Crypto Mobile Phone TopSec GSM

Secure communication – protected against data thieves

Flexibility and mobility are key factors to success; up-to-the minute information and quick decisions have become more important in industry and politics than ever before. Mobile phones are often used to pass on information quickly. Users become more and more aware of the fact that enormous security problems may arise. The usual means of communication – telephone, mobile phone, fax, mail – are the main sources that attract data thieves. Damage caused by industrial espionage in Germany is estimated to run into at least 20 billion marks every year.

Photo 43 756/2

FIG 1 The TopSec GSM looks like an ordinary GSM mobile phone. Inside, however, a complex crypto processor provides extremely secure encryption.

A risk to be taken seriously

One of the security problems in GSM mobile radiocommunications is that calls are only encrypted between mobile phone and base station. From the base station, the calls are routed without any protection via the normal fixed network – often via microwave link. In commercial and governmental environments, efficient encryption should therefore be used to protect confidential communication.

The best way of protecting confidential information against unwanted eavesdroppers and thieves is the use of high-quality encryption devices as offered by Rohde & Schwarz SIT GmbH: their "TopSec" product family ensures extremely secure voice and data communication in ISDN and GSM networks.

This article deals with the TopSec GSM mobile phone (FIG 1) for tap-proof mobile communication.

TopSec GSM: mobile and confidential

The TopSec GSM crypto mobile phone was originally developed by Siemens. In May 2001, Rohde & Schwarz SIT GmbH took over from Siemens the hardware encryption business segment with the associated range of products. Since then Rohde & Schwarz SIT is responsible for further development and marketing of the crypto mobile phone.

Photo 43 756/4

FIG 2 The activated crypto mode is indicated on the display

The TopSec GSM mobile phone looks exactly like the commercial Siemens dual-band mobile phone S 35i, and also has the same performance features: low weight, high speech quality, long talk and standby times, Internet access via WAP, IR interface, etc. Inside, however, it has a crypto module in the size of a postage stamp.

Confidential communication in mobile radio and ISDN networks

The TopSec GSM mobile phone is suitable for encrypted end-to-end voice communication in the GSM frequency ranges of 900 MHz and 1800 MHz and with the ISDN network. The only prerequisite for encrypted calls is that the called station must also be equipped with a TopSec device, which means that end-to-end encryption is not only possible between two TopSec mobile phones, but also between a TopSec GSM phone and an ISDN network subscriber terminal that is protected by a TopSec crypto box. The TopSec 703 from the TopSec product family is a suitable ISDN encryption unit, for example. This encryption unit is connected between the NTBA and the ISDN terminals. Mobile subscribers can make tap-proof calls from their TopSec GSM phones to their office numbers in the fixed network.

Complex, extremely secure crypto technology

A complex crypto processor is the core of the TopSec GSM. For encrypted calls, the GSM data channel with a bandwidth limited to 9600 bit/s is used instead of the voice channel. To enable transmission via the data channel, the voice signal is first compressed by a GSM half-rate vocoder; information for error detection and correction is then added to the signal before it is encrypted. The data protected in this way is provided with further information for synchronization of the called station and sent via the data channel. The speech quality is as excellent as in non-encrypted mode.

The high level of security is ensured by a combination of two algorithms: an asymmetrical algorithm with a 1024-bit key for key agreement, and a symmetrical algorithm with a 128-bit key for voice encryption. For each call, the 128-bit key is randomly selected from 10^{38} possibilities. Security is extremely high: even in 10 million years, 1000 Pentium PCs could test only a very small part of the vast number of possible keys.

In addition to encryption, the TopSec GSM provides authentication as an optional security function. With the aid of special software, several TopSec GSM phones can be combined in closed user groups, allowing encrypted communication only within the same group.

Absolute confidentiality at a keystroke

Of course, the TopSec GSM can also be used for making non-encrypted calls to any partner. It is operated exactly like the Siemens S 35i mobile phone. An encrypted connection can be established at a keystroke. After pressing the call setup key, the calling person only has to activate the crypto function by pressing the appropriate softkey (FIG 2). Everything else is automatic: a data call is initiated and the key is exchanged within 15 seconds.

Key features of the TopSec GSM

- High security level
- Top-quality voice encryption for end-to-end voice communication
- Same high speech quality in encrypted and non-encrypted mode
- Simple handling
- Recommended by the German Information Security Agency

The TopSec GSM features all the benefits of a modern mobile phone

- Ease of operation
- Voice dialling
- Small size
- Low weight
- Internet access via WAP browser
- Soft modem
- IR interface for mobile data transfer

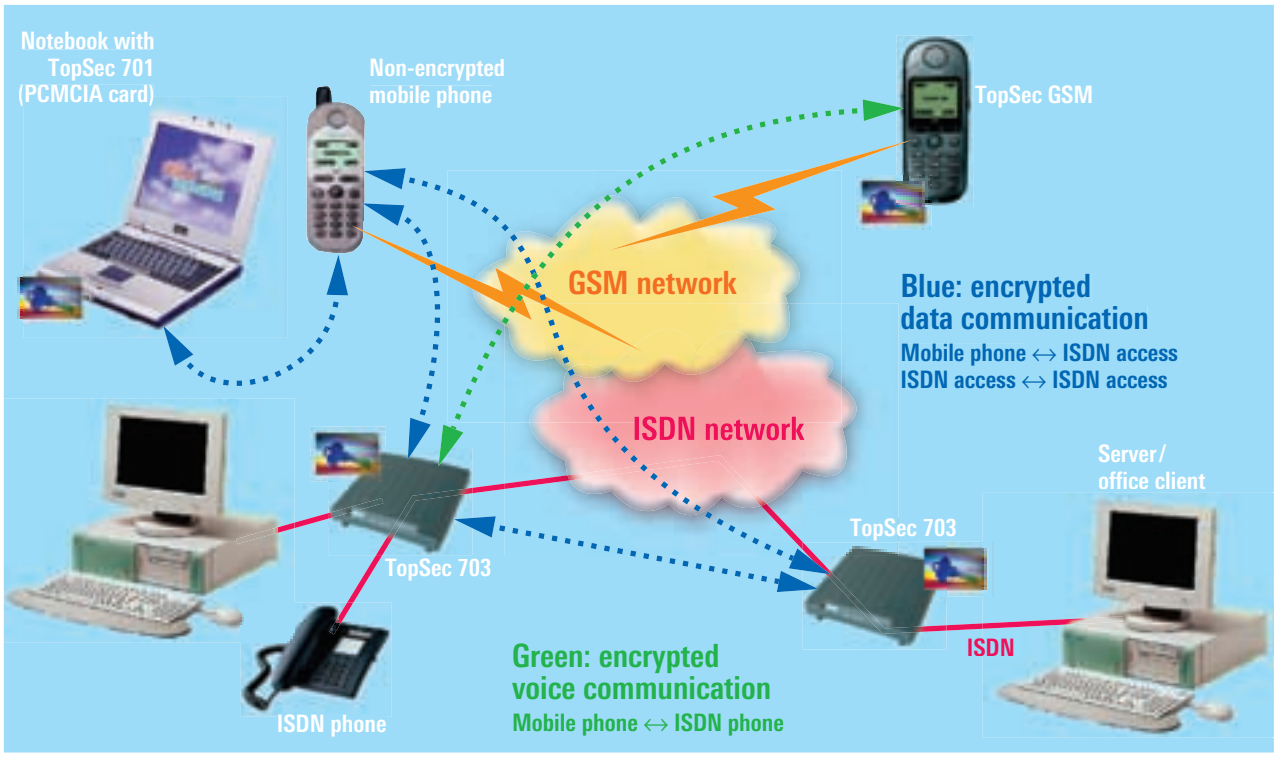

FIG 3 Crypto products from the TopSec family allow secure voice and data communication under any technical conditions

Encrypted calls can be terminated exactly like normal calls by pressing the clear key. Upon termination of the call, the initially generated key is deleted, which is a significant security factor in addition to the enormous key length.

The TopSec product family

Besides the TopSec GSM, the TopSec family comprises the TopSec 703 for ISDN base rate access S_0, the TopSec 730 for ISDN primary rate access S_{2M}, and the TopSec 701 for data transfer. The TopSec 703 and the TopSec 730 can be used for encryption of all services transmitted via ISDN: voice, fax, video and data.

The TopSec 701 is a PCMCIA card for insertion in laptops. It allows encrypted data to be transferred from a laptop via mobile phone to a TopSec 703 or TopSec 730 in a fixed network, or between two TopSec 701 via an analog link using a modem. FIG 3 shows the various possibilities of encrypted voice and data communication provided by the TopSec product family. The whole crypto family will be described in detail in one of the following issues.

Christine Hagn

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

Data sheet TopSec GSM