Security and Privacy in the Digital World

Solutions from the Smart Security Industry

Security of Mobile Devices, Applications and Transactions

Content

June 2012

1. Introduction

Mobile devices like smartphones and tablets have been conquering the market over the past 5 years. Consequently, a large amount of user transactions have been moved from PC-based environments to mobile devices. This includes banking, trading, shopping, data storage, eGovernment as well as other security sensitive procedures. As outlined in the recent European Commission Action Plan on eCommerce[1], the usage of online services and e-Commerce opens up a huge business potential. Security and interoperability are key factors in deploying those services successfully.

Mobility: what's happening?

Many different players are now seeking growth opportunities in areas related to mobility. This can be illustrated by a number of examples:

- In the PC industry, the demand is moving from desktop PCs to laptops and from laptops to tablets.
- In the mobile phone area, the growth is much higher for smart phones than for basic low-cost phones. Smart phones are gradually replacing portable dedicated audio/video players. And Smart phones are by definition open to 3rd party applications.
- Only a few major operating systems like iOS, Android and Windows Phone are dominating the market for mobile devices. Most of the growth and innovation in this area is based on the dynamic of the OS evolution.

Mobility: driving factors

In the consumer area, the two main factors driving the adoption of new technologies are on the one hand, user convenience, and on the other, regulation (national or international authorities enforcing rules, standards). Mobile and permanent connection to social networks, email on mobile or tablet from your sofa, geo-localised based services: these new usages and applications are proving to be extremely convenient for users. The success of smartphones and tablets is clearly driven by user convenience. However, standards and regulations are key success factors to guaranteeing interoperability, contributing very much to user adoption (e.g. user privacy, security certification, etc.).

Mobility: enabling factors

Such user-friendly mobile devices have been made possible by the following enablers:

- Deployment of 3G and LTE cellular networks, as a viable alternative to ADSL networks for Internet browsing.
- Better performance/power consumption ratio for the application processors, enabling good user perception.
- Rich connectivity (WIFI, Bluetooth, NFC, GPS/geo-localisation, FM, etc.) enabling numerous new applications in various configurations.
- Thousands of applications made available through ecosystems built for facilitating development and distribution of applications.

In this environment, it is very clear that the mobile devices represent a major source of growth for the high-tech industry. This will continue and accelerate in coming years.

[1] Action plan on eCommerce «A coherent framework to build trust in the Digital single market for e-commerce and online services», COM(2011)942 of 11 January 2012

Mobility: What about security?

A few years ago, mobile phones had only one task to handle: to ensure that end-users were able to receive and send calls, delivering a voice service with high quality.

Today, since the onset of the smartphone, these devices have the responsibility of handling many new tasks; making voice calls almost a minor feature. The more features end-users have on their device, the less they call. They can play games, browse the Internet, take photos, play videos, exchange over social networks and so on. Smartphones embed and handle a great deal of sensitive assets that concern our privacy.

Mobile as Wallet
(Convergence of applications)

To this end, a strong growing trend is to make one's smartphone a mobile wallet. Although this trend is natural in an increasingly "paperless" world, new consequential threats have to be considered. Indeed, the more sensitive and valuable assets one's phone embeds, the more the need for security will grow.

We are seeing a convergence of most secure NFC applications, such as transportation and payment, into a single device; all sharing the same resources. As a consequence, the different kinds of assets need to be strictly separated within the device.

Furthermore, the evolution of the mobile market has taken a user-centric path, attempting to create a veritable user-friendly experience for a much larger number of applications and services. Such an experience leads to a much more complex and heavy operating system (e.g. Android, iOS, Blackberry OS, Windows Phone). The more complex a system is, the harder it is to secure.

As a matter of fact, end-users have drastically changed their usage of such devices: and new usage entails new needs. One of the major changes is the availability of easy-to-use application stores, giving the ability to users to install a plethora of applications. A transportation application can run beside a banking, VPN or social networking application. It is important to ensure that no sensitive secret used by a banking application leaks to a malicious application. Handling of all the new applications and all the different kinds of assets is important: **isolation is the keyword!**

Up to now, most assets in the mobile phone belonged to the user (emails, contacts, etc) and basic isolation was sufficient to ensure confidentiality and integrity of the user's personal data. The emergence of new applications embedding sensitive data belonging to service providers changes the deal. Indeed, a bank providing an application may want to store some keys to be used for authentication purpose. Those secrets now need to be protected against the user himself – or any other individual assuming his identity.

And last but not least, new sensitive applications need end-to-end security to protect their transactions with service provider back-ends. For example, in classic banking, the security chain starts from a Secure Element and ends at the bank's server, but a terminal (which has been build to ensure trustability) is required for the user to communicate with the Secure Element hosting the banking application. The new challenge is to keep the same security level in transactions where a smartphone replaces a dedicated terminal.

This creates the need for a new level of security. The impact of such secrets being exposed is much more important as it may imply a significant loss for service providers or even for end-users. The combination of a consumer device open to any type of applications induces a shift in the security perspectives: depending on the services hosted in the device, assets may need strong security (e.g. protection against physical attacks for banking assets or protection against software attacks for user assets).

2. Secure Mobile Transactions in Practice

In the following sections we will sketch selected use cases in the field of ePayment and eGovernment. These use cases demonstrate the demands of users in respect to convenience and security.

2.1 Payment

Secure mobile payment can be achieved in the following ways:

- Contactless payment: the phone – if NFC enabled - can be used in a card emulation mode (the phone behaves like a payment card) and relies on the NFC interface to communicate with a contactless payment terminal.
- Remote payment: the phone provides access to:
  - banking applications / websites performing credit transfer. The financial institution is in charge of strongly authenticating the consumer.
  - e-commerce applications / websites for the purchase of goods or services. Card payment schemes are involved for a strong authentication of the consumer.
  - SMS services, billed through the mobile network operator. The operator is in charge of filtering SMS Trojans and authenticating the consumer.

In the case of a contactless payment, a scheme-approved hardware device must be attached to the mobile phone either internally or externally (like a sticker) to be accepted in the payment architecture.

For a remote payment, once the customer is ready to approve a sensitive operation (validating a purchase, consulting a bank account and validating a transfer), he or she is prompted to enter a password he or she knows (a specific PIN code for instance, but different from his bank card PIN). The password is checked by an external device (contactless card, token) or internal (SIM card, etc.) which then will open a secure channel with the distant server to perform a mutual authentication.

As expressed in the Green Paper "Towards an integrated European market for card, internet and mobile payments" from the European Commission , any sensitive personal information must remain in a secure payment infrastructure, whether for data processing or storing.

[2] Green Paper "Towards an integrated European market for card, internet and mobile payments", COM(2011)941 of 11 January 2012

This protection rule concerns the PIN code, which must be protected when sent to the authentication device, and any credentials or cryptographic data sent to the remote server for ID verification.
The Green Paper also recommends that parties having access to authentication data must be limited to those necessary in performing the transaction.

For mobile payment, the use of a Secure Element in the authentication mechanism appears necessary; access rights and methods to this Secure Element must be deeply controlled and secure.

2.2 eGovernment

Most European countries have issued electronic identity cards (eID) over the past years. One big benefit of these new eID cards in comparison to the classical paper-based identification cards is the possibility to use them for electronic government (eGovernment) services such as tax declaration, eVoting or other registry office related services.

Figure 1 - Mobile eID Infrastructure

As explained in chapter 1, the usability of services with mobile devices such as smart phones and tablets is growing in importance. This is especially true for eGovernment services. With the emergence of the NFC technology in these devices, the mobile use of contactless eID tokens is becoming natural (e.g. contactless national identity card). Beside eGovernment services, enterprises would like to use these electronic identity cards for Internet services (eBusiness-Service), such as retailers, banks and insurance organisations.

Imagine the case of a citizen who wants to check his pension records. To get access to these records, a strong authentication with his eID token is necessary. The eID token supports the contactless protocol and hence the citizen can use his tablet with NFC technology in combination with his eID. After entering his PIN code for identification purposes, the authentication process is performed and a secure channel is established from the back-end service to the tablet. The sensitive data is transferred through this channel and the user can check his or her records.

In the case of an error or missing data, the user might want to update his or her records in the pension registry. To do so, he or she can use his or her tablet's camera to scan the relevant data. Furthermore, the person can use his or her eID in combination with the tablet to generate a qualified electronic signature over the new pension data, before it is transmitted through the secure channel to the back-end.

To allow this use case, the following security measures are key:

- The PIN code of the user's eID has to be protected against unauthorised access (malware and trojan horses).
- The sensitive data related to the transaction must not be tampered with.
- The creation of qualified electronic signatures, insuring legal binding, requires the verification of the integrity of the terminal.

3. Threats for Mobile Devices

According to the Malicious Mobile Threats 2010/2011 report from Juniper Networks[3], instances of malware on mobile devices grew 250 percent between 2009 and 2010. Both banks and consumers need to understand how to detect and prevent fraud so that malware attacks do not grow at the same rate, nor exceed the rate, of mobile banking adoption.

Network vulnerabilities

Contrary to computers or tablets, phones are always connected to a network through various interfaces (Wi-Fi, Bluetooth, NFC, GSM, etc.) and thus become more sensitive to fraudsters.

Wireless interface

Even when users are careful selecting a Wi-Fi or GSM network, in places like airports, hotels or libraries, they can fall prey to «Man in the Middle» attacks on mobiles. Here, a fraudster who is positioned between the end-user and the server will eavesdrop or redirect transactions through his computer.

NFC interface

As soon as a device is NFC enabled, it opens a way for new security breaches:
When two devices communicate via NFC, they use RF waves to talk to each other. An attacker can use an antenna to receive the transmitted RF signals and extract the data out of them (eavesdropping technique) or modify the data (transaction data like bank account, transfer amount, etc.) in order for the receiving device to actually receive some valid, but manipulated data.

Focus on mobile applications and transactions

As specific applications become widely adopted and standardised across mobile devices, the applications themselves will become the targets of attack.
There is now a low entry barrier for attackers. Consumers and business users are downloading more applications than ever before with little consideration of potential security concerns.

Browser-Based Threats

Just as web browsers have been a clear means of attack for PCs, mobile browsers can be effectively targeted for intrusions or as catalysts for an intrusion. The Webkit engine, used by iOS, Android, BlackBerry and webOS mobile browsers has already known vulnerabilities that attackers are now targeting. Unlike application-based threats, which rely on users knowingly downloading an infected application, these browser-based attacks are triggered by simply visiting an infected website.

[3] Malicious Mobile Threats Report 2010/2011

OS linked attacks

The most popular platforms have already shown weaknesses against attacks.
Android's open application marketplace model makes it easier for attackers to reach potential victims. A developer can post an application to the official Google Play and have it available immediately, without inspection to block malicious applications.

On BlackBerry devices infected with malware like the ZeuS Trojan, criminals obtained user credentials to gain access to the victim's financial accounts.

Apple's model seems more secure with iOS closed application marketplace. However, with jailbreaking methods that remove limitations on the operating system, users also open breaches in the platform security with an open way for malicious application download.

Lost and Stolen Devices

Mobile devices hold significant amounts of personal information, which if stolen can be used for a variety of malicious purposes, including fraud and identity theft.

If the access is not properly secure through a lock screen, devices present a high risk.

Security into the future

Most mobile banking applications today don't include sophisticated security capabilities, as the focus is more on functionality. As mobile payment / banking goes on growing, security needs to become an integral component of mobile infrastructure planning.

Today's security systems reside in a bank's data centre; tomorrow they need to be on mobile devices and wireless hotspots. Security also should be built into mobile applications, so that the applications can monitor usage patterns and self-analyse a user's own mobile banking activity.

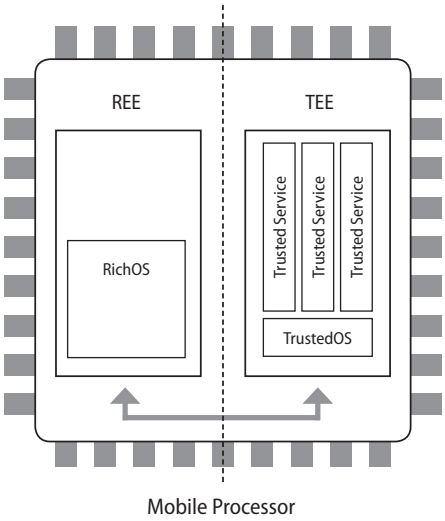
Establishing a secure channel between the two parts of the communication channel (phone and reader, phone and banking web site, etc.) thanks to a standard protocol, based for instance on RSA algorithm; will help fight against a great part of vulnerabilities during the transaction (Man in the Middle, phishing attack, spywares, etc.).

Using a hardware device in the phone (such as a SIM card, a microSD card or an embedded secure element) which stores user credentials, runs trusted applications or opens secure channels appears to be a good way of ensuring improved protection against even stronger attacks like Trojans.

4. Solutions for Enhanced Security

This chapter describes the main technologies to secure mobile applications and transactions. Each of the technologies described fulfils different needs and contributes differently to the security of the complete system. For most of the scenarios, only a combination of the presented technologies will provide a sufficient level of security.

4.1 Trusted Execution Environment



Trusted Execution Environment (TEE) is a standard technology[4] which brings a new execution context for applications on a mobile device processor. This new context runs beside the classical operating system, so called Rich Execution Environment (REE) such as Android and may share the same hardware resources. The two execution environments are strictly isolated. A TEE platform can execute trusted services, which may employ an exclusive access to the peripherals and resources available, including memory, computational units and controllers for the display or touch screen.

The TEE therefore ensures the protection against software attacks compromising the operating system (RichOS, e.g : iOS, Android). No matter what happens inside the RichOS, all secrets and trusted services that are managed by the TEE are kept safe from software intrusions. Many actors may benefit from this, ranging from end-users, to manufacturers and including mobile operators.

To provide such isolation, the TEE platform requires a specific hardware mechanism capable of managing the frontier between both execution contexts.

The concept of the TEE benefits from its deep integration within mobile processor as it can use the powerful resources typically embedded in modern systems. In addition to high performance, it can take advantage of the multiple controllers to bring trust closer to the end user.

A TEE and more especially its Trusted OS is designed to be more compact and robust than a RichOS so that it will be possible to prove its security by certification and to provide increased insurance for use in sensitive applications. The “certifiability” principle chosen for the TEE intrinsically limits its complexity so that the security assessment (which provides an assurance level in its security) can be achievable within reasonable time and cost constraints.

On the other hand, the TEE cannot ensure protection against the same class of attacks that are addressed by Secure Elements, such as physical attacks. Due to the tight integration of the TEE into the system architecture of the mobile device, it’s bound to a short lifecycle, which makes security hardware certification difficult. In the end, the TEE provides a good complement to Secure Elements and Rich OS through its ability to handle sensitive user interaction, session secrets as well as processing assets with medium security needs, while the permanent secrets and most sensitive assets such as those used for e-wallets and proximity payment can remain safely stored and processed in a Secure Element.

[4] GlobalPlatform TEE System Architecture v1.0 http://www.globalplatform.org/sp25x-19g57/g953-ff472.asp

4.2 SIMAlliance OpenMobileAPI

In the ePayment and eGovernment use cases described in section 2, the seamless and interoperable access by application residing on the device to Secure Elements such as SIM cards, secure microd SD cards or embedded Secure Elements is required. This access will allow for such operations as PIN code verification in the case of the mobile payment, or execution of actual authentication towards the government servers.

The SIMAlliance[5], a non-profit trade association gathering together the major actors of the Secure Element industry, has been developing a common vision on the way applications running in a open mobile environment should access Secure Elements. This work has been published in the form of a specification named Open Mobile API, agnostic in terms of device operating system in February 2011 – with an upgrade in November 2011.

This specification describes the interfaces that should be available to applications running in a device in performing basic operations such as:

- Collecting the list of Secure Elements available in the device
- Opening a communication channel with a selected Secure Element
- Transmitting commands and data to the selected Secure Element
- Storing and retrieving sensitive data in the Secure Element
- Managing PIN verification
- Managing files compatible with ISO/IEC standard
- Facilitating the management of digital signatures

While this specification can be implemented in any type of device, its first android compatible implementation has been made available in the project called “seek for android”[6].

The Open Mobile API provides an easy and convenient access to Secure Elements. In order to reduce threats such as unexpected access to Secure Elements by unauthorised applications, the usage of its functionalities is submitted to a security policy, which is under definition in the Device Committee of GlobalPlatform[7].

4.3 Virtualisation

From a user’s perspective it is favourable to be able to perform business and private transactions with only one device. This single device should virtually contain at least one business device (managed by the company) and one private device (managed by the user).

This approach can be realised by virtualisation. The basic idea of virtualisation is to create separate virtual devices to cover the different usage scenarios. This can be achieved by providing different compartments in the device for the different scenarios. Each of these compartments offers a complete operating system as well as the necessary policies and applications.

[5] SIMAlliance http://www.simalliance.org/

[6] Seek for android http://code.google.com/p/seek-for-android/

[7] GlobalPlatform http://www.globalplatform.org/

Figure 2 sketches the architecture for this approach.

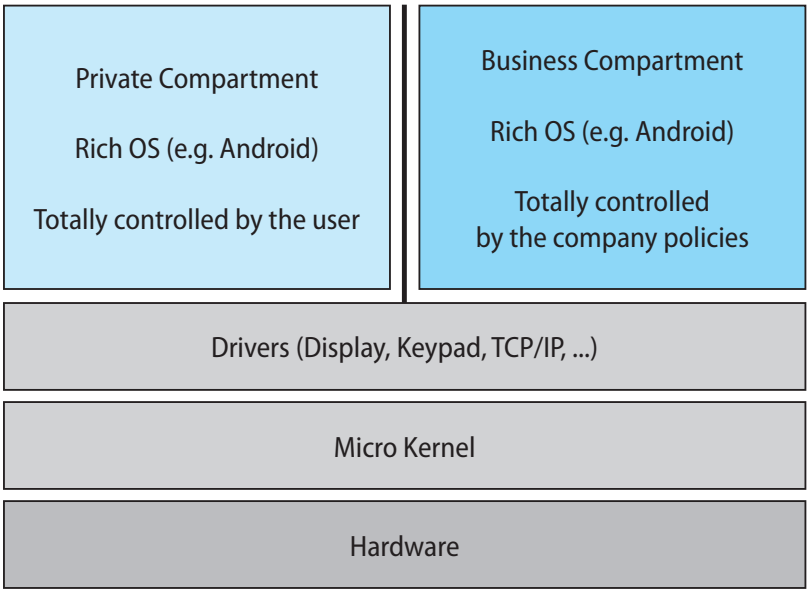


Figure 2 – Virtualisation Architecture

To reach a high level of security, such as VPN access, an additional Secure Element hosting the secret data and authentication mechanisms is an absolute necessity. Virtualisation itself only creates a separation between applications and does not secure the storage of data.

4.4 Mobile Trusted Module

The Trusted Computing Group is an industry consortium[8] gathering major IT companies together for the development of specifications for the Trusted Platform Module (TPM). This module enables any machine hosting a TPM (a PC, a device, a server) to have a trustworthy identity together with the capability to audit its integrity or safely store some keys. With the increase of mobility, the TCG has adapted its technology to define firmware for mobile devices, named Mobile Trusted Module[9]. The targeted use cases are related to mobile banking, mobile payment, strong mobile authentication for corporate solutions and e-health applications. Initial implementations of MTM in smart phones are beginning to be deployed. While having some different levels in the stack of a device, the overlap between services offered by the TEE and MTM is allowed. As an example, MTM services can be implemented as trusted services running in a TEE.

4.5 Secure Elements

Secure Elements are today the only devices capable of receiving security certifications resisting high attack potential. Considered as the “vault” of the system, they are required each time a payment or a transport application is to be offered on the phone. Usually based on certified Common Criteria EAL5+ hardware devices, they are ready to sustain a wide range of attacks, including those on the hardware.

Due to the variety of business models aimed to be supported by the phones, several form factors emerged to fit one another.

[8] Trusted Computing Group http://www.trustedcomputinggroup.org/
[9] Mobile in Trusted Computing Group http://www.trustedcomputinggroup.org/developers/mobile

The 3 main Secure Elements that are the subject of deployment or trials are currently the SIM card, the embedded Secure Element (eSE) and the Secure micro SD card (µSD).

On 25th January 2012, the European Commission proposed a major comprehensive reform of the EU's ***data protection rules*** to strengthen online ***privacy rights***.

This reform includes several key changes, one of them being the reinforcement of data security by encouraging the use of certain IT Technologies, especially privacy ***certification schemes*** as highlighted by the European Commission in its Communication on Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century[10] (page 6) and in its proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of this data[11] (article 39).

The Secure Elements in their different form factors will enable a perfectly safe implementation of such requested mechanisms.

4.5.1 SIM card (UICC)

The SIM card has been present in GSM mobile phones since the very beginning. More recently, the emergence of NFC has triggered the need for a new version of the SIM card, capable of connecting directly to the NFC controller residing in the device. This is a secure SIM communicating with the NFC controller via the Single Wire Protocol (SWP) interface standardized by ETSI (TS 102.613 and TS 102.622). Owned by the mobile network operators, it offers several advantages such as:

- being almost independent of the handset;
- being inter-changeable over time;
- potentially offering over-the-air activation of Secure Element and associated applications.

In the future, allowing for upgradeability and business evolutions, the SWP-SIM is today foreseen in reaching a very high penetration rate inside the global NFC ecosystem.

4.5.2 Embedded SE

Embedded Secure Elements offer handset manufacturers a way of creating their own business models and host secure applications independent from the Mobile Network Operators.
The embedded Secure Element is integrated, at the time of manufacturing the handset and is not removable.

[10] Communication on "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century", COM(2012)9 of 25 January 2012

[11] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012)11 of 25 January 2012

4.5.3 Secure micro SD card

Besides the SIM, the Secure SD card is the most common form factor of removable Secure Elements found today on the market. Their main interest is to offer independence from both operators and handset manufacturers. Banks or service providers developing loyalty programs are seriously looking into these devices to create their own models and services.

Recently GlobalPlatform and the SD Association signed a memorandum of understanding towards standardization around data management on secure element in SD cards.

4.5.4 Trusted Service Management

Trusted Service Manager (TSM) is a third party of trust in the secure services ecosystem. The main role for the TSM is to manage and administrate over the air the different secure elements and trusted services within a mobile device.

Figure 3 - The TSM ecosystem

Service management includes the provisioning, the subscription, the deployment, and the life cycle management.

5. Security Infrastructure Benefits

In chapter 2 we sketched the usage of eGovernment and ePayment in the environment of mobile devices. Furthermore, we've highlighted the necessity of secure input and output as well as the access to secure elements. Using the technologies described in chapter 4 we can sketch a mobile device architecture allowing for strong authentication with secure elements as well as secure input of the user's PIN and protected output of data to the display (see Figure 4).

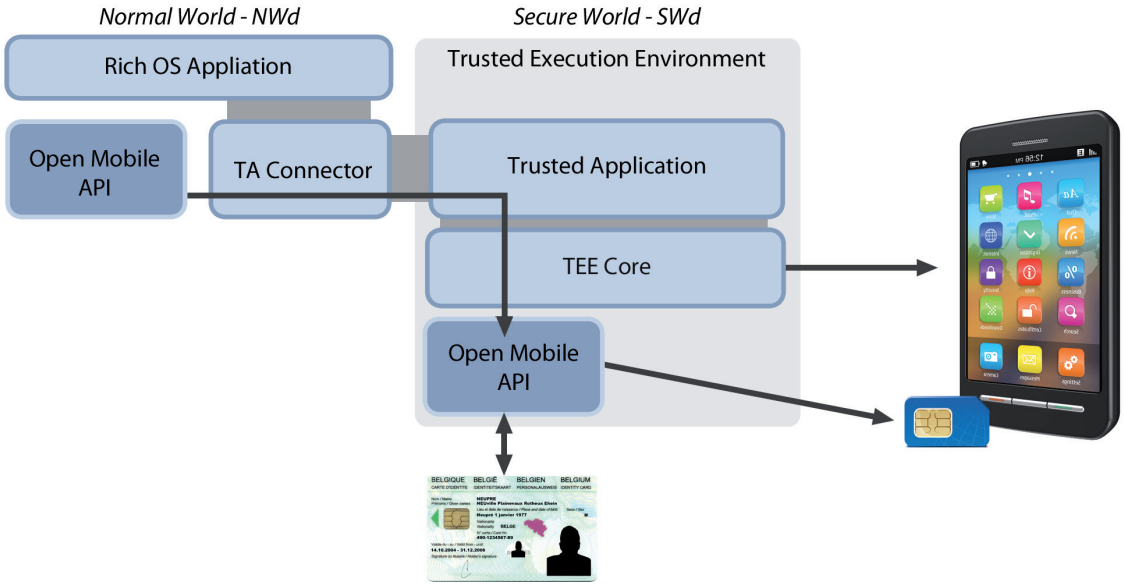


Figure 4 – Secure smartphone architecture

In this use case, the Trusted Execution Environment will realise the secure execution of the relevant authentication procedures as well as secure input and output, which includes the input of the user's PIN. The Open Mobile API facilitates communication with the different secure elements (e.g. SIM card, eID; payment card and eSE).
Only a combination of the different technologies offers a suitable security level.

6. Certification Aspects

6.1. Why security certification?

In a secured application, implying different actors in its deployment, trust must be maintained across the different actors. Let's look at the example of an egovernment solution. Here, government, application provider and device provider should make sure that the devices they rely upon are robust and that security cannot be compromised. The best way to achieve and maintain this trust is to have a shared process among the stakeholders to certify the security of the solution. This also enables easy traceability and maintenance of the security solution.

6.2. Security process principles

Several processes exist for conducting a security certification, but most of them rely on the same steps which are (1) identification of the threats by the stakeholders, based on risk analysis, (2) definition of a common security objective, (3) attacks on the solution, conducted by identified laboratories (attacks, penetration tests (white box or black box), reverse engineering, etc), (4) endorsement of the laboratory report by the liable and central entity, usually called the approval authority (e.g. government or private entity).

6.3. Existing methodology

Depending on the application domain, different certification methodologies exist. They can be 'standard' or what is known as 'private' (meaning that a group of interest defines its own processes and certification conditions, and plays the role of the approval authority). One example of well-known standard certification methods is Common Criteria (referenced as ISO/IEC 15408) designed for certifying computer security products and systems[12]. FIPS 140-2 is another popular scheme, defined by the US National Institute of Standards and Technology, and providing the security requirements for certifying cryptographic modules which include both hardware and software components[13]. For the private scheme, EMVCo or PCI are those which are referenced for the payment industry. A new approach addressing fragmented deployment mode: GlobalPlatform Card Composition Model.

Most of the security certifications actions are conducted in a given application domain, with strong silos. But in the case that multiple actors from different domains are involved in the deployment of a service, the security certification rapidly becomes a complex process to deal with. This multi stakeholder situation, combined with a dynamicity of products during their lifecycle is particularly relevant in the case of mobile service development, such as mobile payment or signature. To address this kind of specific case, GlobalPlatform has developed an innovative means of certifying products containing independent applications[14]. This model takes into account the fact that, for instance, a mobile network operator and a bank would need to collaborate for the issuing of a mobile payment application in a Secure Element, but would prefer to avoid a certification process being necessary each time a new application is deployed in this Secure Element. The model, called the GlobalPlatform Card Composition Model, describes the process to follow in certifying the security of a composite product, together with its compatibility with existing schemes such as Common Criteria and EMVCo.

[12] Common Criteria http://www.commoncriteriaportal.org/cc/
[13] FIPS 140-2 security requirements http://www.nist.gov/itl/upload/fips1402.pdf
[14] GlobalPlatform Card Composition Model v1.0 under http://www.globalplatform.org/specificationscard.asp

6.4. Usability for Secure Element and TEE

All certification schemes described here are widely deployed in the field. As an example, most of protection profile for smart cards defined by Common Criteria are targeting an EAL4+ level, in which the + indicates a resistance to hardware attack. The GlobalPlatform Card Composition Model has been designed for secure element, and thus finds its natural implementation with smart cards, µSD and embedded secure elements.

A specific study is on being undertaken in GlobalPlatform in order to find the best way to certify the security of isolated Trusted Execution Environments. Here, the challenge consists in its complex manufacturing cycle (where TEE provider, chipset maker and handset maker are all involved). An initial GlobalPlatform proposal for certifying a TEE (including a specific protection profile) is scheduled for industry release in December 2012. These issues are tackled in details in Eurosmart Digital Security Reference Paper[15].

[15] Eurosmart Digital Security Reference Paper available on www.eurosmart.com

7. Conclusion

Mobile devices such as smartphones and tablets will become the dominant access devices to services in the future. The biggest drivers for this shift from the traditional PC-based world are user convenience and a wide variety of available services in the cloud.

Due to the very large number of mobile transactions within different field applications, this domain is very attractive for attackers to violate the systems.

We have shown in the previous sections that the security industry already has the right counter-measures in its portfolio to offer strong protection against mobile fraud. For high security applications, the secure elements will continue to play an important role. New technologies like the Open Mobile API and the Trusted Execution Environment will facilitate system-wide security.

Last but not least, the different security certification approaches of secure elements and the Trusted Execution Environment will provide confidence in the delivery of reliable end to end solutions with a proven security.

8. Glossary

API	Application programming interface
CC	Common Criteria
EAL	Evaluation Assurance Level
eID	electronic identity
eSE	embedded secure element
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GSM	Global system for mobile communication
LTE	Long term evolution
MTM	Mobile trusted module
NFC	Near field communication
OS	Operating system
PCI	Payment Card Industry
PIN	Personal identification number
SD card	Secure digital memory card
SIM	Subscriber Identity Module
SWP	Single Wire Protocol
TEE	Trusted Execution Environment
TPM	Trusted platform module
UICC	Universal integrated circuit card
VPN	Virtual private network

Authors

Daniel Borleteau
Nicolas Bousquet
Thierry Crespo
Xavier Dubarry
Jan Eichholz
Virginie Galindo

About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work into dedicated working groups (communication, marketing, security, electronic identity).

Members are largely involved in research and development projects at the European and international levels.

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

EUROSMART
The Voice of the Smart Security Industry

Contact us:

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels
Tel. (+32) 2 506 88 38
Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com
Visit our website www.eurosmart.com