Cryptosmart™

Most companies and public administrations use standard mobile devices for daily communications. They enjoy a large panel of devices and mobile networks with a large coverage. Users want to use cutting-edge attractive devices while having the insurance that their voice and data communications are secured.

To answer these issues, ERCOM offers a full secured solution based on standard devices deployable in Europe but also in the rest of the world.

The Cryptosmart solution secures the mobility of Windows® PCs as well as mobile devices running on Android™.

KEY FEATURES

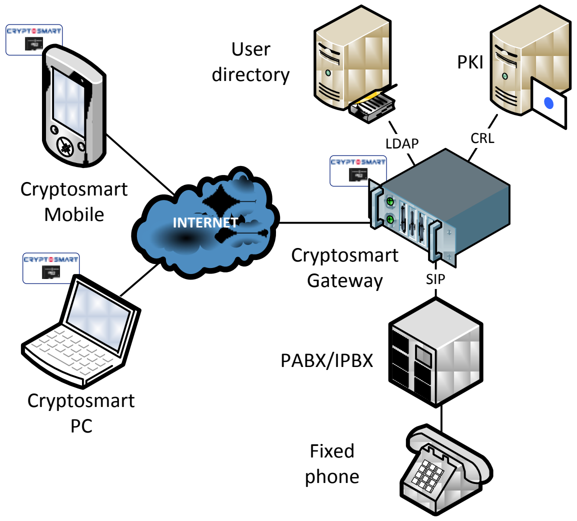
Cryptosmart	PC	Android™
User authentication	■	■
Smart card support	■	■
Remote unlock through secure and one-time PUK codes	■	■
LDAP support for user management	■	■
PKCS#11/CSP interfaces for third party applications	■	■
Local encryption		■
Encrypted signaling	■	■
Presence management	■	■
Encrypted voice (VoIP)	■	■
Inter-group secure voice communications	■	■
Encrypted SMS		■
Data traffic encryption	■	■
Security policies broadcast and enforcement		■
Remote configuration	■	■
Central terminal inventory	■	■
Central activity monitoring	■	■
Remote erasing		■

The functions really available depend of the subscribed license.

CUSTOMER BENEFITS

USERS	ORGANIZATION
▪ Compatible with cutting-edge attractive terminals ▪ Intuitive and ergonomic secure phone application ▪ Transparent security for data communications and local encryption ▪ Secure access to the organization from any country ▪ Secure voice communications between users of distinct organizations	▪ Remote unlock through secure PUK ▪ Transport level VPN requires a single TCP port ▪ NAT and port forward are fully supported ▪ The internal PKI enables an easy key management ▪ Support of organization's PKI ▪ Easy to deploy and to administrate

Security of voice communications

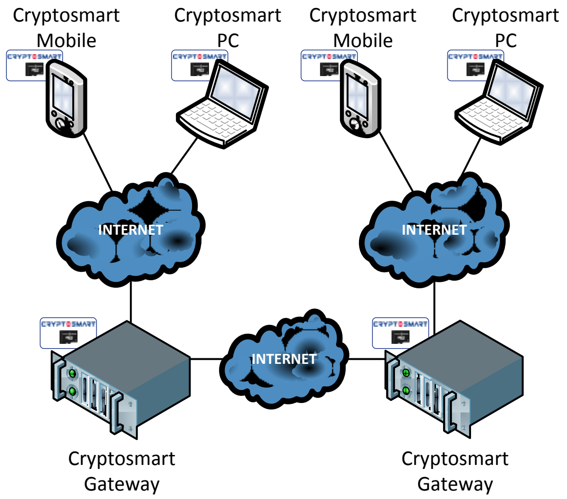


The users of Cryptosmart terminals can establish voice communications that are end-to-end secured.

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.

Voice communications between different organizations

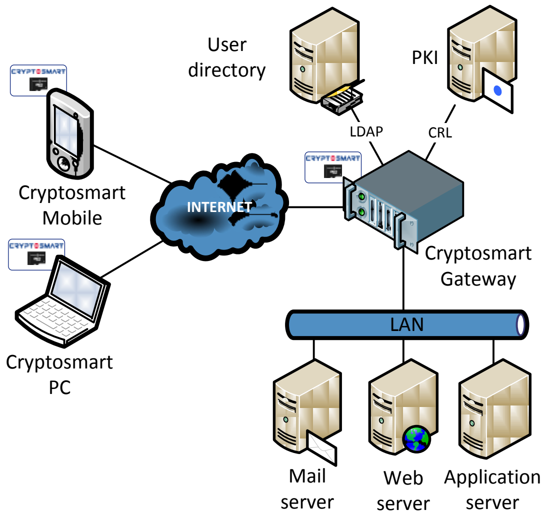


The users of different entities can establish voice communications that are end-to-end secured.

The user's certificates can be issued from the same certification authority (entities of the same organization) or from different certification authorities (distinct organizations).

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

Security of all data traffic

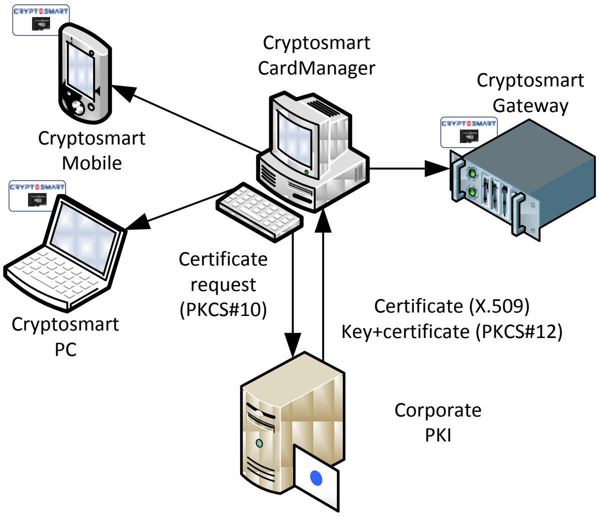


The terminals (smartphone/PC) are connected to the corporate servers to access to mails, web proxies/servers or business applications.

The data traffic is secured between the terminals and the Cryptosmart-gateway. The data flows are transferred through tunnels insuring correspondent authentication, integrity and confidentiality.

The keys insuring the security of the data exchanges are negotiated directly between the smart cards. These keys are renewed periodically and are erased immediately at the end of the session.

Deployment of keys and certificates

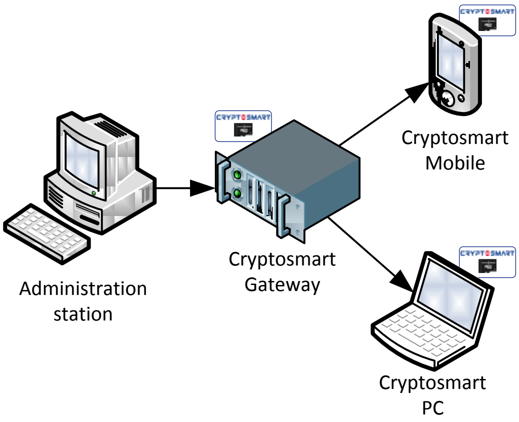


Each actor (user, gateway) of the Cryptosmart system has a smart card in charge of the mutual authentication and of the negotiation of exchange keys (confidentiality, integrity and authenticity).

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. Customers are thus fully independent in terms of cryptography.

Remote administration

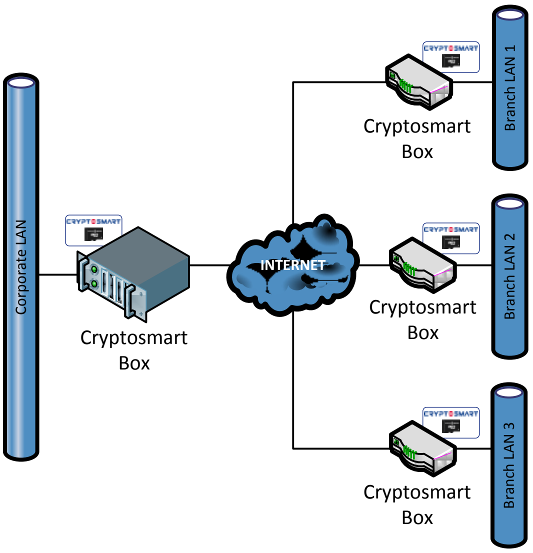


Using the administration tool of the Cryptosmart-Gateway, the administrator defines configurations that are automatically pushed to the user's terminals.

These configurations contain the security policy to be applied as well as other Cryptosmart parameters.

The administrator has the list of terminals as well as information about each of them. In addition, activity monitoring of each terminal is done: secure calls, battery, network, localization...

Network interconnection



The core network of an organization can be securely linked to the LAN of its office branches.

This secured interconnection concerns the data traffic but also the voice communications (TOIP) and videoconferencing flows.

The keys insuring the security of the data exchanges are negotiated directly between the smart cards. These keys are renewed periodically and are erased immediately at the end of the connection.

TECHNICAL SPECIFICATIONS

SMART CARD	
Type of card	• EAL5+ (ISO 15408) certified cryptographic chip • SIM, token or microSD form factor according to usages • MicroSD form factor includes a mass storage space (flash memory)
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 • EAL 4+ (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	• Conform to the X.509 V3 standard • No private extension required
Revocation control	• Use of X.509 CRL • 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
PBX	• Direct link with IPBX using the SIP protocol • Link with PABX using a third-party router for T0/T2 conversion
Inter-groups	• End-to-end secure communication between users of different Cryptosmart-Gateways • Relationship establishment between gateways is managed by administrators
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 • IP traffic (IPsec) is encrypted and secured with AES 256 and SHA 256
Filtering	• Individual management of accesses to internal applications
LOCAL SECURITY	
Integrity	• Anti-rooting • Anti-trapping
Local encryption	• Data encryption (AES 256) • In-place and on-the-fly security
Firewall	• Protection of the physical communication ports • Filtering of incoming and outgoing TCP connections.
ADMINISTRATION	
Users	• User management in the Cryptosmart-Gateway or in an external LDAP directory
Device management	• Creation and deployment of configuration using the Cryptosmart-Gateway • Inventory of terminals on the Cryptosmart-Gateway • Activity monitoring (calls, logs, battery, memory, localization…) centralized on the Cryptosmart-Gateway • Remote erasing
Secure administration of cards	• Done through the Cryptosmart-CardManager
OPERATING SYSTEM OF THE TERMINALS	
PC	• Windows® XP (32 bits) • Windows Vista® (32 bits) • Windows® 7 (32 and 64 bits) • Windows® 8 (64 bits)
Smartphone/Tablet	• Android™ • List of the qualified devices available on demand

Contact ERCOM for the effective availability of each feature.