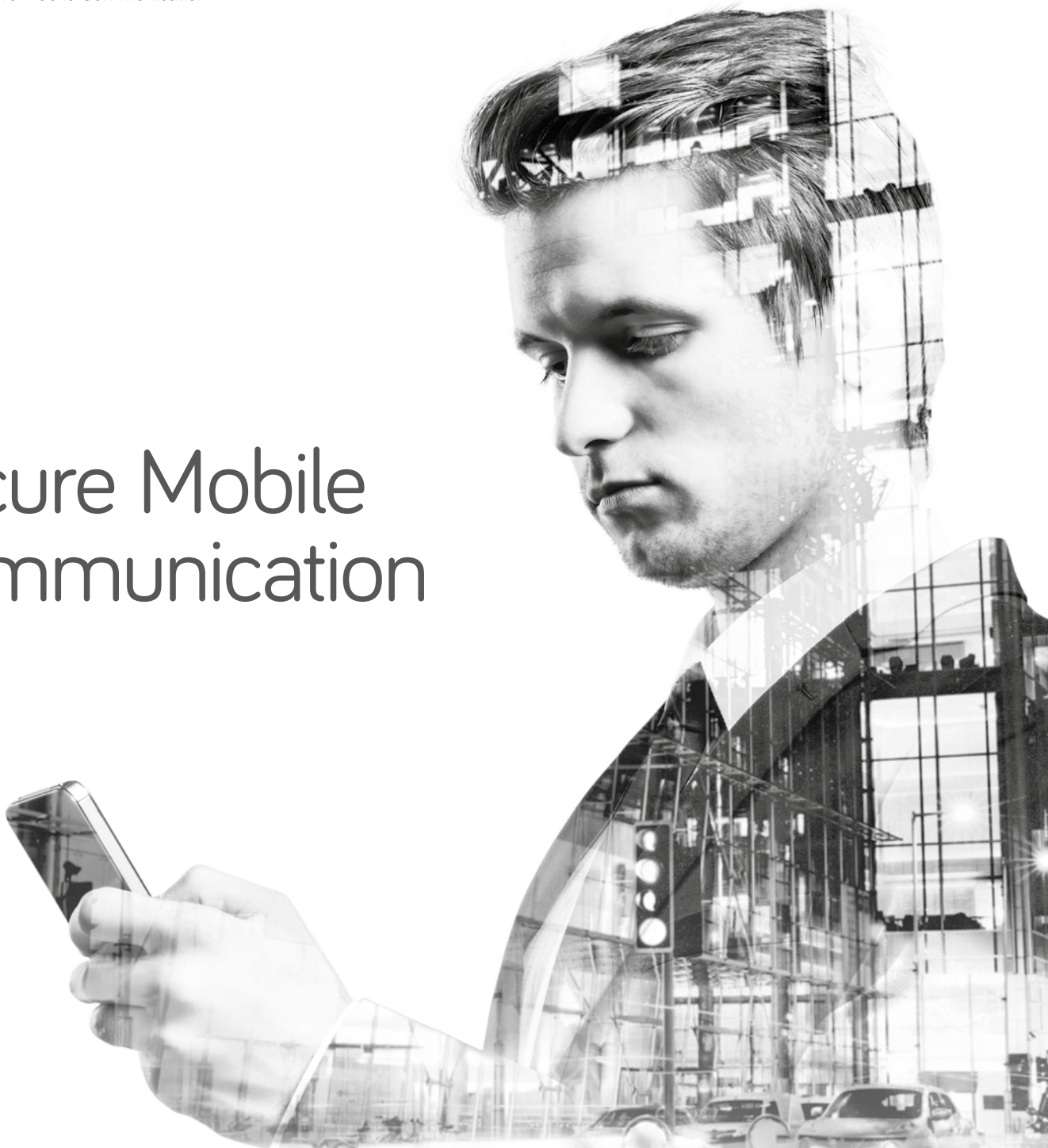# VERJI
Secure Mobile Communication

Secure Mobile Communication

Verji - protects, encrypts & secures mobile communications

Winner at the **European Cyber Security & Privacy Innovation Awards** for Best ICT Security Innovation 2014

ROSBERG
www.rosberg.com

Contents

> Mobile devices now present the Number 1 weakest security link for businesses.
>
> *(CyberEdgeGroup)*

> During 2015, there was a 65% increase in mobile threats from the previous year, with mobile devices providing the easiest entry point to target-rich networks for cyber attackers.
>
> *(Cyberthreat Defense Report 2016)*

> 62% of Information Security Professionals expect a Breach in 2016.
>
> *(Cyberthreat Defense Report 2016)*

1. Introduction

VERJI SMC encrypts mobile communication and protects against hacking attacks.

Most businesses remain unaware of the threat which smartphones present to their organisation and its network infrastructure, staff, customers and stakeholders. SMS attacks, SMS fraud, identity theft, fake cell towers and IMSI catchers are on the increase. The recent Santander SMS phishing - or 'smishing' - scams demonstrate how effective fraudsters are becoming at hijacking genuine text message threads.

In a further cause for concern, the US based '60 Minutes' show were able to hack an American senator's phone remotely, using just the mobile number. The risks are genuine, they are here and they affect every organisation, regardless of size. Smartphone hacking software is cheap and readily available online, allowing criminals to take control of smartphones and access sensitive data and passwords. This is then used to walk right through the door of an organisation's IT security system.
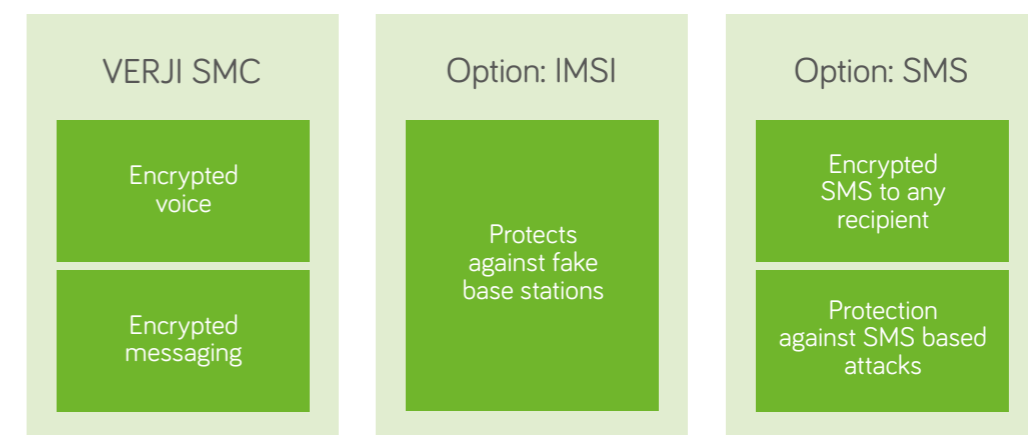
VERJI SMC uses 256 bit AES end to end encryption on speech, messages and attachments, providing superior security. Add any type of attachments directly from DropBox, iCloud Drive or from folders.

VERJI SMC replaces the user's existing text messaging app and is fully integrated with the Telco. VERJI SMC is easy to install and requires no training to use. It can be easily deployed to thousands of employees through the commonly used MDM / EMM systems. If a receiver of a message or call does not have VERJI SMC, the sender is warned that this communication will be without encryption, as a regular SMS or voice call, if approved.

External contacts can be added to the system, enabling encrypted communication invisible to others. What cannot be seen, cannot be traced.

Smartphones are becoming increasingly subjected to silent attacks. Users never know that they are infected and no antivirus can detect these threats.

These stealth attacks are untraceable and until now, there have been no means of protection. The launch of Verji by Rosberg System represents the only scalable, patented, hardware agnostic solution for preventing smartphone attacks.

VERJI SMC	Option: IMSI	Option: SMS
Encrypted voice	Protects against fake base stations	Encrypted SMS to any recipient
Encrypted messaging		Protection against SMS based attacks

2. Encrypted SMS & Voice

Smartphones are becoming increasingly subjected to silent attacks. Users are unaware that their device has been infected and no antivirus can detect these threats.

In other words, these attacks are stealthy, untraceable and until now, there have been no means of protection against them.

For this reason, Rosberg System has developed and patented a solution that combines IP-based highly encrypted messaging with encrypted SMS in one app, replacing the standard SMS app to secure the device.

Send messages to recipients with or without VERJI SMC with ease and securely transfer any kind of file to anyone.

Add to that the ability to defend the smartphone against any type of SMS based attack, as well as the ability to defend against rogue mobile cell towers (IMSI-catchers). It all adds up to a very powerful security solution which, until now, has simply not been available.

The best part? The user will never see it is a security solution, they will just see a very good app that handles everything.

3. Encrypted Messages

All messages between users of the VERJI SMC app use end to end encryption, bypassing the Telco's server all together. Transfer files of any kind, easily, securely & heavily encrypted.

Verji uses the Caller-ID as the identifier, integrating with the phonebook in the same way as the native SMS-app. From the user perspective, it offers secure messaging without having to worry if the user is internal or external. When sending to external users (users who do not have Verji), a warning will be given that the message will be sent to an unprotected recipient. The message will then be transferred to the Rosberg server heavily encrypted,

then the server will decrypt it and deliver it to the Telco as a regular SMS.

Files are also encrypted and sent to the server, placed on a web-server and a link for download is generated and sent as an SMS to the recipient. In this way, the user gets a seamless experience with the same possibilities to devices that can only receive traditional SMS.

VERJI SMC was Awarded *"Best ICT Security Innovation"* at the prestigous European Cyber Security Awards 2014.

4. SMS Based Infections

These attacks use SMS as a means of infecting the phone. One example is the Android vulnerability "Stagefright", which can take complete control of a device after sending a regular MMS message to infect it.

SMS based attacks also use silent SMS messages, which infect the phone at the modem level where the operating system of the modem or SIM card is used to gain access to and install malicious software.

These methods are used by, amongst others, the NSA, with an attack method called Monkey Calendar and by the UK intelligence agency GCHQ through their method, Nose.y.

Who infects?

There are many agencies, governments and industrial entities that resort to espionage. Since SMS is such an old standard and until now not protected, it is fairly easy to infect a smartphone and get access to everything in it. The most advanced infections simply cannot be found. As technology evolves, cheap monitoring solutions have emerged, making it possible to spy on someone's smartphone as easily as checking an e-mail.

Encrypted voice

Wouldn't it be great to have an encrypted voice solution that knows all by itself if the recipient can receive a call encrypted or not?

Wouldn't it be great if all the user had to relate to was just the phone number? And even better, the caller would use this just as they would normally, with no special procedures or hassle.

Verji offers end to end encryption of voice calls for complete security. Talk when no one listens in.

IMSI catcher protection

A mobile phone will always connect to the strongest sender, which opens the possibility for 'a man in the middle' attack using a fake cell tower. These devices are often referred to as IMSI catchers, grabbers or stingrays.

The cheapest can be bought online for less than 2000 USD, while the most advanced can cost up to 2 Million USD.

VERJI SMC protects against IMSI catcher attacks.

5. Benefits of using the award winning VERJI SMC

- Secure voice calls using 256 bit AES end to end encryption
- Secure messaging using 256 bit AES end to end encryption
- Add any file, regardless of file type
- Replaces your existing SMS app
- Protection against SMS based attacks, including silent SMS attacks
- Protection against attacks using fake cell towers
- Buy as a hosted solution or have a dedicated in-house server.
- Easy to install and no training needed to use

- Can be branded with a company logo.
- Provide a branded version of VERJI SMC to valued contacts and enjoy encrypted messaging and speech using unique identifiers known only by the user.
- Intended for corporations, Telcos, ISPs and service providers. Corporations can buy the solution and install it themselves or buy it as a service.
- Available for Android, IOS and Android compatible Blackberry. Windows mobile version currently in development.

6. The complete solution

Users can start out with the two basic components of Verji SMC, the encrypted messaging solution combined with protection against SMS-attacks. This provides an easy to use app, completely integrated with the users' phone book. All messages are highly encrypted to the server and for those sent to others with the same app, end to end encryption provides complete security.

Encrypted file transfer is also included. Add on options are IMSI-catcher protection and encrypted speech, providing the complete protection solution.

7. Verji secures where no one has secured before

There have been security systems available for mobile devices for a long time, but none protect users against infections using SMS. It is like having heavy locks on a front door, whilst leaving the back door unlocked and wide open.

This is why attackers use SMS based attacks. Old school technology and a lack of protection have made it the target of choice. Rosberg System is the first company to provide smartphone users with security in this field without having to buy expensive crypto phones.