ELCRODAT 5-4

Highly secure voice and data communications in digital and analog networks

Data Sheet | 02.02

75 Years of Driving Innovation

ROHDE&SCHWARZ

ELCRODAT 5-4
At a glance

The ELCRODAT 5-4 (ED5-4) is used by military organizations and government authorities for the encrypted transmission of voice and data signals in analog and ISDN networks. It provides secure end-to-end encryption, which protects messages against eavesdropping and manipulation attacks along the entire transmission path.

Existing encryption devices have been used exclusively either in analog telecommunications networks or in ISDN networks and have been interoperable only with each other. The ED5-4, however, has two interfaces (S_0 and a/b), which allows it to operate in both networks and moreover enables the secure exchange of information across networks.

The ED5-4 uses a tried-and-tested NATO algorithm for encryption. Plus, it has an expansion slot that makes it possible to adapt the cryptological capabilities of the device to new or additional requirements.

Key facts

- Encrypted operation possible across networks
- Interoperable with existing voice encryption devices (ELCROVOX 1-4D, STU-IIB, TCE 500/B)
- Encryption keys can be loaded manually via the standardized NATO fill interface or provided automatically via a key distribution center
- Approved for all national and NATO levels of classified information
- Access to all cryptological functions with personal chip card and PIN code

ELCRODAT 5-4
Benefits and key features

Cross-network operation
- Analog networks (a/b)
- ISDN (S_0)
- Satellite connections

▷ page 4

Different modes selectable
- CRYPTO: variables loaded via a key distribution center (KDC)
- SPECIAL KEY: variables loaded via key fill device
- NET KEY: variables loaded via key fill device (only in ISDN networks)

▷ page 5

Ease of operation
- Intuitive operation
- All settings menu-driven via keypad
- Easy-to-understand, straightforward display texts on large LCD (¼ VGA graphics)
- All ISDN features
- Convenient phonebook

▷ page 5

State-of-the-art key management
- Automatically from a KDC
- Locally via the standardized NATO key fill interface using corresponding fill devices (e.g. DTD, KSP1 or KLL1)

▷ page 6

Comprehensive security measures
- Tempest-proof design
- Emergency zeroizing
- Tamper protection
- Protected access to all cryptological functions with personal chip card and PIN code

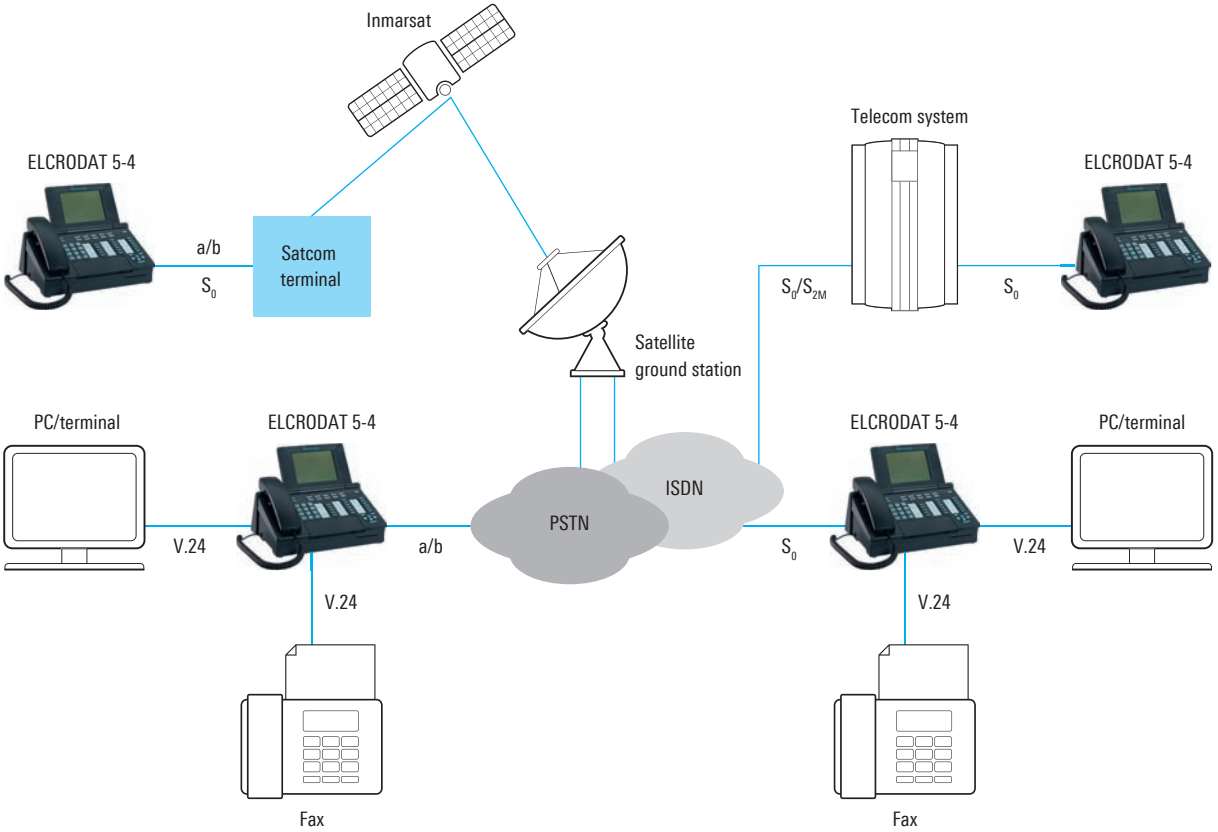
Future-ready
- Expansion slot for a second crypto module to adapt the cryptological capabilities of the ED5-4 to new or additional requirements
- Encrypted software download for additional functionality
- Secure communications interoperability protocol (SCIP) in accordance with SCIP-231 implemented as prototype

▷ page 7

Cross-network operation

Existing encryption devices have been used exclusively either in analog telecommunications or ISDN networks and have been interoperable only with each other. The ED5-4, however, has two interfaces (S_0 and a/b), which allows it to operate in both networks and moreover enables the secure exchange of information across networks. The ED5-4 can also be used in satellite connections.

ELCRODAT 5-4 and its wide range of applications



Different modes selectable

The ED5-4 can set up voice and data connections in PLAIN or CRYPTO mode. Users can switch from PLAIN to CRYPTO during a connection, but not vice versa. Security considerations prohibit the switching from CRYPTO to PLAIN once a connection has been established.

For security reasons, voice and data in the CRYPTO modes (in ISDN) will not be transmitted until the connection between the crypto devices has been set up and crypto-synchronization has been completed successfully.

In analog telephone networks, encrypted data can be transmitted synchronously and asynchronously between two ED5-4 devices at a rate of 9600 bit/s. In ISDN networks, channel bundling makes it possible to achieve synchronous data rates of up to 128 kbit/s. The data terminal (e.g. a PC or fax machine) is connected via the V.24 interface on the ED5-4.

Ease of operation

Intuitive operation

The ED5-4 is very user-friendly. All settings are menu-driven and selected via the keypad. The current device status and the sequence of operating steps are displayed on a large LCD (¼ VGA graphics) and are largely self-explanatory. They are also indicated via LEDs.

The ergonomic graphics display system includes the following features:

- Optical partitioning (frames, dividing lines, info line, status display, softkeys)
- Optical representation (different font sizes, blinking cursor, inverted display)

ISDN features

When used in an ISDN network, the ED5-4 provides all ISDN convenience features such as three-party conference calls, callback and call diversion, but only in PLAIN mode.

Additional functions

The ED5-4 has a phonebook in which up to 200 phone numbers including name, transmission mode and assigned variable memory location can be stored. Entries can be conveniently edited using the phonebook editor.

State-of-the-art key management

Encryption keys are supplied either automatically from a key distribution center (KDC) or locally via the standardized NATO fill interface using the corresponding fill devices (e.g. DTD, KSP1 or KLL1).

Key distribution center (KDC)

The KDC is a customer-end computer system that automatically supplies keys to the customer's registered subscribers.

The subscriber devices must be registered with the KDC by means of their respective subscriber IDs to enable communications in KDC mode. A unique variable (UV) stored in the KDC and the subscriber devices protects the session key, which is transmitted via the network. The session key that is requested for a subscriber connection is generated by a dedicated crypto device and sent to the calling party.

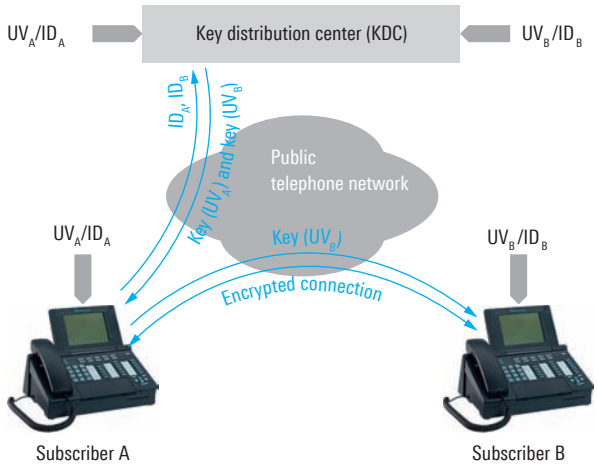
Sequence of events:

- Subscriber A dials subscriber B in CRYPTO mode (KDC mode)
- The ED5-4 autodials the KDC, transmits its own ID and the ID of the called subscriber and requests the session key
- The KDC transmits the session key for both parties to subscriber A, the session key is encrypted with the unique variables (UV) of the respective parties
- The connection to the KDC is cleared down, and the connection to subscriber B is set up automatically
- After the connection has been set up, the session key is transmitted to subscriber B
- The encrypted connection is set up after synchronization has been completed

Local provision of keys

Up to 16 black and/or red keys can be manually loaded via the DS-101/DS-102 interface. Black keys are encrypted with a special key. Red keys are unencrypted and therefore require a high level of protection.

ELCRODAT 5-4 and KDC



Provision of crypto variables by a key distribution center.

Fill devices for manually loading encryption keys.

Future-ready

The ED5-4 has an expansion slot for a second crypto module to adapt its cryptological capabilities to new or additional requirements.

Additional functions can be integrated by means of encrypted software downloads. The secure communications interoperability protocol (SCIP) in accordance with SCIP-231 has already been implemented as prototype.

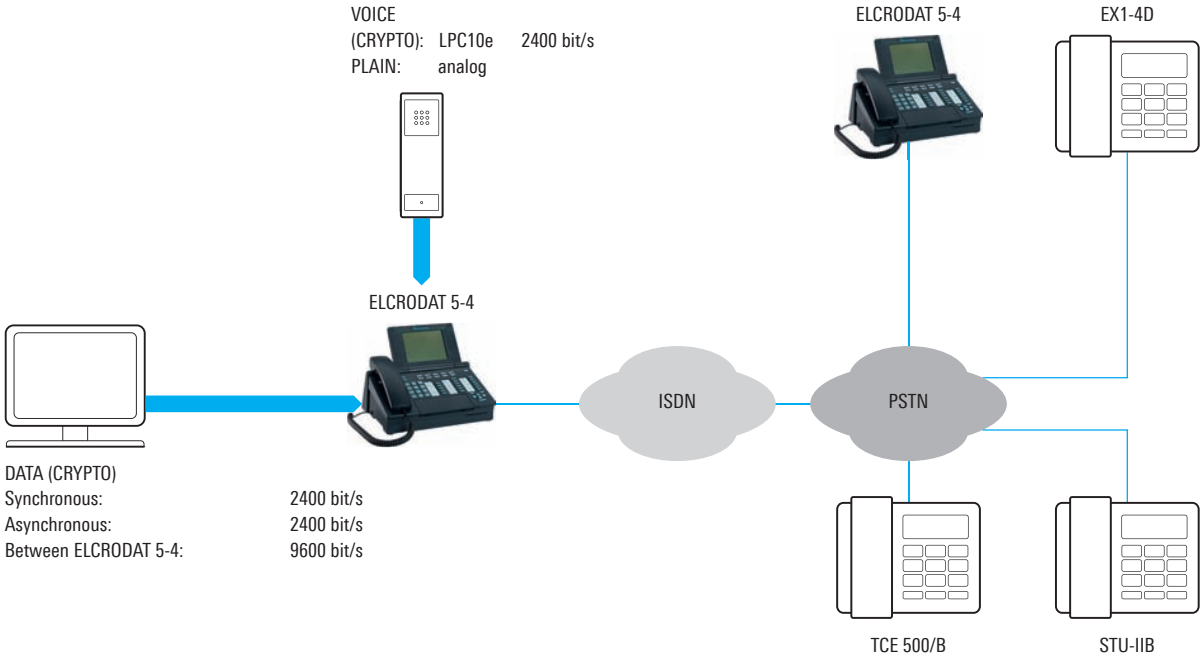
Application examples

Interoperable with existing voice encryption devices

The ED5-4 is interoperable with existing voice encryption devices in different operating modes (see table). The ELCROVOX 1-4D must have a four-wire connection when using V.26 DX; asynchronous data operation with the TCE 500/B is not possible.

Mode	Protocol	Max. data rate (bps)	Interoperable with
VOICE	V.22, 2-wire	2400	EX1-4D
	V.26, 2-wire/ 4-wire, DX and HDX	2400	EX1-4D, STU-IIB, TCE 500/B
DATA	V.22, 2-wire	2400	EX1-4D
	V.26, 2-wire/ 4-wire, DX and HDX	2400	EX1-4D, STU-IIB, TCE 500/B

Interoperable with NATO devices



Specifications

Operation	
Operating modes	
Voice	PLAIN and CRYPTO
Data	PLAIN and CRYPTO
Operation in analog network	
Network interface	two-wire interface (a/b) in line with ETSI TBR21 four-wire interface (IVSN) RJ-12 female connector
Voice coding	LPC 10E (2400 bit/s) in line with STANAG 4198
Modem method	
2400 bit/s	V.22bis, V.26
9600 bit/s	V.32
Data interface	
V.24/V.28 asynchronous	2400 bit/s or 9600 bit/s (depending on modem method)
V.24/V.28 synchronous	2400 bit/s or 9600 bit/s (depending on modem method)
Operation in ISDN	
Network interface	ISDN basic rate access (S_0) RJ-45 female connector DSS1 D channel protocol
Voice coding	voice coding in line with ITU G.711
Data interface	
V.24/V.28 asynchronous	2400 bit/s to 38400 bit/s
V.24/V.28 synchronous	2400 bit/s to 64000 bit/s
Additional interfaces	
Fill interface	DS-101, DS-102
CIK	crypto ignition key (chip card)

General data	
Operating temperature range	+5 °C to +40 °C
Storage temperature range	–20 °C to +55 °C
Radiation emission shielding/EMC	
TEMPEST	in line with SDIP-27 level A (previously AMSG 720 B)
EMC	EN 50081-1 and EN 50082-2
Dimensions (H × W × D)	approx. 195 mm × 290 mm × 260 mm (approx. 7.68 in × 11.42 in × 10.24 in)
Weight	approx. 3.5 kg (approx. 7.72 lb)
Supply voltage	24 V DC from external plug-in power supply (110 V to 230 V, 45 Hz to 66 Hz)
Power consumption	<20 VA
MTBF	>8000 h
Function test	BITE (built-in test equipment)

Ordering information

Designation	Type	Order No.
Base unit (including supplied accessories such as power cable, manual)		
ELCRODAT 5-4		3571.5115.02
Accessories supplied		
ED5-4 power supply		3571.5773.00
ED5-4 chip card		3571.5367.00
2 x RJ-45 cable, ISDN		3543.1402.00
2 x RJ-12 cable, analog		3571.1803.00
Manual		3571.5415.32
Other accessories		
Key Tape Reader	KLL1	5412.2009.02
Key Transfer Device	KSP1	5412.2150.02
ED5-4 fill cable		3571.1884.00
ODU-ODU fill cable		3571.1890.00
Phonebook software		3571.2574.00
D-Sub 25/D-Sub 9 cable		3571.1878.00

Service you can rely on

- In 70 countries
- Person-to-person
- Customized and flexible
- Quality with a warranty
- No hidden terms

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Regional contact

Europe, Africa, Middle East
+49 1805 12 42 42* or +49 89 4129 137 74
customersupport@rohde-schwarz.com
North America
1-888-TEST-RSA (1-888-837-8772)
customer.support@rsa.rohde-schwarz.com
Latin America
+1-410-910-7988
customersupport.la@rohde-schwarz.com
Asia/Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

Certified Quality System
ISO 9001
DQS REG. NO 1954 QM

Certified Environmental System
ISO 14001
DQS REG. NO 1954 UM

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin | +49 30 65884-223 | Fax +49 30 65884184
E-Mail: info.sit@rohde-schwarz.com | www.sit.rohde-schwarz.com

www.rohde-schwarz.com

PD 0758.1564.32 | Version 02.02 | February 2009 | ELCRODAT 5-4
Data without tolerance limits is not binding | Subject to change

*0.14 €/min within German wireline network; rates may vary in other networks (wireline and mobile) and countries.