SITLink

Secure communications on leased lines

- Confidential communications via synchronous leased lines at transmission rates up to 2 Mbit/s
- "Transparent" integration
- Easy to install
- Minimal administration required and low cost of ownership
- Fulfills all legal data protection requirements
- Operates independently of applications and services
- Provides flexible security management
- Can be used for:
  - confidential telephony
  - confidential video telephony
  - confidential video conferences
  - confidential data transmission
- Suitable for a large variety of infrastructures
- High-grade encryption through
  - powerful algorithms
  - 128-bit keys
- Authorization through RSA encryption with 2048-bit key

ROHDE&SCHWARZ

Secure communications on leased lines

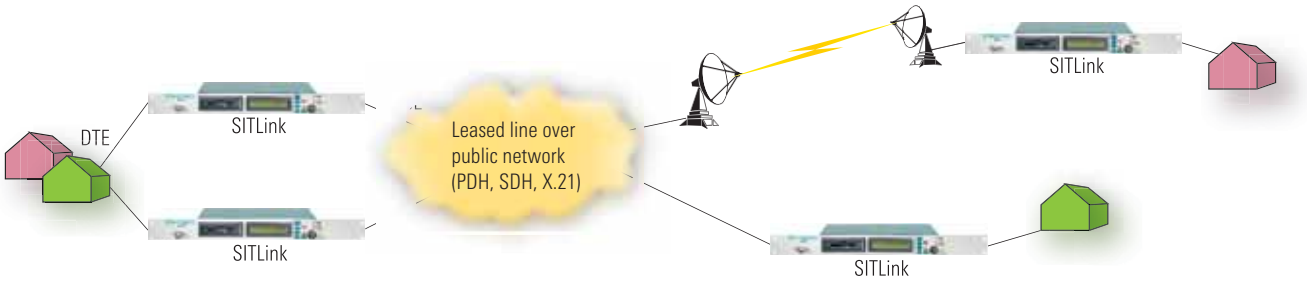

Fig. 1 Encryption of leased-line link by SITLink system

SITLink provides IT security by protecting communications on synchronous leased lines. The system supports transmission rates of up to 2 Mbit/s. Bit-oriented encryption of the transmitted information ensures confidential communications at the primary level. This is the basis for confidential, service-independent, intra-corporate communications (voice, video, and data). Corporate data is protected against eavesdropping, modification, and falsification as well as subterfuge. Both espionage and sabotage are effectively ruled out.

SITLink has been designed to provide a secure backbone for transmission over public connections (Fig. 1) for use in corporate networks with a distributed infrastructure. Solutions of this kind are typical of corporations with trusted and intimate partners or corporations with different subsidiaries and geographically dispersed divisions. Sample applications for SITLink are shown in Fig. 2. Typical environments are the following:

- LAN-LAN link with time division multiplex systems or router and switches
- Coupling of ISDN systems or PDH-based time division multiplexers

Security function

Corporate communications are usually based on leased lines as this structure may be the most effective means of communicating with subsidiaries and partners over the public communications infrastructure. The user is not interested in the transmission media or the route of transmission on the public communications highway. Contrary to popular belief, leased-line connections are not necessarily the shortest physical connection as even satellite and microwave links may be involved.

SITLink protects your data against damage, violation, and attacks such as the following:

- Damage caused by passive attacks with the intention of espionage. These attacks do not affect the transmitted information or operation of the communications system, but try to obtain confidential information such as passwords, subscriber IDs, project details, quotation and price information

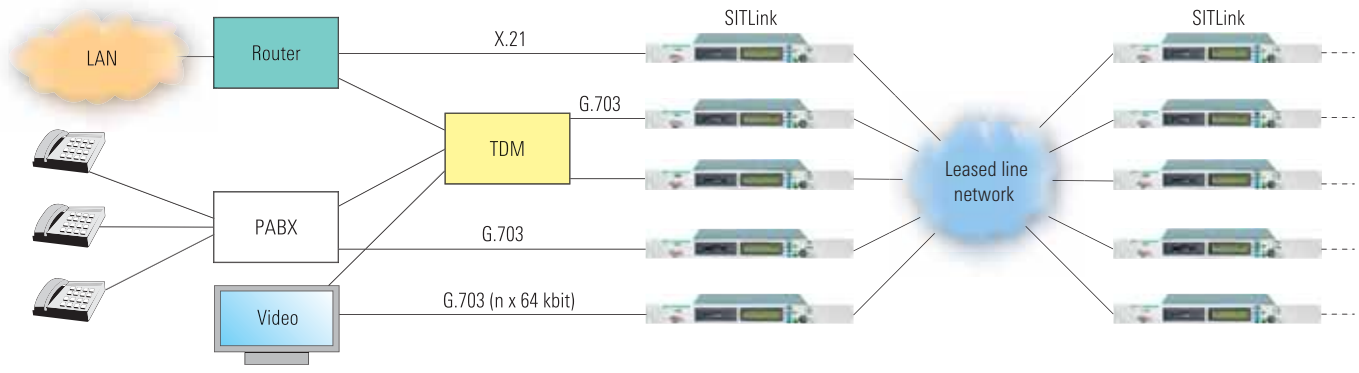

Fig. 2 SITLink environment

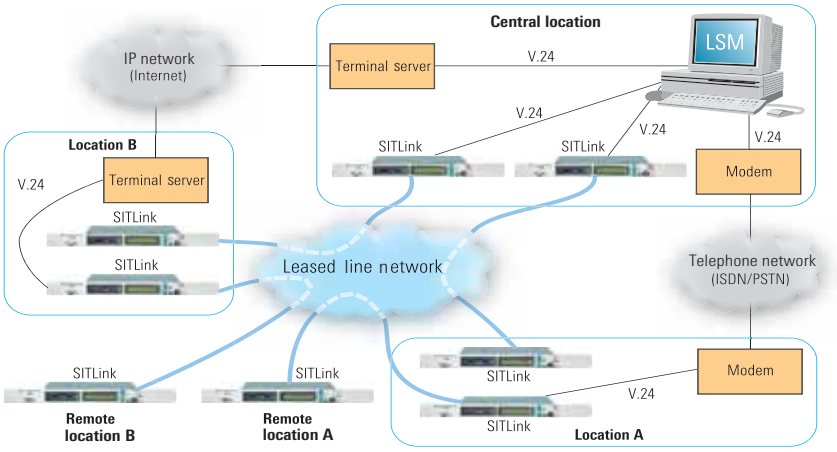

Fig. 3 Connection of local LSM (link security management)

- Damage via attacks that manipulate and distort the information. The intruders may delay, repeat or change transmitted messages by inserting or deleting information. This includes unauthorized access (deception attempts by tampering with the ID codes of communications partners)
- Damage may also be caused by inadvertent loss of information, e.g. when the information does not arrive at its destination because of operating mistakes, software faults, transmission breakdown, or routing errors

Operation

SITLink units are connected to both ends of a public-network line. Terminal equipment connected to the SITLink units "sees" them as belonging to the leased-line system (DCE). SITLink does not reduce transmission performance and the full bandwidth of the line is available to the user.

Encryption is performed on OSI layer 1, i.e. at bit level. SITLink units need a clock and can only operate when connected to a synchronous network. This clock ensures reliable signal reception at the receiver end. If the clock fails, the entire network shuts down. A symmetrical encryption method is used with the same algorithms and keys (128 bits) at both ends of the link. If the symmetry requirement is not met, the recipient, i.e. an unauthorized subscriber, will not receive usable data. Encryption is performed by the Kryptochip SCA95 hardware.

Management

Appropriate tools are available for system management, configuration and monitoring.

SITLink units can be managed locally or controlled from a remote link security management station.

System management performs the following tasks:

- Encrypted saving and storage of sensitive and critical data
- Secure key assignment/management
- Generation of sensitive data (keys, chip card programming, etc)

The system can be accessed in two ways: via the local management port, and via the secured data port connected to the public network.

Remote management via the connection used for information transmission is called in-band management, and management via a separate network is referred to as out-of-band management. The advantage of in-band management is the cost saving as the existing infrastructure required for information transmission is used. Out-of-band management is more reliable and not affected by any failures in the transport network. Furthermore, it does not occupy bandwidth in the network that otherwise could be used for data transmission.

PC-based link security management (LSM) has been designed for managing and monitoring secured links.

Fig. 3 shows possible applications of LSM. For monitoring and management, one of the end nodes on the link to be protected is addressed directly (locally) or via the remote-control network. In this scenario, the serial V.24 link is emulated or tunneled through another network by means of a modem link or through the use of terminal servers (TS). Thus LSM can remotely access the line to be managed. The complementary unit on the link to be secured can then be accessed in-band via the secured data line. A precondition for this is, of course, that an active and secured link has been established between the SITLink units.

Specifications

General data

Dimensions (HxWxD, 19" rackmount)	44 mm x 482.6 mm x 242 mm
Weight	4 kg
Operating voltage	100 V to 240 V AC ±5%, 50 Hz to 60 Hz, optional 48 V DC, self-regulating
Power consumption	peak 30 VA norm <24 VA
Fusing	2AT via fine-wire fuse, accessible from exterior
Safety class	I
Climatic class	3K2, DIN IEC 721
Permissible temperature range	5 °C to 40 °C (ambient temperature)
Operating temperature range	15 °C to 32 °C
Relative humidity	10% to 75%, no condensation
Service port	D-Sub 9-pin connector (V.28) for servicing only
Display	2 x 20-digit LCD, no illumination
Operation	5 keys or management system or service application
Chip card	in line with ISO 7816, incl. cryptocontroller and RSA with 2048-bit key
Management	
Interface Transport Application	D-Sub 15-pin connector, male (ISO 4903) V.24 (RS-232-C) link management LSM: local via V.24 and in-band to complementary unit, remote management via modem or terminal server
Firmware	version 4.x (management interface in V.24 mode)
Line versions	
X.21 link Transmission rate Line coding Electrical interface Connector Clock Latency Other data	 up to 2048 kbit/s NRZ X.27 D-Sub 15-pin connector (ISO 4903) from "public" or "home" interface 1 bit (~1.9 µs to 833 µs) possible also via unframed E1 control of C, I link
G.703 E1 link Transmission rate Line coding Electrical interface Connector Clock Latency Mode	 2048 kbit/s HDB3 or AMI G.703 with G.704 framing (PCM 30/31) D-Sub 15-pin connector (ISO 4903) co-directional 18 bits (~8.8 µs), no jitter 30/31 × 64 kbit/s, structured
G.703 link Transmission rate Line coding Electrical interface Connector Clock Latency Mode	 2048 kbit/s AMI or HDB3 G.703 Sub-D 15 (ISO 4903) co-directional 18 bits (~8.8 µs), no jitter 2048 kbit/s, unstructured

Encryption

Operating modes	
Encrypted Bypass Error	user-selectable channels local activation, setting and activation via LSM in case of a fault, random numbers are sent
Algorithm	Siemens SCA95 algorithm

Approvals/conformity

EN 60950:2000	product safety
EN 55022:1998 class B	EMC, ITE EMI emission
EN 55024:1998	EMC, ITE immunity
EN 61000-3-2:1995	EMC, mains harmonic currents

Certified Quality System
ISO 9001
DQS REG. NO 1954 QM

ROHDE&SCHWARZ

www.sit.rohde-schwarz.com

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