CRYPTOPHONE™

TECHNICAL SPECIFICATIONS

Radio
GSM quad-band 850/900/1800/1900 MHz • UMTS HSDPA/WCDMA 900/2100 MHz with HSUPA support • Up to 2 Mbps uplink, up to 7 Mbps downlink speed

Voice Encryption
Secure voice over IP communication on any network – GSM, 3G, WLAN • strongest and most secure algorithms available today – AES256 and Twofish • 4096 bit Diffie-Hellman key exchange with SHA256 hash function • readout-hash based key authentication • 256 bit effective key length • encryption key is destroyed as soon as the call ends

Message Encryption
Based on the same strong encryption algorithms used for GSMK CryptoPhone voice encryption – 4096 bit Diffie-Hellman initial key exchange, AES256 and Twofish message encryption with 256 bit effective key length. Supports long SMS and encrypted self-destructing "Eyes Only" SMS.

Device Protection
Encrypted storage system for contacts, messages, notes and keys with smart folders protects confidential data against unauthorized access • hardened WM 6.5 operating system with granular security management and streamlined, security-optimized components and communication stacks protects device against outside attacks

GSMK CryptoPhones are the only secure mobile phones on the market with full source code published for independent security assessments. They contain no »proprietary« or »secret« encryption, no backdoors, no key-escrow, no centralized or operator-owned key generation, and require no key registration.

Interoperability
Fully compatible with all GSMK CryptoPhone IP mobile, satellite and fixed-line encryption products • IP PBX integration with virtual extensions

Trustworthy Voice & SMS Encryption

The CryptoPhone 400 comes with full source code available for independent review. Finally, you can perform an independent assessment to ensure that you can rely on strong encryption without any backdoors in the communications device that you entrust your security to. The GSMK CryptoPhone 400 enables you to put the trust where it belongs – in a trustworthy, open and scientific verification process.

GSMK CryptoPhone technology is based on well-researched algorithms for both encryption and voice processing. It features the strongest encryption available combined with key lengths that provide peace of mind today and in the future.

Operational Features
Talk time up to 6 hours • standby time up to 340 hours

Dimensions & weight
103.8 x 57.7 x 11.7 mm • 110g incl. battery • integrated antenna

Display
3.2-inch sunlight-readable touch-sensitive TFT LCD screen with LED backlight @ 480 x 800, 64k colors

Navigation / Buttons
Dedicated talk / hang-up, volume up / down, home and back buttons

Connectivity
Integrated USB/power connector • 3.5mm stereo audio jack • MicroSD memory card slot, SD2.0 compatible • Bluetooth V2.1 with Enhanced Data Rate and A2DP for stereo wireless headsets • GPS • IEEE 802.11 b/g Wireless LAN

Audio Codecs
Encrypted calls: CELP and ACELP® VLBR4 Decoding & playback: WAV, WMA, AMR-NB, AMR-WB, AAC, AAC+, eAAC+, QCP, M4A, MP3, MIDI, polyphonic ring tones
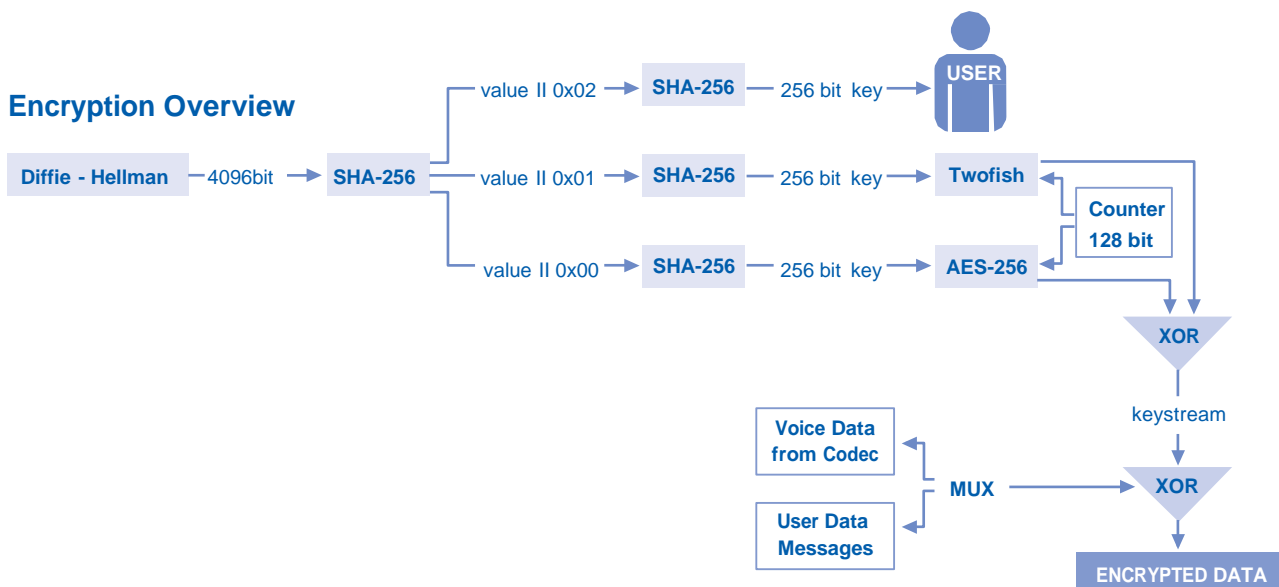
CMOS Camera
5.0 megapixels resolution with auto focus (can be completely disabled upon request)

Standard Accessories
100-240V AC adapter • USB sync cable • stereo headset with microphone

Optional Accessories
12V car charger • solar panel charger • vehicle mount kit

Encryption Overview

Diffie - Hellman → 4096bit → SHA-256 →
- value II 0x02 → SHA-256 → 256 bit key → USER
- value II 0x01 → SHA-256 → 256 bit key → Twofish
- value II 0x00 → SHA-256 → 256 bit key → AES-256

Counter 128 bit → Twofish, AES-256

Twofish, AES-256 → XOR → keystream → XOR → ENCRYPTED DATA

Voice Data from Codec, User Data Messages → MUX → XOR