CRYPTOSMART

BY ERCOM

THE ULTIMATE SOLUTION TO SECURE
MOBILE COMMUNICATIONS AND DEVICES

IN PARTNERSHIP WITH

SAMSUNG

ERCOM - A THALES COMPANY

Mobility and Cybersecurity Concerns

Why is it important?

1/3

organisations admitted that their data had been compromised through a mobile device
source: Verizon (2019)

€250

the price of a mobile interception on the dark web

93 %

of companies are concerned about mobile security issues with the growing number of professional mobile devices
source: IPass (2018)

What are the consequences?

Cybercrime is sometimes described as **"the new 21st century threat*".**
Everyone is affected, multiple risks are associated with it:

- Leaks of classified information
- Theft of industrial secrets
- Loss of sales opportunities
- Theft of customer databases
- Service interruption
- Damage to reputation
- etc.

Mobility solutions offer gateways to organizations' IT systems (governments, administrations, companies). Cyberattacks can result in heavy financial losses and can lead to impacts on national security.

The rules enforced by the latest data protection reform in the EU, require companies to implement adequate measures to protect personal data. In case of compliance failure the companies risk a fine up to 4% pf their total turnover.

* Quote from Mireille Ballestrazzi, Interpol CEO

Market answers

What is the adequate solution?

It is sometimes difficult for organizations to choose from the many solutions that claim to secure mobile communications.
Here is a list of selection criteria to help you make your decision based on your needs.

1 What type of solution?

Software (SW)

Mobile applications are generally compatible with different types of mobile devices and OS (Android, iOS,..). They are mainly used to offer a first level of security.

Software + Hardware (SW+HW)

Solutions based on a hardware element, provide a higher level of security.

2 Which devices?

Consumer electronic devices with application

Compatibility with Android and iOS. Mobile applications offer a first level of security although they do not provide a fully secured environment.

EOM secured devices

They generally provide a secure hardware and software environment. They are usually lagging behind in terms of ergonomics, performance and functionality, all of which can hinder user adoption.

Consumer electronic device with HW+SW solution

They generally offer high-level security, combined with best-in-class consumer electronic device user experience.

3 Which functionalities?

Local device protection

Secure boot and OS, local data encryption and control of USB / Bluetooth ports.

Secured data

Data communications are encrypted in a VPN between the devices and the organization's IT system.

Secured voice

End-to-end encrypted voice call or up to the organization's PABX.

Secured SMS

End-to-end encrypted text messages.

Strong authentication

Use of a hardware element to secure mobile device access.

4 Which security management?

Internalized architecture

The organization has control of the solution as well as total control over the data, servers and encryption keys. This architecture is recommended for a higher level of security.

Externalized architecture / SaaS

The organization hands over the control and administration of the solution to a third party, which can then access the sensitive data. This architecture is secured provided the third party is a trusted partner and the solution is privacy by design.

5 Which security level?

Local and international certifications

Certifications are issued by recognized authorities, based on an evaluation of the classification level for information that can be stored and communicated . Those approvals are based on Common Criteria certifications as well as local or international standards.

Common Criteria

EAL certifications evaluate IT software and solutions to guarantee the compliance with the required assurance level. They are internationally recognized.

Cryptosmart: mobility, security and simplicity

Protect your device and sensitive communications in mobility conditions, and in the event of device loss, theft or eavesdropping.

1 What type of solution?

Software + Hardware (SW+HW)

- Use of the latest features and security measures offered by the Android OS
- Use of a powerful certified cryptographic smart card (micro SD card or SIM)

2 Which devices?

Consumer electronic devices with HW+SW solution

Cryptosmart creates a fully secured environment on the latest Samsung Galaxy devices equipped with a Cryptosmart smart card

3 Which functionalities?

Strong authentication

Full device encryption

Secured data

End-to-end secured voice

End-to-end secured SMS

Samsung Knox Security Features

Mobile Device Management (MDM)

4 Which security management?

Internalized architecture

Cryptosmart infrastructure deployed in the client's organization computer system offers full control over company security and its operational processes

Externalized architecture / SaaS

Cryptosmart infrastructure deployed and operated by Ercom in the cloud provides turnkey security

5 What security level?

Local and International certifications*

ANSSI: Restricted
NATO: Restricted
EU: Restricted

Common criteria certification (ISO 15408)

Cryptographic component
- **EAL5+**

Cryptosmart smart card
- **EAL4+**

They trust us

elysee.fr

Confidential
CAC 40 **OIV**
customers

Restricted*

* Approval restricted for version 5.2 ongoing

Cryptosmart: flexible and user-friendly

A large range of compatible devices

Thanks to a close collaboration with Samsung, Cryptosmart solution is compatible with the latest Smartphones and tablets equipped with Samsung Knox* technology.

SAMSUNG SAMSUNG Knox

The CyberSIM of your choice

Cryptosmart encryption keys are stored in a secure hardware element, the cyberSIM :

- Provided separately from the operator SIM card to benefit from Cryptosmart regardless of your mobile phone contract.
- Provided by your mobile operator to combine your mobile phone contract and Cryptosmart service into a single SIM card.

Accelerated deployment and updates

- NFC or QR code installation.
- Update "over the air".

Secured workspace

SAMSUNG
Galaxy A

Security on mid-range smartphones

SAMSUNG
Galaxy S

Security on top-range smartphones

SAMSUNG
Galaxy Tab

Security for paperless workspace

SAMSUNG
Galaxy Xcover
Galaxy Tab active

Security on rugged smartphones and tablets

Cryptosmart PC: a simple and powerful VPN

To secure remote and critical connections

In order to address the new mobility and remote work stakes, Cryptosmart PC is a sovereign VPN solution to secure the connections of your remote Windows computers.

Authentication and encryption

Cryptosmart encryption keys are stored on a secured hardware, the CyberSIM:

- USB or Smartcard Token
- Cryptosmart applet EAL4+ certified
- Certificate customisation via an external or internal PKI
- Negotiation of shared secrets without possible recovery (Diffie-Hellman 2048 bits)
- PIN code security (4 to 8 figures)
- (Un)blocking with PUK code

Simple deployment

- " Client " mode (software and settings installed on the PC)
- VPN management and administration via Cryptosmart Gateway
- Windows 10 compatible
- Linux version on request

Secured workspace

Use Cases

How does Cryptosmart accompany me when I work remotely?

Cryptosmart offers various security features for remote working:

- full device content encryption
- remote device wipe in case of loss or theft
- assurance that the connection to the company resources is secure: remote or mobile teams can work in confidence there is no risk of intercpetion.

How Cryptosmart secures my communications with my customers and suppliers?

Cryptosmart users can secure calls towards any external contact (partners, customers, suppliers). There are two main scenarios:

External contacts equipped with Cryptosmart:
Different organizations can connect their Cryptosmart systems thanks to the Cryptosmart Intergateway, thus allowing their users to make secure calls with cross-organization end-to-end encryption.

There are multiple usages:

- between different ministries of a government
- between governments of allied countries
- between government entities and private companies
- between private companies

External contacts not equipped with Cryptosmart:
The communication is secured from the Cryptosmart device up to the organizations IT system, and then travels over the standard fixed or mobile network.
For example, a user establishes secure communication from a Cryptosmart device to a non-secure fixed station.

How Cryptosmart secures shared terminals for field teams?

A fleet mode is available and allows the same secure terminal to be shared within a team.

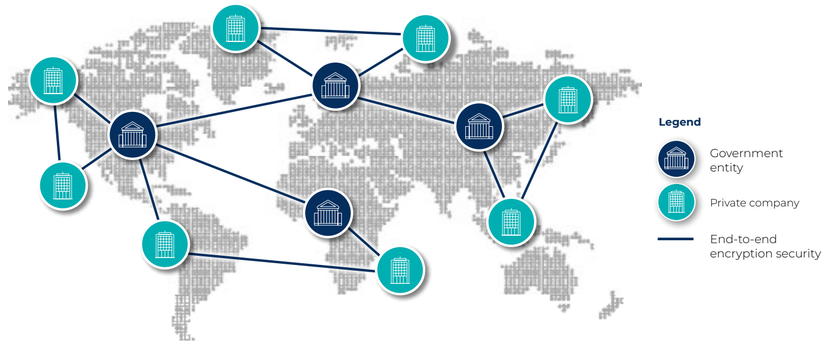
There are multiple usages:

- for maintenance teams
- for field intervention teams
- punctual trips to sensitive locations

Cryptosmart - Architecture

INTERGATEWAY

EXPAND YOUR SECURE COMMUNITY



ERCOM
a Thales company

sales_cybersec_web@ercom.fr

+33 (0)1 39 46 50 50

www.ercom.com/cryptosmart