System support. Whenever you need it.

Introduction
Siemens offers remote-based services using a secure remote connection to a customer system. Due to proactive and faster service we ensure higher system availability.

From the very beginning, we have assigned the highest priority to data security and access protection.
Our security concept is divided into two parts. The first part is about the general operational component and will explain the basic concept of Siemens Remote Service (SRS), our service process and application support as well as the technical capabilities of our products. It is aimed primarily at IT 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. In the second part, we talk about the technical and organizational concept. Here, IT specialists and data security experts learn in detail about the technical and organizational security measures we take to achieve a high level of security and privacy of system data. We will also explain how a connection is established via our SRS platform, what our security infrastructure looks like and what we do to prevent malicious attacks. This document also gives an overview of the IT-security-related measures SRS offers.

The SRS advantage
Remote service provides additional support to optimally service your fire safety, security and building automation systems in the face of growing complexity.

The advantages of SRS include:
- Remote monitoring to proactively detect and correct interruptions in order to minimize system downtimes
- Faster and more efficient determination of the causes of system problems
- Fast, intelligent correction of problems through remote intervention
- Service engineers arrive on-site already well informed and optimally equipped
- Fast user support in case of application issues

Data security comes first
We are committed to a long-term partnership based on trust – and that is why data security is of very high importance to us. When installing SRS, we perform a detailed situation analysis taking into account international and national regulations as well as the technical infrastructure before complementing our service offer with remote connectivity. Our service team carefully evaluates each customer's need for information security and system safety on an individual basis.

Here is a selection of typical customer requirements Siemens answers:
- **Data privacy:** SRS has and will always approach customers' data privacy with the utmost respect. All potential issues and safety measures are clarified before any remote connection is established.
- **Supervised access:** Our customers have the possibility to observe and end any remote service access at their convenience.
- **Traceable Audit Trail:** The details of each individual session are easily retrievable upon customers' or legislators' request.
- **Selective access – individual administration of user rights and data access:** Customers can define access rights to their systems and data.

Information security through multi-stage security concept.

Customer-controlled access
The main prerequisite for every remote service activity is customer authorization. Only our customers can define which service engineer is allowed access to which parts of which system in a legally-binding contract.

Our customers also define when and to what extent a service engineer is allowed access to their system.

Some of the more common access models chosen by our customers are:

- **Access upon request:** Our service engineer can access a customer's system on an individual request basis only. For example, a service engineer might request time-limited access to eliminate a specific problem. This access is not permanent. Such a setup may be contractually agreed and may even be included into the customer's firewall settings.
- **Supervised access:** The customer can watch the service engineer working on the system in real time via remote desktop sharing. The spectrum of services where this option is required and the technical means to restrict access to this level are mutually agreed.
- **Full access:** An expressly authorized service engineer has the customer's permission to connect to the system at any time. Each system access is automatically logged for customer review. Customers commonly choose to grant full access when proactive preventive maintenance and highest possible system availability are their key considerations.
- **Outbound communication:** The customer's system is permitted to send information in real time or at agreed intervals to the Siemens Service Center via the SRS platform. This allows gathering statistical data for system optimization, proactive incident management and preventive maintenance services. Siemens, in close collaboration with the customer, makes sure that only the agreed type of data from the agreed systems is transmitted.

Personnel selection
Only employees who have been trained in data protection and IT security are permitted to work in our SRS unit. We have strict selection criteria and our service engineers have to participate in ongoing training and validation processes.

Authentication and authorization
Every single time a service engineer logs onto our SRS platform, their user ID and password are verified with their corresponding access rights.

The customer-defined access models are mirrored within our SRS platform and converted into authorized IT system access levels. Those access levels are then match-ed with the service engineer's verified identity. Using this mechanism assures that service engineers can only access those parts of customer systems for which they are expressly authorized

Traceable audit trail
Siemens maintains constant readiness to inform customers, which service engineer had access to which data, when and what communication activities were performed on each system. This audit trail is enabled by the following measures:

- Every single access to a customer system is recorded. Entry and exit time stamps
  as well as the engineer's identity are applied.
- Report logs are kept on file for at least twelve months, and holding may be extended upon customer request.

Customer requests for the inclusion of supplementary information in the audit trail can be taken into account as far as they are technically possible.

Verified partner access only
Some services might need the involvement of external service and engineering partners.

To ensure the same reliable level of security is maintained in such cases, our SRS platform features a partner access mechanism. Only after successful completion
of a very thorough and strictly enforced authentication process, verified business partners are granted access to a specifically-defined area of a customer system via the SRS platform.

All verified partner services are recorded with exactly the same precision as the system accesses by our service engineers.

Protection of data transmission
Our SRS platform utilizes state-of-the-art encryption methods to protect customer data from unauthorized access during transmission. A particular emphasis is placed upon integrated encryption as a prerequisite for any communication via
the Internet.

Should a customer request elevated security in response to specific threats, our SRS platform can also provide hardware-based router-to-router encryption solutions for data transfer.

Secure network architecture
The central SRS platform is located within Siemens' own network infrastructure and is protected from unauthorized access from the outside.

Within a demilitarized zone (DMZ), a SRS access server acts like a secure gatekeeper between the Internet and the Siemens network, where the customer data is stored. It establishes a safe connection between the customer system and the service engineer's system.

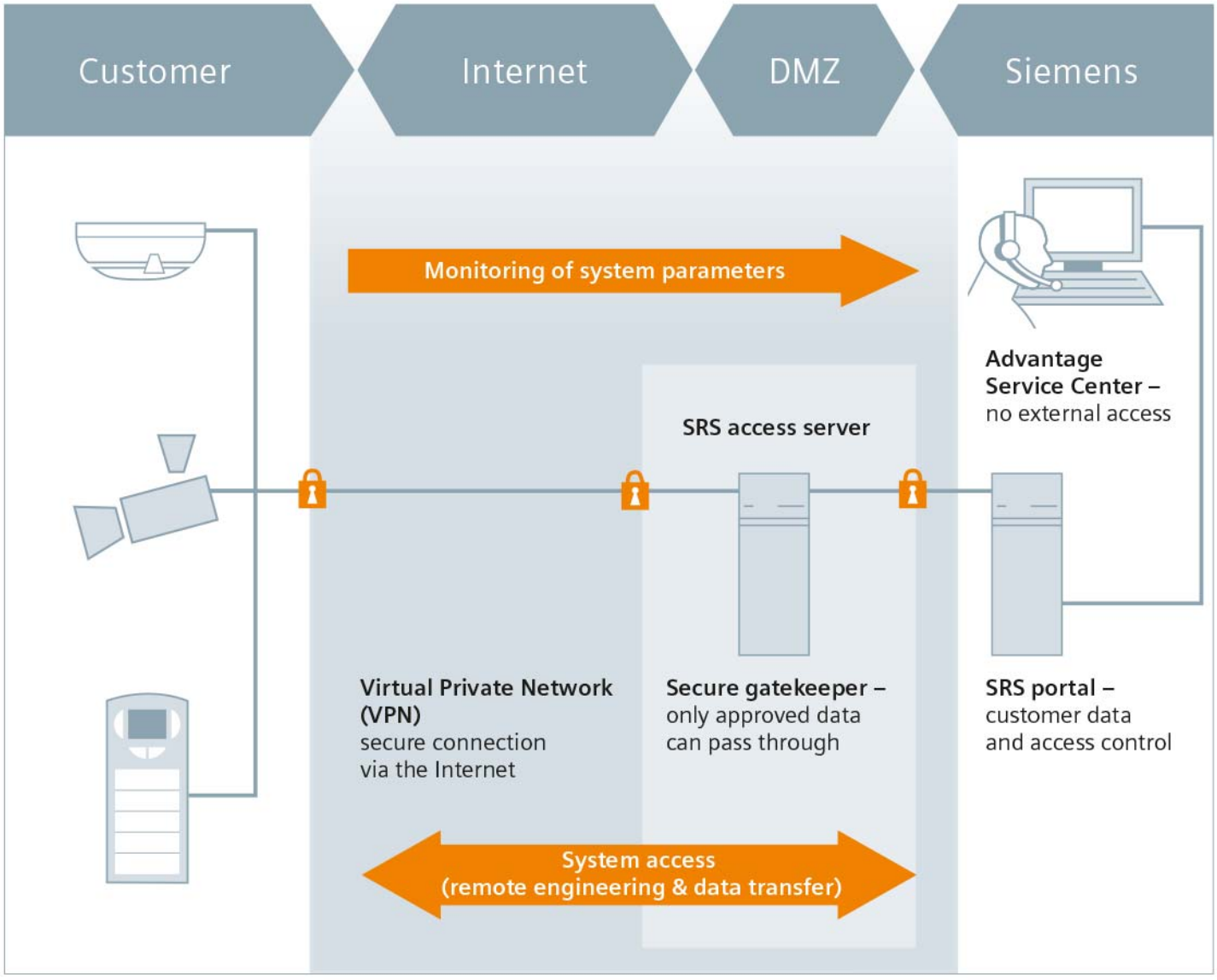
A DMZ with Proxy server technology is a proven network architecture which ensures that only data that has been previously requested by a Siemens-authenticated remote service process is allowed to pass into the Siemens network. This prevents unauthorized or fraudulent access to customer data via the Internet.

Data management
We classify customer data highly confidential and grant access only on a need-to-know basis. The enforcement of this principle is supported by policy-based access control mechanisms that are mapped within an infrastructure and tool landscape that were specially developed for this purpose.

The measures implemented for data management depend on a customer's individual requirements for data protection, the data type and the dictates of relevant legislation. For matters such as individual solutions for data retention, back-up, ownership rights and disposal, we can provide comprehensive consultation.

Platform availability
The availability of our SRS platform is ensured by three fully redundant data centers located in Germany, Singapore and the USA. The capacity of each center is planned in a way that unless two data centers are unexpectedly taken completely offline, the SRS platform will be totally unaffected if a disturbance should occur.

The integration of supplementary disaster recovery (DR) and business continuity management (BCM) plans assure the lowest possible downtime even in the unlikely event of simultaneous catastrophes affecting our data centers.



Audit and certification.

ISO 27001
Siemens was one of the first organizations worldwide to have an internationally accepted information security management system (ISMS) for remote service, certified by the ISO/IEC 27001:2005 standard. Our SRS platform retains ongoing certification by TÜV Süd in Germany and is listed in the International Register of ISMS Certificates found in www.iso27001certificates.com

Siemens CERT auditing
The Siemens Cyber Emergency Readiness Team (CERT) is an internal, independent and trustworthy partner who develops preventive security measures and assesses information security of IT infrastructure. Our SRS platform is audited on a regular basis to ensure valid protection and continuous improvement.

Siemens-provided network hardware
Whenever the use of Siemens-provided hardware for router-to-router encryption proves most adequate, you can rely on industry standard technology in terms of data protection. Industry standard routers with certified IPSec, VPN and HTTPS Proxy capabilities are used exclusively.

Contacts and information
For further information on our SRS platform and remote service portfolio, please contact your local Siemens sales representative.

We will be happy to help you configure your equipment to establish a secure SRS connection.