Common Remote Service Platform (cRSP) – Security Concept
White paper | Common Remote Service Platform (cRSP) – Security Concept | April 2013

Contents

Siemens AG, Sector Industry, Industry Automation, Automation Systems

This entry is from the Technical Support portal.

If you have any questions concerning this document please e-mail us using the following address:
support.automation@siemens.com

3 Introduction
3 1.1 Remote services – motivation and objectives

4 General operational concept
4 2.1 Purpose and usage of this document
4 2.2 Service and maintenance of technical equipment
4 2.3 Using a standard solution

5-9 Technical and organizational security concept
5 3.1 Overview
5 3.1.1 Establishing the connection
5 3.1.2 Access Control
5 3.1.3 Remote access logging
5 3.1.4 Privacy along the transmission route
5 3.1.5 Organizational measures

6-9 3.2 Security infrastructure of cRSP
7 3.2.1 Authentication and authorization of Siemens service personal
7 3.2.2 Demilitarized Zone (DMZ)
7-8 3.2.3 Securing the transmission route
8-9 3.2.4 Security measures in the customer network
8 3.2.4.1 Access to the customer network
8 3.2.4.2 System access
8 3.2.4.3 Protocols
8-9 3.2.4.4 Data transmission from your systems to the cRSP server
9 3.2.4.5 Data transmission from the cRSP server to your systems (optional)
9 3.2.5 Protection against malicious attacks
9 3.2.5.1 Protected cRSP server
9 3.2.5.2 Protecting customer systems
Introduction

1.1 Remote services – motivation and objectives

Remote services have become increasingly more important as companies try to offset rising costs of operations and issues with the availability of facilities and equipment increase. Remote condition monitoring and diagnosis can detect developing faults in the early stages, allowing maintenance to take place when needed, rather than at fixed intervals or when failures occur.

Due to an extensive use of integrated electronics in today’s products and the conversion from mechanical/electromechanical product features to software-based functionality, tomorrow’s product support and service portfolio will look quite different. IT-related and knowledge-intensive expert services will further displace traditional types of services.

Furthermore, networking of products and IT solutions, as well as advanced communication technology will drive demand for new effective remote service offerings. However, security and data privacy are becoming very important in providing remote services.
General operational concept

2.1 Purpose and usage of this document

The security concept described provides insight as to the measures that Siemens takes to protect data, application programs, and IT systems when performing remote services.

Siemens security concept is divided into two main sections. Starting with the general operational concept, the basic concept of Siemens Remote Support Services (SRSS), Siemens service processes, and the technical capabilities of Siemens products is explained. This section is aimed at product users, technical managers, and everyone who is interested in obtaining a basic understanding of how SRSS works. The second part, the technical and organizational security concept, is aimed at IT specialists and data security experts who need to know in detail what measures Siemens is taking to achieve a high level of data security and privacy. This section explains how a connection to Siemens cRSP is established, what Siemens security infrastructure looks like, and what Siemens does to prevent attacks.

2.2 Service and maintenance of technical equipment

Given the growing complexity of modern products and solutions, Siemens has responded to the challenge by providing additional services to support its customers.

Furthermore, 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.

Whether on site or remotely, many situations can be detected and corrected based on technical data from the system. Should access to data sets or images containing sensitive data become necessary, Siemens safeguards the compliance to data privacy guidelines and regulations. In the case of product classes where this is technically impossible, or where the task prohibits it (e.g., when accessing databases), Siemens limits access to this data to the extent necessary and implements specialized technical and organizational security measures.

Features of online support

Remote access to customer systems for online support (e.g., for user questions regarding operation) is also provided through remote desktop managing tools. This allows for a 1:1 display of the customer’s monitor at the Service Center, as well as enables remote control by the Siemens service engineer. This is only possible 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 session and, if necessary, terminate the access provided to the Service Center.

2.3 Using a standard solution

A growing number of manufacturers offer remote services for their products in various configurations. This results in an increasing number and variety of remote connections between the customer and product manufacturers, as well as increased administrative costs for the customer. Additionally, added administrative complexity can also increase the probability of security gaps. Siemens avoids this situation by building a standards-compliant and certified solution.
Technical and organizational security concept

3.1 Overview

3.1.1 Establishing the connection
As a general policy, the degree to which access is granted to a system is determined entirely by the customer.

3.1.2 Access control
As a prerequisite for every service activity, the customer has to expressly grant access to SRSS and controls who is permitted access to the system. Access is only granted to identify or correct errors. After a set period of time during which no action has occurred, the SRSS session at the customer system is automatically terminated.

3.1.3 Remote access logging
Siemens records and time stamps each time it accesses the customer system. In addition, the Siemens service engineer who accesses the system is assigned a unique user identification which is also recorded in this log. As a result, Siemens can inform the customer within an appropriate period of time, which service engineer had access to data, when, and what communication activities were performed on each system. These report logs are retained for a minimum of one year.

3.1.4 Privacy along the transmission route
Siemens utilizes the most modern encryption methods to protect customer data from unauthorized access during transmission. This is a prerequisite for any communications via the Internet. As an option for data transfer on public lines, router-to-router encryption is also offered. For additional information, refer to section 3.2.

3.1.5 Organizational measures
Siemens service engineers understand the need for data privacy and IT security. They realize 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 SRSS. As outlined in the next section, Siemens cRSP security infrastructure contains a secured list of these selected service employees, as well as their corresponding access rights.
3.2 Security infrastructure of cRSP

Within this section, more detailed technical information is provided concerning the following topics:

- Authentication and authorization of Siemens service engineers using cRSP (Ch. 3.2.1),
- The cRSP - DMZ, the “demilitarized zone” between the Siemens intranet and the internet or public lines (Ch. 3.2.2),
- Security measures for accessing the customer network (Ch. 3.2.4), and
- Protocols and services supported by cRSP (Ch. 3.2.5.3).

An architectural overview of Siemens security infrastructure is shown.
3.2.1 Authentication and authorization of Siemens service personnel
The central maintenance and dial-in platform (cRSP access portal) is located within the Siemens intranet and cannot be externally accessed. Access to the cRSP portal is only available through the Siemens intranet and requires a valid cRSP user ID and password. A strong authentication method (PKI with smart card) is utilized.

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

3.2.2 Demilitarized Zone (DMZ)
To protect customer’s and Siemens intranet from reciprocal problems and attacks, Siemens has secured the cRSP server, in a DMZ. Connections between the Siemens service engineer and the customer system are not “put through directly.” They terminate in the cRSP server using a reverse proxy function. This means that a connection established from the Siemens intranet is terminated in the cRSP access server. This server then establishes the connection to the customer’s system and mirrors the communication coming from the customer back to the Siemens intranet. The possibility of a communication between the Siemens intranet and the customer’s network over protocols that are not explicitly authorized is thereby prevented. Mirroring occurs only for predefined protocols and after successful authorization at the cRSP portal. 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)
• Fraudulent use of secure passwords, access data, etc.
• Transmission of viruses or similar harmful programs from one network to the other.

In addition, Siemens does not store any critical data in the DMZ, in particular customer access data.
Within Siemens proactive services, messages and data is frequently sent by the monitored product. Also, this communication is established only after successful authorization of the system requesting the connect. All data sent by the systems is only stored in the DMZ and is then securely transferred to the specified data server within the Siemens intranet.

3.2.3 Securing the transmission route
Virtual Private Network (VPN) via the Internet
Siemens recommends 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
• Access to all cRSP-based services.

Based on current technology, this is implemented via a VPN secured with Internet Protocol Security (IPSec) between the Siemens DMZ and your network portal.

Siemens can provide you with the hardware necessary to use the SRSS (e.g., VPN router). The VPN endpoint on Siemens side is a Cisco router.

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

If you do not have a dial-up infrastructure, Siemens can provide you with a router (e.g., Cisco product) for use with SRSS.

Technical security measures of the transmission route
Siemens offers the following technical measures to provide added security:
• Secure password transmission with Challenge Handshake Protocol (CHAP)
To transfer passwords, Siemens uses CHAP which provides encrypted password transmission. The ten-character CHAP passwords, as well as passwords for Telnet and configuration mode access, are randomly generated from uppercase and lowercase alphanumeric as well as special characters.

• More secure connection with Point-to-Point Protocol (PPP) callback (optional)
When using a dial-up connection, Siemens implements the PPP that can be expanded with an optional callback function. This means that your service router will call back the number stored for the Siemens router once the number has been authenticated. This is designed to prevent the unlikely event of an unauthorized third party managing to guess the username, password and telephone number and then attempting to dial in using this data.
• **Caller authentication with Calling Line Identification (CLI) (optional)**
  With CLI, your service router receiving the call verifies the Multiple Subscriber Number (MSN) of the router making the call. This means that the service router can only be accessed if the transmitted MSN matches the telephone number of the cRSP router stored in the service router. This function is only available for ISDN service routers.

• **IPSec protects data against tampering and being read by others (optional)**
  Siemens uses the established standard IPSec with preshared secrets for encrypted and authenticated data transmission. Preshared secrets are comprised of 12 randomly selected characters. 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, 1024, or 1536-bit key length can be used as symmetrical session keys.

• **Enhanced control capabilities through debugging (optional)**
  If you would like to receive Simple Network Management Protocol (SNMP) or Syslog service messages on your router, or if you would like to see the current service router configuration, please contact your local Siemens representative.

3.2.4 Security measures in the customer network

3.2.4.1 Access to the customer network

Due to the security issues involved, external access to the customer network requires specific attention and measures. The key security features depend on the specific concept and configuration of the Service router (Customer Access Gateway) chosen.

• **Access enabled by customer**
  A general security measure can be used to block any external access when not explicitly authorized or initiated by a component within the customer network. This security measure is, of course, supported by cRSP, but has some considerable limitations, especially if onsite personal are not available. However, when the chosen cRSP supports various mechanisms like single log-in passwords or defined service time-slots, all security measures like authentication, authorization, and logging as described in Ch. 3.2.1 are available without any limitations.

• **Customer supplied access**
  In most cases, if you already have an existing remote access solution in place, this system can be configured to work securely with SRSS infrastructure. To clarify the required configuration and measures, please contact your local Siemens service representative.

• **Service VPN-router / Siemens supplied access**
  Due to cost, performance, and security benefits, Siemens specified VPN-router solution with broadband internet access (e.g., DSL) is preferred. This solution can support high-performance remote service solutions affordably and enables future value-added services.

Specific customer demands for additional security measures of certain applications, network segments or requested onsite firewall features can be provided based on this solution.

3.2.4.2 System access

When remote access to your system is released (either manually by user/administrator or automatically based on system configuration), the Siemens service engineer has to be authenticated by the system before being able to switch the system to service mode.

3.2.4.3 Protocols

Depending on the capabilities of the software on your system,

• the protocols http or preferably https as well as

• the service tools/protocols: Telnet, PuTTY, NetOp, pcAnywhere, WinVNC, TeraTermPro, Timbuktu, Netmeeting, Tarantella, Citrix / MS Terminal Server, SNMP, and X.11 can be used to service your system.

3.2.4.4 Data transmission from your systems to the cRSP server

Diagnostic data is sent from your system to the cRSP server for some of Siemens proactive services, either automatically (based on your system configuration), or at the explicit request of the Siemens service engineer. In such cases, only technical data are transmitted.
Depending on the capabilities of the software, the following services are used:

- **ftp / ftps** (File Transfer Protocol, dto. secure ftp)
- **scp** (Secure Copy)

### 3.2.4.5 Data transmission from the cRSP server to your systems (optional)

Depending on your demands and product capabilities, a Software Update service is available based on cRSP. Here data is sent automatically from the cRSP 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.

### 3.2.5 Protection against malicious attacks

#### 3.2.5.1 Protected cRSP server

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

#### 3.2.5.2 Protecting customer systems

- **No direct threat from the cRSP server**

  A virus infection to your system from the cRSP servers, or distribution of viruses 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 cRSP 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 SRSS purposes, infection by viruses is unlikely due to Siemens security infrastructure. However, should you use your Internet connection for other purposes, Siemens advises you to take appropriate precautions to protect your system.

- **No threat from email traffic**

  Certain types of customer systems send emails (without attachments) to the corresponding cRSP server and in this direction only. Emails sent from a customer system to the cRSP server are forwarded to the appropriate Siemens mail server, and then sent to the recipient. The Siemens mail server scans all email messages for viruses and reacts in accordance with Siemens guidelines to ensure that there is no threat to the Siemens intranet. Since emails are not sent in the other direction (to the customer system), infection of the customer system in this manner is unlikely.

- **Infection of a serviced system through contact with an infected customer system**

  Infection of the cRSP server through contact with an infected customer system is unlikely since there is no direct IP routing between these systems (refer to reverse proxy function explanation in section 3.2.3).