

Protect your mobile communications with secure government solutions



s:PHONE – think safety

Mobile security is a recurring, and ever increasing, concern for businesses and government organizations. While mobile data security has become mass market thanks to mobile email, voice and SMS have remained vulnerable to eavesdropping.

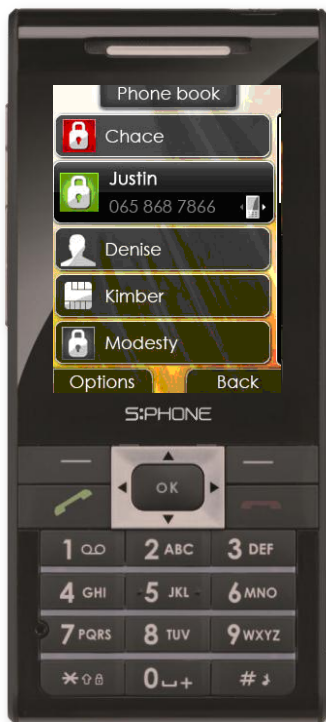
Time Reversal Communications has developed s:PHONE, the first built-in secure mobile phone offering fully integrated protection against stolen terminals, cellular eavesdropping of voice and SMS, intrusion, and personal data theft.

Approved and used at government level, s:PHONE is part of a full security solution that provides secure data access to corporate servers, including email, intranet and file servers.

Security solution have to lie with the IT department, not with a vendor or service provider. s:PHONE secure communications are fully controlled, hosted and administered by the customer's own IT department. It comes with full Device Management enabling remote administration of the mobile devices.

s:PHONE has been co-developed with secure communications specialists ERCOM, using their Cryptosmart™ certified security solution.

Secure Communications



s:PHONE solution overview

Mobile Device

- End-to-End secure voice calls and secure SMS
- Integrated clear and secure communications
- Strong user authentication
- Secure to clear voice calls
- Presence indicator – secure contacts
- Undetectable secure communication
- Full control of all communications ports
- Local Data encryption
- Single-Sign-On – PIN code encapsulated

Remote Device Management

- Phonebook administration
- Security management
- Mobile devices monitoring
- User data wiping

System architecture

- Mobile phone
- Cryptosmart™ microSD - crypto processor & applet
- Cryptosmart™ secure gateway
- Cryptosmart™ CardManager (PC version)



Powered by



s:PHONE solution lies on a central system, made of a Secure Gateway, a CardManager, and implements a Public Key Infrastructure.

The Secure Gateway enables secure interconnection of all the mobile devices of the system, and secure connection to corporate servers and telephone switch (PBX).

The CardManager hosts the Certification Authority of the system and administrates all user's and Gateway security.

Every s:PHONE, PC and internet box embed a Cryptosmart™ card where all critical security operations are executed.

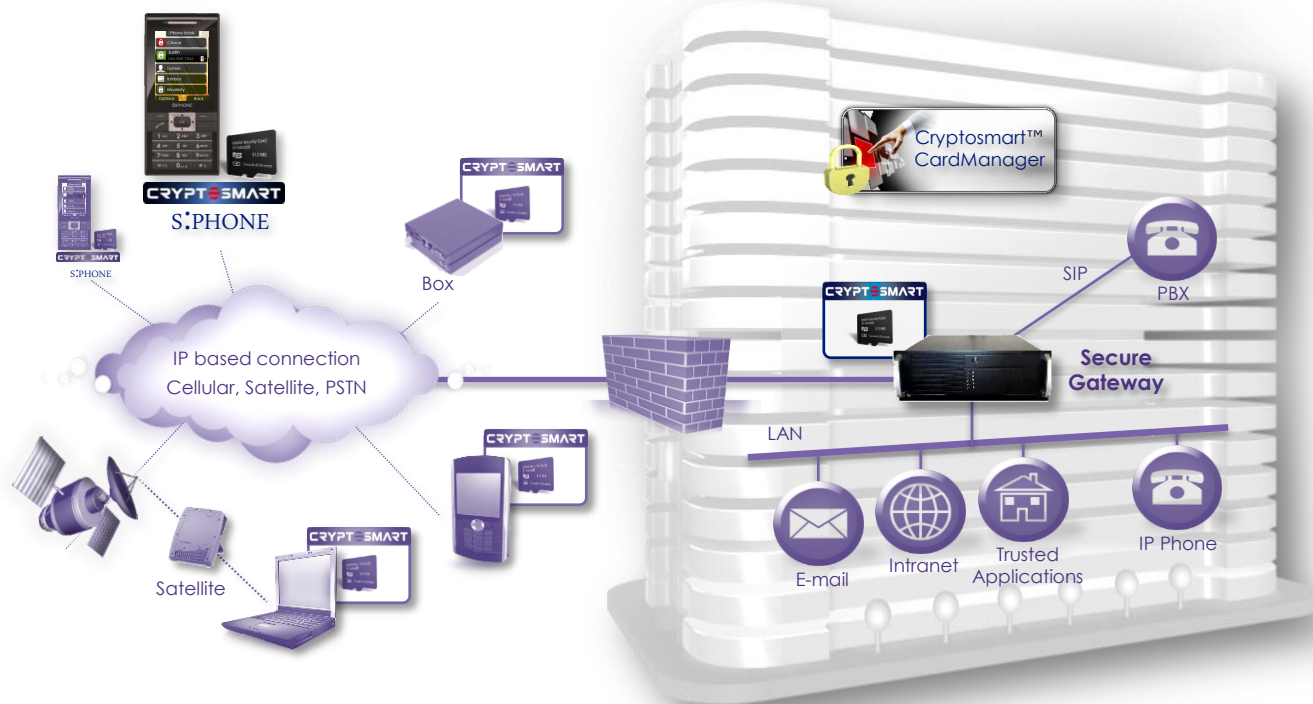
s:PHONE works with standard SIM cards. Voice+Data

subscription is required.

Voice is used for clear calls, while data is used for secure calls (VoIP).

Internet connection for the Gateway is necessary. Optionally, connections to corporate servers through Local Area Network, office phone PBX / IPBX or existing PKI are available.

Time Reversal Communications offers professional services such as system integration, training and annual maintenance.



Mobile phone

- ❑ Rugged Proprietary Operating System RTOS
- ❑ 3G HSPA – 900/2100, 2G EDGE quad band
- ❑ Bluetooth 2.1 (configurable by the admin)
- ❑ Music, FM radio and video players
- ❑ 1.3 Mpx camera, 2.2" screen 240x320 px
- ❑ 112 x 49 x 13 mm, 95 g
- ❑ Local encryption of user's data
- ❑ Firewall (TCP filtering, physical & logical ports control)

Cryptosmart™ security

- ❑ G&D Mobile Security Card - certified EAL5+ (ISO15408)
- ❑ Cryptosmart™ applet EAL4+ certification in progress
- ❑ Possible integration into existing PKI (X509 standard)
- ❑ Authentication of the remote card (2048 bits RSA)
- ❑ Common secret exchange (2048 bits Diffie-Hellman)
- ❑ Protection against man-in-the-middle attack
- ❑ Single usage session key for Voice/SMS
- ❑ Voice and SMS encryption (AES 256)