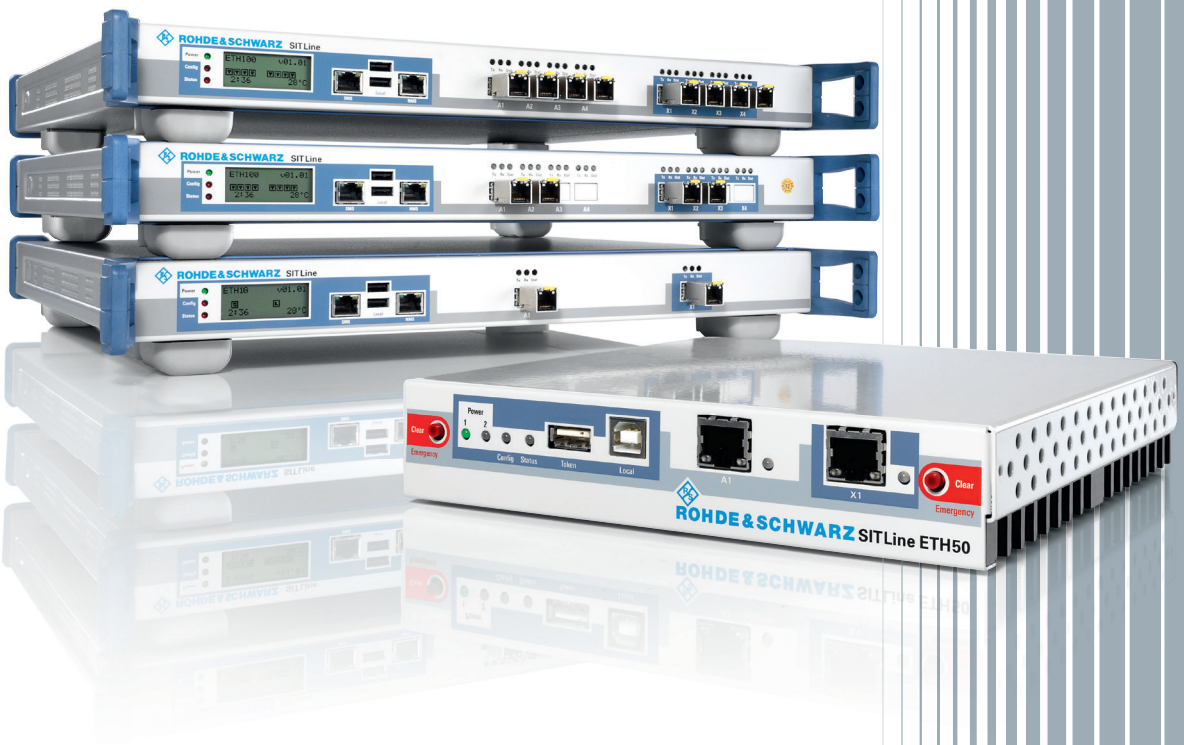
# R&S®SITLine ETH
# Ethernet Encryptor
## Secure data transmission via landline, radio relay and satellite links




ROHDE&SCHWARZ

Secure Communications

Product Brochure | 06.00

# R&S®SITLine ETH Ethernet Encryptor

## At a glance

The R&S®SITLine ETH is a family of devices for Ethernet encryption and for creating secure "layer 2 virtual private networks" (L2 VPN). The R&S®SITLine ETH protects companies and organizations against espionage and manipulation of data that is transported via Ethernet over landline, radio relay or satellite links. The devices in this product family are approved by the German Federal Office for Information Security (BSI) and can be used in a flexible manner in many stationary and mobile applications.

The R&S®SITLine ETH performs encryption on an Ethernet basis – in the ISO/OSI model's data link layer (layer 2) – which makes it ideal for protecting applications where throughput and time are critical. Communications links over public and private networks can be protected. The R&S®SITLine ETH makes it possible to accommodate security requirements in a way that is fully independent of the existing or planned network structure.

Due to the significant cost savings they enable, Ethernet VPNs have become established in recent years as a true alternative to "managed IP connections" (IP VPN) when it comes to site networking. The R&S®SITLine ETH provides different models and performance classes. The R&S®SITLine ETH family of devices is a flexible solution for meeting changing requirements and offers a high level of investment protection.

### Key facts

- Ethernet encryptors in performance classes from 25 Mbit/s to 1 Gbit/s
- Advanced cryptographic methods and standards (elliptic curves, AES, X.509)
- Flexible deployment in advanced transmission networks
  - Encryption based on port, VLAN or group assignment (multipoint)
  - Maximum bandwidth efficiency, avoidance of overhead
  - Convenient online management capabilities for device configuration and for security and networks settings
- Very compact design (1 HU for single-port and multiport devices), very low energy consumption, low total cost of ownership (TCO)
- Approved by the German Federal Office for Information Security (BSI) up to the German restricted ("VS-NfD") and NATO restricted classification levels

R&S®SITLine ETH100.


R&S®SITLine ETH50.

# R&S®SITLine ETH Ethernet Encryptor

# Benefits and key features

### Safeguarding civil, official and military communications

- Confidential communications between sites and within a single site (L2 VPN)
- Safeguarding radio relay and satellite links (SatCom)
- Securing rail control and monitoring networks
- Secure interconnection of data centers and storage area networks (SAN)

▷ page 4

### Low system costs

- Minimal investment for installation and configuration
- Low space and energy costs
- Lower transmission costs than with managed IP
- Low maintenance and service requirements
- Bandwidth efficiency through group encryption (multipoint approach)
- No need for central or internal key servers
- Better transmission performance than with IPsec

▷ page 6

### Professional, certified security

- Securing point-to-point Ethernet lines and Ethernet VLANs
- Innovative group encryption for multicast topologies (ELANs)
- Secure authentication
- Automatic operation of encrypted links
- Flexible encryption hardware
- Manipulation-proof devices

▷ page 8

### Central security management over the network

- Online, convenient and secure
- Virtualization capability and high availability
- Clearly defined roles
- Central point for log files and audits

▷ page 10

### SNMP-based network management

- Support of SNMP v1, v2c and v3
- Extensive monitoring and diagnostic capabilities
- Network management through service providers

▷ page 12

R&S®SITLine ETH1G.

# Safeguarding civil, official and military communications

Originally used only in local area networks (LANs), today Ethernet is a reliable and universal transmission technology for wide area networks (WANs). This makes site interconnection via global networks just as easy as in-house cabling. Unfortunately, this also means a greater susceptibility to attacks from public networks: Eavesdropping, manipulation and disruption are as easy as in any computer network. The BSI-approved R&S®SITLine ETH safeguards communications through encryption on the Ethernet layer.

### Confidential communications between sites and within individual sites (L2 VPN)

Video conferences, VoIP calls, database queries – organizations must safeguard the confidentiality of their internal communications links in order to prevent espionage and undesired manipulation of data. This is especially important when parts of the communications links are established over long distances, as is the case for organizations with geographically dispersed sites, and for networking within a large campus. In such cases, the R&S®SITLine ETH's flexibility and variability are highly beneficial because all devices are interoperable. Depending on the site to be integrated, the optimal device can be selected based on criteria such as the required transmission capacity, the number of connections that are needed and the environmental characteristics. From the encryption of individual lines or applications to the safeguarding of complex structures, interoperability allows the security solution to scale with the network. This provides long-term investment protection for users.

The R&S®SITLine ETH safeguards public and private connections over landline, radio relay and satellite links.

## Safeguarding radio relay and satellite links (SatCom)

Precise, timely information is necessary for strategic command and control of forces in the field. Situation reports with image and video material often need to be transmitted over long distances. Radio relay and SatCom links are used to connect field units to a central station (e.g. control center, headquarters), which in many cases might even be on a different continent. In order to ensure information superiority, the data must be protected against manipulation, and it must not fall into the hands of third parties – reason enough to use strong encryption. However, the encryption must not place any additional load on the already very narrow bandwidth of the radio relay or SatCom link.

Especially scenarios with narrow bandwidths make the R&S®SITLine ETH design advantages clear: The R&S®SITLine ETH requires significantly less protocol information (overhead) to provide encrypted transmission than is required for classic IP encryption. Despite throughput limitations, the information is protected against eavesdropping and manipulation during the entire radio relay transmission or during satellite hops.

For more information on securing satellite networks, see application brochure PD 3606.8189.92 and www.rohde-schwarz.com

## Securing rail control and monitoring networks

Public transport networks are managed in central control centers, which receive information from transport hubs (e.g. railway stations, signal boxes) that may be unattended. Automation enables tighter scheduling of trains and greater punctuality. However, unattended transport hubs require a higher level of protection against manipulation, especially when they are connected to the control center over public networks. In such cases, cryptographic functions can safeguard the integrity of the transmitted data. Special R&S®SITLine ETH models are available for use in more challenging environments (e.g. extended temperature range, installation with top-hat rail/DIN rail, external emergency erasure).

For more information on securing rail control networks, see application brochure PD 3606.6505.92 and www.rohde-schwarz.com

## Secure interconnection of data centers and storage area networks (SAN)

Central corporate data centers often feature a redundant design. These centers must be securely interconnected via high-performance lines. The state-of-the-art transmission technology for this application is Ethernet services with a transmission capacity of at least 100 Mbit/s, and typically several Gbit/s. The R&S®SITLine ETH can be scaled for connections in the Mbit/s and Gbit/s ranges. In addition, the multiport version of R&S®SITLine ETH can be used to efficiently safeguard dedicated Ethernet lines that are connected in parallel.

The R&S®SITLine ETH protects rail control and monitoring networks.

# Low system costs

Compared with other encryption solutions, Ethernet carrier services protected by the R&S®SITLine ETH make it possible to reduce operating costs significantly while maintaining a high level of security.

## Minimal investment for installation and configuration

The R&S®SITLine ETH integrates into a network in a fully transparent manner. Except for the security parameters, no other network-specific configuration steps are required. As a plug & play technology, Ethernet requires almost no configuration effort to get started. That saves installation time and expense.

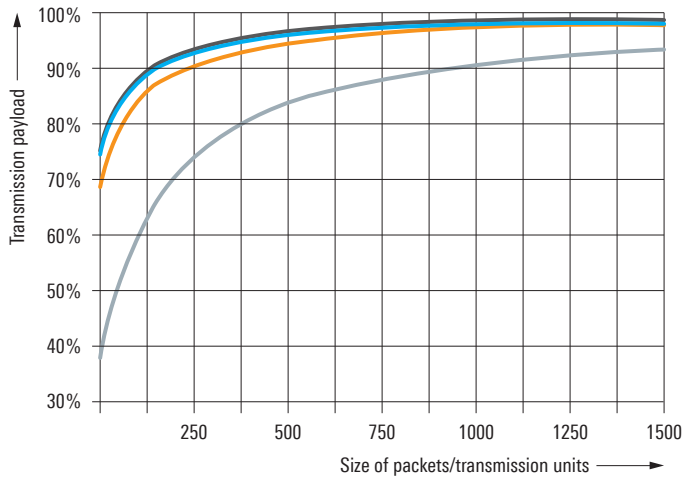
## Low space and energy costs

The compact design, low module height and different device classes make it possible to save both installation space and energy. The multiport device provides the functionality of up to four devices while consuming only the space and power of a single device. The option of safeguarding up to four physical lines with a single device is unique worldwide.

## Lower transmissions costs than with managed IP

The significantly lower overhead for Ethernet encryption improves the net-to-gross transport ratio. Depending on the traffic profile and the selected security functions, the net payload rate only drops by 0% to 13% when using Ethernet encryption. For the sake of comparison: An IPsec-secured L3 VPN reduces the net payload rate by as much as 60%.

### Net payload rate (capacity utilization)




For a medium-sized packet of 250 byte, the R&S®SITLine ETH offers a significantly higher net payload rate than IPsec encryption:
R&S®SITLine ETH: > 90% (L2 encryption)
IPsec encryption: 75%

## Low maintenance and service requirements

Ethernet operates independently of the logical IP network structures. This eliminates the need for adaptations when integrating new applications, changing providers or migrating of higher-level network protocols (e.g. from IPv4 to IPv6). Experience has shown that, due to the long update and upgrade cycles, the service costs for layer 2 systems are significantly lower than for other solutions.

## Bandwidth efficiency through group encryption (multipoint approach)

Classic encryption systems (such as IPsec) establish multiple dedicated connections between the encryption devices, which are each secured using a separate key. Data that is meant for more than just one site (e.g. video conference data) must be duplicated and then sent to the different sites via individual connections.

For such applications, the R&S®SITLine ETH has been equipped with innovative group encryption functionality. This approach employs the multicast capabilities offered by advanced carrier networks without compromising the level of security for the transmitted data. Regardless of the number of recipients, the data is encrypted and transmitted only once; the carrier or network distributes the data.

## No need for central or internal key servers

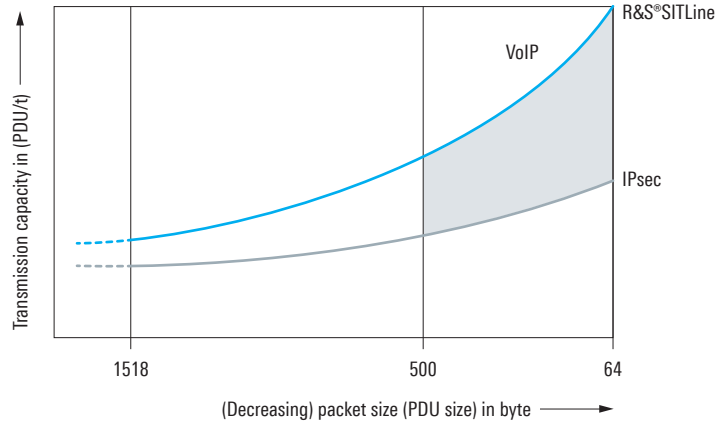
The R&S®SITLine ETH devices employ fully automatic processes to negotiate the session keys required for operation and to distribute them securely to the authorized communications partners. No dedicated encryption key servers are required. Failure of one device has no influence on the operation of the rest of the network, because partner devices find each other automatically and regularly re-establish secure links.

R&S®SITScope, the central security management system for R&S®SITLine ETH (see page 10), is primarily required for installation and monitoring. Once operational, the R&S®SITLine ETH devices organize the encryption on their own without any additional components.

## Better transmission performance than with IPsec

The R&S®SITLine ETH's reduced overhead has a positive effect on transmission quality. This becomes especially clear when using services that employ small packet sizes, such as voice over IP. The shorter response times and lower latencies noticeably improve service quality compared with connections secured with IPsec. It is also possible to establish a higher number of VoIP connections.

### Transmission performance: Ethernet and IPsec encryption




Transmission performance for Ethernet encryption (layer 2) compared with IPsec encryption (layer 3):
Using the R&S®SITLine ETH to provide security offers clear advantages, especially for applications with small packet sizes, such as voice.

# Professional, certified security

Ethernet is a well-established, universal standard for wireline and wireless data transmission. However, it does not protect the confidentiality or integrity of the transmitted data. The R&S®SITLine ETH provides significantly more efficient and effective protection than other solutions. It has been approved by the German Federal Office for Information Security (BSI) for handling classified documents up to the German restricted ("VS-NfD") level.

## Securing point-to-point Ethernet lines and Ethernet VLANs

The R&S®SITLine ETH was developed in compliance with the Metro Ethernet standard and is able to encrypt point-to-point Ethernet lines referred to as Ethernet private lines (EPLs). With this approach, two encryption devices communicate directly with one another using either transport or tunnel mode. The transport mode only encrypts the payload data (e.g. the IP packet) and leaves the Ethernet address information unchanged. In tunnel mode, all traffic – including addresses – is encrypted and then sent as payload data in new Ethernet packets.

In scenarios in which two devices are directly interconnected without a switch, R&S®SITLine ETH100 devices and R&S®SITLine ETH1G devices can be operated in bulk mode. Bulk mode encrypts all Ethernet packets (including address information) without adding overhead, which offers a higher degree of confidentiality while maintaining maximum data throughput.

When a central site needs a secure network connection to multiple remote sites in a star topology, the R&S®SITLine ETH can, based on the VLAN that is being used, allocate the Ethernet traffic to a corresponding R&S®SITLine ETH. This requires the network provider to offer multiple Ethernet virtual private lines (EVPLs) that can be encrypted in a VLAN-specific way using the R&S®SITLine ETH.

## Innovative group encryption for multicast topologies (ELANs)

In fully meshed Ethernet local area networks (ELANs), classic encryption obstructs the carrier network's multicasting capabilities by establishing dedicated paths between the encryption devices. Videos and other live streams that are meant for multiple recipients and are transmitted via multicast have to be duplicated prior to transmission and then encrypted individually for each recipient.


R&S®SITLine ETH50.

In this kind of environment, the R&S®SITLine ETH can be employed for group encryption of the network traffic – without affecting the multicasting capabilities. The security level is identical to that of classic encryption over dedicated channels, because – despite grouping – each R&S®SITLine ETH device continues to use its own session key for the outgoing network traffic.

In addition, group encryption takes any MPLS network into consideration that is present. The MPLS labels that are required in plain form for routing (which are normally part of the encrypted payload data) are detected and then transmitted without encryption.

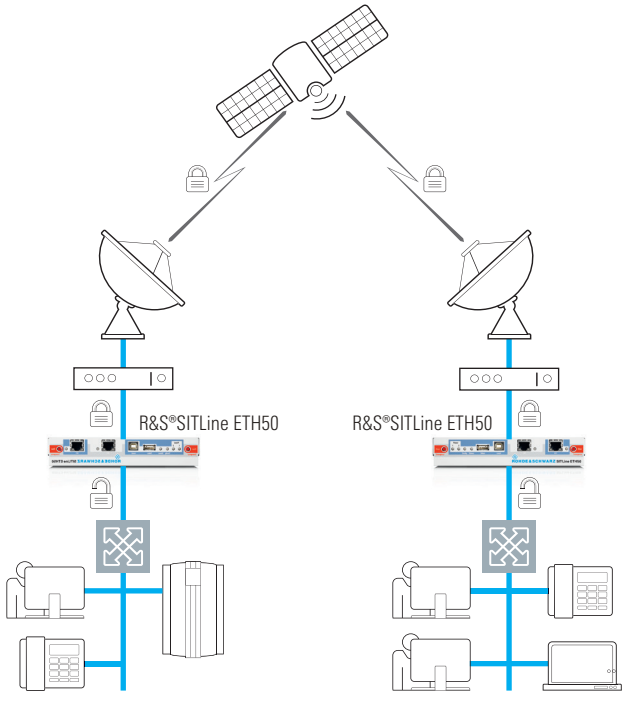
## Secure authentication

The R&S®SITLine ETH uses the following technologies and standards to ensure secure authentication:

- Asymmetric cryptography using elliptic curves with a 257-bit key (roughly corresponds to a 3200-bit RSA key)
- X.509 v3 certificates for persons and equipment
- Secure storage and transport of confidential parameters using smart card technology

Secure authentication of the users based on individual device certificates precedes each link setup. A unique set of keys is generated for each management connection and for each data connection that is to be secured.

**Automatic setup and operation of secure links**




The R&S®SITLine ETH is preconfigured before it is sent to the operating site. On startup, it automatically sets up encrypted L2 links. The same applies to backup devices.

Key agreement is performed in accordance with the Diffie-Hellman process. For key generation, the R&S®SITLine ETH uses a hardware-based random number generator that is certified in accordance with Common Criteria EAL4+.

## Automatic operation of encrypted links

The device certificates determine which partners are authorized to establish a connection. Secure links are set up with each authorized communications partner and then monitored from end to end to ensure that they are working without error. Expired device certificates and session keys are renewed automatically. Secure connections are re-established automatically when changes are made in the network configuration. This rules out the possibility of unintentional or unnoticed communications taking place via unencrypted links.

## Flexible encryption hardware

The system employs symmetric algorithms (AES 256) that are integrated into high-performance hardware. Special customer requests regarding the cryptographic method can be taken into account upon request.

## Manipulation-proof devices

The R&S®SITLine ETH features not only cryptographic core functions but also an intricate system of mechanical and electromechanical security functions. This includes layered security zones, protected memory, protection mechanisms against mechanical manipulation, and other security functions for counteracting attempts to steal or manipulate encrypted confidential information.

# Central security management over the network

R&S®SITScope is the security management system for the R&S®SITLine ETH Ethernet encryptor. R&S®SITScope is based on a client-server architecture and is available as a pre-installed appliance or as separate software for Windows. Smart cards that have been integrated into USB tokens are used to ensure secure handling of user and device certificates.

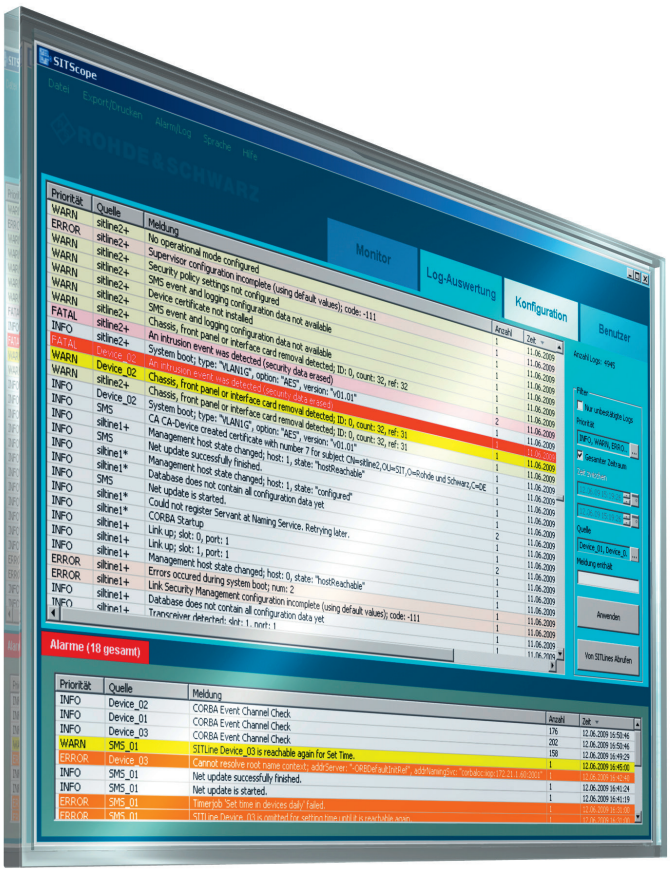
## Online, convenient and secure

The R&S®SITScope server acts like the certificate authority (CA) in a public key infrastructure and is operated in a secure environment (computer center with access control). The client runs on the administrators' workstation computers. Communications between server and client and between server and encryption device take place via TLS/SSL-secured links. R&S®SITScope communicates with the R&S®SITLine ETH via the network that is to be encrypted (inband) or via a dedicated management network (outband).

A central network plan is generated in R&S®SITScope for configuring the R&S®SITLine ETH encryption devices. This network plan contains device parameters (e.g. IP addresses for device management), the devices' operating modes (e.g. bulk and VLAN) and the communications relationships between the devices (encrypted/unencrypted). The device certificates and their private keys are generated and distributed to R&S®SITLine ETH devices in accordance with the network plan.

After the R&S®SITLine ETH has been initialized once using a USB device token, it is available online for all management tasks. Whether they need to reconfigure settings, change a certificate or update firmware – with R&S®SITScope, administrators can accomplish all management tasks from their workstation.

Should any R&S®SITLine ETH devices be stolen, or even compromised, R&S®SITScope adds them to certificate revocation lists (CRL) which are published online in the network. R&S®SITScope is only required for managing the individual devices; during operation, the R&S®SITLine ETH determines the session key itself independently of R&S®SITScope.




The R&S®SITScope security management system is available to administrators for configuring security-relevant settings on the R&S®SITLine ETH.

## Virtualization capability and high availability

If R&S®SITScope is procured as software, the server can also be run in virtual environments (Virtual Box, VM Ware). To ensure hardware security, R&S®SITScope uses a smart card that has been integrated into a USB stick. This root token is used to securely generate and apply the secret upon which the keys are based and must be constantly available on the server during operation.

By employing redundant instances, it is also possible to achieve high availability for R&S®SITScope operations. The network plan and device parameters are synchronized between these instances.

After activation, each R&S®SITLine ETH device searches independently for a path to the R&S®SITScope server. This is accomplished using IP protocols (layer 3) on all available network connections and by querying partner devices via Ethernet (layer 2) for possible R&S®SITScope instances. Should a management connection fail during operation, the R&S®SITLine ETH searches independently and automatically for alternative connections ("self-healing").

## Clearly defined roles

R&S®SITScope offers the possibility of using roles to assign, manage and seamlessly log clearly defined administrator rights. Roles are bound to specific USB user tokens and the related certificate, making it impossible to abuse or manipulate rights. There are supervisor, manager and monitor roles available.

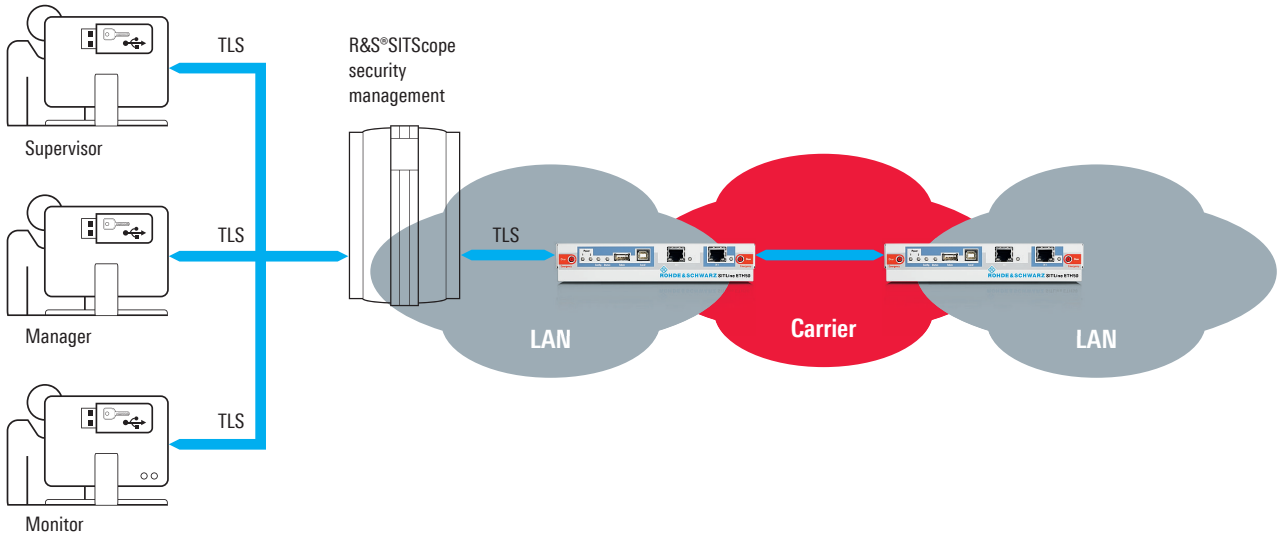
A supervisor is allowed to configure fundamental security management settings and functions and manage user accounts. Supervisors do not manage devices. Managers are responsible for configuring and monitoring the R&S®SITLine ETH devices. Managers are not able to manage user accounts. Monitors are only allowed to monitor the operating status; they cannot make any changes.

Unauthorized access to the independent, closed security management functionality is not possible.

## Central point for log files and audits

R&S®SITScope collects all log information from the individual R&S®SITLine ETH devices and stores this data until it is confirmed by an administrator. R&S®SITScope offers professional audit capabilities for summarizing and analyzing the processes that take place on different R&S®SITLine ETH devices. In addition, log information can be passed on from R&S®SITScope to Syslog servers in the network.

## Security management




Administrators can conveniently configure the security parameters for all devices from their own workstation via the network.
They only need their USB user token to authenticate themselves to R&S®SITScope. R&S®SITLine ETH100/R&S®SITLine ETH1G also have ports for a separate management network (outband).

# SNMP-based network management

Network settings on R&S®SITLine ETH devices can be configured using the simple network management protocol (SNMP). Furthermore, the devices offer detailed data for monitoring as well as extensive diagnostic capabilities via SNMP using any SNMP browser or the R&S®SITLine Admin program delivered with the R&S®SITLine ETH.

### Support of SNMP v1, v2c and v3

Network-relevant settings on the R&S®SITLine ETH encryption devices are configured via the network management. This includes basic configuration settings, such as the Ethernet connection speed and duplex behavior. Extended configurations are also possible, such as Ethernet operation and maintenance (OAM) or preset VLANs for network searches. The necessary user identification is accomplished using community strings when SNMP v1/2c is used. With SNMP v3, the log-in details (user name/password) are set and verified securely.

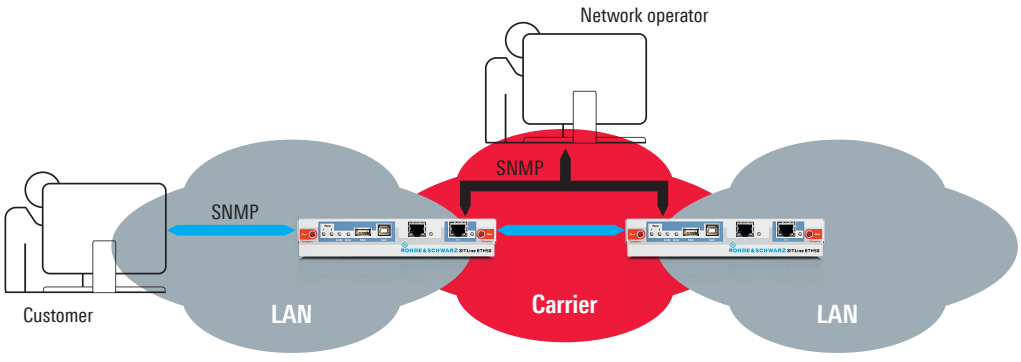
### Extensive monitoring and diagnostic capabilities

Each R&S®SITLine ETH device provides extensive statistics that can be called up via SNMP, such as the number of encrypted/unencrypted Ethernet frames transmitted. If Ethernet frames have been blocked because they were redundant (replay attacks), this is also recorded. The R&S®SITLine ETH uses traps (SNMP v1) or notifications (SNMP v2c/3) to actively inform the SNMP network management about network events. For troubleshooting, loopback diagnostics can be performed for every port (using quick payload diagnostics or long inward diagnostics).

### Network management through service providers

For security management using R&S®SITScope and for SNMP-based network management, separate IP addresses can be assigned to each encryption device. Network management can also be accomplished from the carrier network. This permits the use of outsourcing models in which a service provider can reach the R&S®SITLine ETH for network management via SNMP, although the entire security functionality remains under the customer's direct control.

**SNMP-based network management**




In order to configure network settings and query status information, SNMP is used either within the local network (blue arrows) or from the carrier network (black arrows). Administrators and service providers authenticate themselves to the R&S®SITLine ETH using SNMP community strings or SNMP credentials. Security settings remain unaffected.

# Specifications in brief

| R&S®SITScope | |
|---|---|
| **Minimum system requirements for the R&S®SITScope server software** | |
| Operating system | Windows XP SP2, Windows Server 2003, Windows Server 2008 (32/64 bit) |
| Hard disk | min. 160 Gbyte of free space |
| RAM | min. 2 Gbyte |
| Network (NIC) | min. 1 Fast Ethernet port |
| USB interfaces | min. 4 free USB ports |
| **Minimum system requirements for the R&S®SITScope client software** | |
| Operating system | Windows XP SP2, Windows Server 2003, Windows Server 2008 (32/64 bit), Windows 7 |
| Hard disk | min. 5 Gbyte of free space |
| RAM | min. 2 Gbyte |
| Network (NIC) | min. 1 Ethernet port (100 Mbit/s recommended) |
| USB interfaces | min. 2 free USB ports |
| **Pre-installed R&S®SITScope appliance** | |
| Form factor | rack format (19", 1 HU) with redundant power supply |
| Operating system | Windows Server 2008 |
| Hard disk | mirrored, RAID1 |
| Peripherals | keyboard, mouse, four-port USB hub |


The supplied R&S®SITLineAdmin program is used for network management. Other SNMP browsers such as HP OpenView can also be used.

# Specifications in brief

| R&S®SITLine ETH | | | |
|---|---|---|---|
| | **R&S®SITLine ETH1G** | **R&S®SITLine ETH100** | **R&S®SITLine ETH50** |
| **Ethernet, ports** | | | |
| Number of lines per device | 1 | 1, 2 or 4 | 1 |
| Connector/transceiver | optical, electrical, exchangeable (SFP) | electrical, exchangeable (SFP) | electrical, built-in |
| Performance/throughput per line | 1 Gbit/s | 100 Mbit/s | 25 Mbit/s, 50 Mbit/s, 100 Mbit/s |
| Number of links | 4000 | 4000 | 250 |
| Supported Ethernet services | | | |
| E-Line (EPL, EVPL/VLAN) | ● | ● | ● |
| E-LAN (EPLAN, EVPLAN/VLAN) | ● | ● | ● |
| **Cryptography and security** | | | |
| Transport/tunnel mode | ● | ● | ● |
| Bulk mode (back-to-back) | ● | ● | – |
| Group encryption (multipoint) | ● (MPLS transparent) | ● (MPLS transparent) | ● (MPLS transparent) |
| Asymmetric | 257-bit ECC key (roughly corresponds to a 3200-bit RSA key) | | |
| Key agreement | Diffie-Hellman (DH-ECKAS) protocol | | |
| Digital signature | ECDSA | | |
| Authentication | X.509 v3 certificates | | |
| Symmetric | AES with 256-bit key, CFB interleaved mode, GCM, other standard algorithms or customer-specific algorithms upon request | | |
| External emergency erasure | – | – | ● |
| Emergency erasure after loss of power | after two days | after two days | after one to seven days (can be configured and deactivated) |
| **Management systems** | | | |
| Security and configuration management | with R&S®SITScope online via network | | |
| Security management ports | inband, outband | inband, outband | inband |
| Network management | with SNMP v1, v2c, v3; independent of security management | | |
| | with R&S®SITLine Admin | | – |
| Network management ports | inband, outband | inband, outband | inband |
| **Approvals/certifications** | | | |
| German Federal Office for Information Security (BSI) | German restricted (VS-NfD) | German restricted (VS-NfD) | German restricted (VS-NfD) |
| | NATO restricted | NATO restricted | NATO restricted |
| EANTC | interoperability test | interoperability test | interoperability test |
| Key generation (TRNG) | Common Criteria EAL 4+ | Common Criteria EAL 4+ | Common Criteria EAL 4+ |
| CE approval | ● | ● | ● |
| **General data** | | | |
| Operating temperature range | +5 °C to +50 °C | | –20 °C to +70 °C |
| Storage temperature range (not initialized) | –20 °C to +70 °C | | –40 °C to +70 °C |
| MTBF (availability) | 47 000 h (99.9830 %) | 46 000 h (99.9826 %) | 350 000 h (99.9977 %) |
| Power supply | 110 V or 240 V/50 Hz or 60 Hz, redundant, hot swappable | 110 V or 240 V/50 Hz or 60 Hz, redundant, hot swappable | 24 V DC to 60 V DC, redundant |
| Dimensions and weight | | | |
| Form factor | rack format (19")/1 HU | | half-rack format (7.5")/1 HU, top-hat rail (DIN rail) |
| Dimensions (W × H × D) | 438 mm × 44 mm × 596 mm (17.2 in × 1.7 in × 23.5 in) | | 190 mm × 36 mm × 190 mm (7.5 in × 1.4 in × 7.5 in) |
| Weight | max. 7.6 kg (16.8 lb) (including installation fixtures) | | max. 1.5 kg (3.3 lb) |
| Shipping weight | max. 18,5 kg (40.8 lb) | | max. 3 kg (6.6 lb) |

# Ordering information

| Designation | Type | Order No. |
|---|---|---|
| **R&S®SITLine ETH50, half-rack format (7.5"), 1 HU** | | |
| Ethernet Encryptor, 1 line, 25 Mbit/s | R&S®SITLine ETH50-25 | 5401.8830K02 |
| Ethernet Encryptor, 1 line, 50 Mbit/s | R&S®SITLine ETH50-50 | 5401.8830K02 |
| Ethernet Encryptor, 1 line, 100 Mbit/s | R&S®SITLine ETH50-100 | 5401.8830K02 |
| **R&S®SITLine ETH100, rack format (19"), 1 HU** | | |
| Ethernet Encryptor, 1 line, 100 Mbit/s | R&S®SITLine ETH100-110 | 5401.7004K11 |
| Ethernet Encryptor, 2 lines, 100 Mbit/s | R&S®SITLine ETH100-210 | 5401.7004K12 |
| Ethernet Encryptor, 4 lines, 100 Mbit/s | R&S®SITLine ETH100-410 | 5401.7004K13 |
| **R&S®SITLine ETH1G, rack format (19"), 1 HU** | | |
| Ethernet Encryptor, 1 line, 1 Gbit/s | R&S®SITLine ETH1G-110 | 5401.6820K11 |
| **R&S®SITLine device token (one token required per device)** | | |
| Device token, USB/smart card | | 5410.0650.04 |
| **R&S®SITScope, security management** | | |
| Set consisting of software and tools on CD (server and client software, R&S®SITLine Admin, R&S®SITLine Terminal), USB tokens (3 root tokens, 2 supervisor tokens, 2 manager tokens), USB cable (type A to B) | R&S®SITScope Set | 5410.8400K53 |
| R&S®SITScope Set, pre-installed on server hardware | R&S®SITScope Appliance | 5410.8400K13 |
| **Accessories for R&S®SITLine ETH50** | | |
| USB cable (type A to B), for local initialization | | 1502.0567.00 |
| External power supply for R&S®SITLine ETH50, 110 V to 240 V, 50/60 Hz | | 5401.8898.00 |
| **Accessories for R&S®SITLine ETH100/R&S®SITLine ETH1G** | | |
| Electric SFP transceiver (10/100/1000BaseT) for R&S®SITLine ETH100 and R&S®SITLine ETH1G | | 5401.8198.00 |
| Optical SFP transceiver (1000BaseSX) for R&S®SITLine ETH1G | | 4055.6412.00 |
| Optical SFP transceiver (1000BaseLX) for R&S®SITLine ETH1G | | 5401.8181.00 |
| **Accessories for R&S®SITScope** | | |
| Manager token, USB/smart card | | 5410.0650.02 |
| Root token, USB/smart card | | 5410.0650.03 |
| Supervisor token, USB/smart card | | 5410.0650.05 |
| **Manuals** | | |
| User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, German | | 5401.8900.31 |
| User manual, R&S®SITLine ETH50, German | | 5401.8875.31 |
| User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, English | | 5401.8900.32 |
| User manual, R&S®SITLine ETH50, English | | 5401.8875.32 |
| User manual, R&S®SITScope, German | | 5410.8439.31 |
| User manual, R&S®SITScope, English | | 5410.8439.32 |

**Data sheet for the R&S®SITLine ETH100/1G, see PD 5214.0724.22.**
**Data sheet for the R&S®SITLine ETH50, see PD 5214.4607.22,**
**and www.sit.rohde-schwarz.com**

## Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

### About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

### Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability

Certified Quality System
ISO 9001


**Rohde&Schwarz SIT GmbH**
Am Studio 3 | D-12489 Berlin
Phone +49 30 65884-223 | Fax +49 30 65884-184
E-mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

**Rohde&Schwarz GmbH&Co. KG**
www.rohde-schwarz.com


### Regional contact

- Europe, Africa, Middle East | +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America | 1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America | +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific | +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China | +86 800 810 8228/+86 400 650 5896
  customersupport.china@rohde-schwarz.com



PD 5214.0724.12 | Version 06.00 | June 2013 | R&S®SITLine ETH




5214072412