Version 04.00

February 2007

R&S®SITLine ATM

Encryption of ATM connections

- Professional, high-grade encryption
- Secure Smart USB token initialization
- Separation of security and network functions
- Interface ranges from 34 Mbit/s to 622 Mbit/s
- Up to 4000 individually protected channels
- Protection for data, audio, and video traffic
- Tamper-resistant parameter storage
- High-speed symmetric algorithms
- Public-key agreement method

ROHDE&SCHWARZ

Protected channels in ATM WAN infrastructures

Security for multimedia data

The R&S®SITLine ATM encrypts all types of transmitted data. This includes real-time communications, speech, audio, and video (up to and including video in broadcast and studio quality), as well as non-time-sensitive computer data. The bandwidths range from a few kbit/s to hundreds of Mbit/s.

Encryption is simultaneous and in real-time, and does not impair the transmission quality. A unique key is used for each channel (communications relationship). The negligible device cycle time (only a few µs) and the minimal overhead for the security function ensure continued and unchanged service quality.

The EANTC (European Advanced Networking Test Center) has successfully tested and therefore approved the operation of the R&S®SITLine ATM on public ATM networks.

Ideal performance, reliability and flexibility

The R&S®SITLine ATM safeguards up to 4000 bidirectional ATM channels (asynchronous transfer mode) with a bandwidth from 19 kbit/s to 622 Mbit/s.

An interface pair is configured for each device. The pair consists of one module on the plain, private ("red") side and one module on the encrypted, public ("black") side.

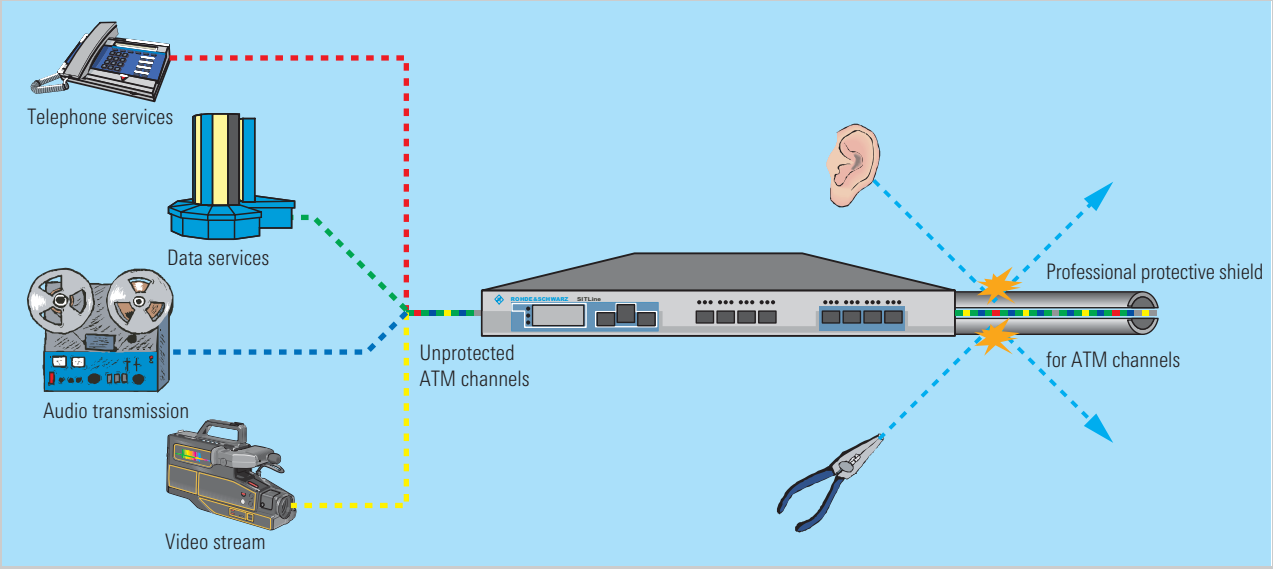
The range of interfaces supports port speeds from 34 Mbit/s up to 622 Mbit/s over PDH or SDH/SONET networks.
The total transmission capacity of an R&S®SITLine ATM device is 622 Mbit/s.

Each interface module can provide one, two or four ports. One port from the private side and one port from the public side combine as a pair to create a transmission connection. These ports have the identical bandwidth and transmission protocol (ATM).

The R&S®SITLine ATM supports redundant links to satisfy requirements for high connection availability.

The device can be adapted to various transmission media. The optical interfaces for 155 Mbit/s and 622 Mbit/s connections (fiber) can be configured with different transceivers to easily integrate the R&S®SITLine ATM into existing network infrastructures.

The support of either permanently set channels (PVCs) or signaled channels (SVCs) in accordance with UNI 3.1 or UNI 4.0 underscores the flexibility of the system.



Multimedia ATM channels protected by the R&S®SITLine ATM

Professional security from every angle

Optimal price/performance ratio

The R&S®SITLine ATM provides highly efficient, economical, and effective data security through the following:

- Low investment costs
  - Per Mbit/s of secured transmission bandwidth
  - Per user
- Optimal use of the available and allocated capacity
  - The additional bandwidth needed for the security functions is less than 0.1% of the user data rate
- Minimal organizational, structural, and operational costs
  - Flexible integration in existing infrastructures (modular interfaces)
  - Separation of rights and privileges in the different areas of responsibility in the device (network administration and security management); IT activities and IT functions can be outsourced

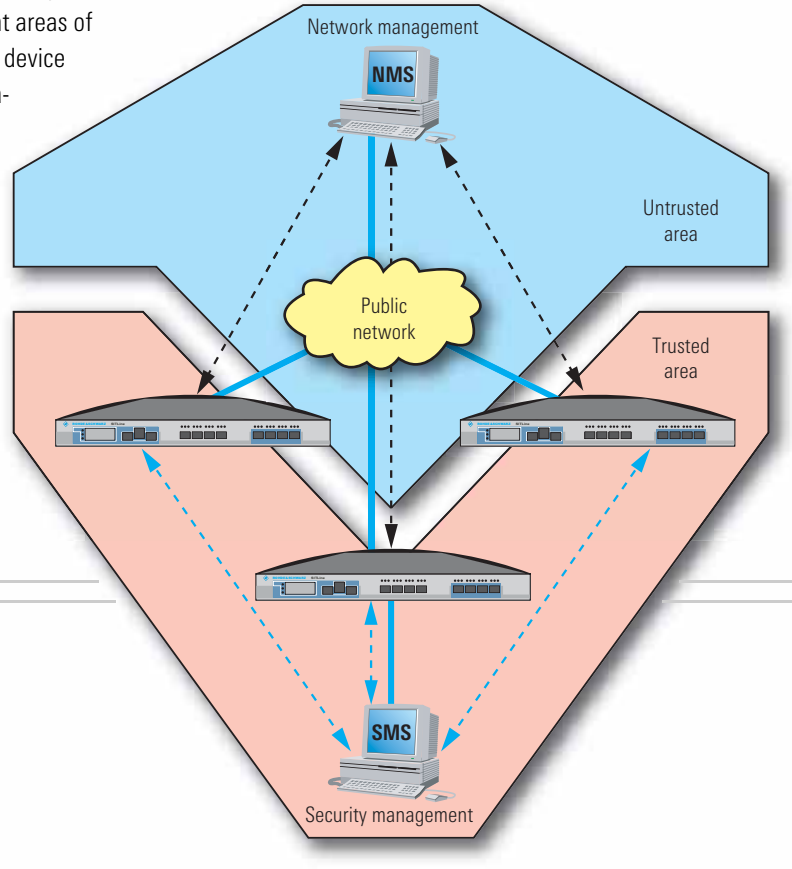
Separation of security and network management

The R&S®SITLine family concept supports the separation of the network transmission and the security functions at all levels. The security manager has ultimate control with overriding rights. Read and write privileges for network functions can be delegated to an independent network manager. The security functions and parameters remain under the sole control and ownership of the security manager.

Rohde&Schwarz SIT provides the security manager with a security management station for setting and managing the device parameters – in particular the security parameters.

Standard databases (MIBs) are available to the network administrator for monitoring the status of the R&S®SITLine ATM within the network. Data is accessed via a standard protocol (SNMP) and can be displayed on conventional management stations.

The R&S® SITLine ATM simultaneously safeguards the availability and monitoring of an expensive, high-grade IT connection. It meets all requirements for maximum confidentiality and security of transmitted data and even allows the device to be installed in an untrusted environment.



Separation of security and network functions eliminates risk

High-grade data encryption

Strong authentication and key management

Certificates in accordance with X.509, using elliptic curves (EC) with a key length of 191 bits (equivalent to RSA with 1571 bits), are used for mutual device authentication and for device security management.

The security management controls the certificates and creates and manages "white" (access granted), and "black" (access denied) lists. The certificates allow the positive, unambiguous identification of each individual device. This allows devices to authenticate themselves to the security manager.

The certificates implement the Diffie-Hellman method during the channel establishment phase to derive a symmetric session key for this channel. High-powered hardware carries out this operation within 200 ms to 500 ms, and up to 15 secured connections can be established per second.

The security of an active connection is rounded out by automatically renegotiated session keys without affecting the user data stream.

Professional online encryption

Special premium hardware is used to implement the encryption function. This hardware encrypts the broadband user data by using symmetric cryptographic processes. TDES or AES, the two state-of-the-art algorithms, are offered as standard solutions. Customized solutions are also available on request. Additional standard algorithms as well as tried-and-tested proprietary solutions can be implemented.

Application-specific encryption modes

It is in the nature of encryption that transmission errors (bit toggle or bit loss) may be multiplied. Each communications service reacts differently to these errors:

- Voice services demand shorter transmission times with a continuous data flow but can tolerate bit errors
- IP data services have less exacting timing requirements but are sensitive to transmission errors and their proliferation, particularly if these errors transcend the block limits

The encryption function provided by the R&S®SITLine ATM satisfies these varying requirements by offering different encryption and operation modes. It is possible to select between ECB (electronic code book) and CBC (cipher block chaining) depending on the class of service. This minimizes the influence of transmission errors in conjunction with each separate service class requirement.

User-specific parameters and rights

Although data encryption begins and ends in the R&S®SITLine ATM devices, identity-proofing and authentication-checking extend beyond the limits of the connection secured by the devices themselves. The security management function defines individual or group-based security relationships and connection rights for ATM terminal subscribers/devices. The R&S®SITLine ATM devices involved in the establishment of the transmission check these rights and, depending on the corresponding security policies, either process or reject the required connection requests.

Independent secured configuration

Tamper-resistant parameter storage

The R&S®SITLine ATM provides additional, passive protection for the security functions. All security-relevant device configuration data is stored in non-readable memory and is erased as soon as the device is opened. The device then reverts to the factory-set state and has to be reinitialized. Deletion will occur even if the device is not powered up.

The security data will also be erased automatically after 48 hours if the device remains in power-down mode.

Device configuration under user control

The R&S®SITLine ATM is delivered without any predefined parameters. Only the necessary algorithms have been integrated into the system hardware. The manufacturer and user are therefore completely separated. The user independently defines and generates all security parameters by using the security management.

The R&S®SITLine ATM is put into operation by a multiple-step process:

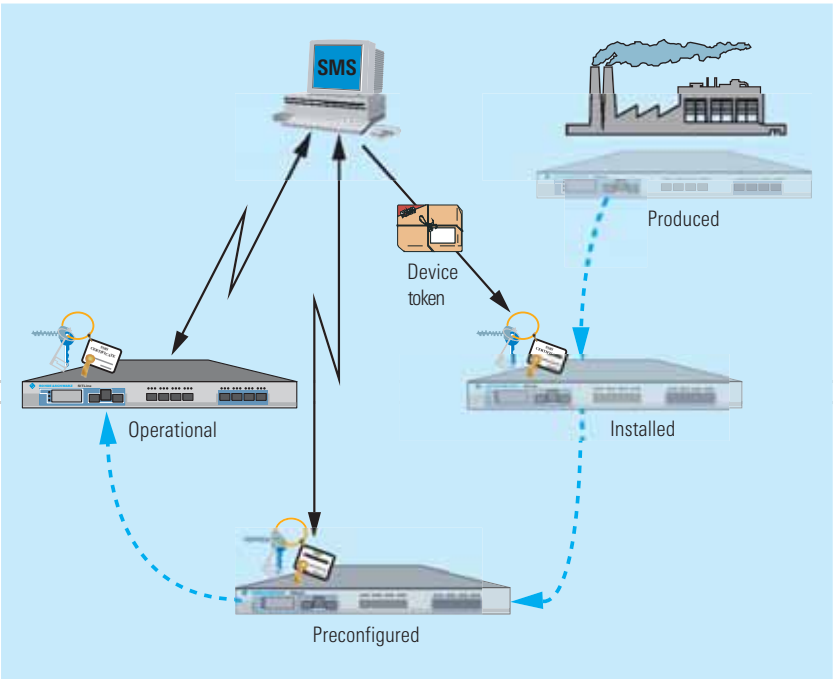
- Produced – The device is ready for delivery by the manufacturer
- Installed – The device has been physically installed on site, and the cables have been connected
- Preconfigured – The base data has been defined and configured by the security management function and transferred to the device by the Smart token
- Operational – The device has registered online with the security management function and received all further configuration data

This step-by-step process ensures independent and unlimited control by the owner.

Secure transport of base data via Smart token

The base data is transported from the security management station to the devices on site using modern, certified SmartCard technology in a USB token. The USB token with a SmartCard plus the local manager user name and the corresponding password are all needed to transfer the data to the device. The device authenticates and registers itself online with the security management to obtain the data necessary to initiate full operation.

The token is removed and stored securely once the device is operational. The token can be used for disaster recovery to reinitialize the device. The security manager determines whether only the specific device (serial number) or also replacement devices with the same configuration can be reinitialized.



Device statuses from production to full operation

Glossary

AAL – ATM adaptation layer	Intermediate ATM layer that adapts data to the requirements and the special characteristics for transmission over ATM networks. Versions 1, 2, 3/4, and 5 are available.
AES – advanced encryption standard	Modern block algorithm in existence since 2001 as a result of an international tendered competition with key lengths of 128 bits, 192 bits, and 256 bits.
Algorithm (encryption algorithm)	A rule (or set of rules) for carrying out mathematical operations using unresolved mathematical problems or non-reconstructible operations to encrypt data.
ATM – asynchronous transfer mode	Serial data transmission for a large number of logical channels that transmit data in fixed packet lengths of 53 bytes (= cells) with a guaranteed quality of service for the connection. The maximum transmission speed is uncapped (currently up to 2.4 Gbit/s).
Block algorithm	Encryption algorithm that processes data blocks as the smallest input unit. The input and output blocks are usually the same size.
CBC – cipher block chaining	Operating mode that combines the processing blocks. Blocks with the same input content will generally result in different output (see also ISO standard 10116).
DES – data encryption standard	Older block algorithm developed by IBM and NIST (American standardization institute). First standardized encryption algorithm.
ECB – electronic codebook	Operating mode that processes each input block separately. The same input blocks will result in the same encrypted output (see also ISO standard 10116).
EC/ECC – elliptic curve/EC cryptography	Encryption process with asymmetric keys based on elliptic curves.
Key	Second input value, along with the user data, used in the algorithm for encrypting and decrypting the user data. The key to decrypt and encrypt is the same (symmetric) or different (asymmetric) depending on the algorithm. Keys are used to secure the transmission of confidential information and must be kept secret.
MIB – management information base	Standardized database for storing device configuration and operation data.
Operating mode	Algorithm applied to a data stream. Transmission error variables, the different attack scenarios, and the synchronization of decryption and encryption need to be accommodated.
PDH – plesiochronous digital hierarchy	Frame-synchronous digital hierachy. The lowest layer, E0, works with a bandwidth of 64 kbit/s. Channels are multiplexed (bundled) over many stages using TDM systems (time division multiplexing). In a PDH structure, multiplexing and demultiplexing can only occur in the next (neighboring) layer. Layers cannot be skipped.
PVC/PVP – permanent virtual circuit/path	A logical communications channel generated by the cell header information. A number of channels is bundled to form a path.
RSA	Asymmetric algorithm named after the developers Rivest, Shamir, and Adleman.
SDH – synchronous digital hierarchy	Standard for synchronous high-speed data transmission with comprehensive mechanisms for the resilience of the SDH network. In contrast to PDH structures, channels can be inserted or extracted directly at all levels of the hierachy.
Security management	Hardware and software for managing and monitoring the security systems using prescribed rules enabled by the security manager.
Security manager	Person responsible for configuring and operating the security elements of an IT infrastructure.
SMS – security management station	Hardware and software for configuring, managing and monitoring the IT security systems.
SNMP – simple network management protocol	Standardized communications protocol between a network management station and the device MIB.
SONET	North American SDH standard with mininum differences to SDH.
SVC/SVP	Signaled, temporary, logical connections or paths (see also PVC).
TDES – triple DES (data encryption standard)	Older block algorithm superseded by AES in which each block is processed by the DES core algorithm three times.
UNI – user network interface	Encompasses a number of standards that describe the transition point between the ATM transmission network and the ATM user.
X.509 certificate	ITU-T standard that describes the form and content of cryptologically generated certificates used for authenticating communications parties.

ROHDE&SCHWARZ

www.sit.rohde-schwarz.com

Customer Support: Telephone: +49 30 65884111 · Fax: +49 30 65884184 · E-mail: info.sit@rohde-schwarz.com