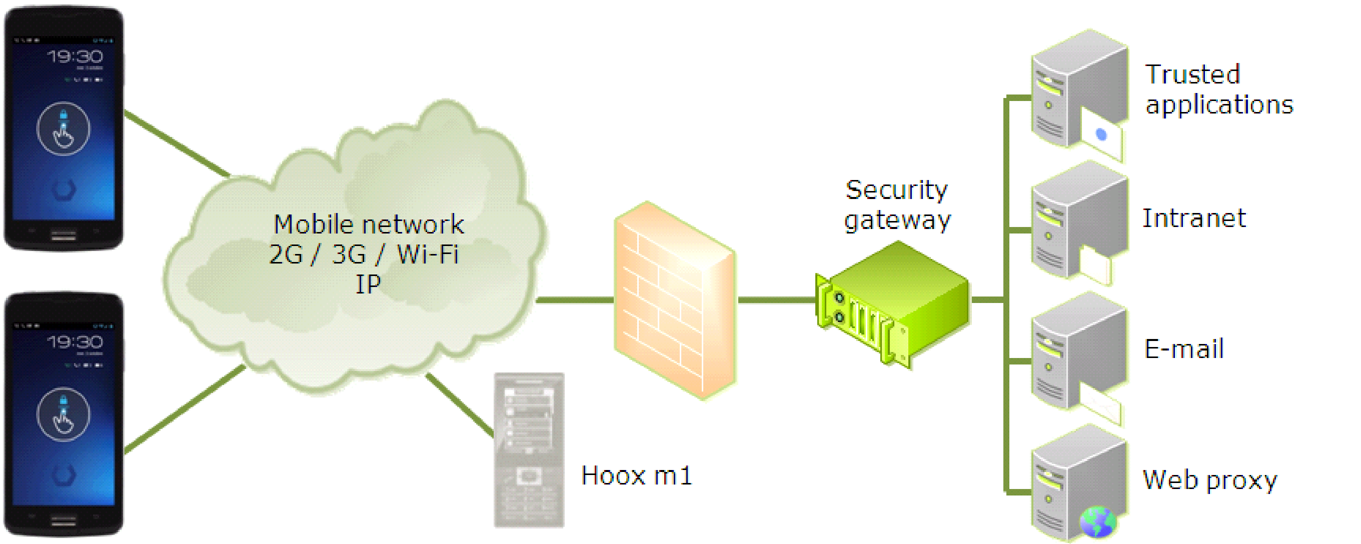
Hoox™ m2

Secure smartphone for professionals

Hoox m2 is a smartphone not only securing voice, SMS and data communications in transit, but also all applications and data at rest.

- **Hoox m2** protects from all cyber threats that a mobile user may experience: loss or theft of the terminal, eavesdropping or fraudulent intrusion, thanks to a government grade solution.
- **Hoox m2** includes a complete security engine, based on a certified technology, embedded in two smart cards for a very high level of security. The first smart card performs cryptographic operations for authentication and encryption, whereas the second operates system and biometrics security.
- **Hoox m2** secures voice, SMS and data communications on mobile and Wi-Fi networks. This is a moderated cost solution, based on a secure operating system. Easy to use and user friendly, it secures every kind of business communications.
- **Hoox m2** provides local security. User data is encrypted, physical and logical ports are under strict control, and Hoox system upgrade is highly secured.
- **Hoox m2** includes a complete remote administration solution for managing the address book and the configuration of the fleet of terminals.

POWERED BY CRYPTOSMART
a trademark of ERCOM



Hoox m2 FUNCTIONNALITES

- End-to-end secure voice and SMS communications
- Secure data communications via a ciphered tunnel (secure access to emails, internet, intranet…)
- Trust chain control for the boot (anti-rooting, operating system cannot be compromised)
- Unified and ergonomic user interface for contacts and SMS (mistake proof secure/clear actions)
- Secure access to Hoox system through cryptographic authentication, and biometry or PIN code
- Local data encryption
- Rugged operating system, subject to periodic security upgrades
- Applications under the sole control of the administrator, with associated security services
- Security engine based on hardware and certified components
- Security administration through a Public Key Infrastructure (PKI)
- Secure Mobile Devices Management (MDM) for an easy fleet administration

Hoox™ m2

Secure smartphone for professionals

TECHNICAL SPECIFICATIONS

LOW LAYER SECURITY, CRYPTOGRAPHY

SMARTCARD AND END USER AUTHENTICATION	
Type of card	• Micro-SD shape, Integrates a C.C. EAL5+ certified component (ISO 15408)
Cryptosmart applet	• Applet is Common Criteria EAL4+ certified (ISO 15408) • Authentication of remote cards (RSA 2048 bits) • Shared secrets negotiated without possible recovery (Diffie-Hellman 2048 bits) • Anonymity of exchanges (AES 256 bits) and protection against MIM attacks • Strict access control policy for sensitive data stored on the card
Logical authentication	• Use of 4 to 8 digits security code, 3 attempts only (controlled by the smart card) • Remote unlock by secure and one-time used PUK codes (8 digits)
Biometric authentication	• Ergonomic and secure fingerprint control (anti-spoofing) • Sensor with hardened coating for long lasting life duration • Secure storage of biometric data

PUBLIC KEY INFRASTRUCTURE	
Certificates	• Conform to the X.509 V3 standard, no private extension required
PKI	• CardManager (internal PKI) or 3rd party PKI: MS, OpenSSL, Opentrust, Linagora…
PKI administration	• Centralized management of the PKI thanks to the CardManager

SECURE VOICE - VOIP (*)	
Signalization	• Secure SIP protocol (AES 256 bits encryption), with presence management
Voice	• Security key negotiation between cards for each call • Voice encryption (AES 256 bits) • Encrypted peer-to-peer file transfer during voice communications

SECURE SMS	
SMS encryption	• Payload encryption (AES 256 bits), encryption key renewal per SMS • SMS database encryption

SECURE DATA FLOW	
Session management	• Security key negotiation between smart cards • Erasing of security keys at the end of each session
Security	• TCP traffic encrypted and secured with AES 256 and SHA 256
Filtering	• Individual management of accesses to corporate application servers

LOCAL SECURITY	
Single Sign On	• GSM PIN code and messaging pass-code are securely stored • Global terminal unlocking via security code or biometry
Local encryption	• Personal data encryption (SMS, files, contacts, e-mails,…) (AES 256 bits) • Encrypted file storage: up to 6 GB • Storage of master encryption key in the smart card

WAN/LAN ACCESS	
Connection	• TCP/IP, UDP/IP • Compatible with all wireless networks supporting IP over 10kbps
Applications	• Compatible with most enterprise applications: mail, intranet, web proxy, corporate application servers…

REMOTE MOBILE DEVICE MANAGEMENT	
Communications	• Encrypted communications for mobile device management (AES 256bits)
Downstream administration	• Terminal temporary blocking, or permanent revocation with data wipe • Phonebook management • Security parameters (locking, data services, Wi-Fi networks) • Enable / Disable peripherals (cameras, GPS, Bluetooth, USB, biometry, Wi-Fi)
Upstream administration	• Terminal statistics (battery level, network, identifiers, version, uptime) • Secure calls statistics (identifiers, duration, cell), confidentiality option

(*) About codecs: Hoox technology uses 15kbps and 6kbps codecs. On a nominal 3G network, handset uses the 15kbps. Handsets may change the codec to adapt secure voice flow to a potential lower bandwidth. In such case, the codec is reduced to 6kbps. Such automatic and dynamic capability enables users to continue their discussion while having a slight decrease in voice quality. Thanks to the full control over the terminal, acoustic latency time has been dramatically reduced to become best-in-class

Hoox^{TM} m2

Secure smartphone for professionals

TECHNICAL SPECIFICATIONS

TERMINAL

GENERAL CHARACTERISTICS	
Dimensions	• Size / Weight: (L x l x thickness) 140 x 69 x 10 mm / ~170g
Energy	• Battery type: 3.7V - 2000mAh - Li-ion • Charging time (USB or wall plug charger): 2h
Display and user interface	• Screen type: capacitive touch-screen QHD 960x540px, 4.68" • Integrated User Interface for secure and clear functions
Frequency bands	• GSM bands: 850, 900, 1800, 1900 MHz • UMTS bands: 900 (VIII) 1900 (II) et 2100 (I) MHz
Processor	• 1.2GHz, quad-core cortex A5
Memories	• Flash: 8GB; RAM: 1GB
Cameras	• Back: 5Mpx Autofocus, flash light • Front: 0.3Mpx
Sensors	• Proximity, accelerometer, ambient light • Geolocalisation: GPS / A-GPS
Languages	• Supported languages: English, French (other languages: please contact us)
Accessories	• Stereo hands free kit (wired) • Charger with removable USB cable, 100-240V-AC, 50-60Hz / 5V-DC, 1A
CONNECTIVITY	
Radio	• HSPA: Downlink 7.2Mbps, Uplink 5.76Mbps (peak rates) • WCDMA: Downlink / Uplink 384Kbps • EDGE: Class 12, Downlink 237Kbps, Uplink 118Kbps (peak rates) • GPRS: Multislot class 10, Downlink 85.6Kbps, Uplink 42.8Kbps (peak rates)
short range radio	• Wi-Fi 802.11 b/g/n • Bluetooth 3.0
Wired ports	• USB 2.0 High Speed (micro USB) • Mini Jack 3.5mm (audio)
APPLICATIONS AND RELATED SECURITY	
Messaging	• E-MAIL: secure messaging client, Exchange compliant • SMS: integrated clear/secure SMS thread, predictive text input and dictionary • MMS : permanently disabled for security reasons
Contact list	• Unified contact scheme for secure, professional and personal contacts • Presence indicator for secure contacts. Favorite contacts management.
Agenda	• Agenda is synchronized with corporate messaging service
Web browsing	• Secure web browser
Other applications	• Professional applications integration & verification on request. Please contact us.
TERMINAL SECURITY AND INTEGRITY	
Boot	• Secure boot (anti-rooting), with system integrity control
Terminal locking	• Exhaustive terminal locking. This lock cannot be disabled by end user. • Terminal unlocking via security code or biometry • Event notifications via icons only (ne preview of sensitive content)
Secure operating system	• Based on Android AOSP 4.1.2 (Jelly Bean) • Additional security processes Strict management of system rights and permissions • Reduction of the surface of attack • Anti-rooting: no possible privilege escalation
Strict control of ports	• IP tunneling to security gateway only • USB: enabled/disabled by administrator, restricted protocols • Bluetooth: enabled/disabled by administrator, restricted protocols • Wi-Fi: enabled/disabled by administrator, restricted protocols • NFC, Zigbee: permanently disabled for security reasons • AT Commands, SIM Tool Kit: restricted set of commands
Secure management of applications	• Secure application installation engine • Strict and centralized management of rights and permissions • Integrity of pre-installed applications verified at each system boot

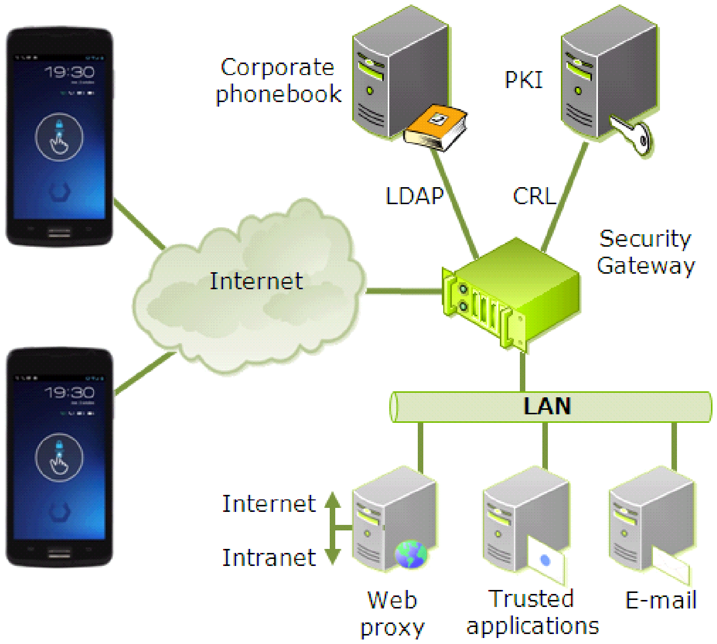
Hoox^{TM} m2

Secure smartphone for professionals

TECHNICAL SPECIFICATIONS

USE CASES

SECURE DATA COMMUNICATIONS

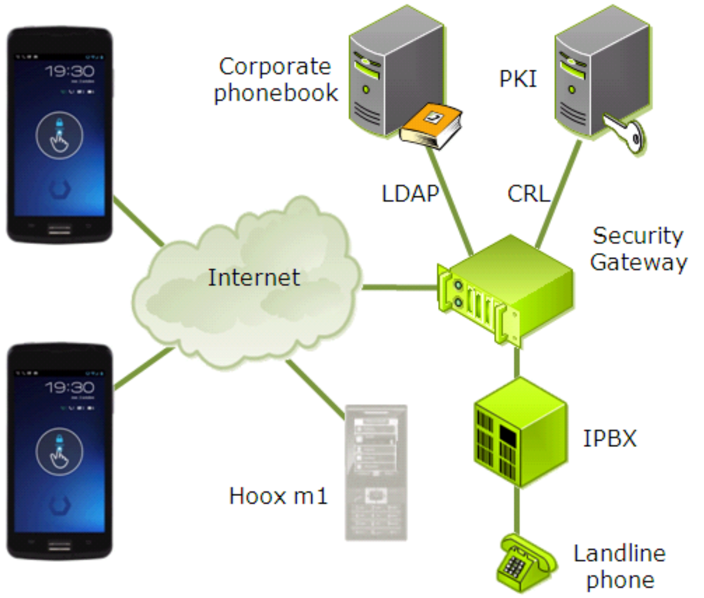


Hoox m2 terminals are remotely connected to different servers in the organization to access messaging, Web proxy or other corporate servers.

Data traffic is secured between **Hoox m2** terminals and the security gateway. Data streams are carried in tunnels providing peer to peer authentication, integrity and confidentiality.

The key to ensure security of each connection are negotiated directly between the smart cards.

SECURE VOICE COMMUNICATIONS



Hoox users can establish voice communications which are end-to-end secured between them.

They can call correspondents on their office phone inside the organization.
Voice communications are secured between the **Hoox** terminals and the security gateway, and in clear mode up to the office phone, through the IPBX connected to the gateway.
Reciprocally, **Hoox** users can be called by the users of fixed phones.

One time used keys insuring the security of the communications are negotiated directly between the smart cards, during each call setup.

CONTACT

TIME REVERSAL COMMUNICATIONS, A BULL GROUP COMPANY

Parc Saint Christophe, 10 avenue de l'Entreprise, 95861 Cergy-Pontoise,
FRANCE
Tel: +33 1 34 43 48 32, E-mail: contact@time-reversal-communications.fr