R&S TopSec product family

Members only – confidential telephone and data communication

Anyone who has suffered damage once will be very careful the next time, that is what the proverb "once bitten, twice shy" is meant to convey. But what happens if you fail to notice the damage in the first place? This may be the case when a business becomes the victim of industrial espionage. So the maxim "better safe than sorry" seems to be the better one, because the losses caused by industrial espionage in Germany alone have been estimated at € 10 billion every year. For this reason, both the German Information Security Agency and the EU Commission advise all businesses to protect, i.e. encrypt, all communication channels used to transmit sensitive information.

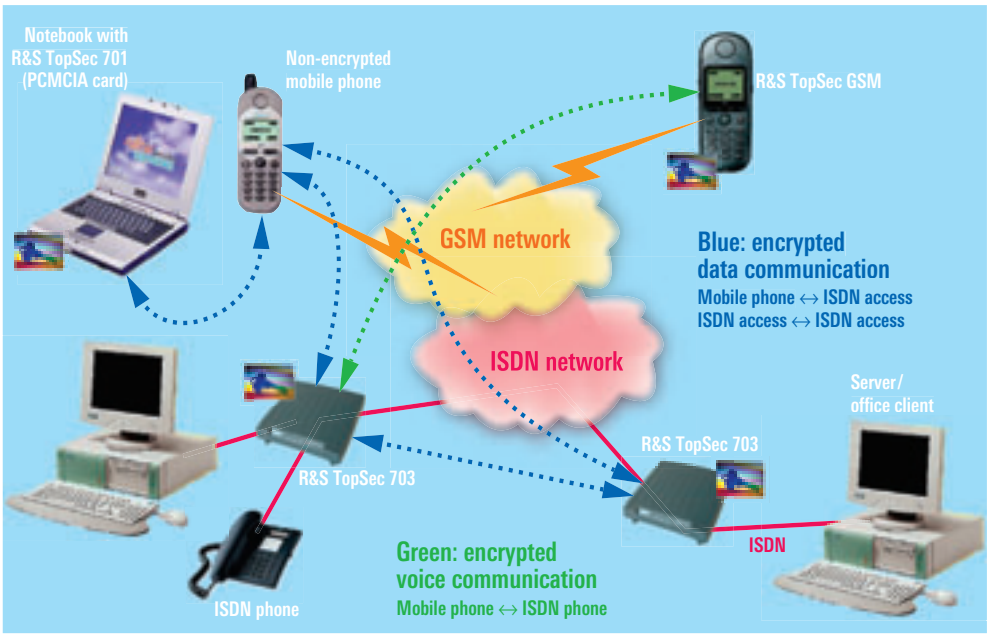

FIG 1 The crypto products from the R&S TopSec family allow secure voice and data communication in any scenario.

IT security products are a must

Have you ever used your mobile phone to talk about confidential business matters? Have you ever downloaded data to your notebook from the corporate network while on a business trip? Is there teleworking in your company? Does your company have different sites between which project and design teams exchange sensitive data? Do you make use of videoconferencing to save travel expenses?

Business people are likely to answer "yes" to most of these questions. Nowadays there are more means than ever for fast transfer of data and information. But that also increases the potential for misuse. The usual means of communication – telephone, mobile phone, fax, e-mail – have enormous security failings. Data theft, eavesdropping and industrial espionage are by no means abstract terms but concrete dangers.

Such dangers can be effectively eliminated by using IT security products from Rohde&Schwarz SIT GmbH. Any of the scenarios described above – and many more – can be secured against information theft by products from the R&S TopSec family.*

* The use of crypto products is subject to the relevant national legislation which must be observed, e.g. when taking crypto products along on business trips.

A product for every need

The name R&S TopSec stands for a series of high-grade encryption devices to protect voice and data communication in ISDN and GSM and also in analog networks. The R&S TopSec GSM crypto mobile phone (FIG 3) already described in News 172 [*] is a good choice for business people or politicians en route who have to talk about confidential matters on the phone. The R&S TopSec 701 is a PCMCIA encryption card for safeguarding data transfer between your laptop and mobile phone and the corporate network. The product family also comprises the R&S TopSec 703 and 703+ encryption units for ISDN basic rate access S_0, and the R&S TopSec 730 for ISDN primary rate access S_{2M}. These devices effectively protect telephone calls, faxes, data transmission, online connections and video conferences against unauthorized access by third parties. FIGs 1 and 2 give an overview of the product family.

R&S TopSec 701

The PCMCIA card R&S TopSec 701 is simply inserted into the PCMCIA slot of a laptop and connected to a modem-capable mobile phone by a data cable (FIG 4). The card is ready for use after installing the driver and configuring the card. The R&S TopSec 701 protects data transferred via mobile phone by high-grade encryption. The only prerequisite is that the called station must be equipped with a partner device from the TopSec family. Connections between two R&S TopSec 701 cards by way of mobile phones suitable for data transmission can thus be encrypted. It is also possible to use the R&S TopSec 703 or 703+ units, in conjunction with the V.110 protocol, at the other end in the Euro-ISDN network. Encrypted communication is furthermore possible on a modem link between two R&S TopSec 701 cards.

FIG 3 R&S TopSec GSM crypto mobile phone (described in detail in previous issue)

R&S TopSec 703 / 703+ / 730

The TopSec devices 703, 703+ and 730 offer encryption of communication via Euro-ISDN B channels. The device is connected between the Euro-ISDN interface and the terminal, e.g. a telephone or router. Setup of a connection only takes about three seconds more than for non-encrypted ISDN calls. The R&S TopSec 703 (FIG 5) and 703+ allow encryption of two B channels independently of each other. In contrast to the TopSec 703, the TopSec 703+ can also encrypt calls to the crypto mobile phone. The R&S TopSec 730 (FIG 6) is ideal for use on the primary rate access and can simultaneously encrypt up to 30 connections (FIG 6). Call status (standby, setup, encrypted, plain) is displayed by a LED for each B channel, or for every three channels in the case of the TopSec 730.

FIG 2 R&S TopSec product family

- **R&S TopSec GSM** Crypto mobile phone
- **R&S TopSec 701** PCMCIA card for data encryption and transmission via GSM mobile phone or modem
- **R&S TopSec 703** Encryption unit for connection to ISDN basic rate access S_0
- **R&S TopSec 703+** For encrypted communication between crypto mobile phone and ISDN network (S_0 interface)
- **R&S TopSec 730** Encryption unit for connection to ISDN primary rate access S_{2M}
- **Administrator software** For configuration of TopSec user groups and parameterization of encryption units (optional)

Powerful encryption

TopSec devices use a hybrid form of encryption, combining an asymmetrical algorithm with a 1024 bit key for key agreement and a symmetrical algorithm with a 128 bit key for user data encryption. In the encryption mode, a 128 bit key is randomly selected from 10^{38} possibilities for each connection established, and immediately deleted when a call is cleared down.

FIG 4 R&S TopSec 701 PCMCIA card

groups. Device IDs and certificates are loaded into user terminals and used for authentication on connection setup with a partner device. Authentication means that user terminals identify each other by exchanging certificates. Subsequent adaptation of user terminal parameters is usually made via an encrypted ISDN connection (remote administration). A terminal may belong to up to three user groups.

Apart from automatic authentication, user groups offer the possibility of excluding certain terminals from the user group by blacklisting them. This will be necessary if a terminal is stolen or lost. The administrator is responsible for handling and updating the black list. On an incoming encrypted call or request for a connection, the certificate exchange procedure checks to see if the particular terminal is blacklisted. Only if this is not the case will the connection be established, otherwise it is denied.

Administrator software enhances operational reliability

In addition to the protection of communication provided by encryption, the security-conscious user can optionally acquire administrator software, which is a powerful tool to enhance the operational reliability of TopSec devices.

This software allows optimum administration of the R&S TopSec devices within the communication network, from mutual authentication through logging of overall activities to dynamic management of several user groups.

Before devices go into operation for the first time, the administrator initializes them and combines them in closed user

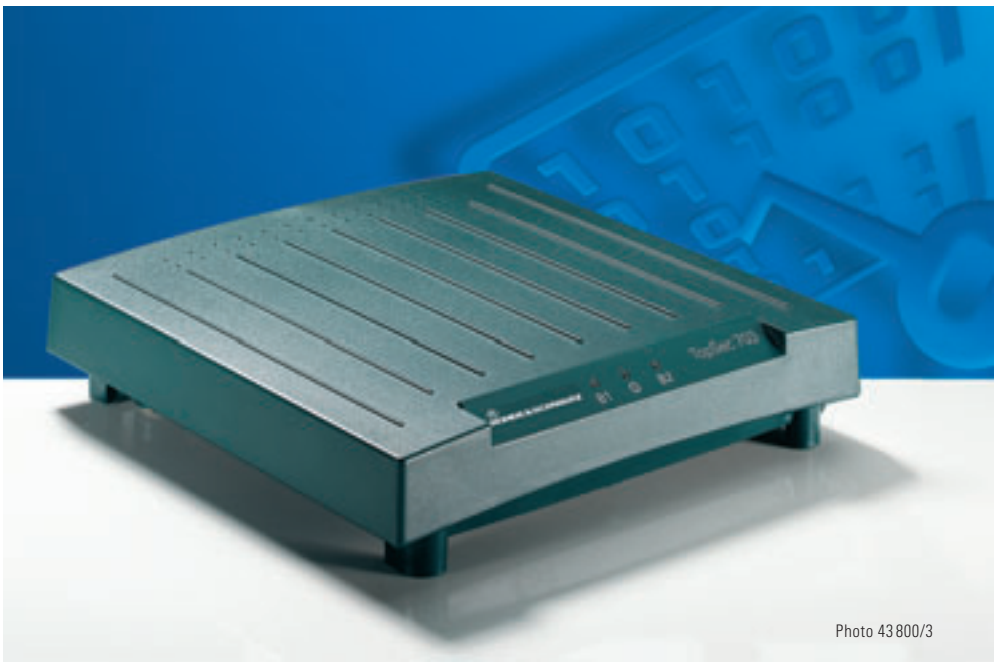

FIG 5 R&S TopSec 703 for encrypted communication on Euro-ISDN B channels

Absolute confidentiality by keystroke

Operation of TopSec devices is extremely user-friendly and limited to selecting the mode of transmission (plain/encrypted). This is done simply at a keystroke, i.e. by dialling a code number before entering the required call number. 0 means plain mode, while 1, 2 or 3 is used to select a specific user group previously configured by the administrator. 9 means that the connection to another TopSec device is to be encrypted without administrator control. If devices are not administered, you can only choose between 0 (plain) and 9 (encrypted). No further entries are required during operation.

FIG 6 R&S TopSec 730 for simultaneous encryption of up to 30 connections

Versatility for enhanced security

TopSec devices ensure confidentiality, authenticity and integrity, and they protect important corporate data against industrial espionage. Data transmission from corporate networks to telework and service stations is protected. Personal data governed by data protection legislation can be securely transmitted and design data confidentially exchanged between distributed project teams.

R&S TopSec is also ideal for protecting fax transmission or video conferences. Service interfaces provided for remote administration can be secured.

Frequently used but completely inadequate security mechanisms like callback are replaced by powerful encryption and authentication procedures.

The user alone is responsible for key management, allowing configuration of closed user groups.

The TopSec products for mobile users – R&S TopSec GSM and R&S TopSec 701 – are small and lightweight and look just like comparable devices without crypto functionality (mobile phones, PCMCIA cards).

Due to their versatility, TopSec products attract the interest of a wide range of users, like corporate executives in many different branches of business, consultants, service providers, mobile and stationary teleworkers, field and service staff and design engineers.

TopSec products are widely used by public authorities and suitable for both national and international use.

Christine Hagn

More information and data sheets at www.rohde-schwarz.com (search term: TopSec)

REFERENCES

[*] Crypto Mobile Phone R&S TopSec GSM: Secure communication – protected against data thieves. News from Rohde & Schwarz (2001) No. 172, pp 49–51