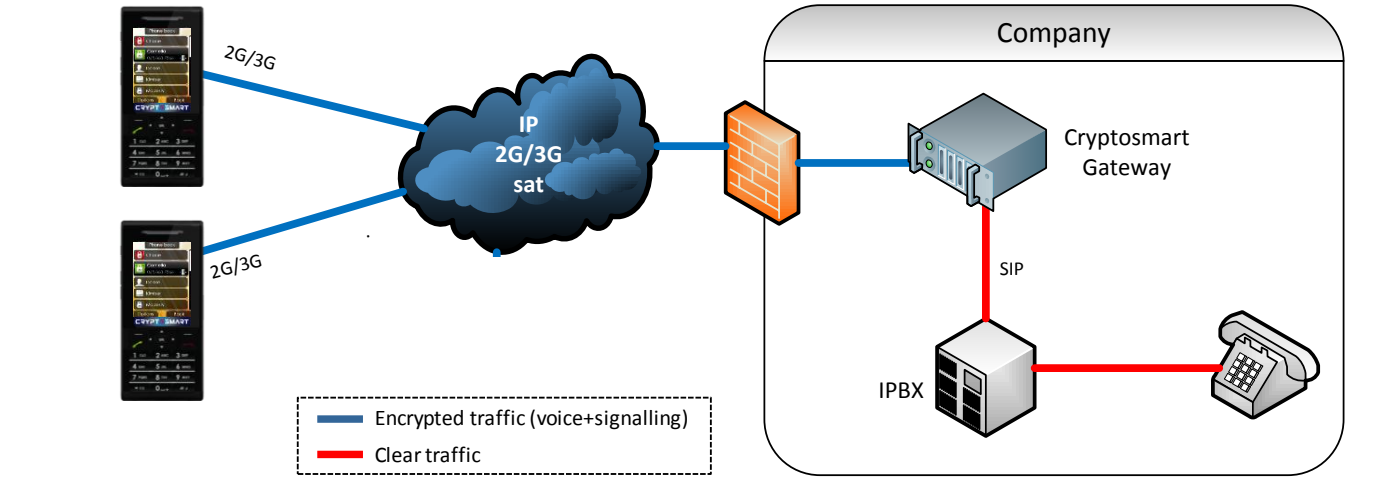
S:PHONE

Secure communications

A secure phone with built-in security, encrypting voice communications, SMS and personal information

- S:PHONE prevents from all threats mobile workers may encounter: lost or stolen terminal, eavesdropping and logical intrusion on handset, thanks to a security solution trusted at governmental level.
- S:PHONE offers secure voice and SMS on GPRS, Edge, 3G, HSPA. It is a cost effective solution based on proprietary Operating System. It provides the first truly user-friendly mobile secure voice solution. S:PHONE enables both encrypted-clear and encrypted-encrypted communications.
- S:PHONE includes a set of security software and a patented encryption technology embedded in a fully secure Smart Card (the chip is certified EAL5+ according to the Common Criteria). An EAL4+ certification of the embedded Java Card applet is in progress.
- S:PHONE features local security as well. All user data are encrypted, all physical and logical communications ports are strictly controlled and device firmware upgrade is under sole TRCom control for each individual device.
- S:PHONE comes with a Device Management ecosystem, enabling remote administration of the phonebooks, remote management of the security and remote monitoring of the devices.

Powered by



S:PHONE - FUNCTIONALITIES — Voice - SMS

- Cryptosmart security engine and smart card
- Encrypted voice (VOIP)
- Encrypted signaling
- Presence management
- Integrated phonebook for secure and clear contacts
- Encrypted SMS
- Integrated User Interface for secure and clear communications management
- Local encryption for personal data (SD memory card, phonebook, SMS database, call history)
- Single Sign On (encapsulating PIN code)
- Device lock screen
- Remote unlock through secure and one-time PUK code
- Remote wiping of user data
- Communication port control
- Comprehensive firewall

S:PHONE

Secure communications

TECHNICAL SPECIFICATIONS

CRYPTOSMART SECURITY

SMARTCARD	
Type of card	• Giesecke & Devrient Mobile Security 3.1 • Includes 1GB mass storage space (flash memory) • Integrates a EAL5+ certified component (ISO 15408)
Cryptosmart applet	• Authentication of remote cards (RSA 2048 bits) • Shared secrets negotiated without possible recovery (Diffie-Hellman 2048 bits) • Anonymity of exchanges (AES 256 bits) • Protection against man-in-the-middle attack • Strict access control policy for the sensitive data stored on the card
Authentication	• Use of security code (4 to 8 digits) • Attempts limited to 3, internally managed by the applet of the card • Remote unlock by secure and one-time PUK codes (8 digits)
PUBLIC KEY INFRASTRUCTURE	
Certificates	• Conform to the X.509 V3 standard • No private extension required
PKI	• Cryptosmart-CardManager (internal PKI) • Third party PKI: Microsoft, OpenSSL, Opentrust, Linagora…
SECURE VOICE	
Signaling	• Use of secure SIP protocol (encryption with AES 256 bits) • Presence management
Voice	• Security key negotiation between cards for each call • Voice encryption (AES 256 bits) • Erasing of security keys at the end of the communication
SECURE SMS	
SMS encryption	• Payload encryption (AES 256 bits) • Encryption key renewal per SMS
LOCAL SECURITY	
Remote terminal erasing	• Administrator sends a one-time secret to the terminal for personal data erasing
Single sign on	• GSM PIN code is securely stored • Access only through Cryptosmart secure code
Local encryption	• Personal data encryption (SMS, files, contacts, call history) (AES 256 bits) • Storage of master encryption key in the smart card
Firewall	• Protection of communication physical ports (USB, Serial Ports) • Reduced set of SIM Tool Kit commands (SIM card embed un-trusted apps) • Filtering of incoming and outgoing TCP connections • Permanent disabling of Java engine to control Midlets • Permanent disabling of Web browser to control malware through the Web • Permanent disabling of GPS to control data transfer • Permanent disabling of NFC interface (Near Field Contact) • Permanent disabling of HAC interface (Hearing Aid Compatibility) • Smart and secure BlueTooth (controlled by administrator, reduced profile set)
MANAGEMENT AND ADMINISTRATION	
Device management	• Full compatibility with recognized market platforms
Cards administration	• Security administration done through Cryptosmart-CardManager

About codec: Cryptosmart's technology uses 15kbps and 6kbps codecs. On a nominal 3G network, the handset uses the 15kbps. Dynamically, the handsets may change the codec to adapt the secure voice flow to a potential reduce bandwidth. In such case, the codec is reduced to 6kbps. Such automatic and dynamic capability enables the users to continue their discussion with no interruption while having a slight decrease in voice quality. Thanks to the full control of the operating system, acoustic latency time has been dramatically reduced to become best-in-class.

S:PHONE

Secure communications

TECHNICAL SPECIFICATIONS

MOBILE PHONE

GENERAL CHARACTERISTICS	
Size	• Dimensions / weight: (L x W x H) 112 x 49,3 x 12,99 mm / ~95g
Power management	• Battery type: 900mAh - Li-ion • Charging time (USB or wall plug charger): 2h • Standby time: 3.5 days • Talk time: 210 minutes (secure call), 270 minutes (clear call)
Display and user interface	• Screen type: 262K colors QVGA, 2.2" , 240x320 pixels • Integrated User Interface for secure and clear functions
Radio	• GSM bands (MHz): 850, 900, 1800, 1900 MHz bands • UMTS bands (MHz): 900 (VIII) and 2100 (I) MHz bands • Type approval: CE / GCF / FCC
Memory	• External: Micro SD HC – 1GB encrypted mass storage on Cryptosmart card
Languages	• Supported languages: English, French
Operating system - Firmware	• Proprietary and 1024 bits RSA firmware signature (S:PHONE unique secret keys)
CONNECTIVITY	
Radio	• GPRS / EDGE: Class 10 • HSDPA: Downlink cat. 8 (7.2 Mbps), Uplink cat. 4 (2Mbps)
Data transfer	• USB 2.0 High Speed • Bluetooth 2.1 EDR (if enabled by administrator) • PC / Mac synchronization
Connectivity plugs	• Mini Jack 3.5mm (audio) and Micro USB
MULTIMEDIA	
Messaging	• SMS: integrated clear / secure conversational SMS with T9 predictive text input • MMS: permanently disabled for security reasons
Videos and pictures	• Camera: 1.3 Mpx, fix focus, 6x digital zoom • Torch on top edge (viewing light) with hardkey • Picture formats: bmp, gif, jpeg • Video playback: 3gp, H263, H264, MPEG4 • Video recording
Music	• Music formats: MP3 , AAC, Wave, AAC+, eAAC+ • Background mode • FM Radio - RDS • Polyphonic ring tones: SP Midi, SMAF, SMF
Localisation	• GPS: permanently disabled for security
CALL MANAGEMENT	
Voice	• Mute mode • Different User Interface for clear and secure calls • Data flow quality indicator for secure calls • Integrated hands-free mode: for secure calls only
Phone book	• Call identification • Integrated phonebook for secure and clear contacts • Personal information management (vCard, etc.)
Advanced	• Silent mode • Conference call: for clear calls only • Call waiting / hold / transfer / forwarding: for clear calls only • Anonymous mode: for clear calls only • Call history • Automatic redial: for clear calls only • Speed dialing: for clear calls only
SPECIAL FEATURES	
Accessories	• Cradle: Yes - Automatic charging cradle • Headset: Stereo headset • CD-ROM: Yes - including User-Guides / PC-Sync tool / USB-drivers • Charger with USB data cable: Yes

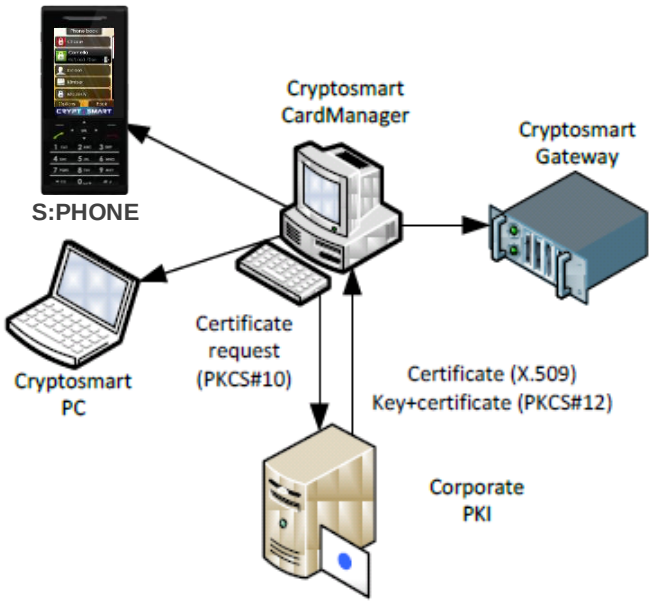
SECURITY OF VOICE COMMUNICATIONS

S:PHONE users can establish voice communications which are end-to-end secured.

In the same way, they can call correspondents on their fixed phone inside the organization.
The voice communications are secured between the terminals and the Cryptosmart-Gateway.
Reciprocally, they can be called by the users of fixed phones.

The keys insuring the security of the communications are negotiated directly between the smart cards. These keys are erased immediately at the end of the communication.

DEPLOYMENT OF KEYS AND CERTIFICATES



Each actor (user, gateway) of the Cryptosmart system has a smart card in charge of the mutual authentication and of the negotiation of exchange keys (confidentiality, integrity and authenticity).

The smart cards contain the private keys of the holder, the associated X.509 certificates and the authority certificates required to authenticate the correspondents.

The smart cards are generated by the Cryptosmart-CardManager tool and are distributed to the different actors. The keys and/or certificates are generated either directly by the Cryptosmart-CardManager or by the corporate PKI.

CONTACT

timereversal COMMUNICATIONS

2 rue du petit Albi
95806 Cergy Pontoise
FRANCE
Tel: +33 1 34 43 48 00
Mail: contact@time-reversal-communications.fr

IBS Varovanje d.o.o
Tomšičeva c. 13
1330 Kočevje, SLOVENIA

tel.: +386 1 546 50 65

INTERNATIONAL BODYGUARD SERVICE