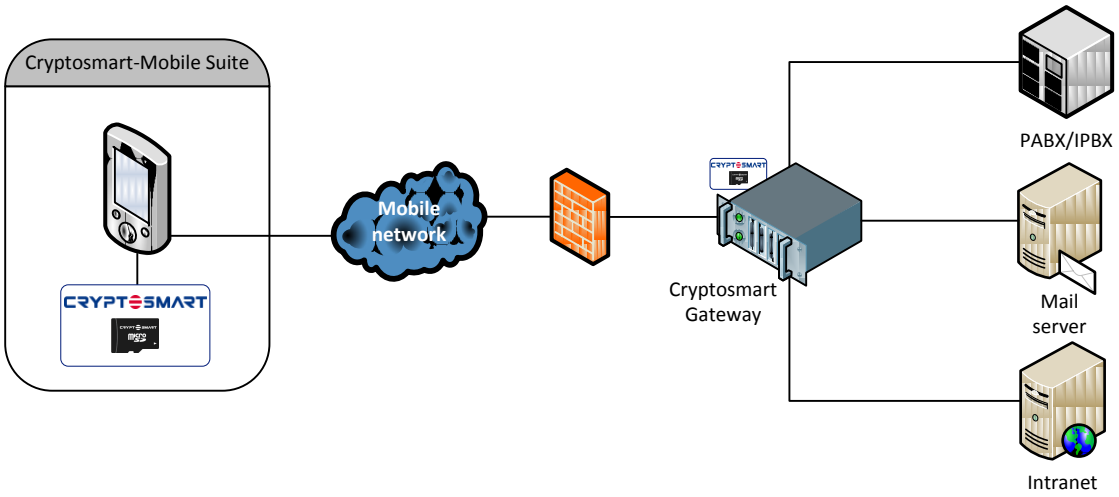
Cryptosmart™ Mobile Suite for Android™



Thanks to its extensive features, Cryptosmart-Mobile Suite prevents against all the threats mobile workers may encounter: **lost or stolen terminals, eavesdropping and intrusion on handsets**.

Cryptosmart-Mobile Suite **secures mobile phones for all communications** (voice, data, mail, SMS) and on all networks (GPRS, EDGE, 3G, HSDPA, LTE™, Wi-Fi®, Satellite, etc). It is a cost effective solution which can be deployed on the latest **Android™** phones. It provides the first truly user-friendly secure mobile voice solution.

Cryptosmart-Mobile Suite includes a set of security software and a patented encryption technology embedded in a fully secured smartcard (EAL5+ smartcard and EAL4+ applet certified according to Common Criteria).

Moreover, it secures all data flows (emails, Intranet/Internet accesses, business applications…) and enables both encrypted-clear and encrypted-encrypted voice communications. Cryptosmart-Mobile Suite also provides strong authentication, a secure lock screen, local encryption of personal data, remote wipe and a local firewall.

CUSTOMER BENEFITS

USERS	INTEGRATION
▪ Covers all user security needs in a simple and coherent way ▪ Transparent security for mail and business applications ▪ Intuitive secure phone application ▪ Single-sign on (only one secret to know) ▪ Compatible with cutting-edge attractive terminals ▪ Remote unlocking through a secure PUK code ▪ Secure voice communications between users of distinct organizations ▪ Secure access to Intranet and Internet	▪ Transport-level VPN requires a single TCP port ▪ NAT and port forward are fully supported ▪ Internal PKI for streamlined secret management ▪ Interoperability with enterprise PKI ▪ Interoperability with Exchange, Lotus® and Linux mail servers

SMART CARD	
Type of card	• EAL5+ (ISO 15408) certified cryptographic chip
Cryptosmart applet	• Authentication of remote cards (RSA 2048 bits/SHA 256 bits) • Negotiation of shared secrets 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 • Access to RSA key by third party applications with PKCS#11 API • EAL4+ (ISO 15408) certified
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	• Conforms 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
Inter-groups	• End-to-end secure communication between users of different Cryptosmart-Gateways • Relationship establishment between gateways is managed by administrators
SECURE SMS	
SMS encryption	• Payload encryption (AES 256 bits) • Encryption key renewal per SMS
SECURE DATA FLOW	
Session management	• Security key negotiation between smart cards • Erasing of security keys at the end of each session
Security	• TCP and UDP traffics encrypted and secured with AES 256 and SHA 256
Filtering	• Individual management of accesses to internal applications
LOCAL SECURITY	
Integrity	• Anti-rooting • Anti-trapping
Remote terminal erasing	• Terminal erasing on invalid security or PUK codes • Administrator can send a one-time secret to the terminal for full erasing
Single Sign On	• GSM Pin code stored in the secure part of the smart card • Access only through Cryptosmart secure code
Local encryption	• User's data (files, emails, contacts, calendar) encryption (AES 256 bits) • Storage of master encryption key in the smart card
Firewall	• Protection of communication physical ports • Filtering of incoming and outgoing TCP connections
WAN/LAN ACCESS	
Connection	• TCP/IP, UDP/IP • Compatible with all wireless networks supporting IP over 10 kbps
Applications	• Interoperable with enterprise applications: email, business applications …
MANAGEMENT AND ADMINISTRATION	
Device management	• Creation and deployment of configurations using the Cryptosmart-Gateway • Security policies broadcast and enforcement • Inventory of terminals on the Cryptosmart-Gateway • Activity monitoring (calls, logs, battery, memory, localization…) centralized on the Cryptosmart-Gateway
Secure administration of the cards	• Done through the Cryptosmart-CardManager
DEVICES	
Operating system	• Android™ V4.2 and upper (list of the supported devices available on demand)

Contact ERCOM for the effective availability of each feature.