THE ULTIMATE SOLUTION TO SECURE MOBILE COMMUNICATIONS AND DEVICES

IN PARTNERSHIP WITH

CRYPTOSMART
BY ERCOM

SAWMUNG
What are the consequences?

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

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

- 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.

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.

What type of solution?

1. 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.

2. Software + Hardware (SW+HW)
   - Solutions based on a hardware element, provide a higher level of security.

Which security management?

1. 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.

2. 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.

Which functionalities?

1. Secured voice
   - End-to-end encrypted voice call or up to the organization’s PABX.

2. Secured SMS
   - End-to-end encrypted text messages.

3. Secured data
   - Data communications are encrypted in a VPN between the devices and the organization’s IT system.

4. Strong authentication
   - Use of a hardware element to secure mobile device access.

5. Local device protection
   - Secure boot and OS, local data encryption and control of USB/Bluetooth ports.

Which devices?

1. 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.

2. 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.

3. Consumer electronic device with HW/SW solution
   - They generally offer high-level security, combined with best-in-class consumer electronic device user experience.

4. Local device protection
   - Secure boot and OS, local data encryption and control of USB/Bluetooth ports.

5. Strong authentication
   - Use of a hardware element to secure mobile device access.

Which security level?

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

2. 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. Thoseapprovals are based on Common Criteria certifications as well as local or international standards.

*Quote from Mireille Ballestrazzi, Interpol CEO

Mobility and Cybersecurity Concerns

Why is it important?

- 1/3 of companies admitted that their data had been compromised through a mobile device (source: Verizon (2019)).
- 93% of companies are concerned about mobile security issues with the growing number of professional mobile devices (source: IPass (2018)).
- The price of a mobile interception on the dark web is €250.

What is the adequate solution?

1. Market answers
   - 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.

2. 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.

3. 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.

4. Which functionalities?
   - Secured voice
     - End-to-end encrypted voice call or up to the organization’s PABX.
   - Secured SMS
     - End-to-end encrypted text messages.
   - Secured data
     - Data communications are encrypted in a VPN between the devices and the organization’s IT system.
   - Local device protection
     - Secure boot and OS, local data encryption and control of USB/Bluetooth ports.

5. 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.

6. Which security level?
   - Common Criteria
     - EAL certifications evaluate IT software and solutions to guarantee the compliance with the required assurance level. They are internationally recognized.
   - 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. Thoseapprovals are based on Common Criteria certifications as well as local or international standards.

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

- 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.
Cryptosmart: mobility, security and simplicity

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

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)

What security level?
- Common criteria certification (ISO 15408)
- Cryptographic component
  - EAL5+
- Cryptosmart smart card
  - EAL4+
- Local and International certifications*
  - ANSSI: Restricted
  - NATO: Restricted
  - EU: Restricted

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

Which functionalities?
- Secured data
- End-to-end secured voice
- End-to-end secured SMS
- Full device encryption
- Strong authentication

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)

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

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

= 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

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*

Restricted* • Approved restricted for version 5.2 ongoing

A large range of compatible devices
- Samsung Galaxy A
  - Security on mid-range smartphones
- Samsung Galaxy S
  - Security on top-range smartphones
- Samsung Galaxy Tab
  - Security for paperless workspace

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
  - NFC or QR code installation
  - Update “over the air”

Accelerated deployment and updates

- NFC or QR code installation
- Update “over the air”

They trust us
- CAC 40
- OIV
- Restricted*
How Cryptosmart secures my communications with my customers and suppliers?

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 interception.

Use Cases

How Cryptosmart accompanies 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 interception.

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.