State-of-the-art encryption for any telephony application

Successfully established on the market, the TopSec Mobile crypto unit provides voice encryption for commercial smartphones. The extended encryption solution allows tap-proof calls with iPhone and Android mobile phones, PCs and laptops as well as calls to the company's fixed network.

The app version of this article has a video that shows how easy it is to use the TopSec Mobile.

Nowadays, companies, government authorities and armed forces want to exchange confidential information via landlines as well as smartphones. However, such calls are relatively easy to eavesdrop, making it very important to protect confidential information with strong encryption. The security solution needs to be simple and flexible while supporting everyday communications processes without undue complexity.

Encryption – a balancing act between convenience and security

A glance at the commercial products that are available or have been announced demonstrates the wide range of solutions that exist with very different features, security characteristics and even costs (Fig. 2). Due to the great diversity of requirements, application environments and possible uses of the devices, there is no dominant technical

Fig. 1: It doesn't get any simpler or more convenient: confidential calls – even via a laptop – can be made using the TopSec Mobile with hardly any additional effort. A special mobile phone is not required.

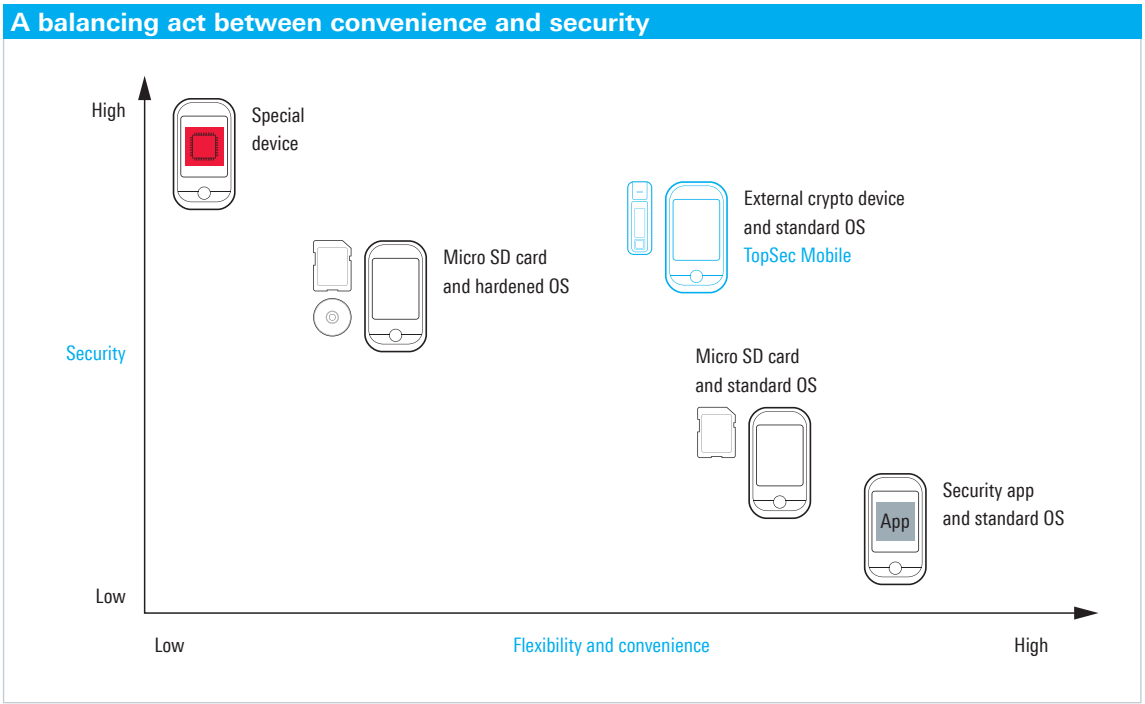

Fig. 2: The solutions that exist for tap-proof telephone calls vary widely in terms of security and ease of operation.

approach. Application-based solutions are the wrong choice if a level of security is needed that professional attackers cannot crack. To satisfy such demanding protection requirements, hardware-based encryption is mandatory. Taking this boundary condition into account, the possibilities come down to two basic concepts: specially developed, hardened crypto phones, or commercial devices with additional hardware security.

Specially hardened crypto phones ensure a high level of security but they are usually associated with trade-offs in the available functions and flexibility. These phones are costly to develop and produce and require time-consuming reworking and recertification in case of product changes.

The second concept involves voice encryption using dedicated hardware components. This includes integrated solutions that encrypt calls inside the phone on a separate smart card. However, such solutions are available for only a few types of phones. Users must choose from among these specific models. Due to the lack of a card slot, smart card solutions are not compatible with the popular iPhone.

There also exist two-device solutions where the voice encryption is performed outside of the telephone. They offer maximum flexibility in the selection of the communications devices. This is the approach implemented in the TopSec Mobile from Rohde & Schwarz SIT (Fig. 3).

Fig. 3: As a stand-alone encryption device, the TopSec Mobile connects via Bluetooth® to iPhones, Android smartphones, PCs and satellite terminals.

TopSec Mobile combines security with flexibility and convenience

The TopSec Mobile is a standalone encryption device that connects to iPhones, Android smartphones, PCs and satellite terminals via Bluetooth®. The device is used whenever a conversation needs to be confidential (Fig. 4). When making secure calls, users talk and listen through the TopSec Mobile's own microphone and speaker while the TopSec Mobile's reliable hardware encrypts the calls. This eliminates the possibility of manipulation by viruses, Trojans and other spyware that might be found on the smartphone. The voice data sent from and to the TopSec Mobile is already secured at the highest possible level when transmitted via the Bluetooth® interface. The communications device is merely used to transmit the encrypted VoIP data. As a result, practically any Android or iOS smartphone or PC with Windows 7/8 can now be easily used for highly secure voice encryption. This translates into enormous savings for teams with changing members or when a pool of devices is needed, for example. Users also like the fact that they can go on working with their preferred communications device.

In tap-proof conference rooms, situation centers and bunker facilities, mobile networks are often unavailable, or the use of mobile phones is not permitted for security reasons. In such environments, the TopSec Mobile can be used to make encrypted phone calls via existing PCs with their network connection.

Encrypted calls to the fixed network

The new TopSec Office Gateway (TSOG) turns the TopSec product family into an all-round solution for tap-proof calls (Fig. 5). The gateway supports encrypted calls between mobile phones and internal telephone sets. This safeguards the link from the TopSec Mobile to the organization's private branch exchange (PBX) against outside attacks. The TSOG receives the incoming calls from other TopSec devices and automatically decrypts them. The calls are routed to the PBX's VoIP interface and then onwards to the desired extension inside the organization.

TopSec Mobile: highly versatile voice encryption

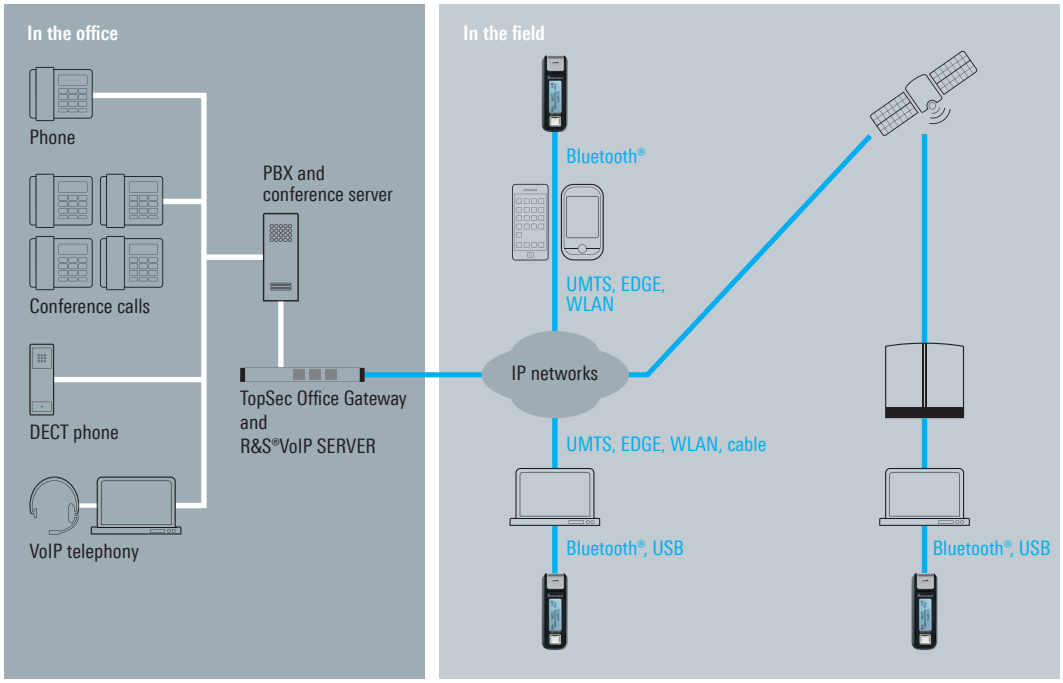

Fig. 4: The TopSec Mobile ensures reliable encryption in any application.

Fig. 5: TopSec Office Gateway: for encrypted calls from mobile phones to a company's internal PBX.

Fig. 6: The R&S®VoIP SERVER ensures top reliability along with ease of use.

Incoming calls from a TopSec Mobile are accepted by picking up the desktop phone as usual. To make an encrypted call from a fixed-network phone to a TopSec Mobile, users simply enter a variable crypto prefix. Outgoing calls are encrypted automatically when the PBX transfers the call to the TSOG and from there to the desired TopSec Mobile. The TopSec Office Gateway dramatically increases the number of parties who can be reached via a secure connection. By achieving better acceptance, the security solution becomes much more effective.

The TSOG is available as a 19" rackmount in two versions: TSOG Medium supports up to eight simultaneous calls between TopSec Mobiles and fixed-network phones while TSOG Large supports up to 32 parallel calls. Custom solutions can be developed for customers with requirements that go beyond these typical performance classes or who need top availability.

The first TSOG installations have already been deployed by European customers.

State-of-the-art encryption methods for perfect forward secrecy*

The TopSec Mobile encrypts calls using the extremely secure AES 256 algorithm. Using the 256-bit encryption, there are 2^{256} possible keys, i.e. 1.15×10^{77}. This algorithm clearly cannot be cracked within a realistic period of time. During each call setup, the encryption devices automatically agree on a new random key, which is deleted immediately upon completion of the call, thereby ensuring perfect forward secrecy.

Like with all VoIP-based encryption solutions, a VoIP server is also used with the TopSec Mobile. The R&S®VoIP SERVER comes in two versions. Also designed as a 19" rackmount, the devices (Fig. 6) handle up to 50 registered users in the Medium version and up to 1000 users in the Large version. Like in the case of the TSOG, high-performance versions can be provided on special request.

The TopSec Mobile is approved by Germany's Federal Office for Information Security for the NATO RESTRICTED classification level.

Christian Reschke

* Perfect forward secrecy ensures that the key cannot be divulged, thereby ensuring confidentiality even if the encrypted communications are recorded.