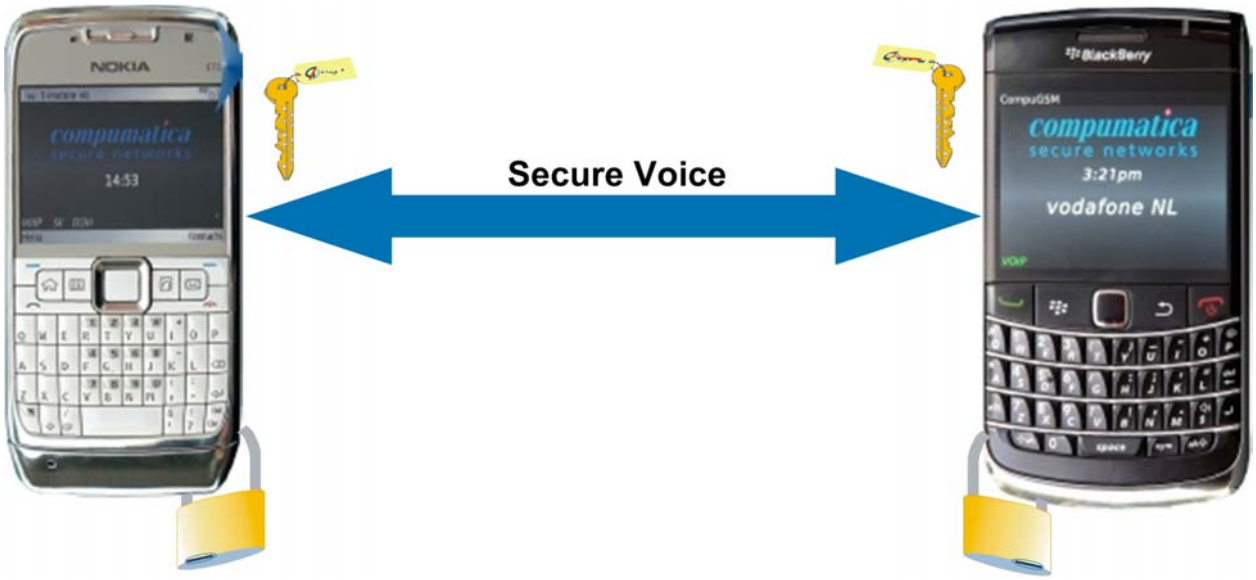
WhitePaper

Compumatica Secure Mobile Concept

The secure voice and SMS solution for organizations and governments

Compumatica secure networks



© 2012 *Compumatica secure networks*

ABOUT COMPUMATICA

Founded in 1991, Compumatica nowadays has offices in Uden (The Netherlands) and in Aachen (Germany) with a total staff of about 60 persons. Compumatica provides high-level security solutions for the protection of highly sensitive data transmitted over public or private networks.

The Compumatica crypto-systems and products are developed and manufactured within Compumatica and are applied in organizations with maximum security demands like public authorities, banks, insurance companies and industrial enterprises. Compumatica products do not have any backdoors like duplicate keys and thanks to this the customer possesses and controls the security management in total.

Compumatica is an expert in security solutions and security products. Most employees graduated from higher professional education institutes or universities and all employees in the Netherlands and in Germany have had a security screening.

Just like the qualified staff, also the Compumatica products are of a high quality. The products meet high severe standards for reliability and security. Some of the solutions have even been approved or certified according to the strict regulations of the Dutch National Communications Security Agency (NLNCSA) and the German Federal Office for Information Security (BSI).

THREATS IN MOBILE COMMUNICATION

Today the world of mobile telecom is more than just a simple telephone. People make use of smartphones, tablets, etc. to communicate with each other. The basic communication types between users are voice (ordinary telephone calls) and the exchange of SMS text messages.

This way, people sometimes use the mobiles for communication about company secrets, contract information, strategic company information, government confidential information and other sensitive information which is not meant for others.

Malicious people will try to eavesdrop the conversations or messages for their own purposes. With rather cheap listening devices it might already be possible to monitor this sensitive data exchanged between mobile phones.

THE CHALLENGES

Although the mobile phone is very easy in its usage, it is from security point of view an attackable medium, especially the traffic between phone and GSM transceiver stations.

Most mobile phone users are probably not aware of the fact that the mobile phone medium is vulnerable for eavesdropping attacks. Because of this ignorance it is often used for exchanging sensitive information:

- Company employees discuss about contracts or strategic company information via the mobile phone;
- Government officials use the phones to discuss sensitive information;
- Armies exchange strategic information among each others;
- Etc.

Above there are some examples of realistic cases in which the mobile phone is used for voice or data traffic with confidential contents.

For the involved parties it is very undesirable that this data leaks to others.

The mobile phone network nowadays has a perfect coverage and the phones are very user-friendly devices. Important is that adding security functionality to the mobile phone platform must not degenerate the user-friendly behavior of the device.

Another challenge to be met is the support of the several platforms. The main platforms are BlackBerry RIM, Android, Symbian and Windows. Since the security solution interferes deeply in the product, there will be different packages for each platform but with a similar user interface adapted to the device.

The solution should be flexible to be deployed for small customers with only a few users as well as to be scaled up for large groups of users.

PROTECTING MOBILE PLATFORMS

There are several approaches to secure mobile phone platforms, however not every solution will be safe enough. Apart from the security, the solution should also be easy in usage for the user and organization.

An approach for a mobile security solution is to make use of the CSD channel. However, CSD has a smaller bandwidth than UMTS and besides, CSD will become obsolete since more and more providers stop supporting it.

A security mechanism completely integrated in the phone platform software will not be that safe. The data could be manipulated by other malicious applets, the generated keys to be used are not the highest random quality, the sensitive data is protected by encryption but the memory is freely accessible. A better approach is to have a dedicated and certified hardware token that handles the security functionality and storage of encrypted sensitive data. This token should have built-in anti-tamper protection.

In case of VoIP it would be attractive to apply a standard VoIP protocol like SIP, or H.323. However, these are open protocols and that is undesirable in a secure product. For this it would be safer to apply a proprietary protocol. An encrypted proprietary protocol is even more secure.

THE COMPUMATICA SECURE MOBILE CONCEPT

Assumed is that the most critical communication functions that need to be protected are voice and SMS traffic since this is in general most frequently used.

Because Compumatica aims for the most secure solution, they chose a VoIP protection with a proprietary encrypted VoIP protocol with a VoIP server developed in house. Also a Key Management System (KMS) is part of the concept. For SMS the standard network is used and all secure SMS messages are sent encrypted through the air and are therefore safe.

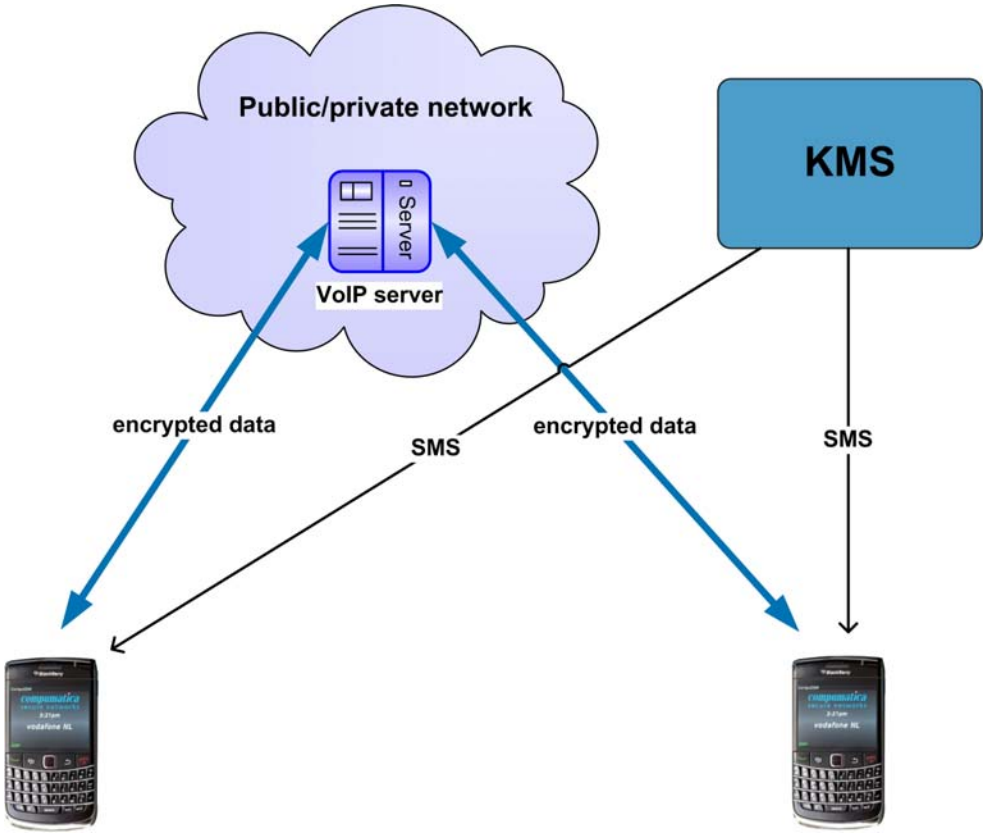


Figure 1: Overview of the Compumatica Secure Mobile Concept

In the above picture the total concept is shown. The VoIP server can be in the public network (internet) or it can be located in a secure area at customer site and can be reached from the mobile devices.

- **VoIP server**

  The VoIP server is a Linux based system. It is configurable via a web interface and it takes care of the connection of the secure devices. The VoIP server is reached by the secure device via a 3G or WiFi connection. The VoIP server makes use of a secure USB dongle which provides security functions. In case the VoIP server is in a public network, it is recommended to protect it with a firewall like the Compumatica CompuWall.

- Mobile phone with **Compumatica Secure Voice application** together with **secure MicroSD card**.

Figure 2: Secure Mobile phone platform with secure MicroSD card

The user interface is intuitive, has the same look-and-feel as the standard users interface and is therefore easy in use. The secure MicroSD card includes an embedded smartchip for the secure functions and retains the encrypted storage of the sensitive data.

- **Key Management System**

  The optional KMS can be used by an organization to manage the key distribution. It sends its key material via secure SMS messages to the mobile devices. In the KMS the group policy is set which determines who can communicate with whom. Thanks to this, user-groups can be created who are allowed to communicate securely with each other. Another function of the KMS is the automated preparation of MicroSD cards with key material (provisioning). The KMS is a Windows application.

The Compumatica secure mobile phone solution fulfils both the high requirements for security as well as for user friendliness. The result is a high-secure product with customer managed Key Management System and VoIP server.

- High secure communications (voice and SMS)
- End-to-end secure voice
- Intuitive user interface
- Own VoIP server
- Own Key management system (option)
- Scalable solution (up to thousands of devices)

The security is guaranteed by the following features:

- Application of MicroSD card with embedded secure smartcard (EAL5+ certified);
- Random data generated from hardware random generators rather than in software;
- Keys, security settings and other sensitive data is stored encrypted in the MicroSD card;
- AES256 encryptions;
- ECDH;
- Groups of users manageable from KMS;
- New session key for each voice session;
- Device reset control possibility from KMS.

The Compumatica Secure Mobile Concept includes a VoIP server with encrypted proprietary VoIP protocol.

Advantages:

- No recognition of the VoIP messages and data by providers; some providers block VoIP.
- No message manipulation possible because of encrypted protocol.
- Polling mechanism that keeps the device connected to the VoIP server even during roaming.
- Own VoIP server, not dependent of a public used VoIP server.

For battery power reduction but also to reduce data traffic costs the device-VoIP server connection can be disconnected in quiet periods. Thanks to an auto-connect mechanism the phone is still reachable for secure incoming calls; in such a case a wake-up SMS will

reconnect the destination device automatically to the VoIP server. As a consequence the destination device will then be able to receive the incoming secure call.

Facts:

Encryption mechanisms	AES256, ECDH, HMAC, SHA256
Security	Usage of MicroSD card in mobile platform with embedded EAL5+ approved smartchip that performs the secure functions.
Random generation	Hardware Random Generator in smartchip.
Supported mobile platforms	BlackBerry RIM OS5, OS7; Nokia Symbian; Android.
Networks	UMTS (3G), WiFi
VoIP server hardware requirements	RAM: 24 GB HD: 120GB SSD/SAS/SATA RAID1 CPU: Intel Xeon i7 W3520 Double source hot switch power supply.
VoIP server software requirements	Ubuntu V10.04 or later. Alternatively: Debian V6.0.
KMS hardware requirements	Any Notebook with internal UMTS SIM slot or USB port for external USB UMTS modem connection; Keyboard: US/English.
KMS software requirements	Windows 7 Professional, English;

CONCLUSION

If you are looking for a secure mobile communication solution and if you want to go for the best without any compromises in user friendliness, then the **Compumatica Secure Mobile Concept** is the best choice you can make.

FLEXIBILITY

The Compumatica concept can be deployed for small cases if you have only a few mobile phones to secure. But even the concept can be scaled up such that it can be used for large-scale networks for securing thousands of mobile phones.

For smaller projects you can choose not to manage and host your own VoIP server. In that case Compumatica offers the possibility to contribute in a VoIP server service, such that you make use of an existing VoIP server, hosted and managed by Compumatica.

Companies or organizations which want to go for the highest security and want to manage the key distribution themselves should incorporate a KMS. With the KMS it is possible to create user-groups each with their own privileges.

BUSINESS PACKAGES

Please contact the Compumatica sales department to discuss the possibilities for a customized package adapted to your needs.

FURTHER INFORMATION

SHORT PROFILE

Compumatica secure networks – based in Germany and the Netherlands – is a fully independent private company with main task securing IP traffic of its customers.

Compumatica develops, produces and implements high level security solutions for all types of IP networks and all types of customers. Customers can be small organizations with just a few countrywide connections up to international enterprises with world-wide networks.

Compumatica staff and products meet high standards of reliability and quality. The products are based on systems that are approved, or even certified, according to the strict regulations of the BSI (in Germany) and the NLNCSA (in the Netherlands). Every single product goes through a quality assurance phase in which it is subject to a long-term test. All *Compumatica* products are backward compatible for more than ten years. Herewith we guarantee our customers investment protection.

Our product range also includes devices from our daughter *.vantronix secure systems* which contain a unique combination of IPv4-IPv6 gateway, router, firewall, network based anti-spam as well as Load Balancer based on OpenBSD. *.vantronix* is a HP AllianceOne partner. The whole software range is therefore available on HP systems.

In the area of mobile communication our range is completed by a comprehensive Secure Mobile Concept that secures voice and SMS and which may be adapted to the individual requirements and needs of the customers.

Our customers are well-known top 500 enterprises as well as government agencies and public organizations in different countries which protect their critical data with the aid of *Compumatica* systems.

As world-wide approved producer and system integrator *Compumatica secure networks* provides complete IT security solutions for networks of each size.

The security of your data is our mission – *we secure YOUR network*.

CONTACT DATA

Germany:
Compumatica secure networks GmbH
Germanusstraße 4
52080 Aachen
Phone +49 (0)241 16 96 400
Fax +49 (0)241 16 96 410
www.compumatica.eu

The Netherlands:
Compumatica secure networks BV
Oude Udenseweg 29
5405 PD Uden
Phone +31 (0)413 334668
Fax +31 (0)413 334669
www.compumatica.eu