Data sheet

Version 02.00

January 2004

R&S® SITMinisafe2

Encryption of modem and radio links

- Connected between modem and PC (RS-232-C COM interface)
- Automatic key generation for secure data transmission
- Integrated high-quality physical random number generator
- Powerful encryption algorithm
- Simple configuration via terminal program

ROHDE&SCHWARZ

The R&S®SITMinisafe2 is connected between the PC (COM interface) and the modem. Device configuration and key management can be performed via any terminal program, which makes the device independent of the user platform and operating system. Data is automatically encrypted before transmission and decrypted by a second R&S®SITMinisafe2 at the receive end. The system has been designed based on German and European information technology security (ITSEC) criteria.

Performance and functions

The device automatically encrypts and decrypts transmitted data up to 115200 bit/s in full-duplex mode. The rate of the incoming data from the COM interface is automatically detected in a range from 1200 bit/s to 115200 bit/s. In addition, a fixed transmission rate can be set. The device supports hardware handshake and the standard protocol with 8 bits, no parity and 1 stop bit.

The R&S®SITMinisafe2 can be used immediately, i.e. no expertise in cryptology is required. The entire crypto process (encryption algorithm, key management and safety functions) automatically ensures high-security data transmission and the protection of sensitive data. A built-in physical random number generator automatically creates data transmission keys of utmost quality. It is also possible to transmit plain data.

Encryption algorithm

Encryption is implemented by means of a powerful, highly secure algorithm using a stream cipher (RC4-compatible). The key length is 128 bits.

Key management

Various keys are available to protect the data transmitted via modem as well as all sensitive information in the device:

- The session key (128 bits) encrypts the data to be transmitted. For each call, a new session key is created by the random number generator and quality-tested.
- The ComSecKey (CSK, 128 bits) encrypts the session key for transmission to the peer station. Encryption takes place during call setup. All R&S®SITMinisafe2 devices taking part in a communication must use an identical CSK. The character string is stored in encrypted form and can be varied only upon entering a personal identification number (PIN). The PIN can be changed; it is likewise stored in the device in encrypted form.
- The device key (128 bits) encrypts all sensitive data in the device. It is a sequence of random numbers unique to each device and created with a random number generator during production. The device key is stored in the microcontroller such that it cannot be read and is protected against manipulation.

Certified Quality System
ISO 9001
REG. NO CERT-01 100 025007

General data

Power supply	from plug-in power supply (6 V to 9 V, 70 mA)
Dimensions	100 mm × 55 mm × 16 mm
System requirements	COM interface (RS-232-C), terminal program
Language options	English and German

Ordering information

R&S®SITMinisafe2	3534.4360
Equipment supplied	R&S®SITMinisafe2, power supply, connecting cable, operating manual

ROHDE&SCHWARZ

www.sit.rohde-schwarz.com

PD 0758.0751.32 · R&S®SITMinisafe2 · Version 02.00 · January 2004 · Data without tolerance limits is not binding · Subject to change