

Security Concept Version 4.3



Siemens Remote Service

Capitalize on a new dimension in system support

www.siemens.com/healthcare

SIEMENS

1. General operational concept	4
1.1. Introduction	4
1.1.1. Purpose, scope and usage	4
1.1.2. Data security as the fundamental prerequisite	4
1.1.3. Service on medical systems	4
1.1.4. Using a standard solution	4
1.2. Remote access in the Siemens service process	5
1.3. Technical capabilities of Siemens products	6
1.3.1. Security and privacy of data are our goals	6
1.3.2. <i>syngo</i> applications software	6
1.3.3. Product classes that do not use <i>syngo</i>	6
1.3.4. Features of online support	6
1.3.5. Proactive service activities	6
2. Technical and organizational security concept	7
2.1. Overview	7
2.1.1. Establishing the connection	7
2.1.2. Access control	8
2.1.3. Four eyes principle	8
2.1.4. Remote access logging	8
2.1.5. Privacy along the transmission route	8
2.1.6. Organizational measures	8
2.2. Security infrastructure of Siemens Remote Service	9
2.2.1. Authentication and authorization of our service engineers	9
2.2.2. Demilitarized zone	9
2.2.3. Securing the transmission route	9
2.2.4. Security measures in the customer network	11
2.3. Protection against malicious attacks	11
2.3.1. Protected SRS access servers	11
2.3.2. Protecting customer systems	11

Siemens Remote Service

Capitalize on a new dimension in system support

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. On real-time remote monitoring and preventive maintenance of medical hardware and software. On proactive analysis and anticipatory logistics when it comes to planning and performing service assignments. And on intelligent processes that help us get better constantly. That's how we safeguard against system failures or quality inconsistencies before they even occur. To keep you on track 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. Not a single click into your system takes place without your approval. Nothing is done to your system without your knowledge.

Our security concept is divided into two main parts. Starting with a general operational part, we explain the basic concept of Siemens Remote Service, our service process, and the technical capabilities of our products. The first part is primarily aimed at radiologists, hospital administrators and technical managers who are interested in obtaining a basic understanding of how Siemens Remote Service works, and what we do to secure and maintain the privacy of data.

The second part, the technical 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 Siemens Remote Service is established, what our security infrastructure looks like, and what we do to prevent malicious attacks.

Life

Siemens Remote Service is an enabler of Life, the unique customer care solution that helps you get the most from your investment. From the moment of your purchase, Life surrounds you with an array of programs and support that enables the continuous development of your skills, productivity and technology. Allowing you to broaden your capabilities. Increase profitability. And take patient care to the next level. Get connected to Siemens Remote Service to take full advantage of Life.

1. General operational concept

1.1. Introduction

1.1.1. Purpose, scope and usage

This security concept describes the measures we at Siemens undertake to protect patient data when performing SRS-based services on our medical engineering products. It is used in conjunction with all products for which Siemens Remote Service is offered.

1.1.2. Data security as the fundamental prerequisite

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

1.1.3. Service on medical systems

Given the growing complexity of modern medical systems, SRS has responded to the challenge by providing additional support to the on-site Siemens service engineer in optimally servicing the system. Further, 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 service engineer on site.

But that's not all. With our proactive services, we act in a preventive manner, rather than reacting after an emergency occurs. Our software independently monitors certain important parameters within the customer's system. If values exceed or fall below the previously defined limits, the system automatically

sends a message to our UPTIME Service Center. The incoming message is then analyzed and, if necessary, preventive remote repair is initiated. The work with patients is not affected. Or, we will 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, where 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 (e.g., when accessing databases), we limit access to patient data to the extent necessary, and implement specialized technical and organizational security measures.

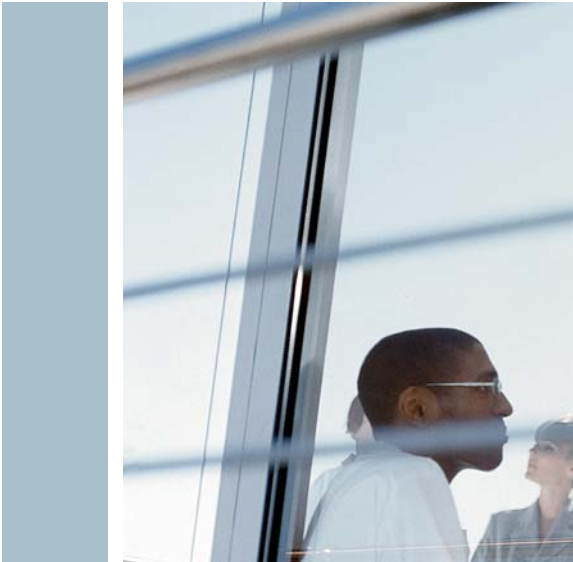
1.1.4. Using a standard solution

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 jointly created and agreed upon by manufacturers from the USA, 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 for customer organizations of differing complexities, as well as the basic legal requirements in the USA (HIPAA), Europe (directive 95/46 EG) and Japan. This makes it much easier for our customers to adhere to the applicable legal requirements.



Siemens Medical Solutions is one of the first manufacturers of medical systems worldwide to implement an internationally valid information security management system (ISMS) for the remote service of medical devices. This has been certified by TÜV Süd in Germany according to the international standard ISO 27001.



1.2. Remote access in the Siemens 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 UPTIME Service 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 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 much deeper 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 working on your problem helped to develop the system.

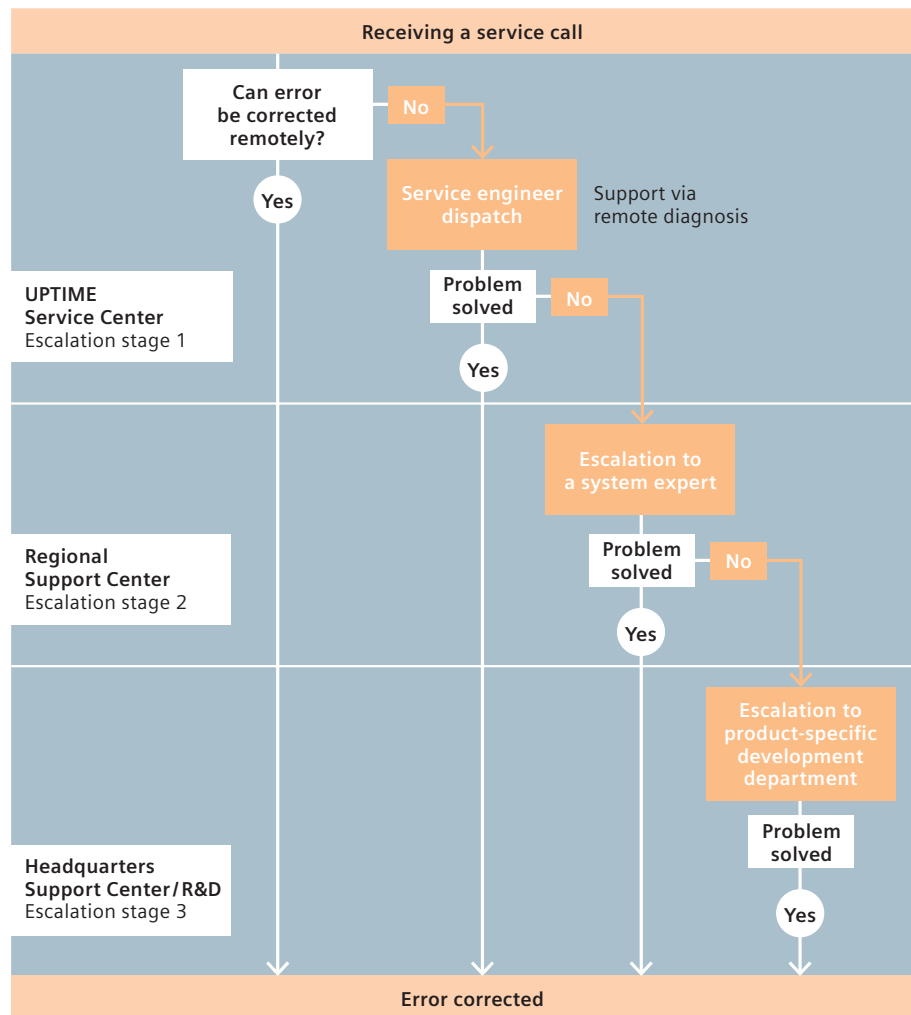


Fig. 1: Escalation process for handling service calls

1.3. Technical capabilities of Siemens products

1.3.1. Security and privacy of data are our goals

With all Siemens Remote Service 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 secure and reliable Siemens Remote Service infrastructure ensures that the confidentiality and privacy of patient data is safeguarded. The infrastructure is based on linking the customer system and Siemens remote server via a VPN connection (Internet, DSL, etc.) or telephone connection (analog or ISDN) using trendsetting maintenance software. The functions available depend on the revision level of the maintenance software and the product. We have to differentiate between products that use our *syngo*® application software, and those products that do not. The latter, in particular, include specific PACS workplaces.

1.3.2. *syngo* applications software

With *syngo*, we have developed an applications software which technically prevents the transfer of patient-related data.

Additionally, the most recent *syngo** version enables customers to preset which users are permitted access to which data at their device.

The decision when to grant our service engineers or your own employees access to which data is therefore entirely yours – and you can block that access at any time.

1.3.3. Product classes that do not use *syngo*

Products not using *syngo* include several PACS workplaces. 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, too, technical and organizational measures (see chapter 2.) along with the secure and reliable Siemens Remote Service infrastructure (see section 2.2.) ensure that the privacy of patient data is safeguarded.

1.3.4. Features of online support

Remote access to customer systems for online support (e.g., for user questions regarding operation) is additionally provided through remote desktop managing tools. They provide a 1:1 display of the customer's monitor at the UPTIME Service Center, as well as enable remote control by the service engineer. However, this is only possible from a technical standpoint if the customer has explicitly granted access. This authorization is required for each individual session. Additionally, in such cases, the customer can track the course of the online support and, if necessary, terminate the access provided to the UPTIME Service Center.

1.3.5. Proactive service activities

As part of our already available proactive services, your device proactively sends predefined system data to the UPTIME Service Center. This includes technical data such as system logs, statistical data (e.g., number of restarts, scans, etc.), or system reliability data. Patient-related data is neither accessed nor transferred in conjunction with these services.

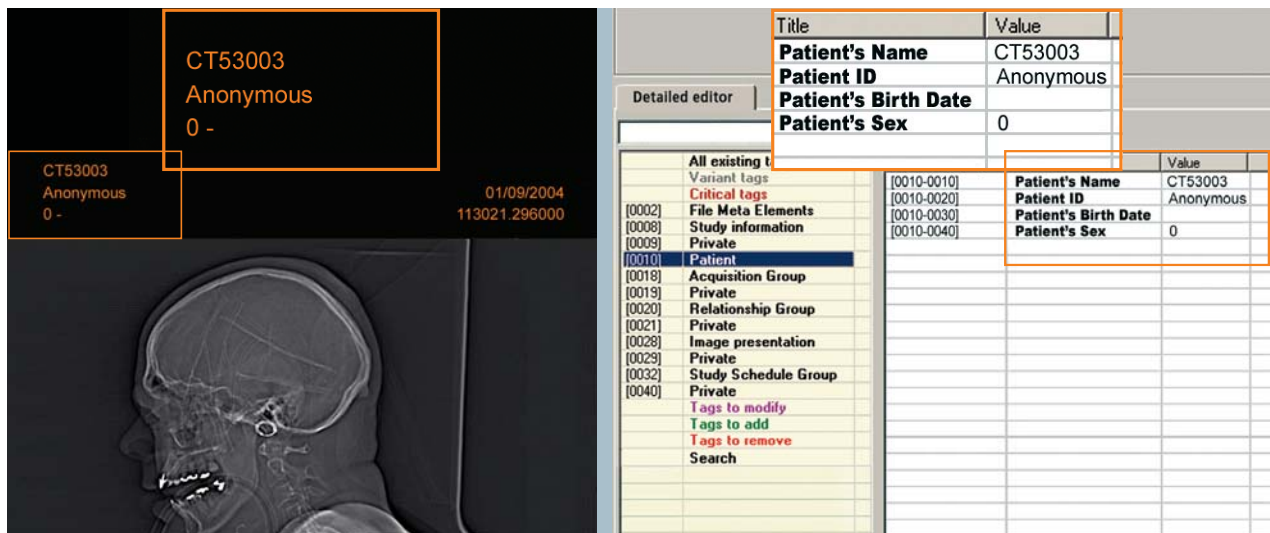
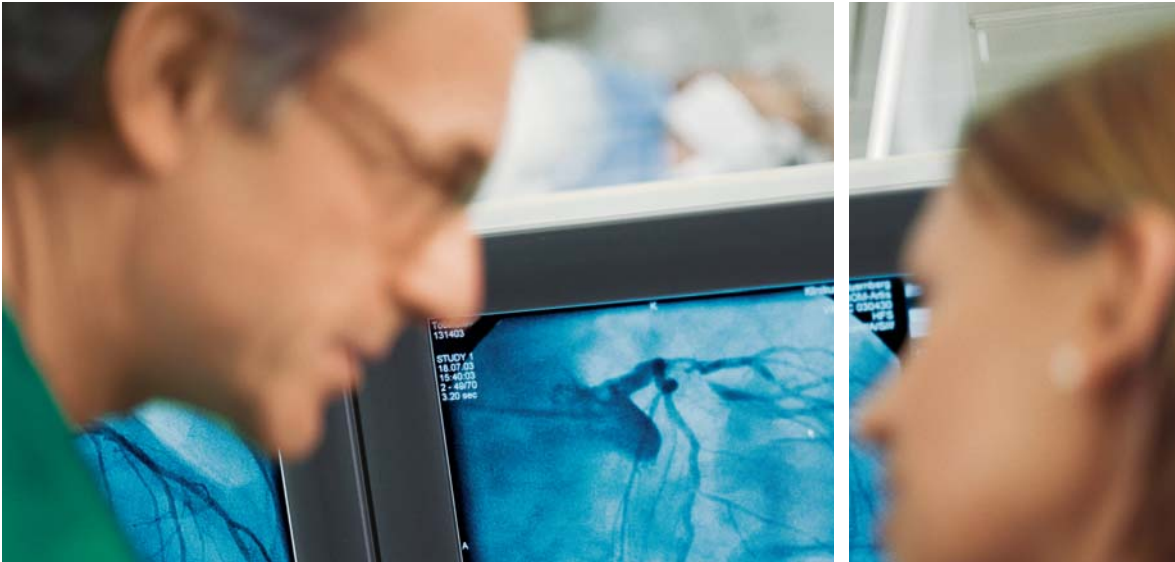


Fig. 2: *syngo* user interface: access to patient-related data is technically prevented

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

2. Technical and organizational security concept



2.1. Overview

The following describes the technical and organizational measures we use to provide the highest possible level of patient data privacy and security. Refer to section 2.2. for detailed information regarding the individual elements of the Siemens Remote Service security infrastructure.

2.1.1. Establishing the connection

The degree to which access is granted to a system utilizing our *syngo* applications software is determined entirely by the customer. When establishing a remote service connection, customers can choose between four access levels:

› No access

The customer provides access only on a case-by-case basis to perform the task approved. Patient examinations on the system can still be conducted.

› Limited access

The authorized Siemens service engineer has limited access to the customer's system. A time limit can be defined. Patient examinations are possible.

› Permanent limited access

The authorized service engineer has permanent limited access to the customer's system, i.e., with no time limit. Patient examinations are possible.

› Full access

The authorized service engineer has full access to the customer's system. Patient examinations are not possible while remote servicing is performed.

Access levels solely 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 control to grant or alter access rights at all times.

While permanent limited access is the most frequently chosen access level, you can always opt for the no access level, in which case a remote service task would work like this:

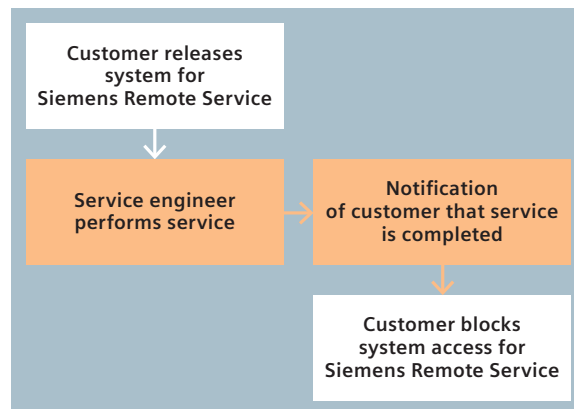


Fig. 3: Workflow of Siemens Remote Service activities at "no access" level

To provide the most secure connection possible, we have firmly established how Siemens 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.



2.1.2. Access control

As a prerequisite for every service activity, the customer has to expressly grant access to Siemens Remote Service, and control who is permitted access to the system. Access is only granted to identify or correct errors. Adjusting measurement parameters, for example, the access to scan protocols, is technically not possible. After a set period of time during which no action has occurred, the Siemens Remote Service session at the customer system is ended automatically.

2.1.3. Four eyes principle

The customer receives a visual indication that remote service activities are in progress. Additionally, our service engineer can speak with the customer on the telephone and explain the actions currently being performed. During each Siemens Remote Service session, customer staff can terminate system access by the service engineer at any time. In such cases, all service programs currently running are immediately shut down in a controlled manner, without any impact on the continued safe operation of the system to be maintained.

2.1.4. Remote access logging

We record every access to the customer system and apply a time stamp. In addition, the service engineer who accesses the system is uniquely assigned a user identification which is also recorded in this log. As a result, we can inform the customer within an appropriate period of time (three working days after receiving the request) which service engineer had access to data, when, and what actions were performed on each system. We retain these log reports for at least one year.

2.1.5. Privacy along the transmission route

We utilize the most modern encryption methods to protect customer data from unauthorized access during transmission. As an option for data transfer on public lines, we also offer router-to-router encryption. For additional information, refer to section 2.2.

2.1.6. Organizational measures

Our service engineers are aware of the need for confidentiality of patient data and understand the severe consequences of not abiding by the applicable requirements. Only service engineers 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 remote server contains an electronic list of these selected service employees, as well as their corresponding access rights.

2.2. Security infrastructure of Siemens Remote Service

This chapter provides additional technical information regarding the following elements of the Siemens Remote Service security infrastructure: authentication and authorization of service engineers at the Siemens Remote Service dial-in platform, the “demilitarized zone” (DMZ) between the Siemens intranet and the Internet or telephone line, the protocols and services used for transmission, as well as any security measures in the customer network.

2.2.1. Authentication and authorization of our service engineers

The central maintenance and dial-in platform (SRS portal) used by the UPTIME Service Center is located on the company intranet, and cannot be accessed externally. Access to the SRS portal is available only through the Siemens intranet, and requires a valid Siemens Remote Service user ID and password. Currently, passwords must be eight characters long and consist of different character types (upper and lower case letters, numerals, special characters).

A multi-level service domain concept defines which users are permitted to access which systems. This means that service engineers only access those customer systems for which they are expressly authorized. Additionally, only those Siemens Remote Service functions for which the engineer is explicitly authorized are released. Other systems in the customer network not maintained by Siemens Medical Solutions cannot be accessed via this platform.

2.2.2. Demilitarized zone

To protect the Siemens intranet and that of the customer 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 to the customer 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 intranet is terminated in the SRS access server. This server then establishes the connection to the customer’s system and mirrors the communication coming from the customer back to the intranet.

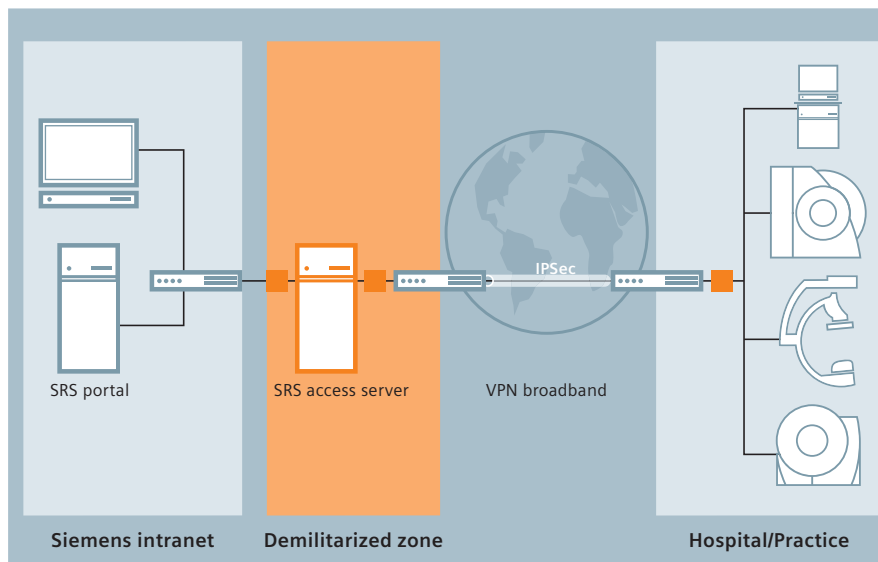


Fig. 4: Security infrastructure of Siemens Remote Service

The possibility of a communication between the Siemens intranet and the customer’s network over not explicitly authorized protocols is thereby prevented. Mirroring occurs for predefined protocols only. This architecture is designed to prevent:

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

In addition, we do not store any critical data in the DMZ, in particular, customer access data.

2.2.3. Securing the transmission route

Virtual Private Network (VPN) via the Internet

We recommend establishing a broadband, secure connection via the Internet which offers you the following advantages: highest possible level of security, best data transfer quality and availability, as well as access to all SRS-based services. Here, an IPSec-secured VPN connection between the Siemens DMZ and your network access offers the best possible technical solution currently available. Perhaps you already have the appropriate infrastructure. If so, our technicians are standing by to assist you in coordinating the parameters needed for the connection, and which then must be safeguarded against unauthorized changes. If you should not have a VPN endpoint, Siemens will provide you with a VPN endpoint needed for the Siemens Remote Service connection (Cisco PIX Firewall).

The VPN end point 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. Should you experience this situation, contact your local Siemens representative.

Virtual Private Network via dial-up connections

If a broadband VPN connection via the Internet cannot be implemented, a VPN may be established via a dial-up connection. If you already have dial-up capabilities, contact your local Siemens representative to coordinate the precise configuration.

If you do not have a dial-up infrastructure, we can provide you with a router (various Cisco products) for use with Siemens Remote Service.

Technical security measures

We offer the following technical measures to provide added security:

› Secure password transmission with CHAP

To transfer passwords, we use the Challenge Handshake Protocol (CHAP) which provides encrypted password transmission. The CHAP password, as well as passwords for Telnet and configuration mode access, are randomly generated from upper and lower case alphanumeric as well as special characters, and are ten characters long.

› More secure connection with PPP callback (optional)

When using a dial-up connection, we implement the Point-to-Point Protocol (PPP). It can be expanded with an optional callback function. This means that your service router calls back the number stored for the Siemens router once it has been authenticated. This is designed to prevent the unlikely event that an unauthorized third party manages to guess the user name, password and telephone number, and attempts to dial in using this data.

› Caller authentication with CLI (optional)

With Calling Line Identification (CLI), your service router receiving the call checks the Multiple Subscriber Number (MSN) of the router making the call. This means that the service router can be accessed only if the transmitted MSN matches the Siemens Medical Solutions telephone number stored on the service router. This function is only available for ISDN service routers.

› Access Control Lists (optional)

Access Control Lists (ACLs) on your service router provide a function similar to firewalls that only permit data traffic to and from known IP addresses. As a result, you can ensure that your service router only allows data to pass between the UPTIME Service Center and the medical system being maintained. It also prevents the access of Siemens Medical Solutions to other parts of your network or access by third parties.

› IPSec (optional) protects data against tampering and being read by others

Siemens Medical Solutions uses the established standard IP Security (IPSec) with preshared secrets for encrypted and authenticated data transmission. Preshared secrets comprise 12 characters selected randomly. The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange encryption key information. The use of an Authentication Header (AH) provides the integrity of data with the Hash method MD5 or SHA1. Encrypted Secure Payload (ESP) provides the confidentiality of data by encrypting with algorithms DES or 3DES. The Diffie-Hellmann key with a 768, 1,024, or 1,536-bit key length can be used as symmetrical session keys.

› 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 representative.

2.2.4. Security measures in the customer network

Firewall

In addition to the security measures presented above, you can route all communication for network access via a self-administered firewall, since there is no end-to-end encryption. This provides you with complete control over the communication.

System access

When you release access to your system, the service engineer has to be authenticated at your system with a time-dependent password before being able to switch the system to service mode. Here, password requirements from Siemens that correspond to international standards apply. These are continually updated.

Protocols

Depending on the capabilities of the software on your system, http or preferably https protocols, as well as service tools such as Telnet, TeraTerm Pro, PuTTY, WinVNC, pcAnywhere, Netmeeting, Citrix, Timbuktu and MS Terminal Server can be used to service your system.

Data transmission from your systems to the remote server

Diagnostic data is sent from your system to the SRS access server for some of our proactive services, 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. Depending on the capabilities of the software, the following services are used:

- › ftp (File Transfer Protocol),
 - › scp (Secure Copy)
- or System Management Tools
- › CA Unicenter
 - › HP Open View

Data transmission from the remote server to your systems

For our Software Updates service, data is sent automatically from the SRS access server to your systems. This includes, for example, anti-virus patterns and Microsoft Hotfixes. This type of transmission is performed only with your prior approval.

2.3. Protection against malicious attacks

2.3.1. Protected SRS access servers

The SRS access servers are Linux servers. Infection by worms, viruses, Trojan horses, or other attacks is therefore extremely unlikely, and has not occurred to date. Nevertheless, we ensure that the SRS access servers are protected using state-of-the-art technology.

2.3.2. Protecting customer systems

No direct threat from the Siemens remote server

A virus infection to your system from the SRS access server, or distribution of viruses from SRS access servers in the direction of your system, is unlikely due to the reverse proxy function described in section 2.2.2.

Threat due to Internet connection

Systems connected to the corresponding SRS access server via the Internet are – as with any connection via the Internet – exposed to a certain level of threat. As long as you use Internet access only for Siemens Remote Service purposes, infection by viruses is unlikely due to our security infrastructure. Should you, however, 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 customer systems send e-mails (without attachments) to the corresponding SRS access server, and in this direction only. E-mails sent from a customer system to the SRS access server are forwarded to the appropriate Siemens mail server and then sent to the recipient. The Siemens mail server scans all mails for viruses, and reacts in accordance with the guidelines of the Siemens CIO to ensure that there is no threat to the Siemens intranet. Since no e-mails are sent in the other direction (to the customer system), infection of the customer system in this manner is unlikely.

Infection of the customer system through contact with an infected customer system

Infection of the SRS access server through contact with an infected customer system is unlikely since there is no direct IP routing between these systems (refer to the reverse proxy function explanation in section 2.2.2.).

On account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this brochure are available through the Siemens sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available in the United States.

The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases.

Siemens reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Siemens sales representative for the most current information.

Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.

Please find fitting accessories:
www.siemens.com/medical-accessories

Local Contact Information

Siemens AG
Medical Solutions
UPTIME Services
Germany
UPTIME-Services@siemens.com
www.siemens.com/uptime_services

Global Siemens Headquarters

Siemens AG
Wittelsbacherplatz 2
80333 Muenchen
Germany

Global Siemens Healthcare Headquarters

Siemens AG
Healthcare Sector
Henkestr. 127
91052 Erlangen
Germany
Phone: +49 9131 84-0
www.siemens.com/healthcare

Legal Manufacturer

Siemens AG
Wittelsbacherplatz 2
DE-80333 Muenchen
Germany

www.siemens.com/healthcare