CRYPTO NEWS I/2004

Launch of new encryption devices

The ELCRODAT 4-2 and MMC3000 have been developed for all branches of the armed and paramilitary services.

The ELCRODAT 4-2 has been designed exclusively for use in NATO countries. The MMC3000 can also be implemented in countries that are poised to join NATO as well as other countries with high-grade encryption system requirements.

Both devices enable encrypted voice and data transmission in fixed networks over HF and VHF/UHF radio links. The instruments include three main function blocks:

- "Plain" signal processing (digitization of voice signals, data processing)
- Encryption
- "Crypto" signal processing (transmitted encrypted signals over a modem)

With the exception of the crypto module, the hardware and the processes are virtually identical for both device versions. Highly flexible, identically designed modules are implemented both at the terminal and the transmission end. The module functions are managed by cryptologically secured, reprogrammable software that can be upgraded at any time. An MMC3000 can be converted to an ELCRODAT 4-2 simply by having the crypto module and software exchanged at our production facilities – a consideration that can be of great interest to the NATO candidate countries.

Voice is digitized by either an LPC10E or a delta codec. The digitized voice signals are transmitted either via built-in modems, a 16 kbps or a V.24 interface. The V.24 interface is available at the terminal end for data transmission. The data transmission is managed directly from the terminal device over the handshake channels. No manual input is needed from the base unit. The external modem is connected to the V.24 interface at the transmission end and can be operated directly from the terminal device in the V.24 Hayes operating mode.

ELCRODAT 4-2

The ELCRODAT 4-2, which is now ready for series production, was developed over the past several years on behalf of the German Federal Office for Defence Technology and Procurement (now IT-AmtBw). It has now been approved for rollout. The first consignment has already been ordered for delivery to the German Armed Forces. The final approval by the German Federal Office for Information Security (BSI) as well as the NATO approval are expected in 2004.

The ELCRODAT 4-2 is a cross-sectional device designed for use in all branches of the German Armed Forces (army, air force and navy) as well as for civil authorities. The Tiger and NH90 helicopters, the K130 corvette and the U 212 submarine will all be equipped with this modern crypto technology.

The German Army will use the VESUV system (system for distributing and managing electronic keys) to provide the ELCRODAT 4-2 with keys.

The device has been equipped with NATO algorithms and is therefore cleared for use only in NATO countries. It has already been selected as a candidate for a number of international programs.

MMC3000

The Multimode Multirole Crypto Device MMC3000 was developed on the basis of the ELCRODAT 4-2 for use in non-NATO countries and countries in line to join NATO. The MMC3000 implements a proprietary, variable crypto algorithm. A corresponding management system called MMC3000 SMS (security management system) is used to generate, manage and distribute the crypto variables. The management system consists of PC software, a KGE (key generation and encryption equipment) external key encoder and a DLD (data loading device) as a key transport device.

The MMC3000 will be available starting in the second quarter of 2004.

End-to-end encryption for TETRA

Rohde & Schwarz SIT is developing a base system for end-to-end encryption of TETRA radio links. The collaboration with R&S BICK Mobilfunk, one of the leading TETRA infrastructure device and system suppliers, offers the customer a single-source solution. The encryption solution is not manufacturer-dependent and can therefore be integrated into any TETRA system.

TETRA provides standard encryption at the air interface. This does not protect the entire user-to-user transmission path. By contrast, the end-to-end encryption base system from Rohde & Schwarz SIT does; it also includes full duplex voice encryption, SDS (short data service) encryption functionality and loadable crypto algorithms.

The base system concept offers maximum flexibility to users:

- The **modular** design allows for the integration of user-specific requirements with cost-efficient adaptation development into the base system. Thus, additional customer-specific functionalities can be integrated.
- The latest-generation smart cards are used as the system's security module. This makes the system virtually **hardware-independent** since the terminal equipment manufacturers only need to adapt the device software. Terminals that are already equipped with a SIM card interface need no modification, making it possible to introduce new equipment at competitive prices.

The Rohde & Schwarz SIT smart card solution offers the following advantages:

Single-source solution

- The close cooperation between R&S BICK Mobilfunk and Rohde & Schwarz SIT provides the customer with an all-in-one solution from Rohde & Schwarz.

Flexible use and handling, money-saving purchase and cost-effective operation

- The solution is independent of terminal equipment manufacturers.
- User-specific algorithms can be loaded.
- Specific user requirements can be integrated economically through adaptive development.
- The smart card can be replaced easily and enables battery-saving operation.

Secured confidentiality

- The smart card approach for end-to-end encryption is supported by the German Federal Office for Information Security (BSI).
- The solution is compatible with the requirements of the Schengen agreement.

Proven approach with excellent prospects for the future

- Smart card technology is largely standardized (ISO, ETSI).
- Continuing developments in smart card technology ensure investment protection.
- Smart cards are a recognized technology in other radio networks.

Trade fair schedule

You will find us at the following fairs and events in 2004:

CeBIT	in Hanover from 18 to 24 March 2004
ILA	in Berlin from 10 to 16 May 2004
SVIAZ	in Moscow from 11 to 15 May 2004
AFCEA	in Bonn from 12 to 13 May 2004
GPEC	in Leipzig from 8 to 10 June 2004
Systems	in Munich from 18 to 22 October 2004

ROHDE&SCHWARZ
www.sit.rohde-schwarz.com

ROHDE & SCHWARZ SIT GmbH
Am Studio 3 · 12489 Berlin
Tel. +49 30 65 88 42 31 · Fax +49 30 65 88 42 23
E-Mail: contact@sit.rohde-schwarz.com

Plug & play solution for secure transmission over serial data connections

Serial data transmission via modems is gaining in significance, a fact that is understandable given the range of possible industrial applications:

- Remote device and system queries (e.g. remote maintenance, counter status, machine monitoring)
- Remote device and system configuration (e.g. parameter settings for ventilation and heating control), remote control (e.g. structural engineering systems)
- Sensitive data transmission (e.g. alarm signals, payment transaction information)

Part of a family: SITMinisafe2 and CM200

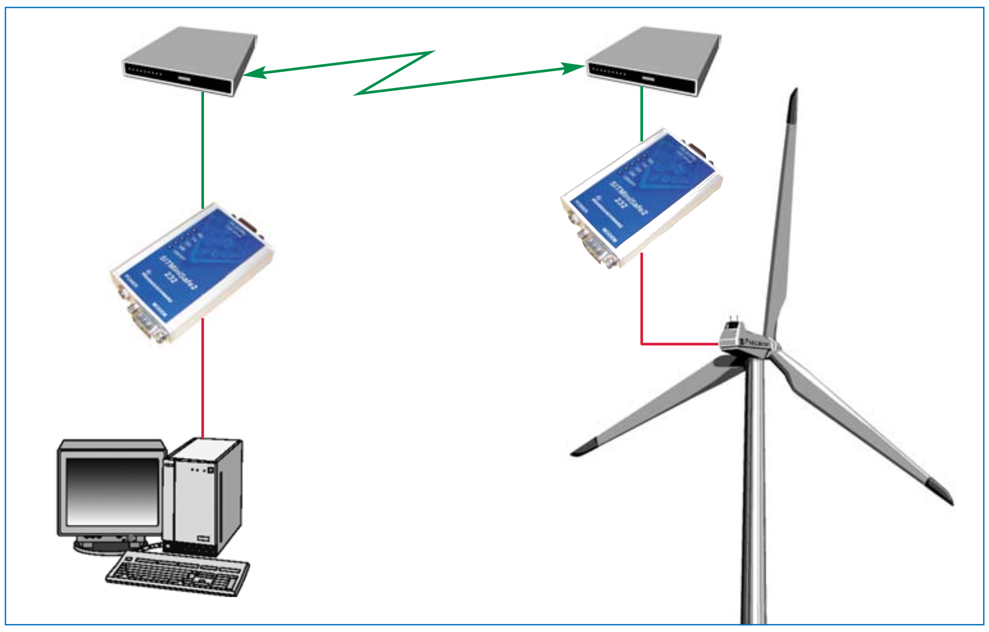
The issues of authenticating the transmitted data and protecting the data against manipulation and eavesdropping are often crucial in the above applications. The SITMinisafe2 and CM200 products from Rohde & Schwarz SIT provide first-class solutions.

The SITMinisafe2 and the CM200 include the following features:

- Authentication (challenge/response method)
- Encryption (128 bit, session key, key generation with physical random generator)
- Key management

This solution can be implemented as a module integrated within another device (CM200) or externally as an add-on device (SITMinisafe2).

The end-user is virtually freed from any concerns about security in a cost-effective and professional manner.



One possible SITMinisafe2/CM200 application: remote management of a power engineering system

Capsat Messenger Inmarsat M4 terminal (Thrane & Thrane) with TopSec 703

Secure satellite links

People would hardly be able to perform their tasks without electronic means of communication. This applies both to fully developed infrastructures in industrialized nations as well as to work in remote locations. Satellite communication has simplified access to even these out-of-the-way regions.

The problem is that it is also extremely easy for eavesdroppers to access satellite communications. It is essential that the transmitted data be safeguarded against tapping and manipulation when used for commercial or confidential applications. This security can be provided by encryption. End-to-end encryption is always the most secure because it is the only method that can be managed and controlled by the user.

A transmission over satellite often functions only as an "extended arm" of a terrestrial link. The goal is to implement an encryption solution that is already in place in terrestrial communications, such as ISDN.

A number of ISDN applications (videoconferences, telelearning, telemedicine, remote LAN access, etc) can be transported via satellite to locations that would otherwise be unreachable using conventional terrestrial systems. These applications still need the protection offered by encryption.

Devices from the TopSec ISDN encryption family operate successfully in providing security for these applications over ISDN and satellite connections – using the Inmarsat M4 service, e.g. with Capsat Messenger terminals from the Danish manufacturer Thrane & Thrane or the Nera World Communicator V4.01 from the Norwegian company Nera ASA.

The ELCRODAT 6-2 ISDN encryption device is ideal for transmitting classified information between government authorities using satellite links.

The STILink G.703 encryption device for leased-line links can be used to protect broadband satellite links. The unit encrypts 2 Mbit/s connections between headquarters and the remote location within the telecommunication system and allows secure communication between these two locations via satellite.

Company news

New support center for security products

Rohde & Schwarz SIT has established a new service and support center to offer our customers direct and even more efficient support in implementing their encryption solutions.

The focus is on application support for devices in the TopSec family and SITLink leased-line encryption devices.

The Rohde & Schwarz SIT Support Center, headed by Dr Harmut Ilse, can be reached at the following phone number and e-mail address:

Phone: +49 30 65 88 41 11
E-mail: support@sit.rohde-schwarz.com

Nellmersbach – a great location for a new plant

With the opening of the new plant near Stuttgart, Rohde & Schwarz SIT GmbH has adequate facilities at three locations: Nellmersbach, the main office in Berlin-Adlershof and Rohde & Schwarz headquarters in Munich.