From €1,700*

*SiMKo3 (incl. smartphone) basic package with 24-month-contract

MAKE YOUR MOBILE COMMUNICATIONS MORE SECURE WITH SIMKO3.

THE GROWING CHALLENGE OF MOBILE SECURITY.

Almost 90 percent of companies equip their workforce with mobile devices – enabling staff to access key internal resources such as e-mail, contacts, calendars and business data while on the go. Vast amounts of data are transferred via public networks and stored on smartphones, tablets and notebooks. But that exposes sensitive business information to a perilous environment, where it is at risk of theft, loss or destruction. In Germany alone, 15,000 devices are lost in buses, trains and taxis each and every month.

What's more, many people use their smartphones for both the professional and the personal, creating additional vulnerabilities for mobile data: users want unfettered access to the cloud, social networks and app stores; they want to browse freely and make use of GPS navigation.

And if confidential information falls into the wrong hands, the consequences can be serious – in financial and also in legal terms: in many countries, executives are responsible for ensuring the security of their employees' communications, and can be made personally liable for any failures.

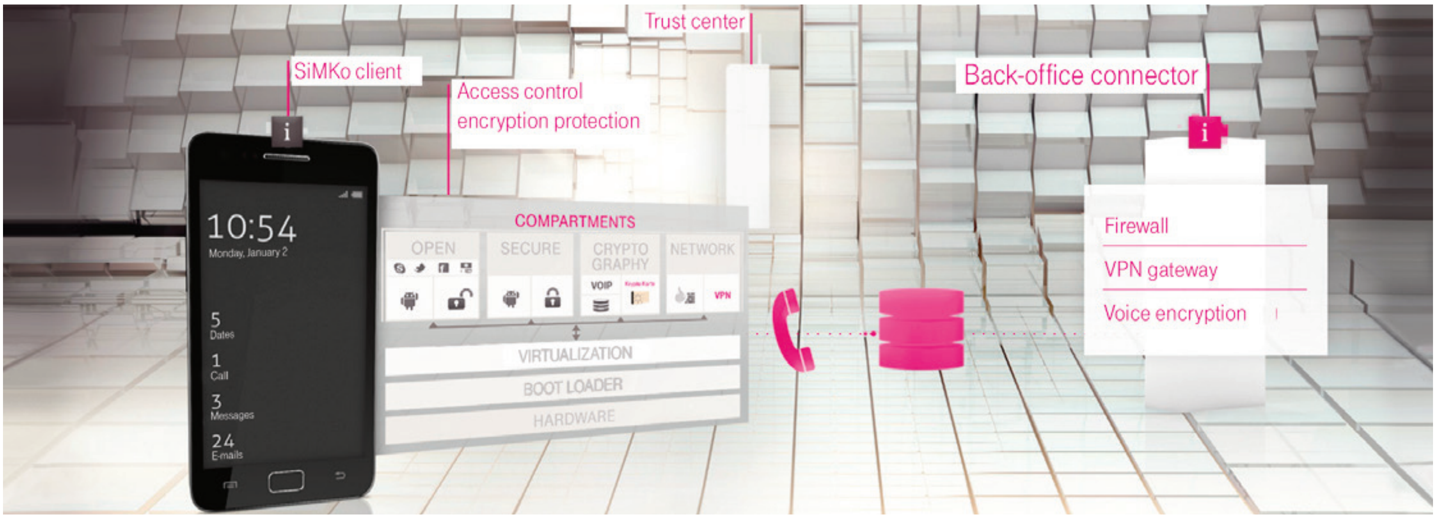
SIMKO3: SECURE SMARTPHONE ARCHITECTURE, THANKS TO VIRTUALIZATION.

Most conventional smartphones have a market life of just six to eight months before being replaced by a successor. This leaves little time to develop and test suitable security mechanisms, leaving them with inadequate protection. T-Systems and Trust2Core have taken a different route. Our secure smartphone architecture is based on virtualization software, enabling two completely different profiles on a single device:

- A personal profile with access to the public cloud for social networks, navigation, telephony and much more.
- A professional profile with secure on-the-road access to all business resources.

The virtualization software forms a layer between the hardware and the smartphone's open and secure application systems. Separating the hardware from the software allows users to access Facebook or Twitter, while protecting sensitive enterprise applications. These are safely hosted at a secure data center and provisioned via a VPN tunnel using an integrated smart card. What's more, segregating hardware and software ensures rock-solid security despite the hectic smartphone innovation cycle.

T · · Systems ·



SECURITY AND MOBILITY – A WINNING COMBINATION!

Devices of the SiMKo3 generation are manufactured under trust-center conditions, leveraging standard consumer products. They are initially of standard design and type. Customers can then tailor the infrastructure and user settings in-house to their specific needs. This ensures that user-related data never leaves the business environment at any time unencrypted. Using standard components and methods, SiMKo devices can be hooked up to a wide variety of groupware systems. And by installing and configuring scalable back-office connectors (BOCs), they can be securely integrated with the customer infrastructure. The BOCs comprise a firewall, which only opens the port required by the VPN; a VPN server to which the devices connect and, if needed, a groupware connector, which supports diverse desktop systems (e.g. MS Exchange, Lotus Notes, Novell, open xchange, Zarafa, Kolab and more) via ActiveSync protocol.

THE SIMKO3 FAMILY.

Secure mobile communications are no longer limited to smartphones and tablets. The evolution of SiMKo2 into SiMKo3 has seen the product portfolio expand to include notebooks. These also comply with the VS NFD security standard. In collaboration with our partners genua, ItWatch, Sirrix AG and Utimaco, we have responded to demands for greater security. SiMKo notebooks offer robust protection anywhere, anytime. Through enhanced back office connectors, SiMKo notebooks can use the same gateways as SiMKo2 and SiMKo3 smartphones and tablets. A gateway concept that spans all mobile access points offers better investment protection. And the concept behind SiMKo3 notebooks is also available for conventional desktops, allowing them to be securely integrated into corporate networks when employees are working from home.

You can choose from a range of hardware configurations from a number of vendors. Customer-specific options are available within the scope of T-Systems' Managed Desktop Services. From planning to application installation, to roll-out, to ongoing operations, the SiMKo3 family offers a secure mobile communications solution geared to your needs.

SIMKO3 AT A GLANCE.

- Samsung Galaxy platform, and notebooks from various vendors.
- Manufactured under trust-center conditions.
- Configured in-house by the customer:
  All user-related data remains within the enterprise.
- End-to-end encryption to the S/MIME standard.
- Voice encryption on VoIP with various security levels, including calls to landlines.
- Integration of all commercially available mail systems using standard components.
- Secure boot loader; hardening of user devices (all backdoors are closed).
- An integrated smartcard stores certificates (digital identity) and generates keys.
- Highly secure VPN tunnel connects to customer infrastructure.
- Virtualization layer based on a secure L4[1] microkernel separates software from hardware, providing independence from devices and their innovation cycles.
- Public profile is completely segregated from business profile.
- Secure app store for customer-specific applications.

[1] L4 is the name of a family of microkernels, based on the designs and first successful attempts at implementation by Jochen Liedtke (1953-2001, German computer scientist and Professor of Systems Architecture at the University of Karlsruhe).

ANY QUESTIONS?
Internet: www.t-systems.com/simko
Or simply send an e-mail to:
SiMKo@t-systems.com

EXPERT CONTACT.
Stephan Maihoff
Head of Secure Mobile Communication
Telephone: +49 (228) 181 38220

PUBLISHED BY.
T-Systems International GmbH
Hahnstr. 43
60325 Frankfurt am Main
Germany

Status 02 / 2013 | Errors and omissions excepted; subject to change without notice | Printed on chlorine-free paper | typix