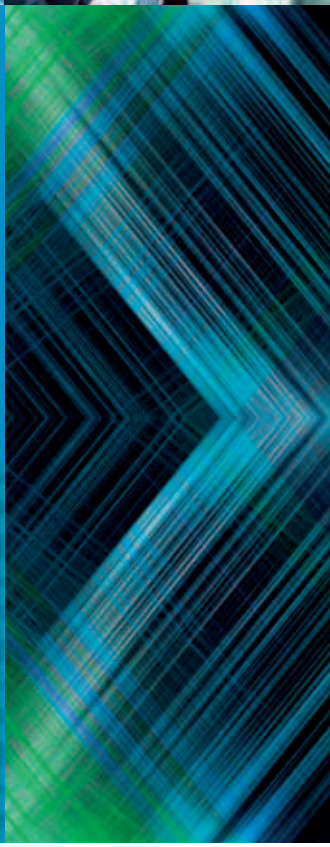
SECURE HIGH BITRATE MOBILE COMMUNICATIONS

[white paper]



DESIGNER, INTEGRATOR & OPERATOR OF MISSION-CRITICAL SYSTEMS

The power of innovation

contents

SECURE HIGH BITRATE MOBILE COMMUNICATIONS

I LIBERTY, MOBILITY, SECURITY

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.

In fact, several simultaneous developments affect the security of communication infrastructures and data storage systems.

- Exponential growth in the volume of exchanged or stored data, the emergence of 4G and the Cloud, and the huge increase in the number of collaborative and/or interactive applications. Cloud computing is the new architecture being used to provide and use computing services (calculation, connectivity, collaborative sharing, storage), networks, physical and virtual machines. Applications and data are no longer under the control of the company and are generally entrusted to an IaaS host (Infrastructure as a Service). This "externalization" and these architectures entail specific security flaws and guarantee neither the integrity nor the confidentiality of data and communications.
- Rapid and widespread use of mobiles to transmit voice, video and data
- Inadequately robust security solutions and technologies, and software encryption that is insufficiently protected against attack.
- The eagerness of the NSA (and of numerous intelligence services) to capture a maximum number of communications using HPDA (High Performance Data Analytics) technology for the analysis of data collected on a large scale.

The threats that result from these developments and which also affect the security of both telecommunications and mobile or fixed terminals and the integrity of information systems, are well known.

I-1/ Interception of communication

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.
This means that confidentiality of communications is compromised and not guaranteed. Following Edward Snowden's revelations, it is clear that tapping or interception by a public authority causes serious problems, especially when it results from the actions of a foreign state or a

malevolent or fraudulent organization. Moreover, laws are applied territorially, which means that data is always subject to local laws. This is why data stored in the United States is always accessible to American authorities (legal interception, Patriot Act, etc.). The Snowden case has revealed and confirmed the reality of this threat.

I-2/ Loss or theft of the terminal

This situation inevitably results in data being compromised, including directories, browsing history, and above all documents stored in mass memory. The more and more frequent use of smartphones as "computer-phones" makes this an increasingly critical threat.

I-3/Intrusion into the terminal

This typically involves an attack using malware that enters via one of the channels of the terminal or infrastructure: downloading of applications, e-mail attachments, wireless communication port. Such intrusions are even easier to carry out if the phone is temporarily stolen.

Interception of telecommunications is a permanent activity that targets almost all professionals using or exchanging information that is secret or sensitive, or information with restricted distribution and/or competitive value. Such attacks – which are increasingly sophisticated— give opponents or rivals a considerable advantage and provide inexpensive access to secret and strategic information.

The threat of theft or intrusion is very real, and differs little from the threat to personal computers. It is thus logical that in administrations or firms, protective measures similar to those applied to computers should be adopted for smartphones, as they are now used in comparable ways. When such steps are taken, hackers have to operate in a way that is more targeted, more complex, and consequently more costly.

To conclude, it is currently difficult to guarantee the security of entire infrastructures, which are very often composed of distributed, disparate, and non-secure elements. Moreover the Cloud has led to large-scale concentration and mutualization, which affects security because the likelihood of an attack against such infrastructures has increased considerably. It follows that the critical nature of data collection—especially as regards professional terminals, smartphones or Ipads—is now a real cause for concern.

II STATE OF THE ART

There are two major categories of encryption methods: software and hardware.

II-1/ Software solutions

It is generally acknowledged that software encryption methods are not sufficiently robust and can easily be compromised or hacked. Confidentiality is compromised when the user logs in, which is precisely the purpose of a terminal! Moreover, software-generated keys are not, in reality, generated randomly, and may in fact easily be broken.

Existing solutions based on software encryption are thus intended for users who handle non-sensitive information. The solution here ivolves downloading the required security applications onto the device (usually a standard mass-market smartphone) without hardening either the terminal or its OS. The increasingly widespread use of mobile devices and tablets in the business world has generated strong growth for these security applications, despite the low level of protection such solutions provide.

II-2/ Hardware solutions

Random generation and protection of encryption keys are fundamental to security. If key generation is not random, the time a hacker needs to break the encryption is considerably reduced, thus making the operation viable. Secret encryption keys must be permanently protected in a physical « safe » designed to make it impossible to take out a key without first having encrypted it before passing it on to an authentified third person. Consequently, encryption and decryption, which are necessarily carried out using unencrypted keys, must take place within the same physical « safe » as the person who has the keys, to prevent data from being compromised. This "safe" can only be a hardware component providing cryptography departments with the range of resources they need to ensure complete digital trust: generation and storage of keys, encryption, decryption, certificate generation and storage, robust authentication, and data hashing.

Smart Card: limited throughput

Smartphones and tablets are used to make voice calls or to exchange and store documents (data). This content, which we know is frequently (indeed systematically) intercepted, must intrinsically resist attack, and the data exchanged or stored must be masked so that it cannot be interpreted by third parties.

So-called "secure" phones are starting to appear on the market. However they are expensive, and their performance falls short of the need for protection and the expectations and requirements of their users. They are mutually incompatible,

and some have serious security flaws (software weaknesses, compromised encryption, gateway issues, etc.)
Moreover, when they include a hardware component, these solutions mostly use a smart card which can sometimes be integrated into microSD form factor; intensity is limited to 1 Mbps, and has reached its limit in 3G networks. These solutions, which are now used chiefly on GSM, have performed very disappointingly.
Their inability to treat very large quantities of data also handicaps their efficiency. Many applications such as collaborative work require a communication channel with high intensity and robust security, which invalidates such solutions.

Existing hardware solutions are mainly based on smart cards either native or under microSD form factor. In both cases, bitrate is restricted by the inherent capabilities of the smart card.
This bitrate may be sufficient to secure applications (although apps are becoming increasingly bitrate-intensive), but it does not make it at all possible to ensure security at network level, as shown later in this document. Security limited to applications covers only app data; it does not apply to metadata, which means it does not completely protect the confidentiality of sensitive elements (who is speaking with whom) nor metadata integrity (DNS liars for instance).

III MONOLITH SOLUTIONS

To respond to the new challenges raised by recent developments such as Cloud computing, mobility and Big Data, CS offers a complete, purpose-built range of solutions that is optimized to meet the broadest and most exacting requirements in terms of security and performance. These products and solutions are innovative, original and exclusive.

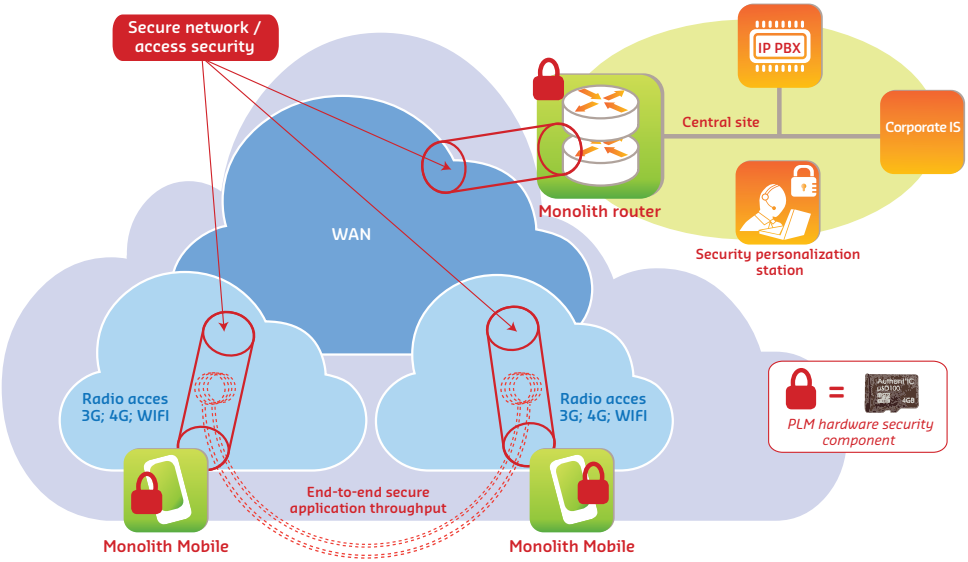


Figure 1: MONOLITH architecture

III-1/ Hardware component

The CS solution is based on the use of a circuit specially developed by ALTIS Semiconductors to respond to all of these needs. This circuit has been designed to provide all the necessary guarantees in terms of digital trust and security. This is the aim of EAL 4+ certification, in compliance with Common Criteria, with respect to security targets that correspond to the concept of use. The necessary and sufficient rating for use of secure telecommunications is EAL 4+. It cannot be obtained by software components that do not possess a physical security module.

With the development of new-generation (LTE) networks and the exchange of more and more voluminous documents, mobile

terminals can exchange data at tens of Megabits per second. The component must thus be able to process these bitrates so as not to restrict or affect use for reasons of security.
To guarantee security of communications, a connected terminal must thus possess a physical security component that carries out user identification and data encryption/decryption procedures, and which permanently protects the secrecy of the encryption keys that are being used.
A high bandwidth (up to a hundred or so Mbps) is thus vital so as not to restrict or affect use for security reasons.

The ALTIS PLM component, AUTHENT'IC µSD 100, fully responds to all these needs, constraints and requirements.

For mobile applications, PLM takes the form of a standard-sized micro SD card, which can be easily and directly integrated into terminals with a micro SD slot. 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. The different functions of the card can be controlled under Android without having to modify the terminal.
When two or more people each use a PLM component associated with a set of specific applications, it is possible to instantaneously obtain and exchange encrypted documents and to encrypt the corresponding communications.
Authent'IC µSD100 is a 'System In a Package' hardware component with microSD form factor, designed to ensure secure communications. A specific circuit (ASIC) developed by ALTIS runs the essential functions of the component from the SD interface. This ASIC uses a secure 32 bit RISC processor and several blocks and accelerators of cryptographic functions for key generation and storage, encryption and signature. It manages data throughput at the native speed of the SD interface: over 100 Mbps.
This component carries the critical microsoftware in its own non-volatile memory zone and implements a range of anti-hacking techniques to ensure a high level of security. It also controls the MLC NAND chips that constitute the mass storage memory of the microSD card.

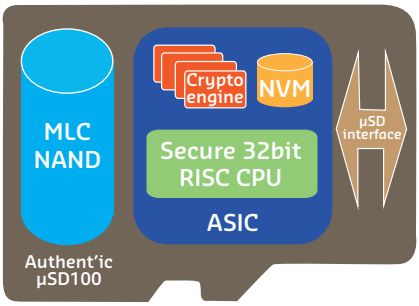


Figure 2: Authent'IC µSD100

III-2/ A secure network

Access Security

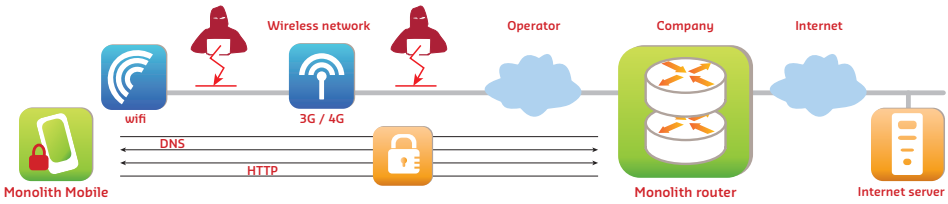
Access and communications on mobile devices sometimes take place on trusted networks (national 3G/4G operators, corporate WiFi networks, etc.). But with on-the-go and international use of such devices, unsafe or hostile networks are frequently used (such as non-secure hotspots in hotels or networks subject to surveillance). VPN login ensures data security on the wireless access network and the service provider's network, i.e. in the areas that are the most critical and where traffic monitoring is usual and easy to implement. Confidentiality is ensured for all traffic and metadata, including traffic from services that do not secure their traffic. For instance, when connecting to a web service, the following types of data are protected:

- HTTP request and response data
- Source and destination IP address of the HTTP request
- Pre-login DNS handshakes, in other words the domain name the user is connecting to

Security provided by VPN comprises the following:

- Data confidentiality: an attacker lurking on an access path seeking to eavesdrop on data (traffic content) or metadata (who is connecting to whom). For example: large-scale data interception organized by certain states
- Data integrity: an attacker lurking on an access path seeking to modify data or metadata. For example: port filtering and blocking carried out by certain access providers, liar DNS servers, application proxies on 3G / 4G networks.

Figure 3 : Access secure network

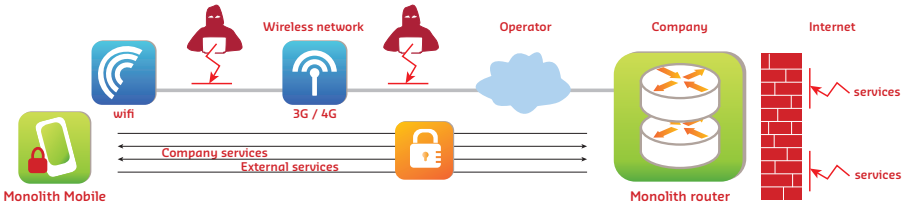


Equipment integration in corporate networks

The VPN connection links the mobile device to the corporate network. This link provides access to corporate resources in the same way as any other in-house system. The nature of this remote access and the internal structure of the corporate network are hidden from the outside world.

In addition, mobile devices linked to corporate networks are subject to the same security policies as other equipment, in particular firewall rules and traffic monitoring, to ensure the same security standards regardless of the context in which the mobile device is being used.

Figure 4 : Common security access for remote and local users



III-3/ Security of services

Besides network security, the architecture handles service security issues. This security is specific to each service, according to its protocol and architecture. A VPN solution alone cannot resolve security issues as effectively as applications can.

The architecture and the chip provide services with a means of authentication, as well as end-to-end confidentiality of communications. This security makes it possible to ensure data confidentiality:

- With respect to the VPN server and the corporate network infrastructure in general, reducing the impact of intrusion or backdoor router access
- With respect to network operators where the service in question is outsourced to a service provider

Email data confidentiality is ensured from client to mail server, and where required from server to server.

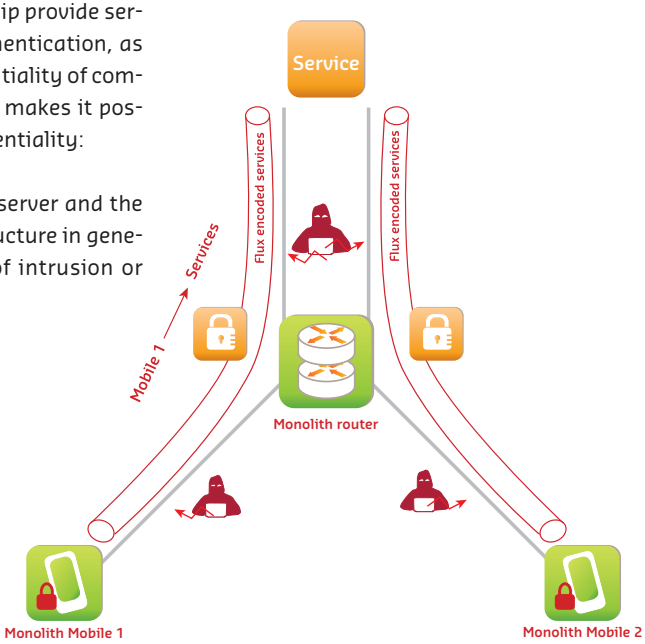


Figure 5 : E-mail confidentiality architecture

Voice data confidentiality is ensured between the two mobile users, and the protocol is able to provide direct connection.

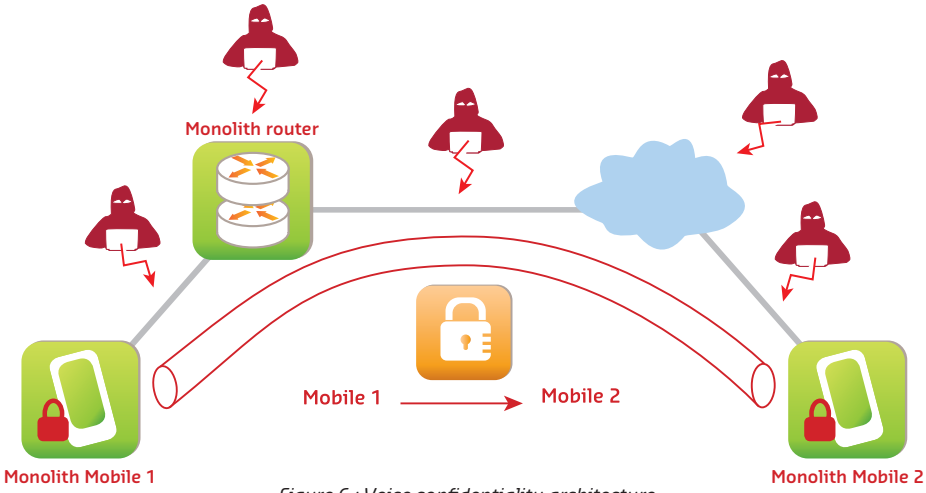


Figure 6 : Voice confidentiality architecture

III-4/Secure terminal

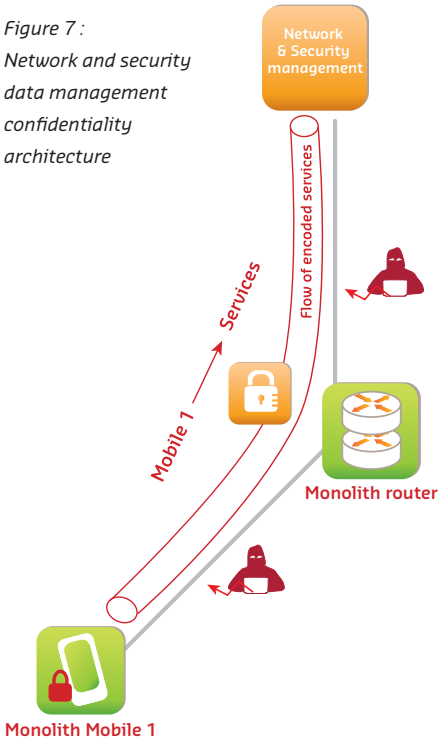
The terminal includes the security circuit to perform all the functions of authentication, key generation, encryption and decryption of data. The circuit is constantly protecting the secret of the used encryption keys. The circuit is µSD form factor and is directly inserted into the µSD interface of 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.

III-5/ Secure manager

Hardware encrypted management throughput

MDM and data security management are encrypted end to end to ensure confidentiality and integrity, as with all sensitive communications:

Figure 7 : Network and security data management confidentiality architecture



Integrated network and security management

In existing mobile communication security solutions, VPNs are set up manually or via management commands initiated by the network administrator. In the context of highly dynamic virtual networks and large-scale deployments, direct configuration of VPNs cannot be carried out manually because it is too time-consuming. Thanks to the network and security management module, network and dynamic VPN configuration is simplified and automated.

Moreover, dialogue between the network management software module and the security management software module must be established in order to achieve a correlation between network and security management events with a view to detecting attacks and improving the overall security of the system.

It is important to remember that standard operations carried out via the network manager can impact the level of security of the services deployed. This means that the security manager needs to be aware of some of these operations, such as restarting equipment, setting up flow duplication services for maintenance purposes, or legal interception. Integrated network and security management helps to increase system security.

IV VITAL REQUIREMENTS FOR CONTROLLED SECURITY

Certified hardware security
Certification of physical security components aims to achieve a high level of trust in terms of cryptographic operations. Level 4+ addresses attacks not only by individual hackers or small groups, but also organizations with substantial resources such as states and organized crime syndicates. This certification is recognized by signatories of Mutual Recognition Agreements (Europe, USA, Canada, Australia, Japan, South Korea, etc.) For an up-to-date list, see www.commoncriteriaportal / ccra / members).
However, the scope of this evaluation is limited to the cryptographic component alone, and therefore does not cover incidents such as denial-of-service attacks. For this, it is necessary to consider the system as a whole; this is the purpose of the CSPN [first-level security] evaluation issued by ANSSI.

Not only does the CS Monolith solution feature a security circuit rated EAL 4+; it also includes submission of the system to CSPN evaluation.

Securing all components (Mobile, Access Router, Manager, etc.)
Since the overall security of a system corresponds to the security level of its weakest component, every system component must be secure. This is the case with Monolith:
a. The security component is a physical component that has been evaluated
b. The terminal is secure
c. The network is secure
d. Applications are secure
e. The manager is secure: secure management flows are hardware-encrypted, and the Manager includes joint network and security management.

Network and Application Security
Network and applications are protected in different ways, both in terms of the type of data and paths:
- The security of applications exclusively covers application data, but along the entire path between source and destination
- The VPN connection covers only part of the path, but it covers all the data (including domain names, IPs, ports, etc).

These types of security are complementary and respond to different attack models. The VPN connection is not enough by itself, but it enhances security where interception is easiest and most harmful. Above all, it provides protection from threats posed by attackers external to the organization. Application security chiefly provides protection from attack by insiders.

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