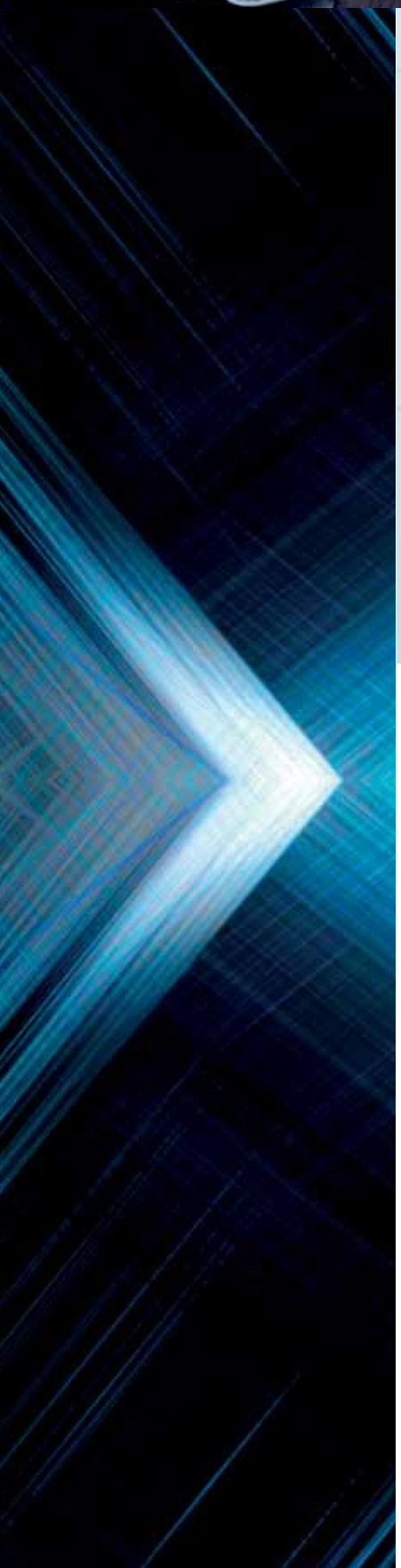
DESIGNER, INTEGRATOR & OPERATOR
OF MISSION-CRITICAL SYSTEMS

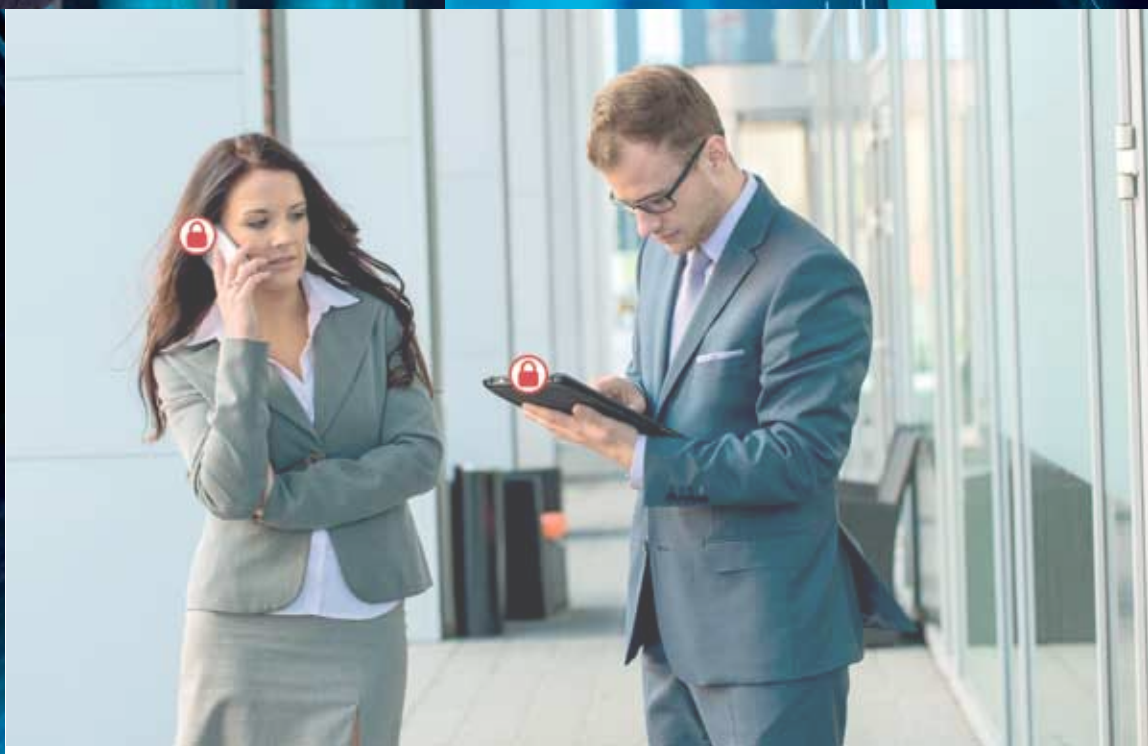
MONOLITH SOLUTION

SECURE HIGH BITRATE MOBILE COMMUNICATIONS

CS

The power of innovation





With the development of Internet and the abundance of new uses this has entailed, both corporate and individual users have, for twenty years now, enjoyed unprecedented advantages in terms of communication, access to information, and information exchange.

However, cybersecurity has not sufficiently kept up with this development to protect users against the risks inherent in these uses. The security of mobile solutions, remote interactions, and data storage has become a key concern for both users and operators of infrastructures.

Mobile telecommunications - voice and data on whatever network - can easily be intercepted. Operators encrypt them, but everybody knows that this encryption is not, in many cases, strong enough to resist attack and/or cryptanalysis.

MONOLITH MOBILE permanently protects the confidentiality and integrity of stored data, applications and the operating system

OUR SOLUTION

MONOLITH MOBILE is the CS solution for securing all environments and applications on smartphones for business, government and military needs to meet the following challenges:

> Securing voice and data on smartphones
> Providing the necessary infrastructure for the connection to the company's IS
> Providing the network management capabilities and security of the associated fleet

The security primitives are provided by a hardware component, the PLM, provided by Altis and under Common Criteria (EAL4+) certification.

MONOLITH FEATURES

MONOLITH currently is the best compromise between security and mobility on the market as it enables:

> Protection of the network and applications
> High throughput (consistent with the expectations of the 4G)
> Storage and cryptographic module in the safety circuit (one µSD slot required in the device)
> EAL4+ certification plus anti reverse engineering capabilities

MONOLITH SECURES ALL COMPONENTS OF THE SYSTEM:

> **The security component is hardware and evaluated**
> **The mobile is secured by the security component**
> **The network is secured by the by the security component**
> **The applications are secured by the security component**
> **The mobile data management system: management data flows are enciphered by the security component and the manager includes joint management of the network and security.**

AN END-TO-END HIGH SECURITY SOLUTION

HARDWARE SECURITY MODULE

Monolith Mobile and Monolith Router rely on a hardware chip, designed under µSD form factor, named PLM, developed and manufactured in France by Altis Semiconductor. This circuit undergoes an evaluation process according to the Common Criteria at the EAL4+ assurance level.

- Hardened 32 bits RISC CPU
- High-speed ciphering, PKCS11 compliant
- TRNG AIS31
- AES 256 bits, 3DES 168 bits
- RSA 4096 bits key length, Elliptic curves P192 to P512, Diffie-Hellman algorithms

SECURITY SERVICES PROVIDED

- Confidentiality (hardware encryption)
- Integrity (verified at boot time)
- Authenticity (certificates are stored in the PLM)
- Availability (multiple radio interfaces, redundancy of management systems)

NETWORK SERVICES PROVIDED

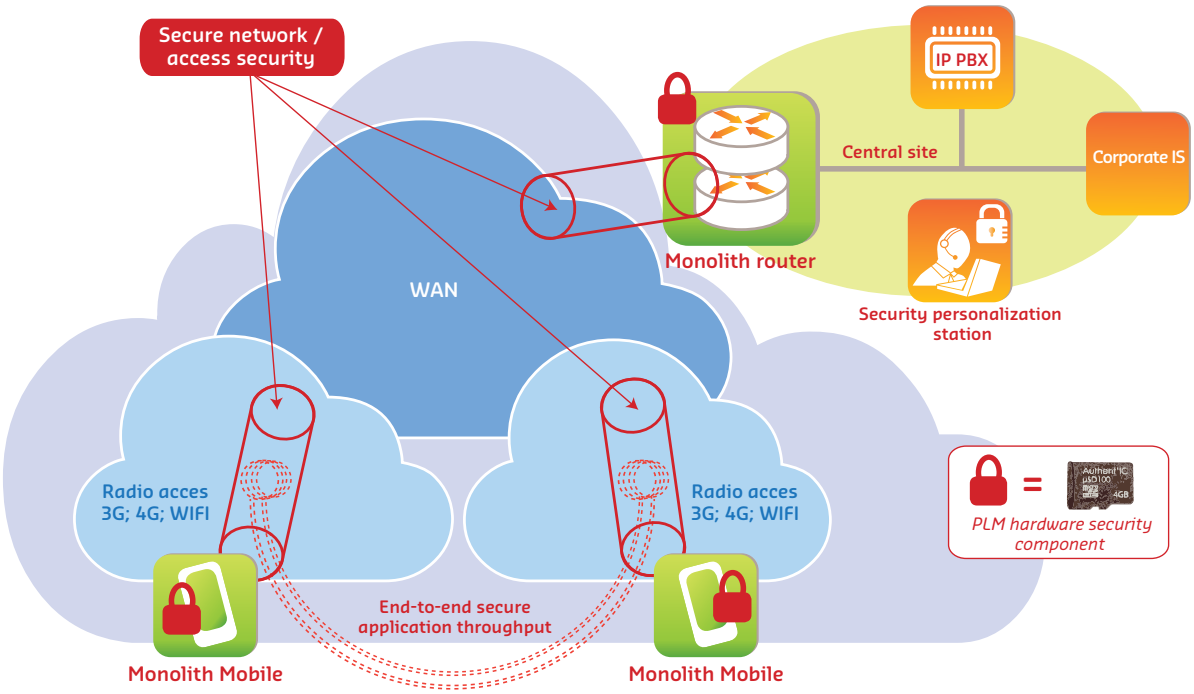
- Encrypted VoIP (including signaling)
- Encrypted SMS
- Encrypted e-mails (subject, body and attachments)
- VPN Service

SECURE TERMINAL

- Tampering detection
- Secure boot with custom keys and periodic device runtime integrity checks of the OS and application software
- Secure data storage
- Secure stealth mode
- Application permission firewall
- IP 67 level water and dust protection
- MIL-STD-810G level shock resistant

EB Tough Mobile secure terminal by Elektrobit

MONOLITH ARCHITECTURE



MONOLITH IS A COMPLETE SOLUTION

It has a secure access to the company's IS, a global management environment, an integrated fleet manager MDM (Mobile Device Management) which allows to remotely control all the MONOLITHs.

> Use of standard protocols for easier integration into the information system; you can keep your favorite telecom provider.
> Intuitive user interface
> Designed and developed by CS in France

SECURITY SYSTEM COMPONENT

MONOLITH MOBILE

Beyond specific security functions of the secure terminal EB Tough Mobile, Monolith Mobile is a complete and innovative solution to address the problem of securing voice and data of mobiles, by integrating several technological components of a high level of security.

This solution consists of a ruggedized Android smartphone and its secure operating system, VoIP applications, SMS, mail and encrypted storage using a hardware security component for encryption of voice, data and VPN services.

Smartphone security features :

The terminal includes the security circuit to perform all the functions of authentication, key generation, encryption and decryption of data. The circuit is constantly protecting the secret of the used encryption keys. The circuit is µSD form factor and is directly inserted into the µSD interface of the device. In this form, it also has its own data storage capacity of 4 or 16 gigabytes, which makes it possible to store both encrypted and unencrypted documents and photos.

MONOLITH ROUTER & SECURITY MANAGEMENT

Monolith Router is a key element for connecting securely to the company's telecommunication infrastructure. Its function is to route the stream from the WAN to the servers in charge of their treatment, making encrypted VPN with mobiles, encrypt and decrypt all the management flow and provide a global view of the security state of the mobile devices and of the central system itself.

Security management ensures:

- Enrolling new devices
- Managing lost or compromised devices
- Resetting PIN codes
- Requiring on the air rekeying
- Revoking devices
- Collecting security events
- Alerting in case of suspicious events

Monolith router is built on different servers according to capacity requirements:

- Number of devices
- Number of simultaneous communications
- Bandwidth requirements
- High availability requirements

The routers also include the security component used to manage the authentication encryption and authorization services.

SECURITY PERSONALIZATION STATION

A global security scheme relies on some fundamental secrets used for identifying and authenticated remote devices.
The manufacturer of the PLM chip provides a factory certificate specific to each chip, but an organization may not want to rely exclusively on this identification and authentication mechanism.

A personalization process is proposed with the Monolith Mobile solution which allows for the organization to override the manufacturer secret elements with its own secret data.

This is performed by a central standalone PC (usually a laptop is sufficient). This machine never gets connected to any network and must be operated and stored in a safe place. The PLM chips must be physically inserted in this station for the initial secrets and organization-specific identifications to be loaded in the one-time writable memory area of the PLM chip.

These new initial secrets can be generated by the PLM chip itself or can be imported from a Public Key Infrastructure (PKI) managed by the organization. The import is done via a dedicated media previously registered to the station. This media must then be either securely erased or destroyed or must be kept in a safe place.

contact.monolith@c-s.fr

COMMUNICATION & SYSTÈMES • 22 AVENUE GALILÉE • 92350 LE PLESSIS-ROBINSON • FRANCE • TEL: +33 (0)1 41 28 40 00 • C-S.FR