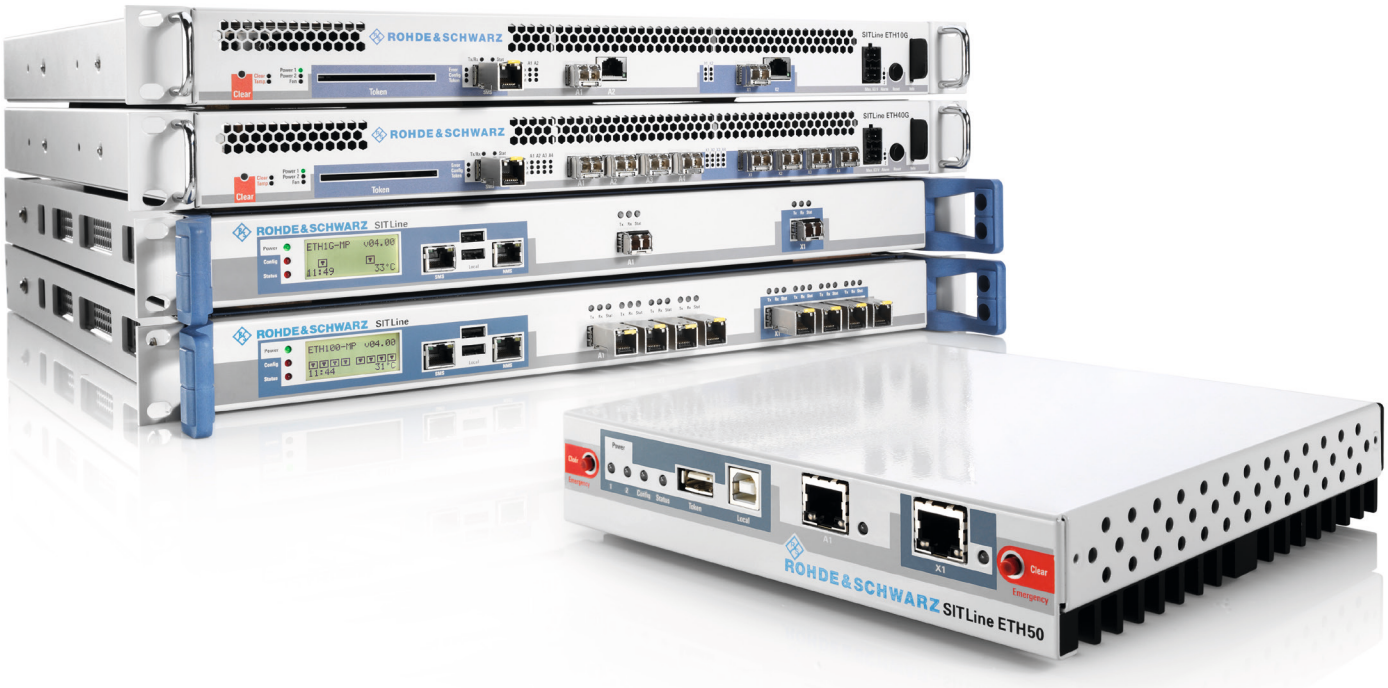
R&S®SITLine ETH
Ethernet Encryptor

Secure data transmission via landline, radio relay and satellite links up to 40 Gbit/s



You act. We protect.
Encryption and IT security
by Rohde&Schwarz SIT.

ROHDE&SCHWARZ

Secure Communications

Product Brochure | 11.00

R&S®SITLine ETH Ethernet Encryptor

At a glance

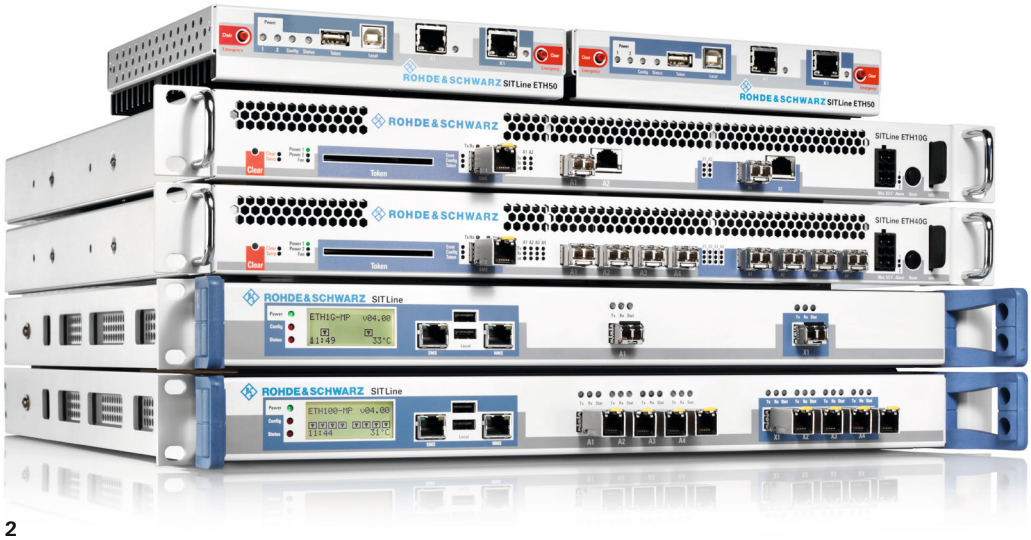
The R&S®SITLine ETH protects companies and organizations against espionage and manipulation of data that is transported via Ethernet over landline, radio relay or satellite links. The devices in this product family are approved by the German Federal Office for Information Security (BSI) and can be used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

The R&S®SITLine ETH performs Ethernet-based encryption – in the 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 existing or planned network structures.

Because Carrier Ethernet significantly reduces costs, it has become established in recent years as a true alternative to managed IP connections 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 for bandwidths from 25 Mbit/s to 40 Gbit/s
- Advanced cryptographic methods and standards (elliptic curves, AES, X.509)
- Flexible deployment in modern 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 network settings
- Very compact design (one height unit for all devices), very low energy consumption, low system costs per Gbyte (total cost of ownership)
- Approved by the German Federal Office for Information Security (BSI) up to the German restricted (VS-NfD) and NATO restricted classification levels



The R&S®SITLine ETH is available in different performance classes and form factors.

R&S®SITLine ETH Ethernet Encryptor

Benefits and key features

Professional, certified security

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

▷ 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
- High availability as standard

▷ page 6

Central security management

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

▷ page 8

SNMP-based network management

- Support of SNMP v1, v2c and v3
- Extensive monitoring and diagnostic capabilities
- Network management through service providers
- Immediate startup with R&S®SITLine Admin

▷ page 10

Professional, certified security

Ethernet is a well-established, universal standard for 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 (EPL). 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 packets) 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 ETH4G, R&S®SITLine ETH10G and R&S®SITLine ETH40G 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 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 (EVPL) that can be encrypted in a VLAN-specific way using the R&S®SITLine ETH.

Innovative group encryption for multicast topologies (ELAN)

In fully meshed Ethernet local area networks (ELAN), classic encryption obstructs the carrier network's multicasting capability by establishing dedicated paths between 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.

In this kind of environment, the R&S®SITLine ETH can be employed for group encryption of the network traffic – without affecting the multicasting capability. 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 into consideration any MPLS network that is present. The MPLS labels that are required in plain form for routing (and are normally part of the payload to be encrypted) are detected and transmitted without encryption.

In just one height unit, the R&S®SITLine ETH40G performs low-latency encryption of up to four 10 Gigabit Ethernet lines.

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 partners 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. Key agreement is based on the Diffie-Hellman protocol. 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 to the network configuration. This rules out the possibility of unintentional or unnoticed communications taking place over unencrypted links.

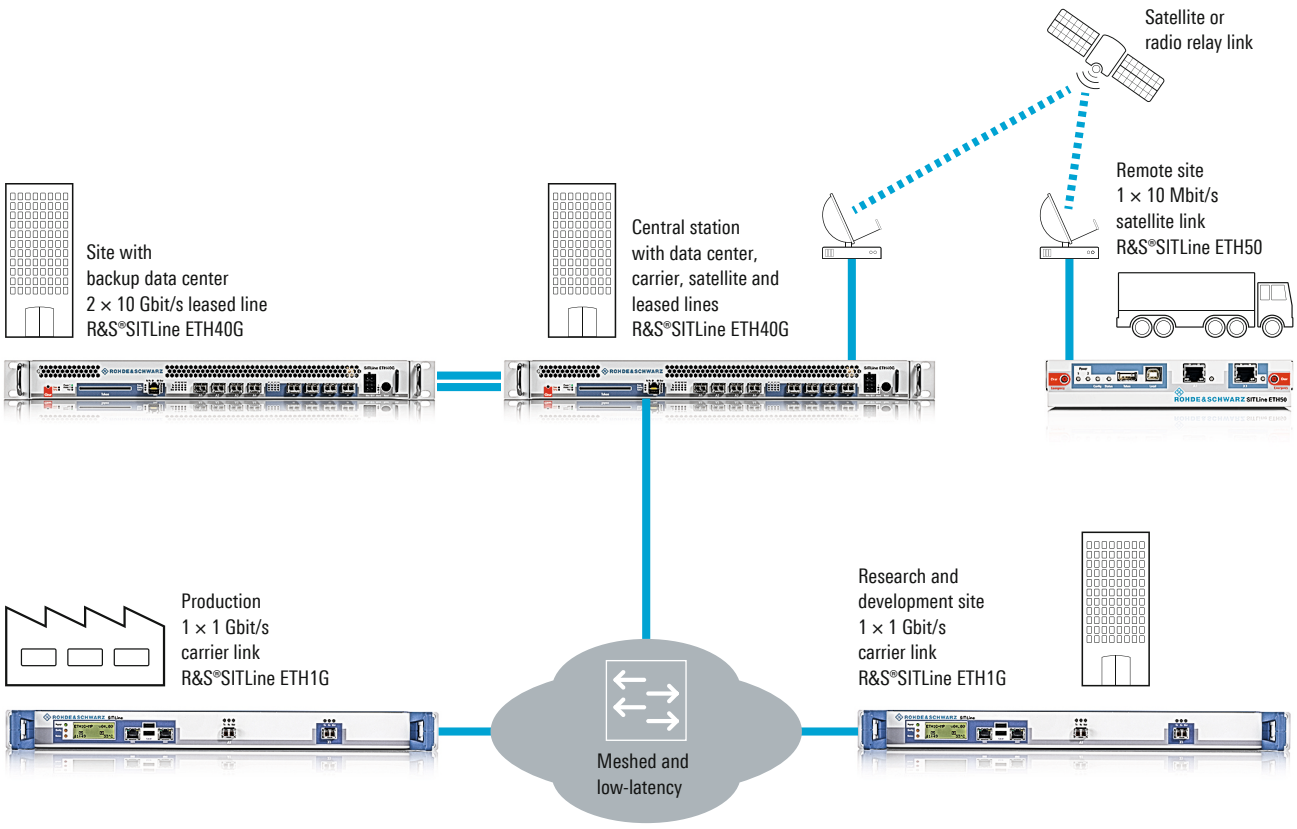
Flexible encryption hardware

The R&S®SITLine ETH employs symmetric algorithms (AES 256) that are integrated into high-performance hardware. Special customer requirements regarding the cryptographic method can be taken into account upon request.

Tamper-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.

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 via Fast Ethernet, 1 Gigabit Ethernet and 10 Gigabit Ethernet. The same applies to backup devices.

Low system costs

Compared with other encryption solutions, networks protected by the R&S®SITLine ETH make it possible to significantly reduce operating costs 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 network-specific configuration steps are required. As a plug&play technology, Ethernet requires almost no configuration effort to get started. This 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 models provide 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.

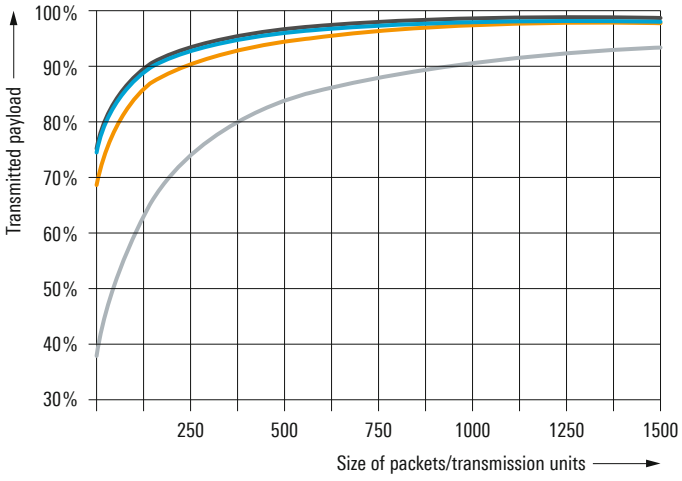
Lower transmission costs than with managed IP

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 data rate (payload rate) only drops by 0% to 13% when using Ethernet encryption. An IPsec-secured VPN, on the other hand, reduces the payload rate by as much as 60%.

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 between 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.

Payload rate (capacity utilization)



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

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. This approach exploits the multicast capability of switched 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

R&S®SITLine ETH devices fully automatically negotiate the session keys required for operation and distribute them securely to the authorized communications partners. No dedicated encryption key servers are required. Failure of one device does not impact 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 devices (see page 8), is primarily used for installation and monitoring. Once operational, R&S®SITLine ETH devices organize encryption automatically without requiring any additional components.

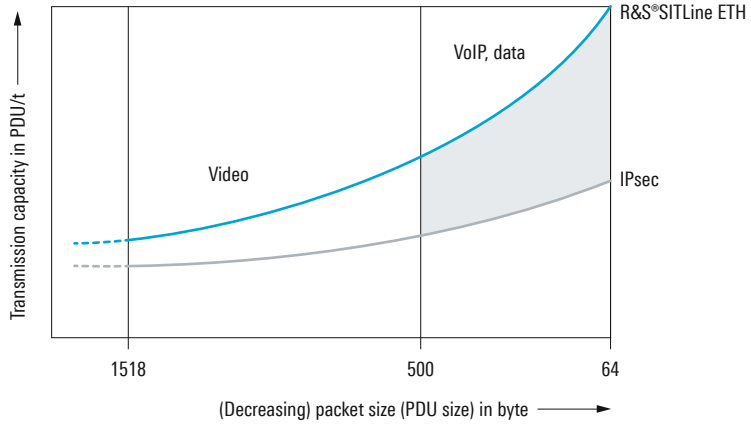
Better transmission performance than with IPsec

The reduced overhead provided by the R&S®SITLine ETH has a positive effect on transmission performance. 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 quality of service (QoS) compared with connections secured with IPsec. It is also possible to establish a higher number of VoIP connections.

High availability as standard

R&S®SITLine ETH devices are optimized for smooth, failsafe operation; even maintenance work does not affect operation. Each model is equipped with a redundant power supply. In addition, the R&S®SITLine ETH4G, R&S®SITLine ETH10G and R&S®SITLine ETH40G offer exchangeable fans while the multiport models provide parallel encryption lines. Power supply units, fans and batteries can be hot-swapped.

Transmission performance: Ethernet versus IPsec encryption



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

Central security management

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

Online, efficient and secure

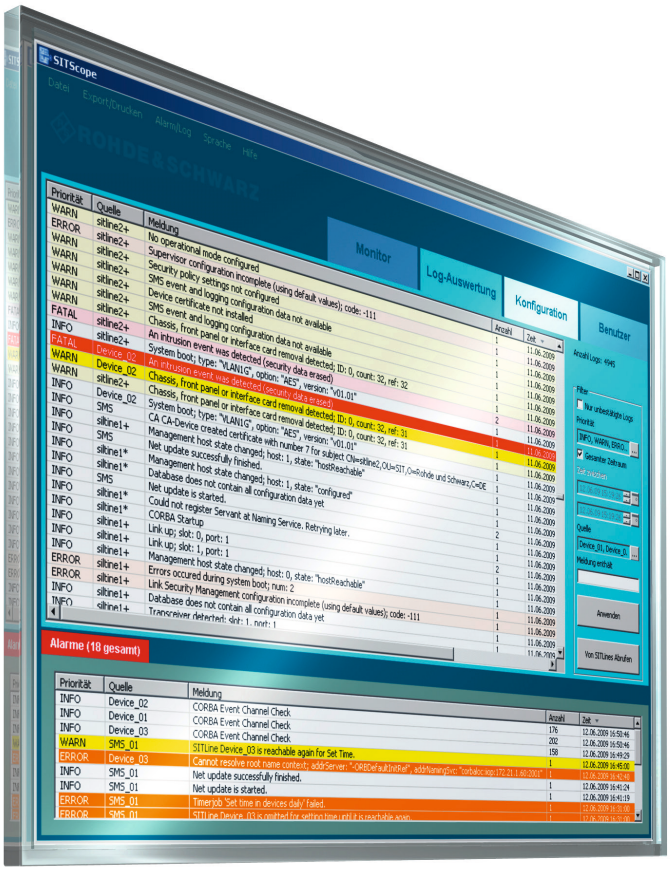
The R&S®SITScope server acts like the certificate authority (CA) in a public key infrastructure (PKI) and is operated in a secure environment (data center with access control). The client runs on the administrators' workstation computers. Communications between server and client and between server and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

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

Should any R&S®SITLine ETH devices be stolen or 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 device initialization; during operation, each 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 (VirtualBox, VMware). To ensure hardware security, R&S®SITScope uses smart card based root tokens. The 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 user tokens and the related certificates, making it impossible to abuse or manipulate rights. Available roles are supervisor, manager and monitor.

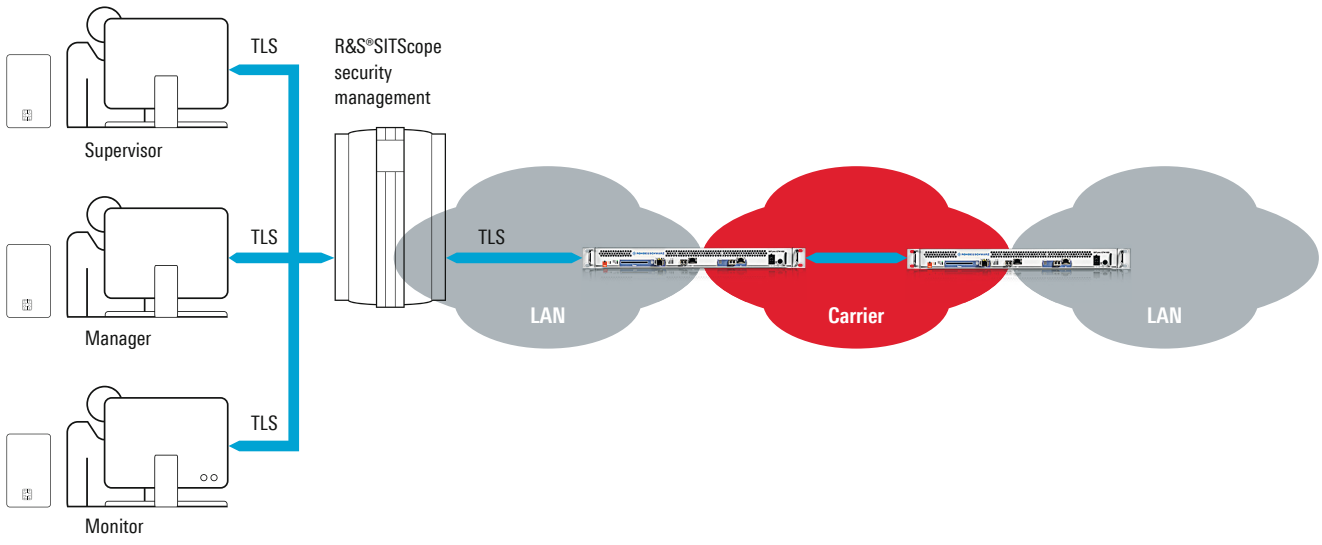
A supervisor is allowed to configure fundamental security management settings and functions and to manage user accounts. Supervisors do not manage devices. Managers are responsible for configuring and monitoring the R&S®SITLine ETH devices. Managers are not able to manage user accounts. Monitors are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

Unauthorized access to the independent, closed security management system 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, R&S®SITScope can forward log information to Syslog servers in the network.

Security management



Administrators can conveniently configure the security parameters for all R&S®SITLine ETH devices from their own workstation via the network. They only need their user token to authenticate themselves to R&S®SITScope. The R&S®SITLine ETH4G, R&S®SITLine ETH10G and R&S®SITLine ETH40G also have ports for a separate management network (out-of-band).

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 software delivered with the R&S®SITLine ETH.

Support of SNMP v1, v2c and v3

Network-relevant settings on R&S®SITLine ETH devices are configured via network management. This includes basic configuration settings, such as the Ethernet ports' speed and duplex behavior. Extended configurations are also possible, such as Ethernet OAM or preset VLANs for network searches. The necessary user identification is accomplished using community strings when SNMP v1/v2c 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/v3) 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).

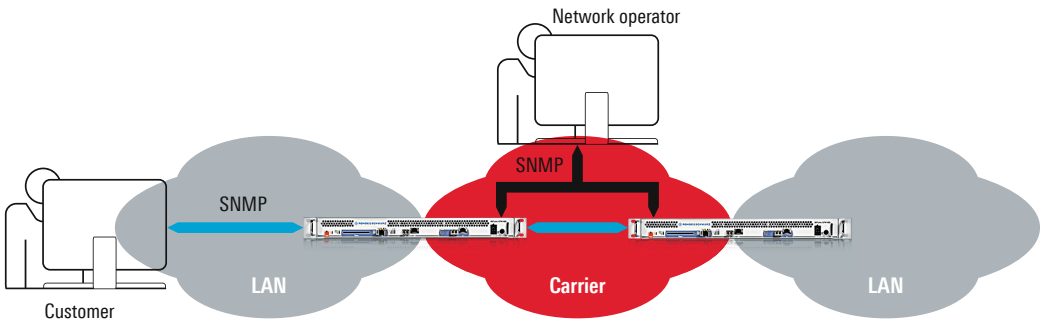
Network management through service providers

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.

Immediate startup with R&S®SITLine Admin

R&S®SITLine Admin is a user-friendly network management tool for R&S®SITLine ETH devices. There is no need to adapt existing SNMP browsers. R&S®SITLine Admin is specially engineered for use with R&S®SITLine ETH devices. A device's front panel is graphically represented showing, for example, current LED displays. Settings, statistics and diagnostics can be made quickly and easily.

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®SITLine ETH50	R&S®SITLine ETH4G	R&S®SITLine ETH10G	R&S®SITLine ETH40G
Performance				
Throughput per device	100 Mbit/s, full duplex	4 Gbit/s, full duplex	10 Gbit/s, full duplex	40 Gbit/s, full duplex
Latency	18 µs	5 µs	3 µs	3 µs
Encryption lines				
Quantity	1 × 100 Megabit Ethernet	4 × 1 Gigabit Ethernet	1 × 10 Gigabit Ethernet	4 × 10 Gigabit Ethernet
Medium	electrical	optical, electrical, cross media	optical, electrical, cross media	optical, electrical
Cryptography and security				
Asymmetric	257-bit ECC key (roughly corresponds to 3200-bit RSA key)			
Symmetric	AES with 256-bit key, CFB ("zero overhead"), GCM, point-to-point and group encryption			
Management	online via R&S®SITScope security management system and token			
BSI approval	•	pending	•	•
Common Criteria	–	certification in line with EAL4+ expected for Q4/2015		
Environmental conditions				
Form factor	compact (7.5", 1 HU, top-hat rail)	rack (19", 1 HU)		
Operating temperature range	–20 °C to +70 °C (ruggedized)	+5 °C to +50 °C (industrial)		
Power supply	24 V to 60 V DC, redundant	choice of 40 V to 72 V DC or 110 V to 240 V AC (50 Hz/60 Hz), redundant, hot-swappable		

Product documentation	Order No.
R&S®SITLine ETH40G: Line and network encryption at 40 Gbit/s – brochure	PD 3607.0017.62
R&S®SITLine ETH: Powerful end-to-end encryption for Ethernet private lines – application card	PD 3607.1313.92
R&S®SITLine ETH: Highly secure data center connection for file and content applications – application card	PD 3606.9527.92
R&S®SITLine ETH: Tamper protection for monitoring networks in banks – application card	PD 3606.8443.92
R&S®SITLine ETH: Securing rail control networks – application brochure	PD 3606.6505.92
R&S®SITLine ETH: Encryption for Romantis UHP-based satellite networks – application brochure	PD 3606.8189.92
R&S®SITLine ETH50 Ethernet Encryptor – data sheet	PD 5214.4607.22
R&S®SITLine ETH100, R&S®SITLine ETH1G Ethernet Encryptor – data sheet	PD 5214.0724.22
R&S®SITLine ETH4G, R&S®SITLine ETH10G, R&S®SITLine ETH40G Ethernet Encryptor – data sheet	PD 3607.0017.22

R&S®SITLine ETH4G, R&S®SITLine ETH10G and R&S®SITLine ETH40G come with redundant power supplies. Power supplies, fan cartridges and batteries can be hot-swapped.

Service that adds value

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

About Rohde&Schwarz

The Rohde&Schwarz electronics group is a leading supplier of solutions in the fields of test and measurement, broadcast and media, secure communications, cybersecurity, and radiomonitoring and radiolocation. Founded more than 80 years ago, this independent global company has an extensive sales network and is present in more than 70 countries. The company is headquartered in Munich, Germany.

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde&Schwarz SIT GmbH
Am Studio 3 | 12489 Berlin, Germany
Phone +49 30 65884-223 | Fax +49 30 65884-184
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 82 28 | +86 400 650 58 96
  customersupport.china@rohde-schwarz.com

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG
Trade names are trademarks of the owners

PD 5214.0724.12 | Version 11.00 | March 2015 (ch)
R&S®SITLine ETH Ethernet Encryptor

Data without tolerance limits is not binding | Subject to change
© 2008 - 2015 Rohde&Schwarz GmbH&Co. KG | 81671 Munich, Germany

5214072412

5214.0724.12 11.00 PDP 1 en