Datenblatt

Version 01.00

Februar 2006

R&S®LineCrypt L

IP-Verschlüsselung im Internet und LAN

- 256 Tunnel gleichzeitig
- Online-Nutzdatenverschlüsselung mittels IDEA (128 bit)
- RSA-Schlüsselgenerierung (1024 bit) im kundeneigenen Trust-Center
- VS-NfD zugelassen

ROHDE&SCHWARZ

Das R&S®LineCrypt L dient der geschützten Datenübertragung über IP-Netze auf Ethernetbasis. Es stellt das Bindeglied zwischen einem geschützten internen und einem ungeschützten externen Netz dar. Das R&S®LineCrypt L basiert auf IP-Kommunikation, das heißt, es verhindert die Weiterleitung aller anderen Protokolle, beispielsweise IPX, zwischen interner und externer Seite. Die verschlüsselten Daten überträgt es durch einen IP-Tunnel. Auf diese Weise wird mit zwei oder mehreren R&S®LineCrypt L in einem ungeschützten Netz ein geschütztes Virtual Private Network (VPN) errichtet.

Management

Das R&S®LineCrypt L lässt sich durch Anpassung seiner Konfigurationsdaten sehr variabel einstellen. Die Konfiguration des Gerätes wird über sogenannte Managementobjekte vorgenommen, die eine Rechtedatei für das Gerät enthalten. Diese können entweder lokal oder mit Hilfe des Remote-Managements in das Gerät eingespielt werden. Die Rechtedatei enthält Konfigurationsdaten für den Betrieb des Gerätes, die im Folgenden beschrieben werden.

Gerätespezifische Parameter

- Passwort
  - Schutz vor unbefugter Änderung der Gerätekonfiguration
- Security Policy-Parameter
  - Einrichtung von bis zu 1024 Policies
  - Festlegung des lokalen und entfernten IP-Adressbereiches
  - Behandlung der zu übertragenden Pakete:
    verschlüsselt
    unverschlüsselt
    weiterleiten
    verwerfen
- Ethernet-Parameter
  - Verbindungsgeschwindigkeit und Duplex-Modus
- TCP/IP-Parameter
  - IP-Adressen, Verzeichnisdienst
- SNMP-Parameter
  - Geräteabfrage mittels SNMP (Simple Network Management Protocol)
- Logging-Funktion
  - für Fehlersuche vorgesehen und im Normalbetrieb deaktiviert

Berechtigungslisten

- Alias-Liste
  - Interne Zuordnung der Namen von Kommunikationspartnern zu den Zertifikats-ID
- Benutzergruppenliste
  - Festlegung der Gruppenzugehörigkeit
- Black-List
  - Ausschluss von Teilnehmern
- White List
  - Festlegung der Teilnehmer, die ausdrücklich befugt sind, mit dem Inhaber des R&S®LineCrypt verschlüsselt zu kommunizieren
- CA-Liste
  - Festlegung der akzeptierten Zertifikate
- Systemverwalterliste

„Personalisierte Karten“

Sicherheitsrelevante Daten werden ausschließlich auf den Chipkarten gespeichert. Das Gerät funktioniert nur mit eingesteckter Karte. Die Karten werden von den Benutzern selbst verwaltet und beim Kunden mit folgenden Sicherheitsparametern ausgestattet:

- Zertifikate vom R&S®LineCrypt CA
- Gerätezugehörigkeit
- Public-Key des Kunden
- Bindung an bestimmte Geräte

Die Chipkarte erzeugt und wählt rein zufällig den 128 bit breiten Sitzungsschlüssel. Die Karten inklusive Software wurden nach ITSEC mit E4 hoch evaluiert.

R&S®LineCrypt CA – kundeneigene Zertifizierungsinstanz

Der Kunde kann mit Hilfe des R&S®LineCrypt CA seinen eigenen RSA-Schlüssel generieren und verwenden, um Authentisierungsfunktionen im R&S®LineCrypt L auszuführen. Damit hat er die Möglichkeit, Smart Cards zum Anwenden und Speichern geheimer Schlüssel zu personalisieren.

Weitere Funktionen

Neben der Generierung und Personalisierung von Smart Cards leistet das R&S®LineCrypt CA folgende sicherheitsrelevante Aufgaben:

- CA-Card generieren (Zertifikate von User Cards signieren)
- User Card freischalten
- Zweites Zertifikat signieren (bei Bedarf)
- CA-Liste erstellen
- Gleichzeitiges Generieren mehrerer Karten
- Importieren von RSA-Schlüsseln
- Generieren von RSA-Schlüsselpaaren für die CAs und User Cards

CA-Handling

Der Anwender entscheidet, welche Zertifikate auf die User Card geschrieben werden. Dank dieser Funktion lassen sich geschlossene Anwendergruppen erstellen.

Anhand der auf den User Cards enthaltenen Zertifikate und Signaturen erfolgt eine beidseitige Authentisierung.

Die Aufgaben umfassen:

- Lesen/Anzeigen der lesbaren Informationen auf den User Cards
- Anzeigen von Datenbanken mit Filterfunktionen
- Klonen der CA-Card als Backup
- Export von User-Schlüsseln, falls diese während der Personalisierung gespeichert wurden

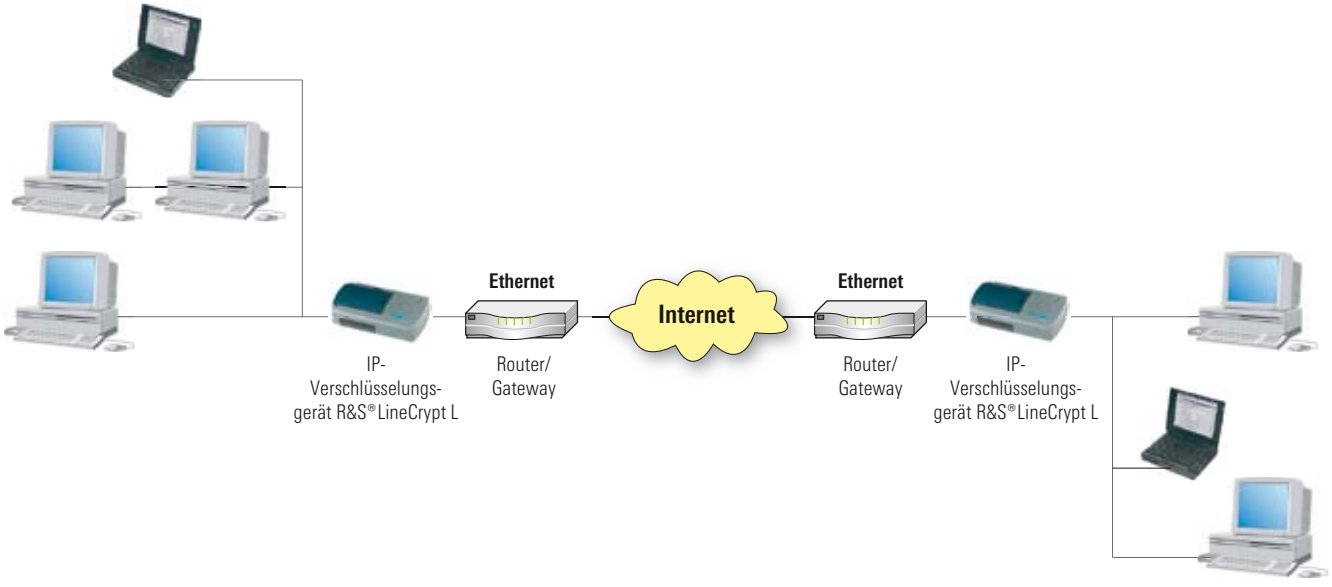
Technische Daten

Leitungsversion	
Ethernetschnittstelle	2 × 10BaseT UTP 10 Mbit/s, Halbduplex/Vollduplex Cu Western RJ-45-WE8/8-Buchse
Netzwerkprotokolle	IP, IPSec (ESP, Protokoll 50) ICMP (Fehlerhandling, Protokoll 1)
PC/Managementschnittstelle	Serielle V.24 Mini DIN 8 115,2 kbit/s
Sicherheitsmechanismen	
Gerät	Evaluiert und zertifiziert nach ITSEC, E3 hoch
Authentisierung	Patentiertes Authentisierungs-protokoll 1024 bit RSA RSA-Schlüssel/Zertifikate auf Smart Card X.509v3
Nutzdaten	128 bit IDEA™ Software, IPSec-Protokoll Session-Key-Generierung mittels eingebauter Smart Card Tunnel Modus
Kartenspeicher	3DES RipeMD160 – Hash
Karte	
TCOS	Evaluiert nach ITSEC: E4 hoch (Hard- und Software)

Allgemeine Daten	
Stromversorgung	Eingebautes Schaltnetzteil: 110 V bis 230 V, 50 Hz bis 60 Hz, 5 VA
Abmessungen	200 mm × 115 mm × 48 mm
Systemvoraussetzungen	Windows 2000/XP Ethernet
Sprachauswahl	Deutsch und Englisch
Zulassung	NfD (Z 0108-1) – ergänzt 2004

Bestellangaben

Bezeichnung	**Typ**	**Bestellnummer**
IP-Verschlüsselung	R&S®LineCrypt L	3554.9722.02
Lieferumfang		
R&S®LineCrypt L inkl. LCC-Konfigurations-software-CD		3554.9722
User Cards		3554.9768
CA-Cards		3554.9816
Betriebsanleitung CD		3554.9716
Optional		
R&S®LineCrypt CA		3554.9739
Remote Management		3554.9151



Weitere Informationen unter
www.rohde-schwarz.com
(Suchbegriff: LineCrypt)

ROHDE&SCHWARZ

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