Datenblatt

Version 02.00

November 2003

R&S®SITMinisafe2

Verschlüsselung von Modem- und Funkverbindungen

- Zwischen Modem und PC geschaltet (COM-Schnittstelle: RS-232-C)
- Automatische Generierung hochwertiger Schlüssel für die Datenübertragung
- Integrierter physikalischer Zufallsgenerator von höchster Qualität
- Anerkannter und leistungsfähiger Verschlüsselungsalgorithmus
- Einfache Konfiguration über ein beliebiges Terminalprogramm

ROHDE&SCHWARZ

R&S®SITMinisafe2 wird zwischen PC (COM-Schnittstelle) und Modem geschaltet. Durch Konfiguration und Schlüsselverwaltung über ein beliebiges Terminalprogramm ist das Gerät unabhängig von Anwenderplattform und Betriebssystem. Alle zu übertragenden Daten werden automatisch verschlüsselt und in der ebenfalls mit R&S®SITMinisafe2 ausgerüsteten Gegenstelle entschlüsselt. Grundlagen für Entwurf und Entwicklung des Systems sind deutsche und europäische Kriterien für die Sicherheit in der Informationstechnik (ITSEC).

Leistungs- und Funktionsparameter

Das Gerät verschlüsselt und entschlüsselt automatisch die übertragenen Daten bis zu einer Geschwindigkeit von 115200 bit/s im Vollduplex-Modus. Die Verbindung zur COM-Schnittstelle verfügt über eine automatische Erkennung der Übertragungsgeschwindigkeit von 1200 bis 115200 bit/s. Die Übertragungsgeschwindigkeit kann auch fest voreingestellt werden. Unterstützt werden Hardware-Handshake und das Standardprotokoll 8 bit, keine Parität, 1 Stoppbit.

R&S®SITMinisafe2 lässt sich auch ohne spezifische Kenntnisse auf dem Gebiet der Kryptologie sofort einsetzen. Das implementierte Verfahren (Verschlüsselungsalgorithmus, Schlüsselmanagement und Sicherheitsfunktionen) regelt automatisch die hochsichere Übertragung der Daten und den Schutz sicherheitsrelevanter Daten mit R&S®SITMinisafe2. Die notwendigen Schlüssel für die Datenübertragung werden automatisch über den integrierten physikalischen Zufallsgenerator in höchster Qualität erzeugt. Bei Bedarf können auch Daten im Klartext übertragen werden.

Verschlüsselungsalgorithmus

Für die Verschlüsselung kommt ein leistungsfähiger und hochsicherer Algorithmus mit einer Stromchiffre (RC4-kompatibel) zum Einsatz. Die Schlüssellänge beträgt 128 bit.

Schlüsselmanagement

Die Daten bei der Modemübertragung und alle sensiblen Informationen im Gerät werden mit den folgenden Schlüsseln gesichert:

- Der Session-Key (128 bit) verschlüsselt die zu übertragenden Daten und wird per Zufallsgenerator vor jeder Verbindungsaufnahme neu erzeugt und auf Qualität geprüft
- Der ComSecKey (CSK, 128 bit) verschlüsselt den Session-Key bei seiner Übertragung zur Gegenstelle während der Verbindungsaufnahme. Der CSK muss bei allen kommunizierenden R&S®SITMinisafe2-Geräten identisch eingestellt werden. Die Zeichenfolge wird verschlüsselt gespeichert und lässt sich nur nach einer PIN-Eingabe variieren; die PIN kann geändert werden; sie ist ebenfalls im Gerät verschlüsselt
- Der Device-Key (128 bit) verschlüsselt alle sicherheitsrelevanten Daten im Gerät. Der für jedes Gerät individuelle Zufallswert wird per Zufallsgenerator bei der Fertigung erzeugt; er ist im Mikrocontroller so gespeichert, dass er weder ausgelesen noch manipuliert werden kann

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

Allgemeine Daten

Stromversorgung	Über Steckernetzteil (6 V bis 9 V, 70 mA)
Abmessungen	100 mm x 55 mm x 16 mm
Systemvoraussetzungen	COM-Schnittstelle (RS-232-C) Beliebiges Terminalprogramm
Sprachauswahl	Deutsch und englisch

Bestellangaben

R&S®SITMinisafe2	3534.4360
Lieferumfang	R&S®SITMinisafe2, Netzteil, Verbindungskabel, Betriebsanleitung

ROHDE&SCHWARZ

Rohde&Schwarz SIT GmbH · Am Studio 3 · 12489 Berlin
Telefon (030) 65884-223 · Fax (030) 65884184 · E-Mail: contact@sit.rohde-schwarz.com · www.sit.rohde-schwarz.com

PD 0758.0751.31 · R&S®SITMinisafe2 · Version 02.00 · November 2003 · Daten ohne Genauigkeitsangabe sind unverbindlich · Änderungen vorbehalten

Printed in Germany (Pe bb)