Data sheet

Version
01.00

February
2006

R&S®LineCrypt L

IP encryption on the Internet and LANs

- 256 simultaneous tunnels
- Online payload encryption via IDEA (128 bits)
- RSA key generation (1024 bits) in customer-defined trust center

ROHDE&SCHWARZ

The R&S®LineCrypt L is used to protect data transmission over IP networks based on Ethernet. It represents the link between a protected internal and an unprotected external network. The R&S®LineCrypt L is based on IP communications, i.e. it prevents all other protocols such as IPX from being transferred between the internal and external network environments. The encrypted data is transmitted through an IP tunnel. Thus, a protected virtual private network (VPN) can be set up within an unprotected network by using two or more R&S®LineCrypt L devices.

Management

The R&S®LineCrypt L can be adapted to a wide variety of conditions by changing its configuration data. The device is configured by means of management objects, which contain a rights file for the device. The management objects can be loaded on the device either locally or by using the remote management tool. The rights file contains configuration data for operating the device. The data is described below.

Device-specific parameters

- Password
  - Protection against unauthorized changes in the device configuration
- Security policy parameters
  - Creation of up to 1024 policies
  - Definition of the local and remote IP address range
  - Handling of the packets to be transmitted:
    Encrypted
    Plain
    Transfer
    Deny
- Ethernet parameters
  - Connection speed and duplex mode
- TCP/IP parameters
  - IP addresses, directory service
- SNMP parameters
  - Device querying via SNMP (simple network management protocol)
- Logging function
  - Provided for troubleshooting; deactivated during normal operation

Access rights lists

- Alias list
  - Internal assignment of the names of communicating parties to the certificate IDs
- User groups list
  - Definition of user group characteristic
- Black list
  - Excluded users
- White list
  - Specification of users expressly authorized to communicate in encrypted format with the owner of the R&S®LineCrypt
- CA list
  - Definition of accepted certificates
- System administrator list

"Personalized cards"

Security-relevant data is stored exclusively on the chip cards. The device will not function unless the card is inserted. The cards are managed by the individual users and provided with the following security parameters by the customer:

- Certificates of the R&S®LineCrypt CA
- Device group
- Customer's public key
- Assignment to specific devices

The chip card generates and selects the 128-bit session key on a purely random basis. The cards, including the software, received an ITSEC E4 High evaluation.

R&S®LineCrypt CA – customer-defined trust center

The R&S®LineCrypt CA enables customers to generate and use their own RSA key for performing authentication functions on the R&S®LineCrypt L. Thus, customers can personalize smart cards for using and storing secret keys.

Other functions

In addition to generating and personalizing smart cards, the R&S®LineCrypt CA performs the following security-relevant tasks:

- Generates CA cards (signs certificates of user cards)
- Activates user cards
- Signs a second certificate (if necessary)
- Generates a CA list
- Generates multiple cards concurrently
- Imports RSA keys
- Generates RSA key pairs for the CAs and user cards

CA handling

The individual user determines which certificates are written to the user card. This function makes it possible to create closed user groups.

Authentication for both ends is carried out by means of the certificates and signatures on the user cards.

The tasks include the following:

- Read/display the readable information on the user cards
- Display databases with filter functions
- Clone the CA card as backup
- Export user keys if stored during personalization

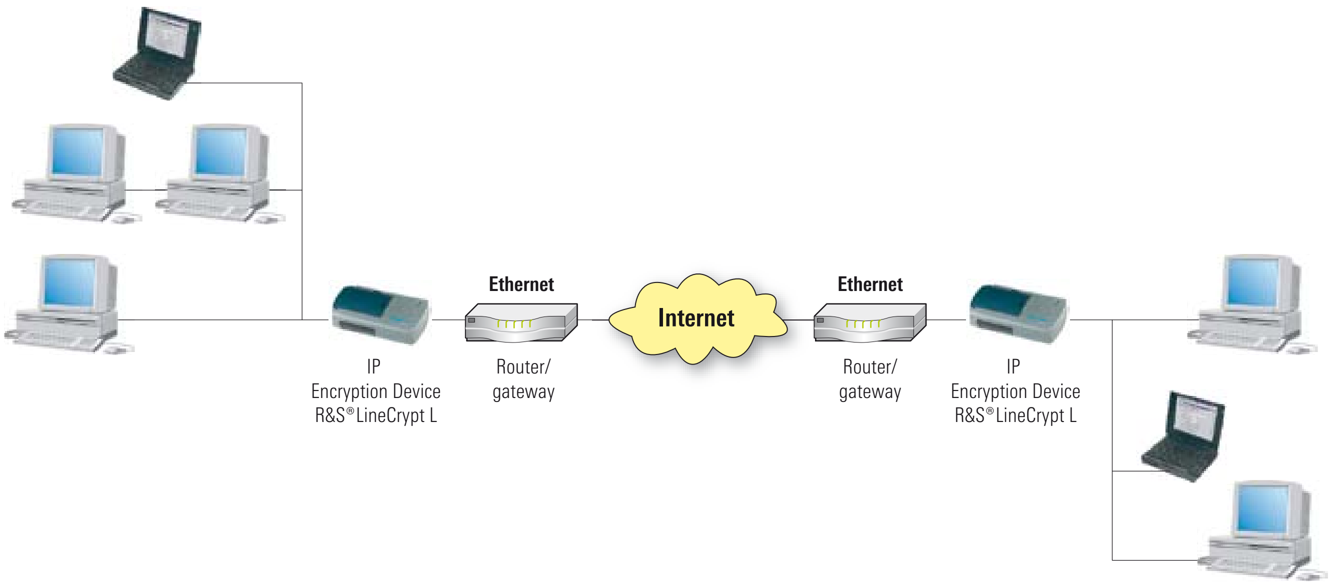
Specifications

Cable version	
Ethernet interface	2 × 10BaseT UTP 10 Mbit/s, half-duplex/full-duplex Cu Western RJ-45 WE8/8 socket
Network protocols	IP, IPSec (ESP, protocol 50) ICMP (error handling, protocol 1)
PC/management interface	serial V.24 mini DIN 8 115.2 kbit/s
Security mechanisms	
Device	evaluated and certified ITSEC E3 High
Authentication	patented authentication protocol 1024-bit RSA RSA keys/certificates on smart card X.509v3
Payload	128-bit IDEA ™ software, IPSec protocol session key generation via smart card tunnel mode
Card memory	3DES RIPEMD160 hash
Card	
TCOS	evaluated ITSEC E4 High (hardware and software)

General data	
Power supply	integrated switching power supply: 110 V to 230 V, 50 Hz to 60 Hz, 5 VA
Dimensions	200 mm × 115 mm × 48 mm
System requirements	Windows 2000/XP Ethernet
Available languages	English and German

Ordering information

Designation	**Type**	**Order No.**
IP Encryption	R&S®LineCrypt L	3554.9722.02
Equipment supplied		
R&S®LineCrypt L incl. LCC configuration software CD		3554.9722
User cards		3554.9768
CA cards		3554.9816
Operating instructions CD		3554.9716
Options		
R&S®LineCrypt CA		3554.9739
Remote management		3554.9151



More information at
www.rohde-schwarz.com
(search term: LineCrypt)

ROHDE&SCHWARZ

www.rohde-schwarz.com
Europe: +49 1805 12 4242, customersupport@rohde-schwarz.com
USA and Canada: 1-888-837-8772, customer.support@rsa.rohde-schwarz.com
Asia: +65 65 130 488, customersupport.asia@rohde-schwarz.com

PD 5213.6535.32 · R&S®LineCrypt L · Version 01.00 · February 2006 · Data without tolerance limits is not binding · Subject to change