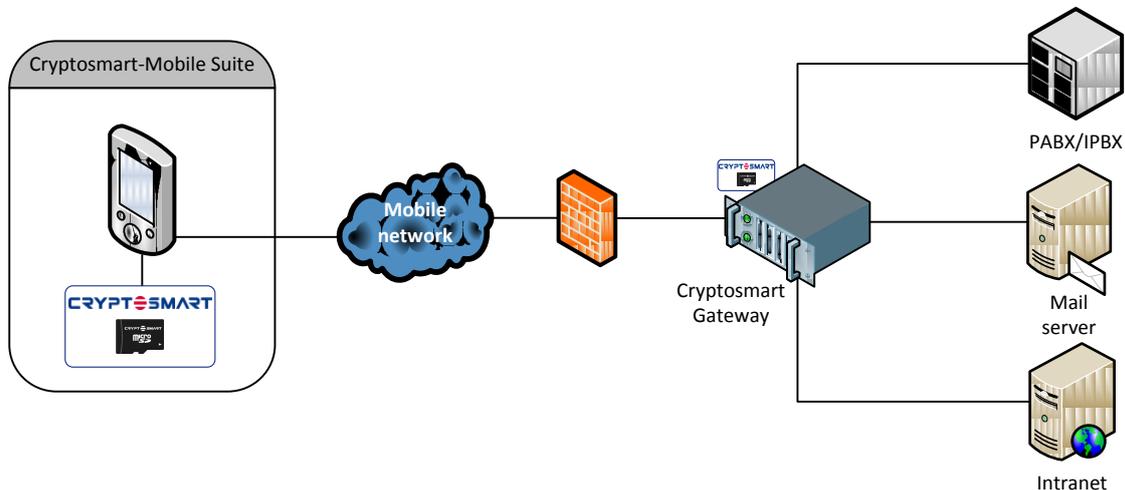


## Cryptosmart™ Mobile Suite for Android™



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
<ul style="list-style-type: none"> <li>▪ Covers all user security needs in a simple and coherent way</li> <li>▪ Transparent security for mail and business applications</li> <li>▪ Intuitive secure phone application</li> <li>▪ Single-sign on (only one secret to know)</li> <li>▪ Compatible with cutting-edge attractive terminals</li> <li>▪ Remote unlocking through a secure PUK code</li> <li>▪ Secure voice communications between users of distinct organizations</li> <li>▪ Secure access to Intranet and Internet</li> </ul>	<ul style="list-style-type: none"> <li>▪ Transport-level VPN requires a single TCP port</li> <li>▪ NAT and port forward are fully supported</li> <li>▪ Internal PKI for streamlined secret management</li> <li>▪ Interoperability with enterprise PKI</li> <li>▪ Interoperability with Exchange, Lotus® and Linux mail servers</li> </ul>

## TECHNICAL SPECIFICATIONS

<b>SMART CARD</b>	
<b>Type of card</b>	<ul style="list-style-type: none"><li>EAL5+ (ISO 15408) certified cryptographic chip</li></ul>
<b>Cryptosmart applet</b>	<ul style="list-style-type: none"><li>Authentication of remote cards (RSA 2048 bits/SHA 256 bits)</li><li>Negotiation of shared secrets without possible recovery (Diffie-Hellman 2048 bits)</li><li>Anonymity of exchanges (AES 256 bits)</li><li>Protection against man-in-the-middle attack</li><li>Strict access control policy for the sensitive data stored on the card</li><li>Access to RSA key by third party applications with PKCS#11 API</li><li>EAL4+ (ISO 15408) certified</li></ul>
<b>Authentication</b>	<ul style="list-style-type: none"><li>Use of security code (4 to 8 digits)</li><li>Attempts limited to 3, internally managed by the applet of the card</li><li>Remote unlock by secure and one-time PUK codes (8 digits)</li></ul>
<b>PUBLIC KEY INFRASTRUCTURE</b>	
<b>Certificates</b>	<ul style="list-style-type: none"><li>Conforms to the X.509 V3 standard</li><li>No private extension required</li></ul>
<b>PKI</b>	<ul style="list-style-type: none"><li>Cryptosmart-CardManager (internal PKI)</li><li>Third party PKI: Microsoft®, OpenSSL, OpenTrust®, Linagora™...</li></ul>
<b>SECURE VOICE</b>	
<b>Signaling</b>	<ul style="list-style-type: none"><li>Use of secure SIP protocol (encryption with AES 256 bits)</li><li>Presence management</li></ul>
<b>Voice</b>	<ul style="list-style-type: none"><li>Security key negotiation between cards for each call</li><li>Voice encryption (AES 256 bits)</li><li>Erasing of security keys at the end of the communication</li></ul>
<b>Inter-groups</b>	<ul style="list-style-type: none"><li>End-to-end secure communication between users of different Cryptosmart-Gateways</li><li>Relationship establishment between gateways is managed by administrators</li></ul>
<b>SECURE SMS</b>	
<b>SMS encryption</b>	<ul style="list-style-type: none"><li>Payload encryption (AES 256 bits)</li><li>Encryption key renewal per SMS</li></ul>
<b>SECURE DATA FLOW</b>	
<b>Session management</b>	<ul style="list-style-type: none"><li>Security key negotiation between smart cards</li><li>Erasing of security keys at the end of each session</li></ul>
<b>Security</b>	<ul style="list-style-type: none"><li>TCP and UDP traffics encrypted and secured with AES 256 and SHA 256</li></ul>
<b>Filtering</b>	<ul style="list-style-type: none"><li>Individual management of accesses to internal applications</li></ul>
<b>LOCAL SECURITY</b>	
<b>Integrity</b>	<ul style="list-style-type: none"><li>Anti-rooting</li><li>Anti-trapping</li></ul>
<b>Remote terminal erasing</b>	<ul style="list-style-type: none"><li>Terminal erasing on invalid security or PUK codes</li><li>Administrator can send a one-time secret to the terminal for full erasing</li></ul>
<b>Single Sign On</b>	<ul style="list-style-type: none"><li>GSM Pin code stored in the secure part of the smart card</li><li>Access only through Cryptosmart secure code</li></ul>
<b>Local encryption</b>	<ul style="list-style-type: none"><li>User's data (files, emails, contacts, calendar) encryption (AES 256 bits)</li><li>Storage of master encryption key in the smart card</li></ul>
<b>Firewall</b>	<ul style="list-style-type: none"><li>Protection of communication physical ports</li><li>Filtering of incoming and outgoing TCP connections</li></ul>
<b>WAN/LAN ACCESS</b>	
<b>Connection</b>	<ul style="list-style-type: none"><li>TCP/IP, UDP/IP</li><li>Compatible with all wireless networks supporting IP over 10 kbps</li></ul>
<b>Applications</b>	<ul style="list-style-type: none"><li>Interoperable with enterprise applications: email, business applications ...</li></ul>
<b>MANAGEMENT AND ADMINISTRATION</b>	
<b>Device management</b>	<ul style="list-style-type: none"><li>Creation and deployment of configurations using the Cryptosmart-Gateway</li><li>Security policies broadcast and enforcement</li><li>Inventory of terminals on the Cryptosmart-Gateway</li><li>Activity monitoring (calls, logs, battery, memory, localization...) centralized on the Cryptosmart-Gateway</li></ul>
<b>Secure administration of the cards</b>	<ul style="list-style-type: none"><li>Done through the Cryptosmart-CardManager</li></ul>
<b>DEVICES</b>	
<b>Operating system</b>	<ul style="list-style-type: none"><li>Android™ V4.2 and upper (list of the supported devices available on demand)</li></ul>

Contact ERCOM for the effective availability of each feature.