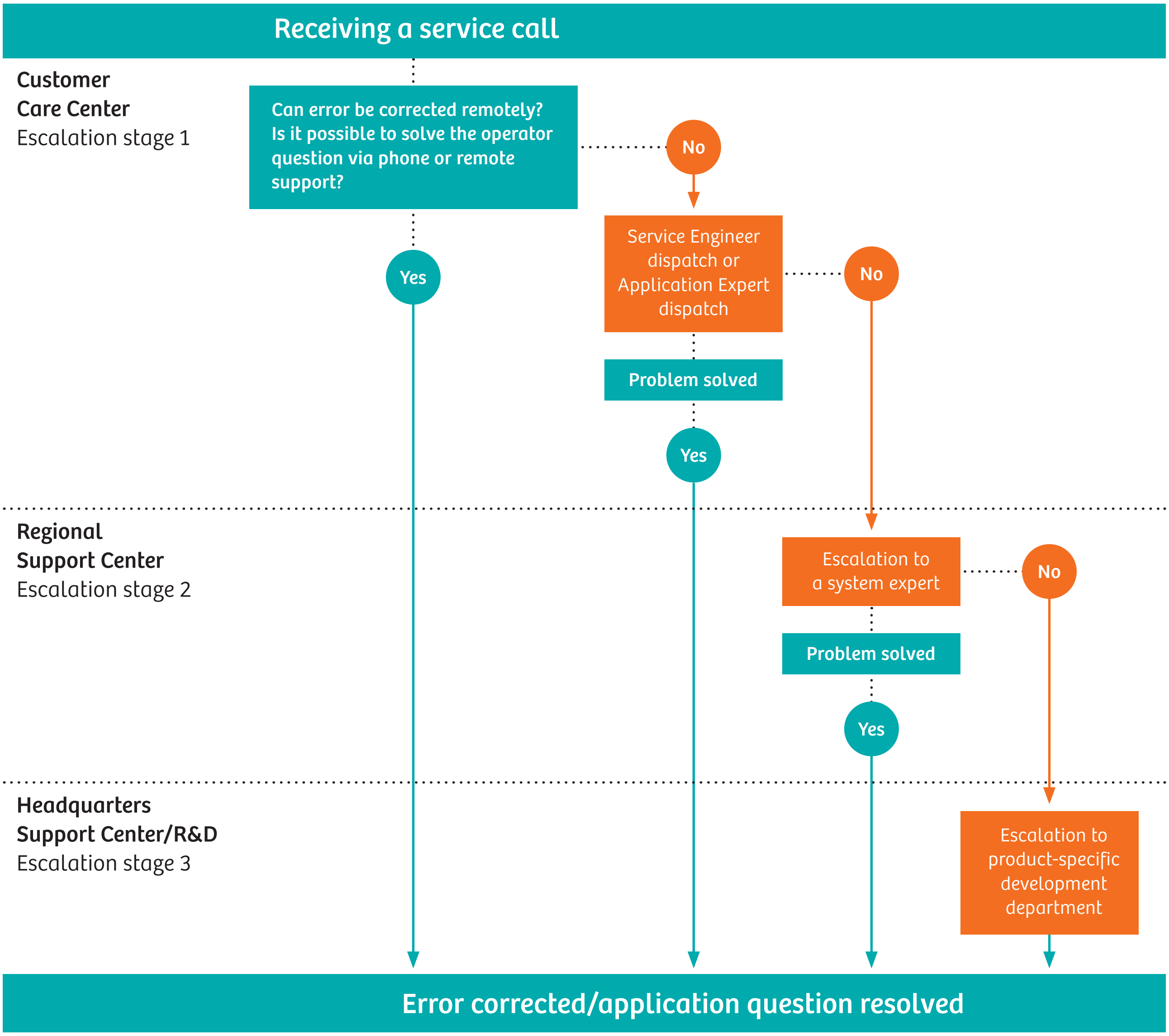

Receiving a service call
Customer Care Center
Escalation stage 1
Can error be corrected remotely? Is it possible to solve the operator question via phone or remote support?
No
Yes
Service Engineer dispatch or Application Expert dispatch
No
Problem solved
Yes
Regional Support Center
Escalation stage 2
Escalation to a system expert
No
Problem solved
Yes
Headquarters Support Center/R&D
Escalation stage 3
Escalation to product-specific development department
Error corrected/application question resolved

Fig. 1:
Escalation process for handling service calls

Application support

The multitude of applications and parameter settings in an existing system can result in user questions that require immediate answers. With SRS, we can access your system – provided that you have given us your approval. The procedure is easy: If you need help, just contact our Customer Care Center. With the help of our secure SRS infrastructure, the Service Center will connect to your system. You will receive a session ID from our specialist. This ID must be inserted into the appropriate dialog box. Only after confirmation of a pop-up, which contains a data privacy disclaimer stating that the Siemens Healthineers employee could potentially view patient data, will your screen be shared. Now our specialist will be able to guide you through the application step by step.

Technical capabilities of Siemens Healthineers products

Security and privacy of data are our goals

With all SRS activities, our goal is to access patient data only when absolutely necessary, and only to the degree technically required. By consistently implementing this standard, we have already met this goal in most of our product classes.

Together with organizational measures, the secured and reliable SRS infrastructure supports that the confidentiality and privacy of patient data is safeguarded. The infrastructure is based on linking your system and the Siemens Healthineers remote server via a VPN connection using trendsetting maintenance software. The functions available depend on the version of the software and the product. We have to differentiate between products that use our *syngo*®[1] application software and those products that do not. In particular, the latter include specific PACS workplaces.

syngo applications software

With *syngo*, we have developed a software that, in case of proactive technical service, masks out patient data just before being transferred to our Customer Care Center. In addition, the most recent *syngo* software version[2] enables you to preset the users who will be permitted to access specific data at their device. The decision when to grant our Service Engineers or your own employees access to specific data is therefore entirely yours – and you can block that access at any time.

Product classes that do not use *syngo*

Managing databases is the primary function of these products, which technically limits our ability to hide or suppress patient-related data. Depending on the problem in question, maintenance activities on databases sometimes require accessing the data therein. Here our technical and organizational measures (see chapter “Technical and organizational security concept”, starting on page 7) together with the secured and reliable SRS infrastructure (see section “Security infrastructure of SRS” on page 9) are designed to ensure that the privacy of patient data is safeguarded.

Features of online support (application support)

Remote access to your systems for online support (for example for user questions regarding operation) is also provided through remote desktop-managing tools. They provide a 1:1 display of your monitor at the Customer Care Center, as well as enabling remote control by the Application Expert. However, from a technical standpoint this is only possible if you have explicitly granted access. This authorization is required for each individual session. Throughout the entire session you are connected to your Siemens Healthineers contact via phone. In addition, in these cases you are able to track the course of the online support and, if necessary, terminate the access provided to the Customer Care Center.

Proactive service activities

One of our proactive services has your device proactively sending predefined system data to the Customer Care Center. This includes technical data like system logs, statistical data (for example number of restarts and scans), and system reliability data. These proactive services do not require access or transmission of patient-related data.

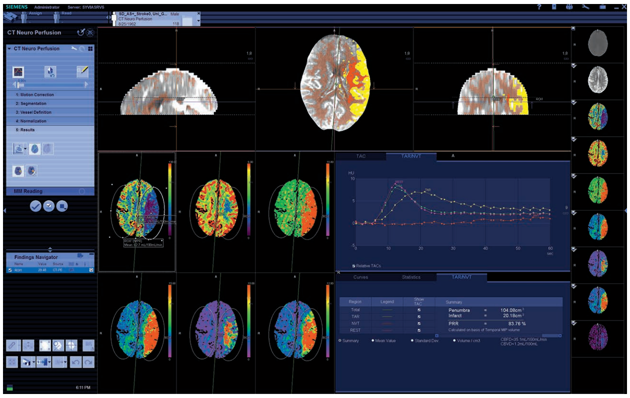


Fig. 2:
syngo user interface: Making patient health information anonymous

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

Overview

The following describes the technical and organizational measures we employ to provide a high level of data privacy and security. Refer to section "Security infrastructure of SRS" on page 9 for detailed information about the individual elements of the SRS security infrastructure.

Establishing the connection

The degree to which access is granted to a system utilizing our *syngo* application software is determined entirely by the customer. In order to establish an application support session, a session password must be generated. In other words, you share your monitor with our expert on a case-by-case basis; after solving the problem, the connection is terminated. Access to your systems without your permission is not possible. When establishing a remote service connection, you can choose between four access levels:

- **No access**
  You provide access only on a case-by-case basis to perform the task approved. Patient examinations using the system can still be conducted.

- **Limited access**
  The authorized Siemens Healthineers Service Engineer has limited access to your system. A time limit can be defined, and it is possible to conduct patient examinations.

- **Permanent limited access**
  The authorized Service Engineer has permanent limited access to your system. In other words, there is no time limit. Patient examinations can be conducted.

- **Full access**
  The authorized Service Engineer has full access to your system. Patient examinations are not possible while remote servicing is being performed. Access levels alone determine the degree and time frame for which you wish to grant access to your system. No matter what access level you choose, before transmission patient data is automatically blocked out, and you have the control necessary to grant or alter access rights at all times.

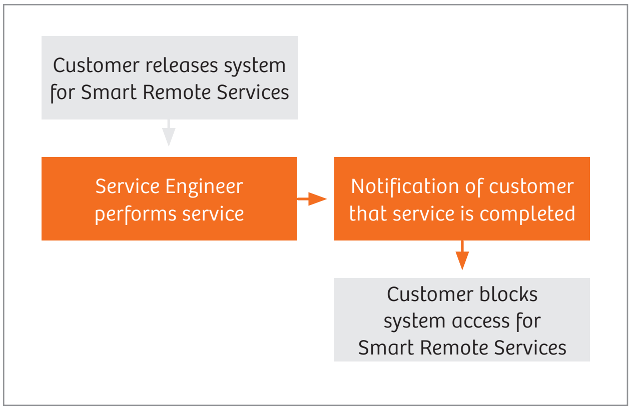

Customer releases system for Smart Remote Services
Service Engineer performs service
Notification of customer that service is completed
Customer blocks system access for Smart Remote Services

Fig. 3:
Workflow of SRS activities at "no access" level

While permanent limited access is the most frequently chosen access level, you can always opt for the no-access level. Figure 3 shows the workflow of a remote service task at this level. To provide the most secure connection possible, we have firmly established how Siemens Healthineers Service Engineers can and may access customer systems. Depending on technical capabilities, the actual device or customer-specific implementation may deviate from that which is presented here.

Access control

As a prerequisite for every service activity, you have to expressly grant access to SRS and control who is permitted access to the system. Access is only granted to identify or correct errors. Adjusting measurement parameters such as access scan protocols is technically possible only during application support and with your permission. After a fixed period of time during which no action has occurred, the SRS session at your system is ended automatically.

Four eyes principle

The customer receives a visual indication on its system screen that remote service activities are in progress. Our Service Engineers/Application Experts also speak with you on the telephone and explain the actions currently being performed. During each SRS session, the customer's employees can terminate system access by the remote service expert at any time. In this case, all service programs currently running are immediately shut down in a controlled manner, with no impact on the continued safe operation of the system being maintained.

Remote access logging

We record every direct access to your system in the SRS platform and apply a time stamp. In addition, the Service Engineer/Application Expert accessing the system is assigned a unique user identification, which is also recorded in this log. As a result, we can inform you within an appropriate period of time (three working days after receiving the request) the name of the expert who had access to data and when. We retain these log reports for at least one year.

Pre-Connect e-mail notification

Optionally we can activate upon request an e-mail service through the Siemens Healthineers remote server providing you the connection details upon each remote connection to your technical, clinical, and/or management staff. This e-mail can be complemented by a second message upon disconnection which contains the reason for the intervention and a free text to include, for example, the details of the activities performed or the successful completion of the task.

Privacy along the transmission route

We utilize modern encryption methods to protect customer data from unauthorized access during transmission. All connections via Internet are generally encrypted. For additional information, refer to section "Security infrastructure of SRS" on page 9.

Organizational measures

Our Service Engineers/Application Experts are aware of the need for patient data confidentiality, and understand the severe consequences if they do not abide by the applicable requirements. Only Service Engineers/ Application Experts who have been trained in and are committed to data privacy and security issues are authorized to perform remote services on medical systems. The Siemens Healthineers remote server contains an electronic list of these selected service employees as well as their corresponding access rights.

Security infrastructure of SRS

This chapter provides additional technical information regarding the following elements of the SRS security infrastructure: authentication and authorization of Service Engineers/Application Experts at the SRS platform, the "demilitarized zone" (DMZ) between the Siemens Healthineers intranet and the Internet, the protocols and services used for transmission, as well as any security measures in the customer network.

Authentication and authorization of our Service Engineers and optional Business Partners

The central maintenance platform (SRS portal) used by the Customer Care Center is located on the company intranet. Access to the SRS portal is strongly secured and requires a valid two-factor authentication with smart card. As fallback an authentication by SRS user ID, password and onetime PIN via SMS/e-mail is also possible. A multilevel service domain concept defines which users are permitted to access which systems. This means that Service Engineers/Application Experts can directly access only those customer systems for which they are expressly authorized. Additionally, only those SRS functions for which the engineer is explicitly authorized are released. Other systems in the customer network not maintained by Siemens Healthineers cannot be accessed via this platform. Comprehensive services for our customers sometimes require the involvement of service partners. To ensure the same level of security to these Business Partner Services, an optional extension to our security infrastructure is available. Business Partners need to authenticate themselves using two-factor authentication methods to get access to specific system(s) as authorized by Siemens Healthineers. Besides our high security standards, seamless logging of all remote service activities is provided.

Demilitarized zone

To protect both your and Siemens Healthineers' intranet from reciprocal problems and attacks, we have secured the SRS access server (which is a Linux server) in a demilitarized zone (DMZ). Connections from the Service Engineer/Application Expert to your system and vice versa are not put through directly. They terminate in the SRS access server using a reverse proxy function. This means that a connection established from the Siemens Healthineers intranet is terminated in the SRS access server.

This server then establishes the connection to your system and mirrors the communication coming from you back to the intranet. The possibility of a communication between the Siemens Healthineers intranet and your network over non-authorized protocols is thereby prevented. Mirroring occurs for predefined protocols only. This architecture is designed to provide better protection from:

- Unauthorized access from one network to the other (for example, hackers)
- Access from a third-party network (for example, the Internet)
- Transmission of viruses or similar harmful programs from one network to the other

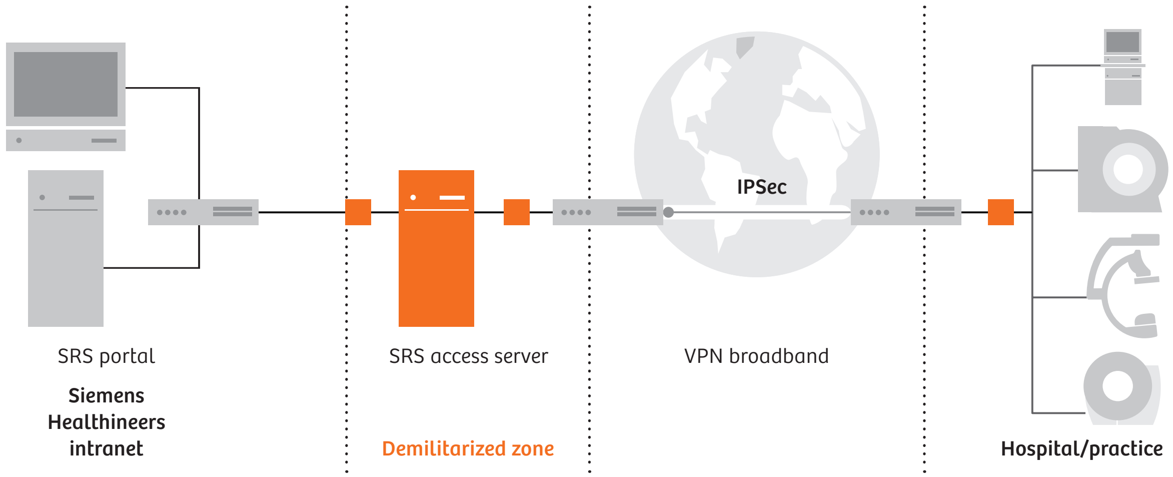


Fig. 4: Security infrastructure of SRS

Securing the transmission route

Virtual Private Network (VPN) via the Internet

We recommend establishing a secure broadband connection via the Internet, which offers you the following advantages: high level of security, very high data transfer speed, and permanent availability, as well as access to all SRS-based services like electronic provision of software updates. An IPSec-secured VPN connection between the DMZ and your network access offers a state-of-the-art technical solution currently available. For mobile systems, we also offer a secure socket layer (SSL)-based VPN between the system and the DMZ. Perhaps you already have the appropriate infrastructure. If so, our technicians are standing by to help you coordinate the parameters needed for the connection, which must then be safeguarded against unauthorized changes. If you do not have a VPN endpoint, Siemens Healthineers will provide you with the Cisco VPN endpoint required for the SRS connection.

The VPN endpoint on our side is also a Cisco router. Please note that, in rare cases, it may not be possible to establish a functioning connection with models from other manufacturers due to system compatibility issues. If you experience this situation, contact your local Siemens Healthineers representative.

Technical security measures

We offer the following technical measures to provide added security:

- **Access control lists**
  Access control lists (ACLs) on your service router provide a function similar to firewalls: they only permit data traffic to and from known IP addresses. The data traffic is directed via the reverse proxy in the DMZ to the system: see chapter “Demilitarized zone” on page 9. They also prevent access by Siemens Healthineers to other parts of your network, and access by third parties.
- **IPSec and SSL protect data against tampering and viewing by others**
  Siemens Healthineers uses the established standard IP Security (IPSec) with preshared secrets for encrypted and authenticated data transmission. Preshared secrets consist of an arbitrary string of random characters. The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange encryption key information. The use of an authentication header (AH) ensures the integrity of your data using the Hash method MD5, SHA1, SHA-256,SHA-384, or SHA-512. Encrypted secure payload (ESP) provides data confidentiality through encryption with algorithms 3DES, AES, or AES-GCM (AES-128, AES-192, AES-256, AES-GCM 128, AES-GCM 192, AES-GCM 256). Various Diffie Hellman Groups (1-768 bit, 2-1024 bit, 5-1536 bit, 14-2048 bit, 15-3072 bit, 16-4096 bit, 19-256 bit ec, 20-384 bit ec, 21-521 bit ec, 24-2048/256 bit) can be used for key-exchange security.
  For mobile devices, the SSL protocol is used. Before establishing a connection, the device must be registered with a one-time password (OTP). This OTP will be generated using the unique data of the system, and is only valid for this registration process. The SSL-connection to the VPN server can only be established if the server’s certificate was signed by a Siemens internal certification authority (CA). This ensures that only this specific device can communicate with the SRS servers. An additional hardware-based hash ensures that no unauthorized software copy can set up a connection to SRS.
- **Enhanced control capabilities through debugging (optional)**
  If you want to receive service router SNMP or Syslog messages on your router, or if you want to see the current service router configuration, contact your local Siemens Healthineers representative.

Security measures for Internet-based connectivity

Internet-based connectivity (IBC) is based on the SRS security concept using SSL VPN technology. This technology provides a secured and private communication mechanism for data and other informational transmissions between IBC and SRS by establishing a direct network tunnel with encrypted data. This supports your data protection from disclosure and virus infection introduced by unauthorized third parties during an SRS connection. SSL VPNs are quickly being recognized through-out the industry as a highly viable and economical solution for remote access.

IBC allows customer systems to be connected to the SRS portal based on an Internet connection with no additional hardware requirements and IP address dependency. This offers greater system mobility while still maintaining SRS connectivity and security.

Security measures in the customer network

Firewall
In addition to the security measures presented above, you can route all communication requiring network access through a self-administered firewall. This provides you with complete control over your communication.

System access
When you release access to your system, the Service Engineer/Application Expert must be authenticated at your system with a time-dependent password before being allowed to switch the system to service mode. Password requirements from Siemens Healthineers that correspond to international standards apply here, and they are continuously updated.

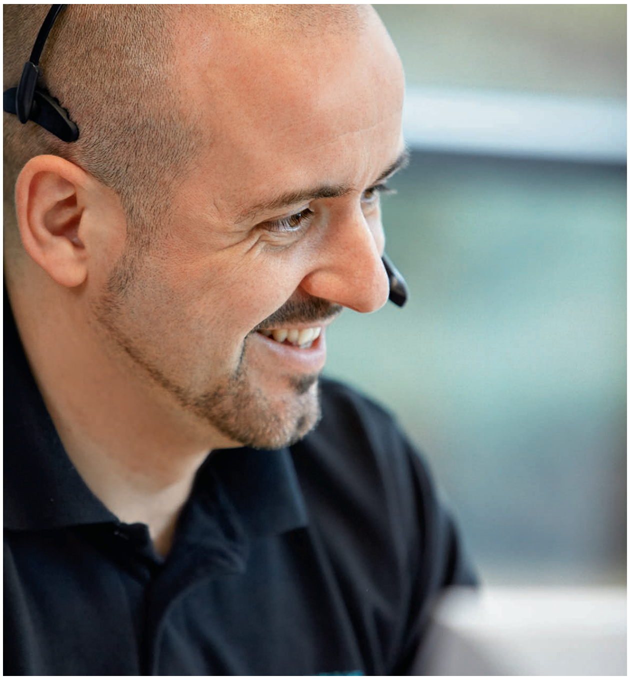
Data transmission from your systems to the remote server
For some of our proactive services, diagnostic data is sent from your system to the SRS server either automatically (based on your system configuration) or at the explicit request of the Service Engineer. In such cases, only technical data, not patient data, is transmitted.

Data transmission from the remote server to your systems
For our software updates services, Remote Software Distribution and Virus Protection, data is sent automatically from the SRS servers to your systems. This includes, for example, antivirus patterns. This type of transmission is performed only with your prior approval.

Protection against malicious attacks

Protected SRS servers

The SRS access server is a Linux server and is operated according the Siemens Information Security guidelines. The effectiveness of the protection measures is audited on a regular basis to ensure that the SRS servers are operated with state-of-the-art technology.



Protecting customer systems

With connecting your systems to our DMZ, you will not only benefit from the security measures which are given by the platform's architecture – see "Demilitarized zone" on page 9, but the connections to your systems will also be secured by state-of-the-art technology. As long as you use your Internet access for SRS purposes only, virus infections are unlikely due to our security infrastructure. However, if you use your Internet connection for other purposes, we advise you to take appropriate precautions to protect your system.

No threat from e-mail traffic
Certain types of systems send e-mails (without attachments) to the SRS access server, and they are sent in this direction only. E-mails sent from your system to the SRS access server are forwarded to the appropriate Siemens Healthineers mail server and then sent to the recipient. The Siemens Healthineers mail server scans all e-mails for viruses, and reacts in accordance with the guidelines of Siemens to ensure that there is no threat to the Siemens Healthineers intranet. Since no e-mails are sent in the other direction (to your system), infection of the system in this manner is unlikely.

No threat through contact with infected customer systems
Infection of the SRS access server through contact with an infected customer system is unlikely because there is no direct IP routing between these systems (refer to the reverse proxy function explained in section "Demilitarized zone" on page 9).

The products/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.

Siemens Healthineers Headquarters
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen, Germany
Phone: +49 9131 84-0
siemens-healthineers.com

Published by Siemens Healthcare GmbH · iPDF · 6219 0718 · ©Siemens Healthcare GmbH, 2018