Celtic-Plus
Smart Connected World

Project Achievements

UPSC

Project ID: C2013/2-3

Start Date: 1 May 2014

Closure date: 30 November 2016

Partners:

Curay Soft, South Korea

Intrinsic-ID B.V., Netherlands

Kuveyt Türk, Turkey

Result XL, Netherlands

Smart Soft, Turkey

Tekno A Advanced Network & Security Solutions, Turkey

Turkcell, Turkey

Co-ordinator:

Rahmi Cem Cevikbas

Turkcell, Turkey

E-mail: cem.cevikbas@turkcell.com

Project Website

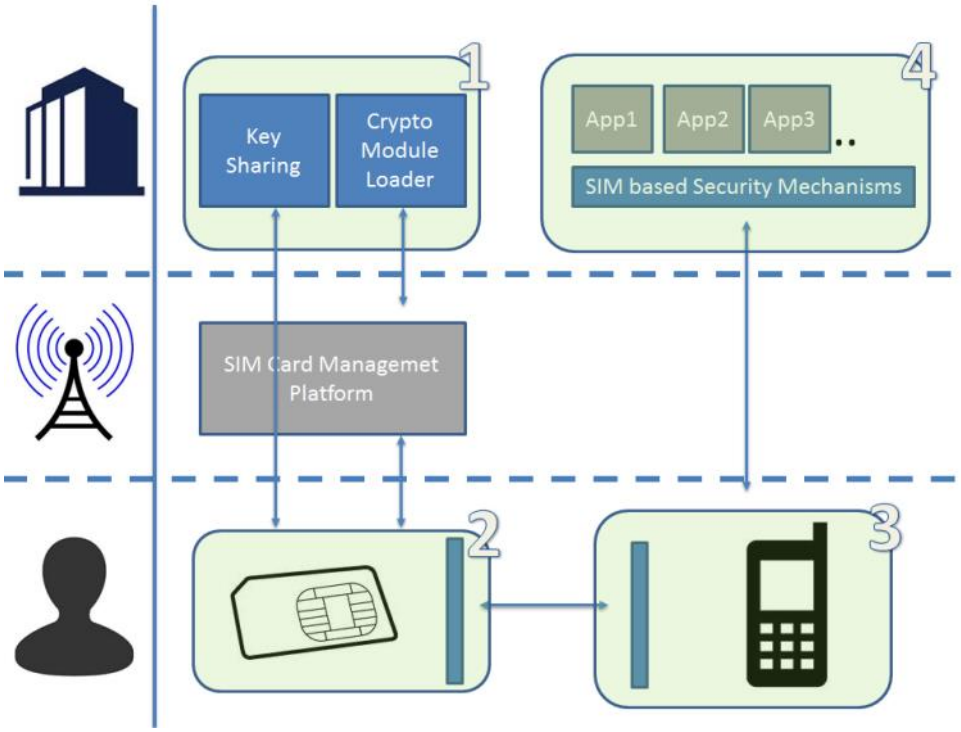
www.celticplus.eu/project-upsc

Unleash the Power of SIM

Mobile technology does not only provide voice communication but also provides a broad digital world where we can experience many vertical e-services. Identity and security of data transmission in this digital world is very critical for the success of these e-services. However, by looking at the number of different mobile brands and open–source operating systems like Android, it might be difficult to provide a secure environment. Right at this stage, SIM cards take an important role as a security service provider. They have been used for many years to preserve the security keysand algorithms for authenticating and encryption of data. Recently, new SIM cards can hold more than 512K Bytes of data, they have more CPU power, and they are enhanced with cryptographic modules. Certified factories, where also credit cards are produced, are choosen to produce these SIM cards. SIM cards have a large local distribution and support from the GSM operators. Thus, SIM cards provide the ideal environment for security requirements of new mobile e-services. However, the complexity of accessing SIM card functions is a real challenge when it is used by mobile applications. UPSC project faces this challenge and provides an easy to use software framework for mobile application developers.

Main focus

The thread of phishing, virus and sniffer attacks is a serious barrier to adoption of banking and transactional services on mobile devices. The SIM-card within connected mobile devices is not yet unleashed to its full potential, instead user-unfriendly security mechanisms around single factor authentication methods as password and log-ins are used. The UPSC project facilitates and speeds up the development process for mobile applications that are using SIM card features. The application developers will just need to include related Software Development Kits(SDK) within their mobile applications and the security functions of the SIM card will be used intrinsically. The project also includes example scenarios like remote payment, mobile signature, etc to demonstrate how the framework is used.



Approach

Today, SIM card is only used as a secure service provider either through Over the Air (OTA) platforms for mobile signature, or as a smart card for Near Field Communication(NFC)services. There is also SIM Alliance's "Open Mobile API " standard describing how to reach SIM card, however the interface is hard to use and provides a more generic approach rather than being practical.

The UPSC project provides easy-to-use frameworks to application and service providers by hiding the challenges of SIM card usage.

For instance; without the UPSC framework, an application developer should access to the sim card, select the applet and prepare the APDU(Application Protocol data Unit) messages to be sent to SIM card just for making a symmetric encryption on the SIM card. On the other hand, the same application developer would initialize the UPSC framework and call encrypt method of the framework if UPSC framework has been used. The same developer could call not only security related functions but also request to generate symmetric and asymmetric keys.

Achieved resultsUPSC project not only achieved to provide following deliverables but also speeded up mobile application transaction durations. A remote payment scenario that lasts about 10 seconds without UPSC now ends in a few seconds.

Figure 1 shows the main deliverables of UPSC framework and their relations to each other. Each deliverable embeds following technological innovations introduced by the project;

- A server side architecture which includes downloading of crypto algorithms and secure keys to SIM card without the knowledge of the GSM operator.
- A SIM card framework architecture where crypto algorithms can be called from terminal applications. Since the capabilities of SIM cards might differ, the registry application on the SIM card should have the capability to inform the terminal framework about the crypto functions that it can provide.
- An intelligent terminal framework which decides whether to reach SIM card directly through SIM card framework or OTA depending on the capabilities of the terminal.
- Enhancement of security mechanisms of E-services mostly in finance and authentication services. Following demonstrative applications are implemented;
    a. Multiple document e-signing: A single mobile signature takes a few seconds, however if there are multiple documents to be signed that the same process is repeated many times and the transaction may take minutes. UPSC framework shortens this duration by asking the signature PIN only once and sending document hashs to SIM card not through OTA but through direct link between terminal and SIM card.
    b. Remote Payment: In this scenario Credit Card PIN is encrypted after the SIM card asks for the PIN. Than the encrypted PIN is sent back to the Service provider.
    c. POS(Point of Sale) and card emulation: These demonstrations show how UPSC framework can be utilized to make complex calculations required to emulate a POS terminal and a credit card.
    d. Mobile Banking Application: This demonstration showed that UPSC framework can also cater the requirements of a real mobile banking application.

Impact

The outcome of this project has a potential of changing the way of implementing higher security applications. Following change of paradigms are expected at the end of this project;

Application Providers: The application providers utilize SIM cards for higher security requirements.

Service Providers: The service providers provide more capabilities to their users when they know that the fraud attacks are minimized. Eg: The remote payment limits may be increased.

SIM card vendors: SIM card vendorsenable crypto modules even in their basic SIM cards.

Mobile Phone vendors: More and more mobile phone vendors provide SIM card access API when they see that Application & Service providers can use SIM card easily.

Mobile Operators: Mobile operators have other ways of creating revenues when they let their SIM cards being used as a security provider.

Users: Users feel safer when they know that the operator is involved in the security of the services that they use.

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new „Smart Connected World" paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the intergovernmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies or universities and research organisations. Even companies outside the EUREKA countries may get some possibilities to join a Celtic-Plus project under certain conditions.

Celtic Office

c/o Eurescom, Wieblinger Weg 19/4

69123 Heidelberg, Germany

Phone: +49 6221 989 381

E-mail: office@celticplus.eu

www.celticplus.eu

EUREKA