SECURE MOBILE COMMUNICATION
MOBILE ENCRYPTION APP

Mobile device management and device security are fundamental components of today's mobile communication solutions. However, complete protection also calls for encrypted transmission beyond the classic provider network standards. The Mobile Encryption App closes this gap securely, quickly and at a manageable cost. The solution encrypts voice data and messages for a wide variety of smartphones. The Mobile Encryption App can be easily installed on smartphone fleets of all sizes. The app can be used on any device that needs to be integrated in this highly secure communication system.

PROTECT TRADE SECRETS

The fight for the raw material called knowledge is in full swing. Industrial espionage is happening right now across the globe. Revelations about eavesdropping practices in mobile communication catch our attention and make us aware more than ever that it can happen to any company. Phone calls and records of call data are always an attractive way for criminally-minded competitors to acquire information. TC infrastructure products that have been compromised or feature back door access are actively pushed into the market. This means it's high time to safeguard particularly sensitive data – as found at Board level, or in strategy, research and development – from eavesdropping and tapping.

The Mobile Encryption App provides verifiable end-to-end encryption for voice communication and messaging.

To use the Mobile Encryption App, the user must have a relevant mobile service contract with a VoIP provider.

T · · Systems ·

KEEP THE CONTENT OF YOUR CALLS AND CALL DATA TO YOURSELF

HOW MOBILE ENCRYPTION WORKS

Download to start
The first step in end-to-end encryption is installation of the Mobile Encryption App on the mobile devices of all communication subscribers. This can be done through a corporate app store or an installation link – without having to "collect" all the devices.

Call encryption
The encrypted call is transmitted through a VoIP connection. At the beginning of every call, a new session key (one-time key) is generated between the two devices used by the call participants. The Mobile Encryption App has no preinstalled keys, since the keys are created on the device in hand. The key is deleted when the call ends. Because the key is deleted immediately, man-in-the-middle attacks by criminals usingopen keys (pretending to be the other caller) can be prevented.

Call data encryption
In addition to encryption of the call content, metadata containing information about sensitive connections is also protected, so that unauthorized persons have no access to information about connections.

Technical requirements
The Mobile Encryption App requires just 4.8 kilobit/s bandwidth, which is much less than other encryption tools. It is therefore suitable for use even in areas with limited network performance. It doesn't even strictly require 3G network coverage – 2G GPRS is fully sufficient. The following operating systems are supported: Android 4.x, iOS 6 and higher.

Encryption facts
- Encryption with the strongest algorithms and longest key lengths
- 4096 bit Diffie Hellman key exchange
- Redundant encryption with two parallel algorithms: AES256 and Twofish (both 256 bit)
- No preinstalled keys
- Security against man-in-the-middle attacks

WHY T-SYSTEMS

When you're ready to start using the Mobile Encryption App, you have access to support at any time. T-Systems will handle the company-wide implementation, rollout and integration for you – for as many devices as you like, for as many individuals and for a wide range of modern smartphones.

- Easy-to-use, comprehensive package with 360° service from T-Systems
- Rapid rollout and scalability for any number of devices
- Optional subscription to the mobile device management platform from T-Systems
- End-to-end solutions for absolute secure mobility

KEY FACTS AT A GLANCE

- **Comprehensive security:** Protection for voice and messaging
- **Rapid implementation:** Comprehensive service from T-Systems
- **Maximum confidentiality & reliable redundancy:** Encryption through two parallel algorithms
- **Reliable redundancy:** Encryption through two parallel algorithms
- **Unpredictable keys:** No preinstalled keys
- **Highly reliable:** Low bandwidth requirement of only 4.8 kbit/s ensures reliable operation even in GPRS and Edge networks
- **Made in Germany:** Mobile security and services made in Germany by Deutsche Telekom

T-Systems offers you 360° service for all matters related to consulting, provision, startup and operation of your Mobile Encryption App encryption solution. So you can always be certain that your sensitive information transmitted through mobile communication only ends up where it belongs!

GET A TRIAL AND VIEW SOURCE CODE

Please visit the website for more information.

ANY QUESTIONS?
Internet: http://security.t-systems.com/solutions/mobile-encryption-app
or simply e-mail to
mobile-enterprise@telekom.de

PUBLISHED BY
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main, Germany