



# SECURE MOBILE SOLUTION

The practical and comprehensive solution for  
totally secure mobile voice communications,  
instant messaging and e-mail

## Mobile communication – an underestimated risk.

In the global competitive market, technical means are used by hackers, criminal organizations, states and increasingly by competitors in order to obtain sensitive information. Diplomats, government ministers and top managers are especially at risk because of their frequent voice and data communications across public mobile and wireless networks. These can be monitored quite easily.

### Mobile and wireless networks are unsafe

Mobile voice and data communications are easy to monitor or to manipulate. Conventional unprotected mobile phones and modems are unsuitable for exchanging classified, confidential information. An additional security risk is that aggressors can make use of malware to penetrate deep into an organization's communication system.

### The solution: encrypted information and protected end devices

To avoid monitoring, manipulation or infiltration by unauthorized parties, information must be highly securely encrypted, and generated and transmitted by secure end devices. Omnisec's Secure Mobile Solution does exactly that. This comprehensive and easily implemented solution

allows governments and enterprises to communicate globally via voice and data channels across mobile and wireless networks with complete security up to the level of TOP SECRET.

### Secure mobile-to-mobile und secure mobile-to-landline

Based on the security architecture OmniCrypt™, Omnisec's Secure Mobile Solution meets the most exacting of criteria for secure communication. The confidentiality, authenticity, integrity, and non-repudiation of transmitted information are guaranteed. In combination with the Secure Telephone Solution, highly secure mobile-to-landline (PSTN) as well as mobile-to-mobile connections are supported.



Omnisec Secure Smartphone  
(original size)

# A comprehensive solution, completely under your control.

The Secure Mobile Solution from Omnisec consists of numerous elements that are totally controlled by the user. In addition to convenient and highly secure smartphones, a high-security Communications & Management Server is used for configuring and monitoring the core systems and communication services. The Key Management Center allows the user to autonomously generate and manage the cryptological keys.

## Using a convenient smartphone as end device

The highly secure Omnisec  $\mu$ SD Security Modules transform smartphones into powerful encryption devices, enabling voice, and optionally instant messages and e-mails, to be exchanged with maximum security worldwide. The encryption and decoding of information takes place inside the Secure Smartphones, which are protected against any attack. The current mobile and wireless standards (Triband UMTS, Quadband GSM und WLAN) are supported. The smartphone also provides an encrypted memory for securely saving all data, as well as a mailbox, in which voice messages, protected against eaves-dropping, can be stored.



Omnisec  $\mu$ SD Security Module (original size)

## A new type of risk.

2004 marked the year in which malware for mobile phones first appeared (Caribe, Brador, Mosquit). Unlike computers, which have been attacked for over 25 years, no comprehensive security solution has yet been developed for mobile phones. This is an alarming situation, as an increase in targeted espionage on mobile phones is more than likely, using malware that cannot be recognized by conventional protective software.

## The Omnisec $\mu$ SD Security Module

A special hardware Security Module containing the core security and key storage is installed in the smartphone. It serves to identify the user, to securely store long-term cryptological keys, to generate Session Keys, and to store encrypted configuration data, as well as encrypting all communication within the secure network. The user autonomously programs the 256-bit long-term keys by means of the Key Management Center.

## The high-security Communications & Management Server is located on your site

The heart of the solution is the highly secure Communications & Management Server. The hardware, which hosts a hardened operating system, is a scalable, reliable, high-performance platform that permits modular expansion up to 100, 500, 2000 or more users. Specially developed to meet the demands of worldwide mobile VIP users, the client/server communication application satisfies the most rigorous of requirements.

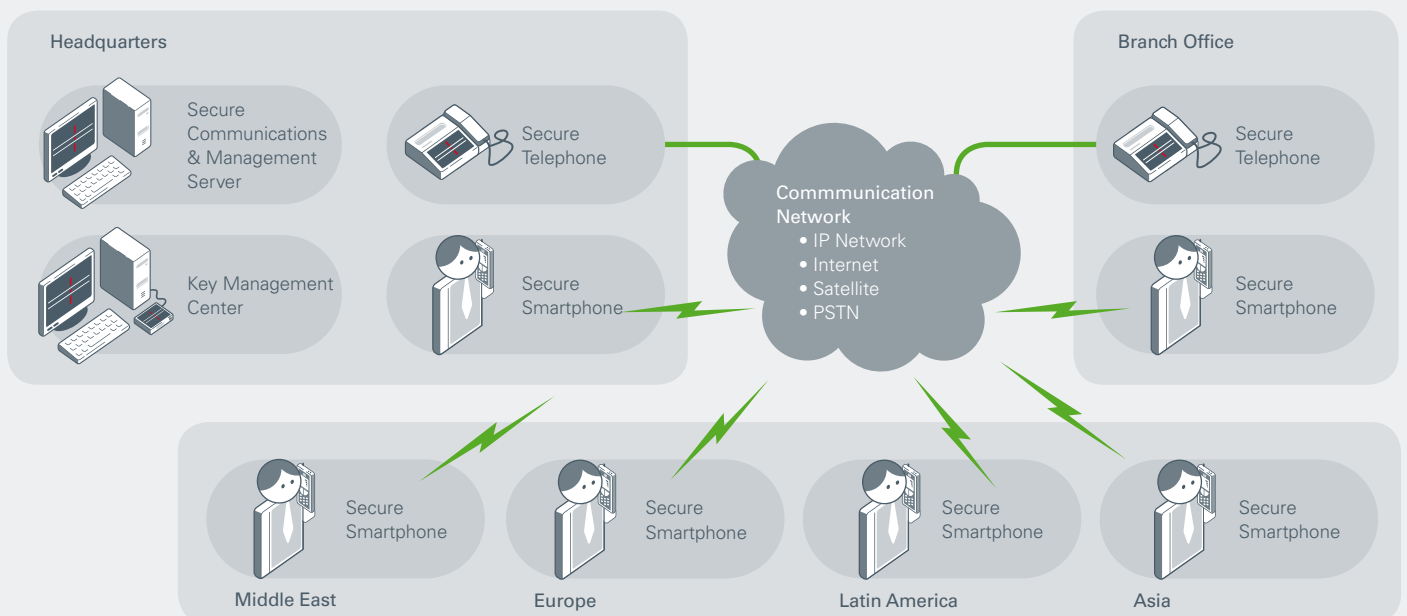


The resources and communication services are configured and monitored by the integrated Network Management Center. This allows lost Secure Smartphones, for instance, to be instantaneously disabled.

**The highly secure keys are under your control as well**

The cryptological keys required for secure (encrypted) communication between the Secure Smartphones are produced and managed by the Key Management Center. The confidential long-term keys are generated from a physical noise source and individually programmed into the  $\mu$ SD Security Modules.

The Communications & Management Server as well as the Key Management Center are installed and run in a specially equipped security zone. All of the system's components can be completely and exclusively controlled by the user at all times.





#### The Omnisec Secure Mobile Solution at a glance

- The most secure solution for encrypted voice communication, instant messaging and e-mail up to the level of TOP SECRET
- Eminently suitable for public authorities, governments and enterprises that store, use and exchange classified information with mobile devices
- User-friendly due to convenient, highly secure smartphones as end devices
- Instant connection establishment und superior speech quality
- The solution is completely controlled by the user
- Simple to use, requires minimal training
- Economical operation and maintenance; high Return on Security Investment
- Simple and secure administration; lost Secure Smartphones, for instance, can be remotely disabled instantaneously
- Perfectly augments the Secure Telephone Solution for protected landline communications (PSTN)

