SITLink

Sichere Kommunikation über Standleitungen

- Sichert vertrauliche Kommunikation über synchrone Standleitungen bis zu 2 Mbit/s
- Ist „transparent" zu integrieren
- Einfach zu installieren
- Kaum Administrationsaufwand und Betriebskosten
- Erlaubt, die Anforderungen des gesetzlichen Datenschutzes zu erfüllen
- Anwendungs- und dienstunabhängiger Betrieb
- Bietet flexibles Sicherheitsmanagement
- Wird eingesetzt für:
  - vertrauliche Telephonie
  - vertrauliche Bildtelephonie
  - vertrauliche Videokonferenzen
  - vertrauliche Datenübertragung
- In verschiedensten Infrastrukturen einsetzbar
- Bietet eine hochwertige Verschlüsselung durch
  - starke Algorithmen
  - 128-bit-Schlüssel
- Authentisierung mit RSA-2048-bit-Schlüssel

ROHDE&SCHWARZ

Sichere Kommunikation über Standleitungen

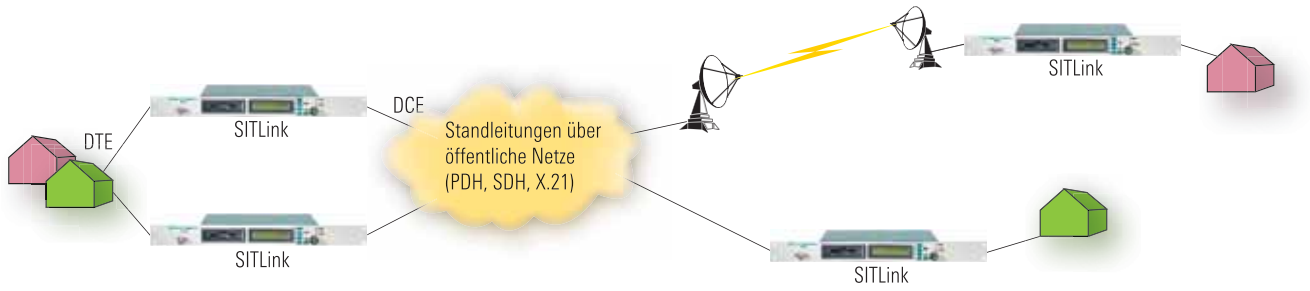

Abbildung 1: Verschlüsselung einer Standleitungsverbindung durch das System SITLink

SITLink bietet IT-Sicherheit durch geschützte Kommunikation über synchrone Standleitungen. Das System ermöglicht eine Übertragungsgeschwindigkeit von bis zu 2 Mbit/s. Die bitorientierte Verschlüsselung der zu übertragenden Informationen gewährleistet die Vertraulichkeit von Informationen an der Basis der IT-Infrastruktur und ist unabhängig vom übertragenden Dienst (Telefon, Video oder Daten). Die Unternehmensdaten werden vor Abhören, kontrollierter Modifikation und Verfälschung sowie vor dem unautorisierten Einfügen von Informationen geschützt. Spionage und Sabotage werden grundlegend verhindert.

SITLink ist für den Einsatz in Unternehmensnetzen mit verteilter Infrastruktur konzipiert und dient in erster Linie der Absicherung einer Backbone-Struktur über öffentliche Wege und Netzwerke (Abbildung 1). Solche Lösungen sind charakteristisch für Unternehmen mit festen und eng kooperierenden Partnern oder für Unternehmen mit verschiedenen Niederlassungen oder abgesetzten Unternehmensbereichen. Einige mögliche Anwendungen für SITLink sind in Abbildung 2 dargestellt. Die typischesten sind:

- die LAN-LAN Kopplung über Time Division Multiplexer-Systeme (TDM-Systeme) oder Router und Switches
- die Kopplung von ISDN-Anlagen oder von PDH-basierten Time Division Multiplexern

Schutzfunktion

In solchen Strukturen bilden Standleitungen oft die Basis der Unternehmensnetze. Damit wird eine kostengünstige direkte Kopplung der Niederlassungen oder Partner, Abteilungen oder Nebenstellen über öffentliche (public) Netzwerk-Infrastrukturen ermöglicht. Der Nutzer kennt dabei in der Regel weder die im einzelnen genutzten Übertragungsmedien, noch den realen Weg, den solche geschalteten Standleitungen über die öffentlichen „Datenautobahnen" gehen. Standleitungen führen nicht immer über die kürzeste, direkte Verbindung, und drahtlose Satelliten- oder Richtfunkstrecken sind mit einbezogen.

SITLink schützt vor Angriffen und Schäden verschiedener Art:

- Schäden durch passive Angriffe, welche sich auf Informations-Spionage beschränken. Die Angriffe nehmen keinen Einfluss auf die übertragenen Nachrichten oder den Betrieb des Kommunikationssystems, verschaffen sich aber unerlaubt vertrauliche Informationen wie Passworte, Teilnehmerkennungen, Projekt-, Angebots- und Preisinformationen

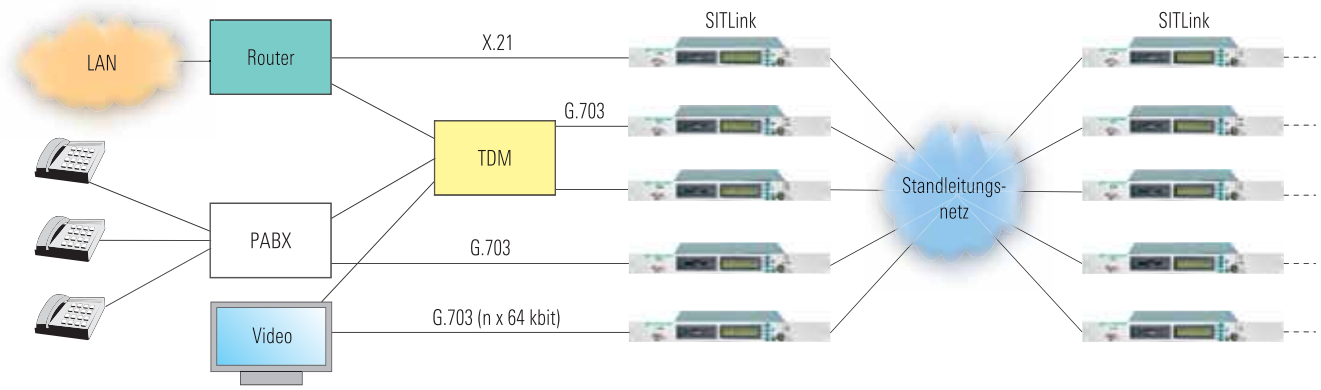

Abbildung 2: Anwendungsumgebung SITLink

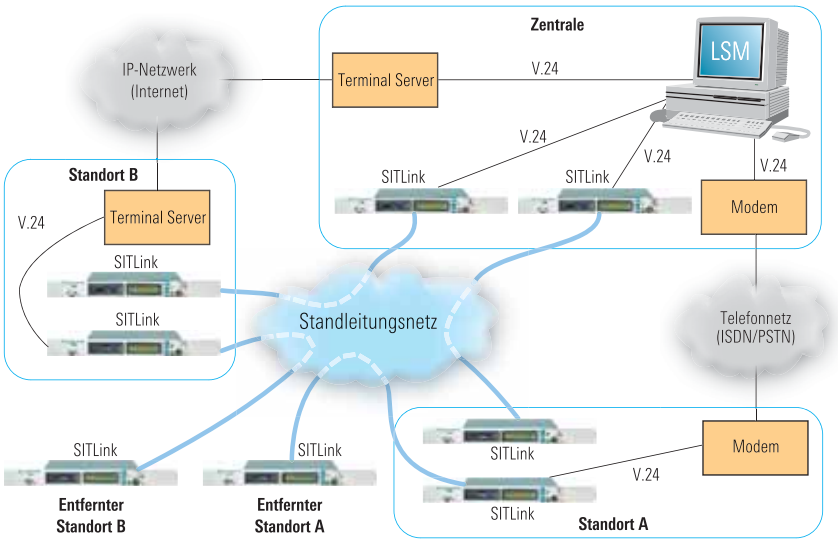

Abbildung 3: Anschluss des LSM (Link Security Management)

- Schäden durch aktive Angriffe, welche den Kommunikationsfluss verändern. Solche Angriffe können Nachrichten verzögern, wiederholen oder durch Löschen bzw. Einfügen inhaltlich verfälschen. Auch Täuschungsversuche durch falsche Identitäten des Kommunikationspartners fallen in diese Kategorie
- Schliesslich können auch Schäden durch unbeabsichtigte Informationsverluste auftreten, wenn etwa durch falsche Bedienung, Softwaremängel, Übertragungspannen oder Fehl-Routing Informationen nicht an ihrem Zielort ankommen

Funktionsweise

Die SITLink-Geräte werden an den Endpunkten einer öffentlichen Leitung installiert und verhalten sich zum Endgerät hin wie das Standleitungssystem. Dabei wird die Leistungsfähigkeit der Datenübertragung durch SITLink nicht beeinträchtigt, dem Benutzer steht die volle Bandbreite der Leitung zur Verfügung.

Die Verschlüsselung wird auf der Schicht 1 (nach OSI-Referenzmodell), also auf Bit-Übertragungsebene realisiert. Voraussetzung für den Betrieb des SITLink-Systems ist ein synchrones Netzwerk, das einen Takt vorgibt. Dieser Takt ermöglicht die verlässliche Übernahme von Signalen auf der Empfängerseite. Wird die Taktversorgung unterbrochen, ist das Netzwerk nicht mehr funktionsfähig. Die Chiffrierung erfolgt mit einem symmetrischen Verfahren, bei dem auf beiden Seiten der Verbindung gleiche Algorithmen und gleiche Schlüssel (128 bit Schlüssellänge) aktiv sind. Erfüllt die Verbindung diese Bedingungen nicht, erhält der Empfänger, z.B. ein unautorisierter Teilnehmer, unbrauchbare Daten. Die Verschlüsselung erfolgt über Hardware mit dem Kryptochip SCA95.

Management

Zur Verwaltung, Konfiguration und Kontrolle der Systeme stehen entsprechende Managementwerkzeuge zur Verfügung.

Die installierten SITLink-Geräte können lokal oder entfernt (remote) von einer Link Security Management-Station verwaltet werden.

Folgende Verwaltungsaufgaben werden durch das System-Management realisiert:

- Verschlüsselte Speicherung sicherheitsrelevanter Daten
- Gesicherte Schlüsselverteilung/ Schlüsselmanagement
- Generierung sicherheitsrelevanter Daten (Schlüssel,Chipkartenprogrammierung etc.)

Prinzipiell ist das System über zwei Wege erreichbar. Zum einen über den lokalen Management Port und zum anderen über den am öffentlichen Netz angeschlossenen, abzusichernden Datenport.

Die Fernwartung (remote Management) über die eigentliche Kommunikationsleitung wird als In-Band-Management bezeichnet. Die andere Möglichkeit über ein separates Netzwerk wird Out-of-Band-Management genannt. Die Vorteile des In-Band-Managements liegen in der Nutzung der vorhandenen, für die Informationsübertragung notwendigen, Infrastruktur und demzufolge in den geringeren Kosten. Das Out-of-Band-Management bietet dagegen eine höhere Sicherheit gegen Ausfälle des eigentlichen Transportnetzwerks und belegt keine Bandbreite in dem für den Datentransfer genutzten Netzwerk.

Das PC-basierte Link Security Management (LSM) ist für die Verwaltung und Kontrolle von abzusichernden Leitungen (Links) konzipiert.

Die Abbildung 3 zeigt mögliche Anwendungen des LSM. Für die Überwachung und Verwaltung wird eins der Enden einer abzusichernden Strecke direkt (lokal) oder über ein Fernnetz angesprochen. Dazu wird die serielle V.24-Verbindung durch eine Modemverbindung oder die Nutzung von sogenannten Terminal Servern (TS) über andere Netze emuliert bzw. getunnelt. Auf diese Weise erhält das LSM einen Fernzugriff auf die zu verwaltende Leitung. Das für den zu sichernden Link komplementäre Gerät wird dann „in-band" über die gesicherte Verbindung erreicht. Voraussetzung dafür ist natürlich eine funktionierende, abgesicherte Verbindung zwischen den SITLink-Geräten.

Technische Daten

Allgemeine Daten

Maße (H × B × T, 19" Rackmontage)	44 mm × 482,6 mm × 242 mm
Gewicht	4 kg
Betriebsspannung	100 V bis 240 V AC ±5 %, 50 Hz bis 60 Hz oder 48 V DC selbstregulierend
Leistungsaufnahme	Spitze 30 VA Norm <24 VA
Sicherung	2 A T über Feinsicherung von außen zugänglich
Schutzklasse	I
Klimaklasse	3K2, DIN IEC 721
Betriebstemperatur	5 °C bis 40 °C Umgebung
Nennbetriebstemperatur	15 °C bis 32 °C
Luftfeuchtigkeit	10 % bis 75 % ohne Kondensation
Serviceport	Sub-D-9 (V.28) nur für Geräteservice
Anzeige	2 × 20-stelliges LCD, unbeleuchtet
Bedienung	5-Tastenfeld oder Management-system oder Serviceapplikation
Chipkarte	nach ISO 7816, incl. Kryptocontroller und RSA mit 2048-bit-Schlüssel
Management	
Schnittstelle Transport Applikation	Sub-D-15 (ISO 4903) V.24 (RS-232-C) Link-Management LSM: lokal über V.24 und „in-band" zum komplementären Gerät, remote Anbindung per Modem oder Terminal Server möglich
Firmware	Version 4.x (Managementschnittstelle im V.24-Mode)
Leitungsversionen	
X.21 Link Geschwindigkeit Leitungscodierung Schnittstelle elektrisch Stecker Takt Verzögerung Sonstiges	 bis 2048 kbit/s NRZ X.27 Sub-D-15 (ISO 4903) von der „public" oder von der „home" Schnittstelle 1 bit (~1,9-833 µs) auch über unframed E1/DS1 möglich Steuerung der C, I Leitung
G.703 E1 Link Geschwindigkeit Leitungscodierung Schnittstelle elektrisch Stecker Takt Verzögerung Mode	 2048 kbit/s HDB3 oder AMI G.703 mit G.704 Framing (PCM 30/31) Sub-D-15 (ISO 4903) codirektional 18 bit (~8,8 µs) ohne Jitter strukturiert 30/31 × 64 kbit/s
G.703 Link Geschwindigkeit Leitungscodierung Schnittstelle elektrisch Stecker Takt Verzögerung Mode	 2048 kbit/s AMI oder HDB3 G.703 Sub-D-15 (ISO 4903) codirektional 18 bit (~8,8 µs) ohne Jitter 2048 kbit/s unstrukturiert

Verschlüsselung

Betriebsarten	
Verschlüsselt Bypass Fehler	Kanäle frei einstellbar Aktivierung nur lokal am Gerät, Einstellung und Freigabe über LSM im Fehlerfall werden Zufallszahlen gesendet
Algorithmus	**Siemens SCA95 Algorithmus**

Genehmigungen/Konformität

EN 60950:2000	Produktsicherheit
EN 55022:1998 class B G.703, class A X.21	EMC, Störaussendung ITE
EN 61000-6-2	EMC, Störfestigkeit ITE
EN 61000-3-2:1995	EMC, Netzoberschwingungsströme

Certified Quality System
ISO 9001
DQS REG. NO 1954 QM

ROHDE&SCHWARZ

ROHDE & SCHWARZ SIT GmbH · Am Studio 3 · 12489 Berlin
Tel. (030) 65884-223· Fax (030) 65884-184 · E-Mail: info.sit@rohde-schwarz.com · www.sit.rohde-schwarz.com

Printed in Germany (bb)