Version 04.00

Februar 2007

R&S®SITLine ATM

Verschlüsselung von ATM-Verbindungen

- Professionelle, hochwertige Sicherheit
- Smart USB-Token Sichere Initialisierung
- Trennung von Netzwerk- und Sicherheitsfunktionen
- Schnittstellen von 34 Mbit/s bis 622 Mbit/s
- Bis zu 4000 individuell gesicherte Kanäle
- Sicherung von Daten, Audio und Video
- Zugriffsgeschützte Parameterspeicherung
- Key-Agreement durch Public-Key-Verfahren
- Schnelle symmetrische Algorithmen

ROHDE&SCHWARZ

Geschützte Kanäle in ATM-WAN-Strukturen

Sicherheit für Multimedia-Daten

R&S®SITLine ATM ermöglicht die Verschlüsselung aller Arten von zu übertragenden Daten. Dies können in der Echtzeitkommunikation Sprache, Audio, oder Videodaten (bis hin zu professioneller Broadcast- und Studioqualität) oder nicht zeitsensible Computerdaten sein. Die Bandbreiten reichen von wenigen kbit/s bis zu hunderten von Mbit/s. Die Verschlüsselung erfolgt simultan in Echtzeit ohne Beeinträchtigung der Übertragungsqualität. Je Kanal (Kommunikationsbeziehung) werden individuelle Schlüssel genutzt. Die geringen Durchlaufzeiten (nur wenige µs) und ein minimaler, notwendiger Overhead für die Sicherheitsfunktionen gewährleisten volle Servicequalität.

R&S®SITLine ATM ist vom unabhängigen Testlabor EANTC (European Advanced Networking Test Center) für den Betrieb an öffentlichen ATM-Netzen erfolgreich geprüft worden.

Bestwerte in Leistung, Zuverlässigkeit und Flexibilität

R&S®SITLine ATM bietet Sicherheit für bis zu 4000 bidirektionale ATM-Kanäle (Asynchronous Transfer Mode) mit einer Bandbreite von 19 kbit/s bis 622 Mbit/s.

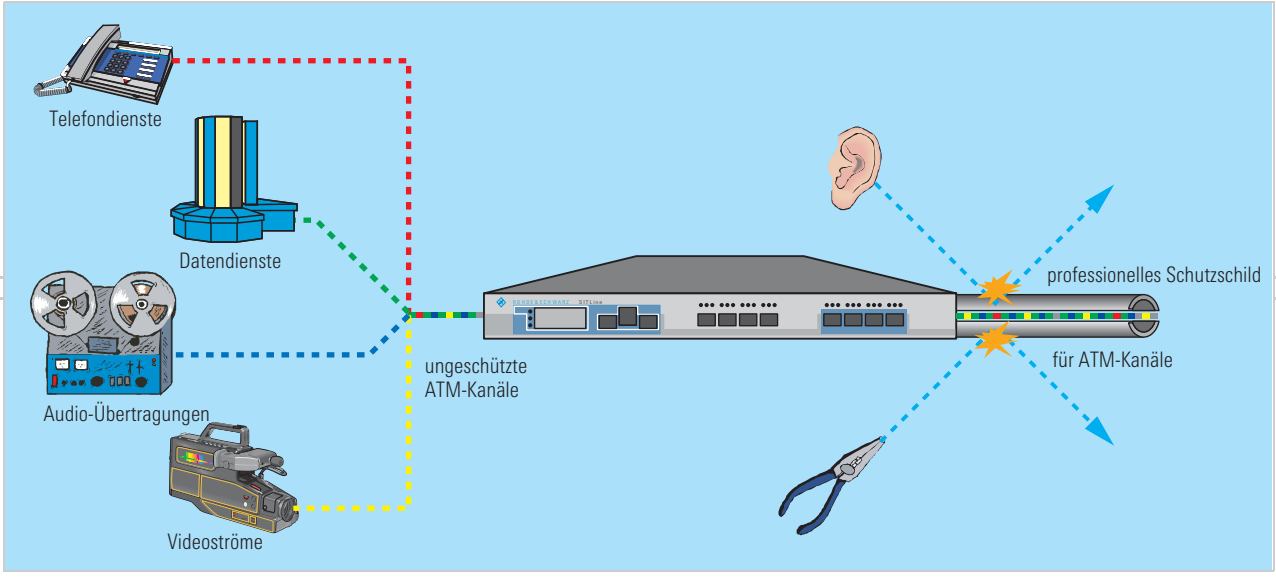
Für jedes Gerät wird ein Interfacepaar konfiguriert, das aus je einem Modul auf der unverschlüsselten privaten Seite („rote Seite") und auf der verschlüsselten öffentlichen Seite („schwarze Seite") besteht.

Die Interface-Palette umfasst Portgeschwindigkeiten von 34 Mbit/s bis zu 622 Mbit/s über PDH- oder SDH/SONET-Transportnetze. Die gesamte Übertragungsleistung des R&S®SITLine ATM beträgt 622 Mbit/s.

Jedes Interface-Modul kann 1, 2 oder 4 Ports bereitstellen, dabei sind für die Transportverbindung je ein Port der privaten und der öffentlichen Seite zu einem Paar verknüpft. Sie sind bezüglich Interface-Bandbreite und gesichertes Protokoll (ATM) identisch. R&S®SITLine ATM unterstützt redundante Leitungen und erfüllt somit alle Anforderungen bezüglich einer hohen Verfügbarkeit von Verbindungen.

Die Anpassung an verschiedene Übertragungsmedien ist möglich. Die Schnittstellen für optische 155 Mbit/s- und 622 Mbit/s-Verbindungen (Fiber) können mit unterschiedlichen Transceivern konfiguriert werden. Dadurch lässt sich R&S®SITLine ATM flexibel in vorhandene Netzwerkstrukturen integrieren.

Diese Flexibilität wird durch die Unterstützung von permanent gesetzten Kanälen (PVCs) oder signalisierten Kanälen (SVCs) nach UNI 3.1 oder UNI 4.0 abgerundet.



Mit R&S®SITLine ATM geschützte multimediale ATM-Kanäle

Professionelle Sicherheit in jeder Hinsicht

Optimales Preis/Leistungs-verhältnis

R&S®SITLine ATM bietet bei der Datensicherung hohe Effizienz und Effektivität durch

- Niedrige Investitionskosten
  - pro Mbit/s gesicherter Übertragungsbandbreite
  - pro Nutzer
- Optimale Nutzung der verfügbaren und bezahlten Kapazität
  - für die Sicherheitsfunktion erforderliche zusätzliche Bandbreite liegt unter 0,1% der Nutzrate
- Minimale organisatorische, strukturelle und operative Kosten durch
  - Flexibilität bei der Einbindung in vorhandene Strukturen (modulare Schnittstellen)
  - Teilung von Rechten und Pflichten verschiedener Verantwortungsbereiche im Gerät (Netzwerkadministration und Sicherheitsmanagement); Outsourcing von IT-Aufgaben und IT-Funktionen wird dadurch ermöglicht

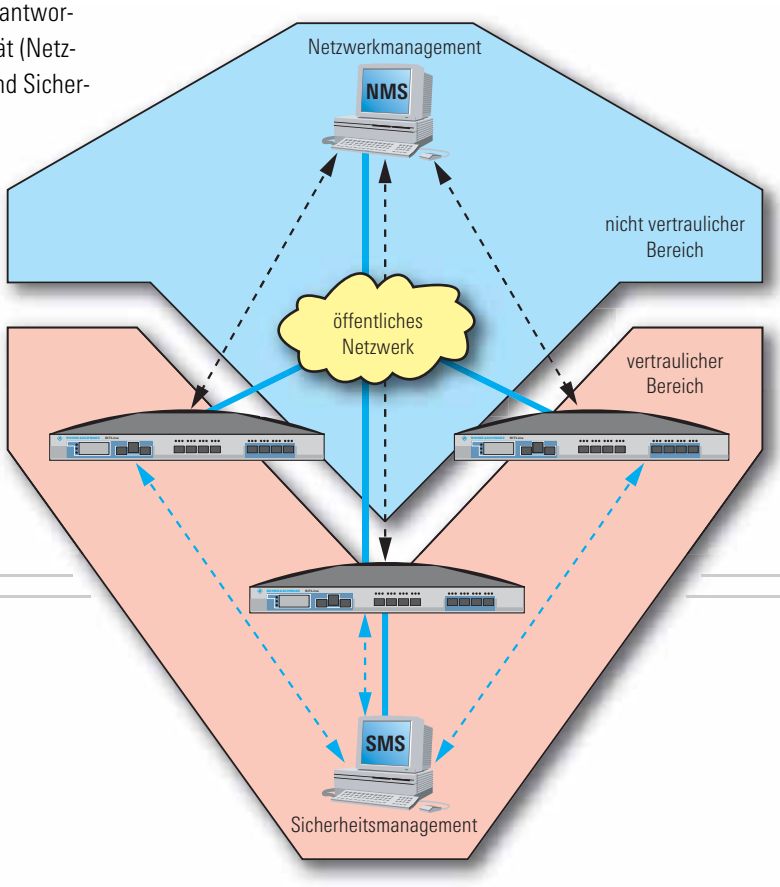
Getrenntes Sicherheits- und Netzwerkmanagement

Das Gesamtkonzept der R&S®SITLine-Familie ermöglicht auf den verschiedensten Ebenen eine Trennung von Netzwerktransport und Sicherheitsfunktionen. Die Hoheit über das System liegt stets beim Sicherheitsmanager. Netzwerkfunktionen können aber differenziert und kontrolliert einem unabhängigen Netzwerkmanager (Lesen oder Schreiben) zur Verfügung gestellt werden. Die Kontrolle und der Besitz von Sicherheitsfunktionen und Parametern werden nicht abgegeben.

Für den Sicherheitsmanager liefert Rohde&Schwarz SIT eine Security Management Station, um die Verwaltung und Einstellung der Geräteparameter – insbesondere der Sicherheitsparameter – zu ermöglichen.

Für die Überwachung des Netzwerkstatus des R&S®SITLine ATM stehen dem Netzwerkadministrator Standarddatenbanken (MIBs) zur Verfügung, die über ein Standardprotokoll (SNMP) abgefragt und auf gängigen Managementstationen dargestellt werden können.

R&S®SITLine ATM erfüllt alle Ansprüche hinsichtlich maximaler Vertraulichkeit und Sicherheit der zu übertragenden Daten, indem es gleichzeitig die Verfügbarkeit und Überwachung einer teuren, hochwertigen IT-Verbindung sicherstellt. Somit ist eine Installation in nicht vertraulicher Umgebung möglich.



Trennung von Sicherheits- und Netzwerkmanagement

Hochwertige Datenverschlüsselung

Starke Identifikation und Key-Management

Zur Identifizierung der Geräte untereinander und gegenüber dem Sicherheitsmanagement werden Zertifikate nach X.509 unter Nutzung von elliptischen Kurven (EC) mit einer Schlüssellänge von 191 bit (entspricht etwa RSA mit 1571 bit) genutzt.

Das Sicherheitsmanagement verwaltet diese Zertifikate und erstellt Gültigkeits- und Sperrlisten. Die Zertifikate ermöglichen die eindeutige Identifizierung jedes einzelnen Gerätes. So können sich Geräte gegenüber dem Sicherheitsmanager authentisieren.

Beim Aufbau eines Kanals kommen die Zertifikate unter Nutzung des Diffie-Hellman-Verfahrens bei der Vereinbarung des symmetrischen Sitzungsschlüssels für diesen Kanal zum Einsatz. Dank hochwertiger Hardware ist dieser Prozess für jeden ATM-Kanal innerhalb von 200 ms bis 500 ms abgeschlossen. Pro Sekunde können bis zu 15 gesicherte Verbindungen aufgebaut werden.

Die Sicherheit einer laufenden Verbindung wird durch die automatische Vereinbarung neuer Sitzungsschlüssel ohne Beeinflussung des Nutzdatenstroms abgerundet.

Professionelle Online-Verschlüsselung

Zur Realisierung der Verschlüsselung kommt hochwertige Hardware zum Einsatz. Diese verschlüsselt die breitbandigen Nutzdaten durch symmetrische kryptografische Verfahren. Neuesten Erkenntnissen und Anforderungen entsprechend werden der TDES oder AES als Standardlösung angeboten. Ferner lassen sich kundenspezifische Lösungen vereinbaren. Der Einsatz weiterer Standardalgorithmen wie auch bewährter proprietärer Lösungen ist möglich.

Anwendungspezifische Verschlüsselungsmodi

Es liegt in der Natur der Verschlüsselung, dass Übertragungsfehler (Bitfehler oder Bitverluste) vervielfältigt werden können. Jeder zu übertragende Service reagiert auf diese Fehler anders:

- Sprache fordert kurze Übertragungszeiten bei kontinuierlichem Datenfluss, ist aber tolerant bezüglich sporadischer Bitfehler
- IP-Daten sind weniger anspruchsvoll bezüglich der Zeit, dafür aber empfindlicher gegen Übertragungsfehler und deren Fortpflanzung über Blockgrenzen hinaus

Diesen unterschiedlichen Bedingungen wird die Verschlüsselung durch R&S®SITLine ATM gerecht, indem verschiedene Verschlüsselungs- und Betriebsmodi zur Auswahl stehen. Es kann – je nach Verbindungsklasse – zwischen ECB (Electronic Code Book) und CBC (Cipher Block Chaining) gewählt werden. Dadurch lässt sich der Einfluss von Übertragungsfehlern entsprechend den Anforderungen der Anwendung minimieren.

Nutzerspezifische Parameter und Rechte

Obgleich die Chiffrierung der Daten im R&S®SITLine ATM beginnt und endet, reicht die Identifizierung und Authentisierung der zu sichernden Verbindungen über diesen Bereich hinaus. Über das Sicherheitsmanagement werden individuelle oder gruppenbasierte Sicherheitsbeziehungen und Verbindungsrechte für ATM-Endanwender/-Geräte definiert. Die an dem Aufbau der Verbindungen beteiligten R&S®SITLine ATM prüfen diese Rechte und bauen entsprechend den Sicherheitsvorgaben die geforderten Verbindungen auf oder lehnen diese ab.

Unabhängige gesicherte Konfiguration

Sichere Speicherung von Parametern (Tamper Resistant)

R&S®SITLine ATM bietet zusätzlichen passiven Schutz der Sicherheitsfunktionen. Alle sicherheitssensitiven Konfigurationsdaten der Geräte sind so abgelegt, dass sie nicht auslesbar sind und gelöscht werden, sobald versucht wird, das Gerät zu öffnen. Das Gerät ist dann im Zustand „produziert" und muss neu initialisiert werden. Das Löschen erfolgt auch im abgeschalteten Zustand des Gerätes.

Im Falle einer längeren Außerbetriebnahme des Gerätes werden die Sicherheitsdaten nach spätestens 48 Stunden ebenfalls automatisch gelöscht.

Gerätekonfiguration in Nutzerhand

R&S®SITLine ATM wird ohne vordefinierte Parameter ausgeliefert. Einzig die erforderlichen Algorithmen sind in der Hardware des Systems integriert. Eine vollständige Entkopplung von Hersteller und Anwender ist somit gegeben.

Alle Sicherheitsparameter werden vom Nutzer unabhängig über das Sicherheitsmanagement erzeugt und definiert. Die Inbetriebnahme des R&S®SITLine ATM erfolgt in mehreren Stufen:

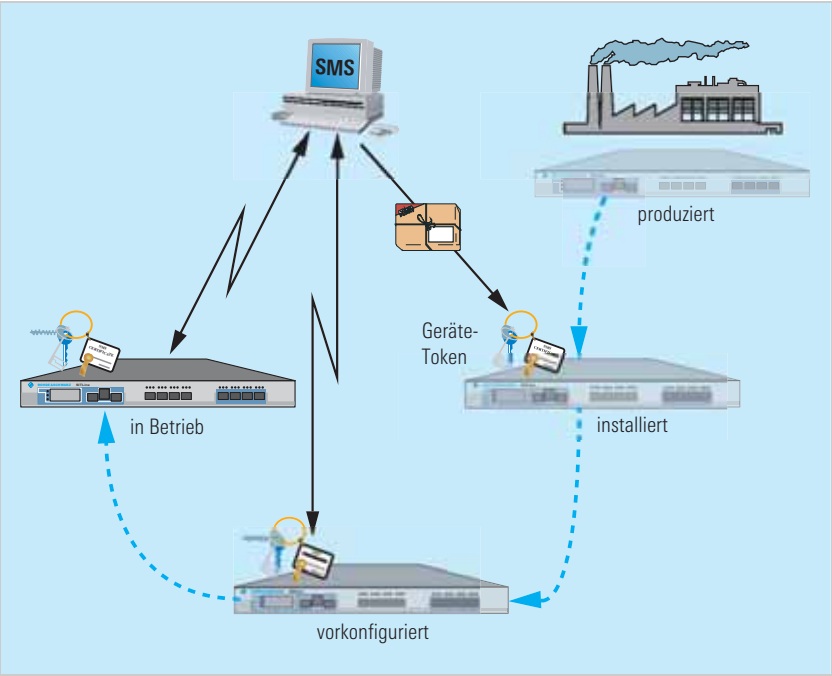
- Produziert – das Gerät ist zur Auslieferung durch den Hersteller bereit
- Installiert – das Gerät ist vor Ort physikalisch installiert, die Kabel sind angeschlossen
- Vorkonfiguriert – die Basisdaten wurden vom Sicherheitsmanagement definiert und konfiguriert sowie per Smart Token in die Geräte übertragen
- In Betrieb – das Gerät hat sich online an der Sicherheitsmanagement-Station angemeldet und alle weiteren Konfigurationsdaten erhalten

Dieses schrittweise Vorgehen gewährleistet die unabhängige und souveräne Kontrolle durch den Eigentümer.

Sicherer Transport der Basisdaten per Smart Token

Basierend auf moderner, hoch zertifizierter SmartCard-Technologie im USB-Token werden die Basisdaten von der Sicherheitsmanagement-Station zum Gerät vor Ort transportiert. Zur Datenübernahme im Gerät sind der USB-Token mit SmartCard, Nutzerkennung des lokalen Managers und ein dazugehöriges Passwort erforderlich. Die für den vollen Betrieb notwendigen Daten holt sich das Gerät online, indem es sich beim Sicherheitsmanagement authentisiert und anmeldet.

Der Token wird dann abgenommen und sicher aufbewahrt. Er kann im Havariefall das betreffende Gerät neu initialisieren. Es ist dabei vom Sicherheitsmanager grundlegend festzulegen, ob nur das jeweilige Gerät (Seriennummer) oder auch Ersatzgeräte mit gleicher Konfiguration neu initialisiert werden können.



Die Zustände des Gerätes von der Produktion bis zum vollen Betrieb

Glossar

AAL – ATM Adaptation Layer	ATM-Zwischenschicht zur Anpassung der zu übertragenden Daten nach ihren Anforderungen und Besonderheiten über ATM-Netze. Es gibt die Varianten 1, 2, 3/4 und 5.
AES – Advanced Encryption Standard	Seit 2001 aus einer internationalen Ausschreibung hervorgegangener neuer moderner Blockalgorithmus mit Schlüssellängen von 128 bit, 192 bit und 256 bit.
Algorithmus (Verschlüsselungsalgorithmus)	Vorschrift zur Ausführung mathematischer Operationen unter Nutzung mathematisch ungelöster Probleme oder nicht rückverfolgbarer Operationen zur Verschlüsselung von Daten.
ATM – Asynchronous Transfer Mode	Serielle Übertragungstechnik für eine große Anzahl logischer Kanäle, die Daten in Paketen mit einer festen Länge von 53 byte (= Zellen) und einer zugesicherten Verbindungsqualität überträgt. Die Übertragungsgeschwindigkeit ist nach oben nicht beschränkt (gegenwärtig realisiert: bis zu 2,4 Gbit/s).
Betriebsmodus	Art der Anwendung eines Algorithmus auf Datenströme. Dabei sind Aspekte der Übertragungsfehler wie auch der Angriffsmöglichkeiten und der Synchronisation von Ent- und Verschlüsselung zu berücksichtigen.
Blockalgorithmus	Verschlüsselungsalgorithmus, der die Daten in Blöcken als kleinste Eingabeeinheit bearbeitet. In der Regel sind Ein- und Ausgabeblock gleich groß.
CBC – Cipher Block Chaining	Betriebsmodus, bei dem die zu verarbeitenden Blöcke verknüpft werden. Blöcke mit gleichem Inhalt unterscheiden sich im Allgemeinen nach der Verschlüsselung (siehe auch ISO-Norm 10116).
DES – Data Encryption Standard	Älterer von IBM und dem amerikanischen NIST entwickleter Blockalgorithmus. Erster standardisierter Chiffrieralgorithmus.
ECB – Electronic Codebook	Betriebsmodus, bei dem jeder Eingabeblock separat bearbeitet wird. Gleiche Eingabeblöcke sind auch nach dem Chiffrieren gleich (siehe auch ISO-Norm 10116).
EC/ECC – Eliptic Curve/EC Cryptography	Verschlüsselungsverfahren mit asymmetrischen Schlüsseln, basiert auf elliptischen Kurven.
MIB – Management Information Base	Standardisierte Datenbank zur Ablage von Konfigurations- und Betriebsdaten eines Gerätes.
PDH – Plesiochrone Digital Hierarchy	Rahmen (Frame)-synchrone digitale Hierarchie. Die unterste Stufe E0 arbeitet mit einer Bandbreite von 64 kbit/s. Mit Hilfe von TDM-Systemen (Time Division Multiplexing) werden über mehrere Stufen Kanäle gebündelt. In einer PDH-Struktur kann immer nur in der nächsten Ebene gebündelt oder entbündelt werden. Ebenen können nicht übersprungen werden.
PVC/PVP – Permanent Virtual Circuit/Path	Durch Kennung in den Köpfen der Informationscontainer markierter logischer Kommunikationskanal. Werden mehrere Kanäle als Bündel behandelt, bilden diese einen Pfad (path).
RSA	Nach seinen Entwicklern Rivest, Shamir, Adleman benannter asymmetrischer Algorithmus.
Schlüssel	Vom Algorithmus neben den Nutzerdaten verwendeter zweiter Eingabewert zur Ver- und Entschlüsselung dieser Nutzerdaten. Je nach Algorithmus sind Schlüssel zum Chiffrieren und Dechiffrieren gleich (symmetrisch) oder ungleich (asymmetrisch). Schlüssel ermöglichen die Übertragung vertraulicher Informationen und sind daher geheim zu halten.
SDH – Synchronous Digital Hierarchy	Standard zur synchronen Übertragung von Daten mit hoher Geschwindigkeit und umfangreichen Mechanismen für die Ausfallsicherheit eines SDH-Netzes. Im Unterschied zu PDH-Strukturen können hier Kanäle direkt in allen höheren Hierarchieebenen eingefügt und extrahiert werden.
Sicherheitsmanagement	Hard- und Software, die durch den Sicherheitsmanager zur Verwaltung und Überwachung der Sicherheitssysteme nach vorgegebenen Regeln befähigt wird.
Sicherheitsmanager	Für die Konfiguration und Bedienung der Sicherheitselemente einer IT-Infrastruktur verantwortliche Person.
SMS – Security Management Station	Hard- und Software zur Konfiguration, Verwaltung und Überwachung der IT-Sicherheitssysteme.
SNMP – Simple Network Management Protokoll	Standardisiertes Protokoll zur Kommunikation einer Netzwerkmanagement-Station mit der MIB eines Gerätes.
SONET	Nordamerikanischer Standard zu SDH. Es bestehen geringfügige Unterschiede zum SDH.
SVC/SVP	Signalisierte, nicht permanente logische Verbindungen oder Pfade (siehe PVC).
TDES – Triple DES (Data Encryption Standard)	Älterer, vom AES abgelöster Blockalgorithmus, bei dem jeder Block den Kernalgorithmus DES dreimal durchläuft.
UNI – User Network Interface	Umfasst eine Summe von Standards, die den Übergabepunkt zwischen ATM-Übertragungsnetz und ATM-Kunden beschreiben.
X.509 Zertifikat	ITU-T-Standard, der die Form und den Inhalt von kryptografisch erstellten Zertifikaten zur Authentisierung von Kommunikationspartnern beschreibt.

Printed in Germany (bb)

ROHDE&SCHWARZ

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