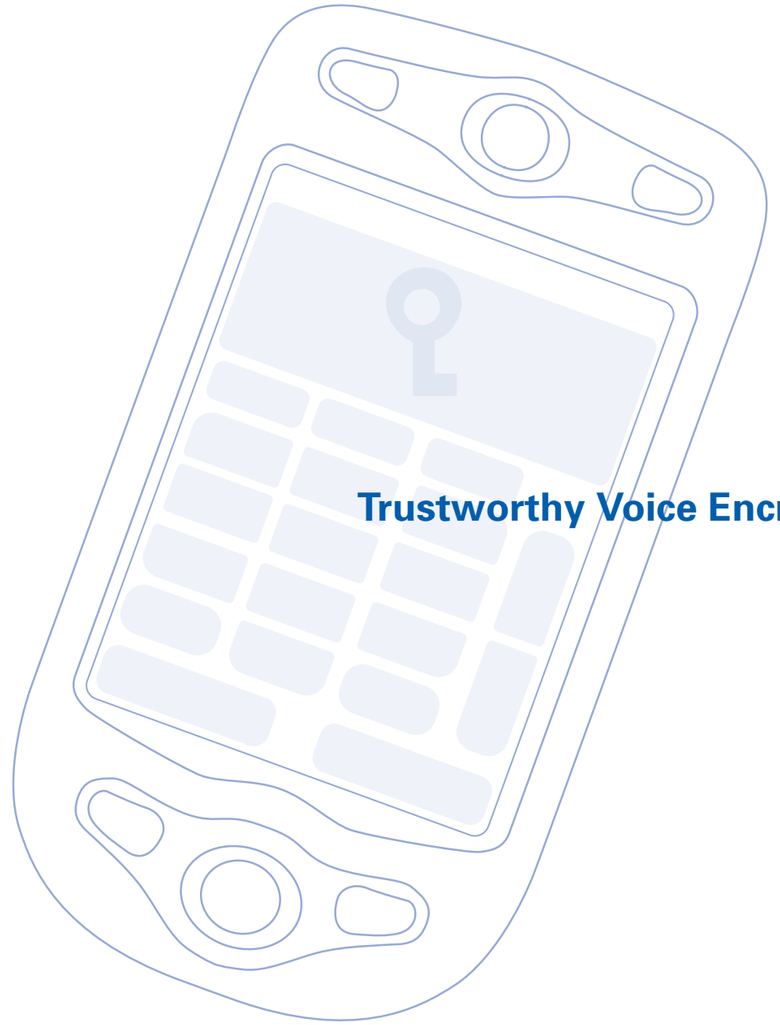
GSMK CryptoPhone 200
Secure Tri-Band GSM Phone



Trustworthy Voice Encryption

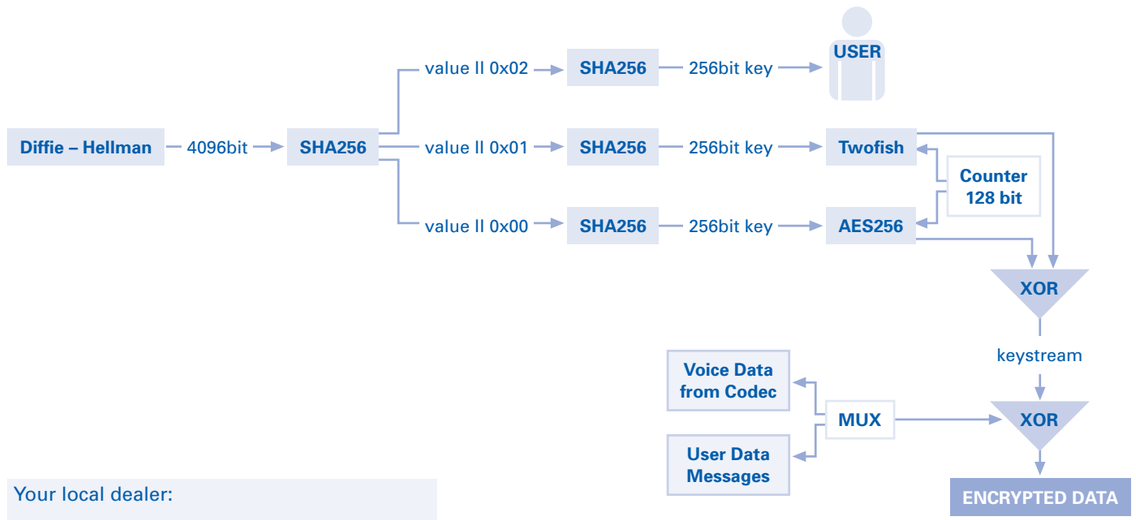
Technical Specifications

Encryption

- Strongest and most secure algorithms available today – AES256 and Twofish
- 4096 bit Diffie-Hellman key exchange with SHA256 hash function
- Only secure mobile phone on the market with full source-code published for independent security assessments.
- Readout-hash based key authentication
- 256 bit effective key length
- encryption key is destroyed as soon as the call ends

- Standby: 180 hours
- Talk time: Secure up to 3 hours 15 minutes, Unsecured up to 5 hours 30 minutes

- Works in any GSM **900/1800/1900** network that provides data-call service (CSD data usually supported while roaming)
- No »proprietary« or »secret« encryption, no backdoors, no key-escrow
- No centralized or operator-owned key generation, no key registration, no extra »security SIM« – just call securely
- Provides effective and affordable protection against both IMSI-catchers and network based interception
- Security of the GSMK CryptoPhone can be independently verified with the published source-code
- Public, standards-based communication protocols for verification and development of compatible products
- Free GSMK CryptoPhone for Windows™ client enables secure telephony between landline users and the mobile GSM CryptoPhone 200, using just a computer with a modem
- Good speech quality (CELP)
- Can also be used with the enclosed professional quality headset (not required for operation, provides both ear-clip and headband mode)
- Packaged in a rugged watertight transport and storage case
- Large display, user-friendly and simple interface
- Based on commercial PDA-phone, accessories are available at normal prices from usual retailers



Your local dealer:

GSMK Gesellschaft für Sichere Mobile Kommunikation mbH Berlin, Germany
Tel: +49 700 CRYPTTEL (27978835)
Fax: +49 700 CRYPTFAX (27978329)
E-mail: sales@cryptophone.de
http://www.cryptophone.de/

CRYPTOPHONE™

GSMK CryptoPhone 200

Trustworthy Voice Encryption

[… Telecommunications interception has developed into a major industry in the last two decades. Intelligence agencies and private organizations within all countries routinely intercept calls that may yield sensitive political, military or economic information.

The Problem

All telecommunication networks worldwide are subject to routine call interception. The use of wiretapping has become so widespread, simple and uncontrolled that you must assume that records of your private calls end up in the wrong hands. Equipment for wireless interception of mobile phone calls has become available at such low prices that it is deployed frequently even in comparatively small business conflicts. So using encryption to protect your privacy is the prudent choice. But protecting your information with strong and trustworthy encryption has become difficult. »Proprietary« or »Secret« algorithms of dubious quality, and encryption that is too weak to protect against modern computing power are commonplace in the telecommunications market. These weaknesses are masked by marketing efforts, suggesting that you need to rely on »the secrecy of the algorithm« or »government classification« – certified by the same intelligence agencies that are actually in charge of telecommunications interception.

Today's Solution

Now there is a solution that you can trust, because it can be verified by you or by your experts. The GSMK CryptoPhone 200, the first secure Tri-Band mobile phone that comes with full source-code available for independent review – is available now. Finally, you can perform a independent assessment to ensure that there is no weak encryption and no backdoors in the device you entrust your telecommunications security to. You don't have to believe us when we say it is secure – you can verify that claim yourself. The GSMK CryptoPhone is not a black-box-device with scarce technical information, like other products in the market. We will give you all the details of its inner workings – even before you buy.
The GSMK CryptoPhone 200 enables you to put the trust where it belongs – into a trustworthy, open and scientific verification process.
The GSMK CryptoPhone technology is based on well-researched algorithms for both encryption and voice processing, the strongest encryption available combined with key length that provides peace of mind today and in the future (See reverse side for technical details).

The GSMK CryptoPhone encrypts your calls with the two algorithms that are regarded strongest by the cryptographic community – AES and Twofish.

Ease of use

The GSMK CryptoPhone 200 is easy to use too. It has a simple interface using a bright and crisp touch screen with large keys and easy to read display, making it an ideal solution for both less technical inclined users and those with slight vision impairment. The included professional quality headset gives you the option to phone handsfree when necessary and to enhance your privacy while phoning in a public place. However, unlike other products, the GSMK CryptoPhone 200 does not require the headset for operation.
The GSMK CryptoPhone 200 hardware is based on a standard GSM equipped PDA-phone. So you can buy accessories on the open market at normal price from your normal retailer channels. Since the GSMK CryptoPhone 200 device is not distinguishable from the »normal« hardware it is based on, you will not get suspicious looks at the airport or border control. You enjoy your privacy – in private.

Landline and satellite telephony solutions

For secure communication from a standard analog (POTS) or ISDN landline with a mobile GSMK CryptoPhone user, you can choose between a dedicated Desktop GSMK CryptoPhone device or the free GSMK CryptoPhone for Windows software. The Desktop GSMK CryptoPhone offers secure communication to other landline, mobile and satellite GSMK CryptoPhone products.[1)] The free GSMK CryptoPhone for Windows software is an excellent way to establish secure communication with partners who do not yet own a GSMK CryptoPhone device. GSMK CryptoPhone Satellite Solutions are perfect for use in areas with bad or no mobile phone coverage. GSMK CryptoPhone Satellite Solutions are becoming available for a number of different satellite systems, such as Thuraya, Globalstar and certain Inmarsat modes. (Please contact us for detailed availability information)
All GSMK CryptoPhone devices and solutions use the same encryption, are fully interoperable and offer the same level of protection against interception across communication networks.
The free GSMK CryptoPhone for Windows software, the full source-code of the GSMK CryptoPhone solutions as well as further product and background information is available in english language at http://www.cryptophone.de/ …]

[1)] Depending on your GSM operator, you may need a separate analogue data-call number to be called from a analogue landline with the GSMK CryptoPhone for Windows software. The sourcecode for the software is also available for review. For further information see user manual and FAQ.