THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, **Series A,**
Volume 14, Special Issue 2013, pp. 373–377

MOBILE SMARTPHONES AS SECURE SIGNATURE-CREATION DEVICES

Adrian FLOAREA[*], Mihai TOGAN[**], Ionut FLOREA[*]

[*] certSIGN, , Bucharest, ROMANIA
[**] Military Technical Academy, Bucharest, ROMANIA
Corresponding author: Adrian FLOAREA, E-mail: adrian.floarea@certsign.ro
Mihai TOGAN, E-mail: mtogan@mta.ro
Ionut FLOREA, E-mail: ionut.florea@certsign.ro

Directive 1999/93/EC of The European Parliament and of the Council on a Community framework for electronic signatures establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. The legal act defines the specific conditions to be fulfilled by an electronic signature in order to obtain legal recognition. One of the key elements to create electronic signatures with legal value, the advanced electronic signatures, is the usage of secure signature-creation devices. Creation of electronic signatures using a computer is a straightforward process. As mobile devices begin to provide the same services as Personal Computers the creation of electronic signatures is a requirement emerging from the end users. This paper analyses the possibility to create electronic signatures on mobile devices and identifies the challenges: key generation, entropy sources, key management, and protection of the keys on the equipment. It identifies the current possibilities to create advanced electronic signatures on mobile devices and proposes a unified approach to allow the development of a standardized mechanism that turns the smartphones and tablet PCs into secure signature-creation devices.

Key words: electronic signature, key generation, secure element, encryption, smartphones.

1. APPROACH OF SECURITY ISSUES AND SOLUTIONS IN THE MOBILE WORLD

As new technology emerges, new user typologies, mentality shifts and new concerns arise. With the user-centric philosophy it is easy to attract new users and with the always connected paradigm that is even easier to create permanent bonds to pieces of technology, even dependence to the permanent evolution towards complete connectivity.

With the emergence of the new mobile platforms, started with the launch of the first iPhone, the level of information dissemination grew almost exponentially. This means that as we speak, a tremendous, almost unthinkable amount of information travels around us, using various wireless technologies. And much of this information is sensitive at best; part of it is business related info, maybe secret, while another part may be strictly personal.

To secure all this information raises a number of specific problems, related to several aspects:

- The user experience
- The hardware limitations
- The platform limitations
- The difficulty of integrating already developed solutions

By solving the above problems, a robust security solution adapted for mobile platforms will follow some general guidelines:

- Securing the information while in transit
- Securing the information on the device
- Securing the device itself
- Providing the user with tools so that he can tweak and secure his user experience

2. DEVELOPMENT OF SECURITY APPLICATION FOR SMART PHONES

The difference between a PC and a smartphone is that on a smart phone you have to work with much more limited CPU, limited RAM memory and of course, limited SDKs and API.

Developing security application for smart phones requires attention to details as they have a higher risk to be handled by unexpected users if the phone was lost or stolen.

Developing security application on iOS and Android is also a little bit different. Android and iOS are two very different mobile operating systems with very different philosophy. The connection point for compatibility between Android and iOS application can be a portable and well tested crypto library like openSSL [3].

For the implementation of the cryptographic engine on mobile devices there are several options available:

1. Use the Security APIs of each operating system (iOS Security APIs, Android Security APIs, BlackBerry Security APIs, etc.). This approach is recommended to develop applications for a single system and the strongest argument to support it is fast development time.
2. Use the openSSL library. This approach is suitable to develop applications for maximum two mobile operating systems as it is simple to keep compatibility between file format, SMS, emails, etc.
3. Use the openSSL library with a wrapper over openSSL and creating a SDK. This is the best option when developing applications for several mobile operating systems as its provides a unified approach for the software developer. The heaviest part lies upon the developer of the SDK.

To ensure a high degree of cross-platform scalability of a solution, a good common and validated foundation is needed. This kind of foundation is represented by the openSSL libraries, which have many years of development and support on their side, alongside with peer and third party wide support, including applications, infrastructure and backbone. By using openSSL one can be sure that the product of cryptographic operations, by example, obtained on a platform, will be compatible with the solution developed on another openSSL based solution. Also openSSL provides a wide variety of tools, and an entire community that helps to maintain and fix possible bugs and vulnerabilities.

On the other hand, there is no standard build configuration for openSSL to obtain libs especially for iPhone or Android. This means that some effort must be put in adapting the configuration files and the sources so that the libraries can be build, and another effort in testing the results. Also, not all the openSSL modules can be built for mobile platforms, and beside this, between platforms the availability for certain modules differs. As an example, it is more work invested in configuring the build files for iOS, but after that, everything works just fine, as plain C, C++ and objective C can be managed in a unitary way when developing for iPhone.

On Android on the other hand, much more effort must be put in singling out modules that cannot be built for NDK (the Native Development Kit), and then again, additional effort must be put in interfacing the native part of the solution (i.e. the actual engine) by the java side. This implies extended use of JNI (Java Native Interface) as since Android 2.3 native support has been extended to Activity level and solutions based on openSSL can be created and run in an entire native environment.

2.1. Creating electronic signatures on mobile devices

To create electronic signatures on mobile devices it was considered the Option 3 presented above. An SDK, Cryu Base SDK, was developed upon openSSL providing API libraries and developer tools necessary to build, test, and debug security apps for mobile devices. Currently the SDK is available for iOS and Android and the applications developed using the SDK is cross platform interoperable (iOS, Android, PC) as it provides compliance with international standards.

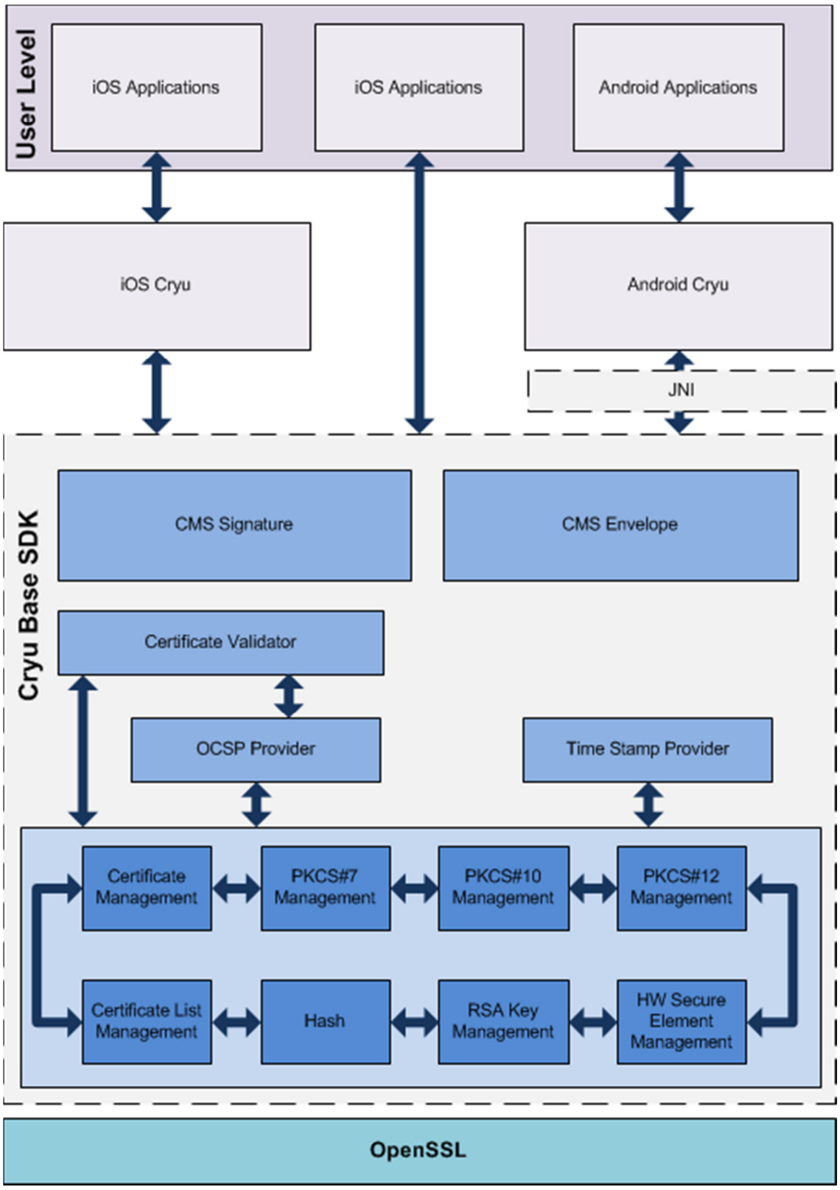

Fig. 1 – SDK Structure.

The structure of the SDK is presented in Fig. 1 and consists of:

- Basic cryptographic functions
  - Key management, hash creation, electronic signature creation, etc.
- Interface with other services: certificate validation, time stamp, etc.
- Interfaces for iOS and Android operating systems

An important element of the SDK is the interface with external secure elements that are generating and storing the cryptographic keys. This allows creation of electronic signature using keys stored on the following secure elements:

- PKCS#11 smart card – Oberthur [5] and Feitian [4]
  - Available only for Android
- Secure SD card with PKCS#11 interface
  - Available only for Android
- SIM card with PKCS#11 interface
  - Available for Android and iOS
- CAC/PIV card – Thurby [6]
  - Available only for iOS

Technically, the electronic signature can be created on mobile devices. Applications that are creating electronic signature were developed using Cryu Base SDK on both Android and iOS. An important constraint is represented by the portability of the secure element, the cross platform interoperability and the ability to be used both on a mobile device and a PC.

From EU Directive 1999/93/EC [1] the security certifications of the secure elements is a key factor for advanced electronic signature creation. An important criteria here is the existence of a security certification for the secure element that is guaranteeing both that the keys were generated correctly, with an acceptable entropy level, that are protected while stored on the device, the access is controlled and the keys cannot be copied. Not all the manufacturers conducted such certifications but, at this moment, it is possible to use several secure elements to protect the keys and create the signature.

Another option investigated was the storage of the keys directly on the mobile device. These offer several entropy sources and built in function to generate random material:

- iOS - `arc4random` function that is also the recommendation from Apple. For a better entropy the following can be added:
  - current system time
  - last values of accelerometer
  - last values of the user touch positions
- Android - the operating system provide access to `/dev/random` and `/dev/urandom`. Due to the fact that mobile operating systems are very rarely shut down, using the /dev/random mechanism is a guarantee that the entropy of our random is a very good one.

The key generation can offer a fair security level but the keys cannot be stored, at this moment, in such way they cannot be copied. This is a major drawback from creating advanced electronic signatures, even if the access to the keys and the security of the device are protected by PIN codes and other configurations that allow even the wipe of the data in the event the mobile device is stolen or an attacker tries a brute force attack over the PIN.

Currently the chip and smart card manufacturers as Intel and Gemalto are working to develop trusted chips to be installed directly on board of the mobile devices. Such chips should allow secure key generation and storage and, in the end, obtain industry certification allowing them to protect keys and create electronic signatures compliant with advanced electronic signature requirements.

3. CONCLUSIONS

The current capabilities of the mobile devices allow users to use them as replacement of the personal Computers and laptops. The demand for electronic signature creation on these devices will emerge in the future and the software manufacturers and hardware producers shall be prepared to answer to this.

Currently there are several technical mechanisms to create electronic signature on mobile devices and some secure elements to store the cryptographic keys are available.

There are differences regarding the interfaces a mobile device provides for connecting a secure element and at this moment a common secure element that can be connected on all equipment using a unique interface does not exist. This is a drawback that reduces portability therefore the keys cannot be used to create electronic signature on different flavors of mobile devices (iOS and Android) as well as on the PC. Several hardware adaptors and connectors are available but they have a limited lifetime as the interfaces are updated frequently.

For the creation of advanced signatures the devices must obtain a security certification, either Common Criteria ELA or FIPS, to guarantee a sound protection of the cryptographic keys.

Currently the manufacturers are conducting research in this area but there is not a strong trend towards migrating electronic signature from the PC to the mobile devices. Cryu Base SDK is an example of cryptographic software development kit that was created and used to develop electronic signature applications on Android and iOS, the mobile platforms with the largest market coverage.

Small market size and the usage of advanced electronic signature only within the boundaries of the European Union is one factor that is doubled also by the adoption of alternative authentication mechanisms, such as OTP. Authentication is widely considered enough secure for the protection of a transaction, even if the integrity of the data is not guaranteed by it.

The adoption of the new EU Regulation [2] on electronic identification and trust services for electronic transactions in the internal market which aims to enhance trust and generate a wider adoption of electronic business can create a larger security market and generate a new momentum for extending the usage of electronic signature. Availability of the mechanisms to create electronic signature using user oriented devices is a key element for the success of this initiative.

REFERENCES

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: http://europa.eu/legislation_summaries/information_society/other_policies/l24118_en.htm
2. Draft Regulation *on electronic identification and trusted services for electronic transactions in the internal market*: http://ec.europa.eu/information_society/newsroom/cf//itemdetail.cfm?item_id=8544
3. Openssl opensource project, www.openssl.org
4. Feitian Technologies: www.ftsafe.com
5. Oberthur Technologies: www.o**berthur**.com
6. Thursby Software: http://www.thursby.com/

Received July 15, 2013