Secure Payment With NFC Mobile Phones In The Smart Touch Project

Marc Pasquet, Joan Reynaud, Christophe Rosenberger

"Payment with mobile NFC phones" How to analyze the security problems

Marc PASQUET, Joan REYNAUD, Christophe ROSENBERGER
marc.pasquet@ensicaen.fr
joan.reynaud@ensicaen.fr
christophe.rosenberger@ensicaen.fr
Tel: (+33) 2-31-53-81-51
Fax : (+33) 2-31-53-81-10
Laboratoire GREYC
ENSICAEN – Université de CAEN – CNRS
6 boulevard Maréchal Juin
F-14020 CAEN (France).

ABSTRACT:
We present in this paper a method to analyze the security problems which can occur in a NFC mobile phone payment. In the first section, we give a simplified description of the technical realization for this pilot limited to a part of the system. In the second section, we present the security concepts as a major issue in this scenario. Roughly main requirement is to have same level of security as standard payment EMV transaction. The methodology described in the third section concerns the application payment and its communication with the payment terminal through a NFC link. This study, realized for the ITEA SmartTouch project, starts from a pilot experience that is carried out at Strasbourg in France, in 2007. This trial is the first experiment of a NFC-based payment application that fully supports the international EMV standard and the PayPass program. The end of this article presents different research perspectives to overstepping the encountered problems.

KEYWORDS:
NFC, mobile phone, contactless EMV payment, secure payment, secure transactions, security analysis, Common Criteria.

1. Introduction

Contactless payment is one application of a contactless smart chip technology. It is simply a contactless payment transaction that does not require a physical connection between the consumer payment device and the POS[1] terminal. Contactless payment was firstly developed on credit cards and an important implementation of that type of contactless payment is the PayPass program [1] of VISA and MasterCard with 2 Millions cards issued in US and 1 million in Europe[2].
But, this contactless payment application is limited for several reasons:

- A credit card has no batteries and so, it is no able to initiate the transaction, limiting by that way the contactless possibilities. Nxp Semiconductor splits contactless possible applications to four categories based on how consumers will use the applications and only the two first are possible without batteries. Those categories are [14]:
  - *Touch and Go* where applications such as micro payment allows consumers to just wave the device over the POS-terminal without having to confirm the transaction.

[1] POS : Point Of Sale
[2] 2007 figures

    - *Touch and Confirm,* such as mobile payment where the user has to confirm the interaction by entering a password or just accepting the transaction.
    - *Touch and Connect,* Linking two devices to enable a peer to peer transfer of data or money
    - *Touch and Explore*, where devices may offer more than one possible function. The consumer will be able to explore the device's capabilities to find out which functionalities he wants to use.
- The card has neither screen nor keyboard and if the card identification by the POS is easy to realize, the cardholder PIN-code authentication is possible only on the POS keyboard. In fact, contactless payment can be divided to micro and macro payments. Micro payment does not usually require any confirmation (signature, PIN-code) and the transaction is executed with a wave of contactless payment device over the point-of-sale terminal. Upper limit for micro payment in the United States is $25, and if the price is higher, the payment will be referred as macro payment. It means that a customer, who is paying, will be asked to confirm the payment by entering a PIN-code or a signature. It means that the European customer who wants to pay, has to wave the contactless payment device over the point-of-sale terminal, to tape his PIN-code on this POS and to wave again a second time. This procedure gets back the contactless benefits: this authentication method is neither quick nor easy.

So, to overpass these contactless payment limits, it is interesting to use a device wears well by a large part of the population which has a screen, a keyboard and batteries: the mobile phone. We use the RFID[3] acronym to point out the contactless cards technology (ISO 14 443 and ISO 7816 norms) and NFC acronym for contactless capability mobile phone (ISO 18092 NFCIP-1 and ISO 21481 NFCIP-2 norms) [2]. The NFC mobile phone can be compliant with the four categories set by NXP and its keyboard and its screen allowed the customer to confirm the transaction by entering a password or just accepting the transaction without POS interaction.

Implemented on the mobile phone, the contactless payment capability is possible on two ways:

- The dual chip where the SIM is dedicated to the mobile usage (to send and to receive call, SMS, MMS…) and the NFC[4] chip which includes a proper payment application. Those chips are completely separated.
- The single chip is about adding payment application to a SIM[5] Card environment, the NFC chip is dedicated to the RF exchange. This implies a new type of multi-applications card by merging a SIM card and a payment card into a unique entity.

An end user with such a NFC mobile phone can then either:

- Use his mobile as usual, send and receive call, SMS, MMS, update his phone book
- Use his Mobile to launch contactless applications in order to perform a payment (as a mean of payment like a standard credit card).

This study starts from a pilot experience that is carried out at Strasbourg in France, since 15th of November 2006, for six months duration (end in May 2007).

This trial is the first one of a NFC-based payment application that fully supports the

[3] RFID : Radio Field Identification
[4] NFC : Near Field Communication,
[5] SIM : Subscriber Identity Module

international EMV standard (Integrated Circuit Card Specifications for Payment Systems, defined by Europay, MasterCard and VISA) [4]. The application is stored on the Subscriber Identity Module card in the phones (single chip) also for the first time for an NFC payment trial.

This trial is a mobile contactless payment and not mobile payment. In mobile payment, GSM network used to carry banking transactions and handset as payment terminal; in this case, existing payment infrastructures (same authorization system, same clearing / settlement systems) was reused.

This trial security analysis is in progress in the ITEA[6] SmartTouch project [15] and this article mainly presents one of the security analysis methodology used for this European research and development project.

In the section two, we give a simplified description of the technical realization for this pilot limited to a part of the system. In the section three, we present the security concepts as a major issue in this scenario. Roughly, the main requirement is to have the same level of security as a standard payment EMV transaction. The methodology described in the section four concerns only the payment application and its communication with the payment terminal through a NFC link, and not all the EMV transaction. We finish this article on the different perspectives.

2. Pilot description

The pilot experience that is carried out at Strasbourg in France is a NFC single chip mobile payment trial (see figure 1) where the user has to confirm the interaction by entering a password and accepting the transaction *(Touch and Confirm)*.

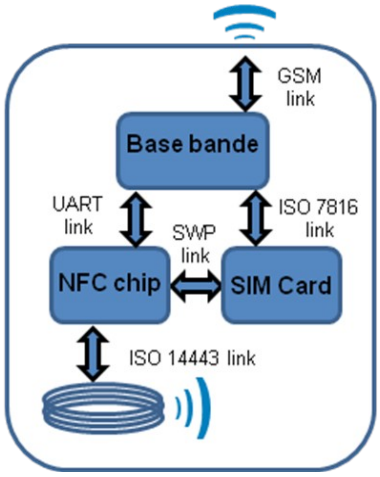

Figure 1: Single chip mobile phone

This trial is full EMV and PayPass compliant. The figure 2 shows the General outline of a PayPass-NFC payment transaction.

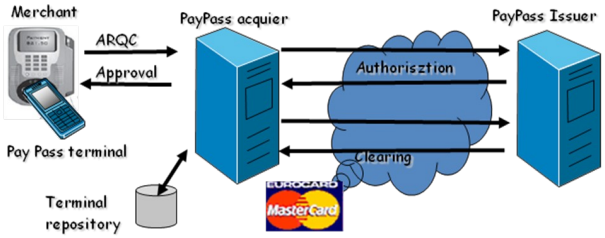

Figure 2: PayPass schematic

Payment application uses only PayPass Online profiles to execute transactions; the Offline profiles are not supported. The method CDA[7] is used during the Online transaction for the transaction data authentication by the issuer.

The contact mode, as defined by the PayPass-Mchip specification [1], is disabled as the SIM always remains in the mobile and communicates to the terminal only using the contactless mode.

In addition, the application can execute under two different modes depending on the terminal capability.

- The manual mode that must be explicitly selected. The handset owner shall explicitly select this mode when the transaction is to be done with a terminal that does not support the automatic mode.

[6] ITEA : Information Technology for European Advancement

[7] CDA : Combine Data Authentication

The user selects the application from the menu, which lists the on-card applications. He chooses the bank application. When the manual mode is validated, the bank application sends this message to the user:

"Payment Transaction, please enter your code XXXX"

The user inputs and validates his PIN code, the applet checks it and sends back the message:

"Please move your handset near to the payment device"

The user brings his mobile close to the terminal, the payment transaction carries out, and a message is displayed on the mobile to inform the user on the correct transaction progress

"Transaction completed"

- The automatic mode is the defaultone. It is the preferred functioning mode to make transactions with terminals supporting the automatic mode. The transaction is executed in two steps in this mode. The users directly presents his mobile to the terminal, a preliminary phase for the payment transaction starts, then the application sends to the handset the message:

  "Payment Transaction: XX euros, please enter your code"

  The users removed his mobile from the terminal RF field in order to enter and validate his PIN code, the applet checks it and sends back the message:

  "Please present your handset to the payment device"

  The user brings a second time his handset close to the terminal, the payment transaction carries out and a message is displayed on the mobile to inform the user on the transaction correct progress.

  "Transaction completed"

3. Security issue

The main objective of the security study [5] is the protection against fraud:

- Transaction denial
- Transaction forgery
- Protection of the SIM holder privacy.

Conforming to these objectives, the security target should be focused on the following security functions:

- Protection of the payment application sensitive data
- Secure operation of the payment application
- Secure operation of the software platform
- Hardware tamper resistance

The method is based on the Common Criteria analysis (ISO 15408). Common Criteria is a very powerful tool to evaluate and rate the security properties of an IT product.

Attack methods for the product range of NFC mobile payment cover diverse fields of expertise such as physics, informatics and cryptography. The use of these different types of expertise for attacks is very complex. This makes it very difficult for a single organization to ensure "state of the art" coverage of the whole range of attacks when relying only on its own resources. Ideally, the experts in security and security testing of a defined product range in IT would come together, pool their knowledge and compose a list of analyses representing the state-of-the-art.

- Identify Assets
- Identify Threats
- Identify Risks
- Identify Protections / counter-measures

Fortunately the NFC mobile payment conception follows lots of good practices and two laboratories (Gemalto private security laboratory and Greyc public research laboratory) are working together to research

the different possible attack methods in the ITEA[8] SmartTouch project.

Two preliminary tasks are necessary:

- Delimit clearly the perimeter of the security analysis. Here we are studying only the telephone parts involved in the NFC mobile payment and the specific NFC data exchange. We can consider that the contactless card transmission, the RF-POS and the payment network are studied by Visa and MasterCard before the PayPass implementation.
- Break it into elementary functional blocks to isolate the Target of Evaluation[9]. In the particular case of the NFC mobile payment, the evaluation target is composed of:
  - The SIM smart card with its IC, the software platform including the OS, the Java Card functionalities (JCVM, JCRE, JCAPI standards), the card manager & Open Platform functionalities (Global Platform standard) and the payment application.
  - The NFC chip with its IC and embedded software
  - The SWP link

  The interfaces with the outside system are:
  - The ISO 7816 link (contact)
  - The ISO 14443 link (contactless) [12]
  - The link with the baseband processor (standard UART)

The figure 3 shows the TOE and the operational environment during the user phases for the NFC mobile phone payment.

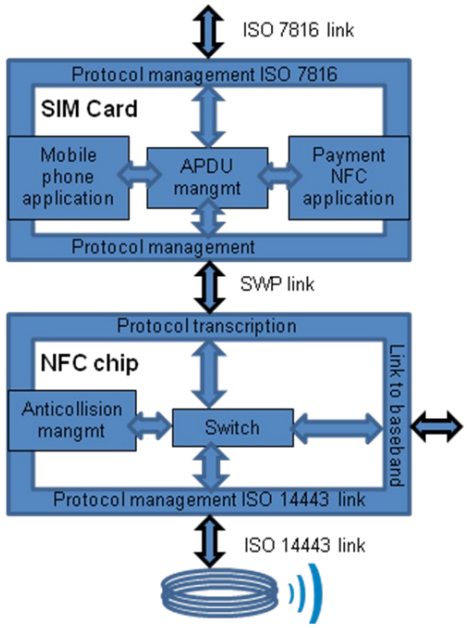

Figure 3: TOE and operational environment

The security evaluation is realized following the schematic diagram in the figure 4

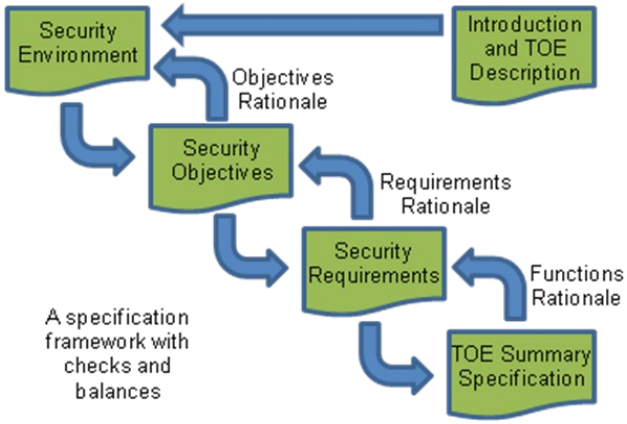

Figure 4: Common criteria schematic

Common Criteria V2.0 specifications [6, 7, 8, 9, 10] are used to define a Protection Profile[10] [11] and a security target which takes care not only of the user phases but so of all the life cycle of the TOE. Consequently we have:

- To describe the TOE as a product and position it in the life cycle of the SIM and the NFC Chip
  - Development (SIM and NFC Chip)
  - Production (SIM)

[8] ITEA : Information Technology for European Advancement
[9] TOE : Target of Evaluation
[10] PP : Protection Profile

  - SIM personalization with the application software (mobile phone and payment NFC)
  - Mobile phone application personalization (SIM number, network, PIN, Keys and certificates)
  - Payment application personalization (cardholder data, PIN, keys and certificates). The actual problem comes from the need to create a complete separation between the telecom operator and the bank issuing the payment keys and certificates. For the trial described here, the personalization is realized by a trust partner company, smart touch project member.
  - Payment application usage
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the development, production and user phases. In this test project, the environment is composed of:
  - The interfaces of the two chips
  - The threats on the payment application sensitive data, the threats on the payment application itself, threats on the software platform and direct hardware threats.
- To describe the security objectives for the TOE and for its environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development and production phases. Mainly in that case:
  - Protection agains transaction denial and transaction forgery
  - Protection of the SIM holder privacy
  - Protection of the keys and certificates
- To specify the security requirements, these includes the TOE security functional requirements and the TOE security assurance requirements. Here, we have to specify:
  - Secure storage of the payment application sensitive data
  - Secure operation of the payment application
  - Secure operation of the software platform
  - Hardware tamper resistance

This specification framework will leads us to modify possibly the SIM and NFC chip specifications.

Today, we are trying to apply the Common Criteria method on the test project and we are finishing a first step without retroaction (figure 5).

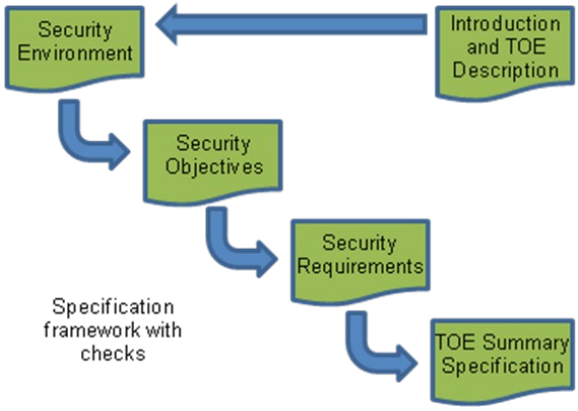

Figure 5: The state of the security evaluation

If we can consider that the security level for a NFC mobile phone, use to realize a payment transaction, must be the same than a payment smartcard, the assurance level for this PP must be "EAL[11] 4 augmented", the target is very difficult to reach. The NFC mobile phone is a more open device (3 or more chips) compared to the smart card (one chip) which is a much closed component easier to protect.

[11] EAL : Evaluation Assurance Level

(EAL1 to EAL4: correspond to current systems of good quality and the use of good practices. EAL5 to EAL7: correspond to systems conceived with high security methods).

The next step of the study will be to apply completely the Common Criteria V2.0 specifications to define a Protection Profile and to evaluate the EAL level for this NFC mobile payment application.

4. Conclusions and perspectives

The ITEA[12] SmartTouch project and its work package security have one year more to conclude the application of the Common Criteria method on NFC mobile payment.

But, beyond that project, we have point out two main problems concerning the Common Criteria in our study that can limit the generalization that security research:

- One concerns the Common Criteria method application
- The second concerns the point two of the Protection Profile definition. The security environment during the life cycle of the SIM

Concerning the Common Criteria method application, the difficulty for a single organization to ensure "state of the art" coverage of the whole range of attacks on a multi chips and complex system as the NFC mobile payment, can be bypassed on two ways. The first consists in creating a study consortium like the cooperation between Gemalto security lab and Greyc public laboratory. The second solution consists in the creation of specialized companies.

Concerning the point two of the Protection Profile definition (the security environment during the life cycle of the SIM and particularly its phase of personnalisation), a more completed description of the problematic is nessesary.

Mobile phone services and payment services require a strong authentication following specific modes. The main goal is to provide a solution for the management of those applications that is sure, standardized, and compliant with the intellectual property of the service providers.

For the test project, the third trust Partner Company (Gemalto) was already involved in France, with a large part of the personalization business has keep possible the trial.

Beyond that localized operation, the only solution, for a large scale implementation is for the bank to post personalize the operator SIM, locally or by a remote processing.

The technological developments on the SIM card and the Java Card and Global Platform specifications [13] make it possible to consider the SIM card like platforms where several applications with very diverse uses and in perfect separation can be implementing. The solution should allow the management by telephone operator of applications provided by banks, while respecting all the requirements of these actors: safety and with the respect of the intellectual properties.

This is why, supporting on the Global Platform v2.2 specifications, it is necessary to seek implementation solutions.

The NFC mobile payment has very good perspectives:

- Easy to use,
- Look like secure
- Can profit from two marketing networks, the telecom operators and the banks
- More convenient for the cardholder, quick and easy,
- Compliant with the existing payment networks and the MasterCard and VISA PayPass standard.

[12] ITEA : Information Technology for European Advancement

The challenge is to prove that the security level for a NFC mobile phone, use to realize a payment transaction, is the same than a smartcard payment.

The use of the Common Criteria method is a good comparative solution for security even if the application is not very easy. The study is on the track and the very first conclusions lead us to be very optimistic.

5. REFERENCES

[1] MasterCard PayPass – ISO 14443 Implementation Specification Version 1.1 – March 31, 2006

[2] Esko Strömmer, Mika Hillukkala, Arto Ylisaukkooja, "Ultralow Power Sensors with Near Field Communication for Mobile Applications", IFIP (International Federation for Information Processing) Volume 248/2007, pp 131-142

[3] R. Anderson, "Why Cryptosystems Fail," Comm. ACM, Nov. 1994, pp. 32-41; ftp://ftp.cl.cam.ac.uk/users/ rja14/wcf.ps.gz.

[4] EMV 2000 specifications can be found at http://www.emvco.com/specifications.cfm

[5] A. Pfitzmann et al., "Trusting Mobile User Devices and Security Modules," Computer, Feb. 1997, pp. 61-68.

[6] Common Criteria for Information Technology security Evaluation Part 1: Introduction and general model CCIB-98-026, version 2.0 May 1998,

[7] Common Criteria for Information Technology security Evaluation Part 2: Security Functional Requirements CCIB-98-027, version 2.0 May 1998,

[8] Common Criteria for Information Technology security Evaluation Part 2 annexes CCIB-98-027A, version 2.0 May 1998,

[9] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIB-98-028, version 2.0 May 1998,

[10] Common Criteria are available at the following address: http://www.crsc.nist.gov/cc

[11] Protection Profile is available at the following addresses:
http://www.scssi.gouv.fr,

[12] Dominik Haneberg, Wolfgang Reif, and Kurt Stenzel, "A Construction Kit for Modeling the Security of M-commerce Applications", Lecture notes in computer science, Volume 3236/2004, pp 72-85

[13] Global Platform 2.1.1 card specifications – March 2003

[14] Nxp semiconductors http://www.nxp.-com/

[15] Smartouch project:
http://ttuki.vtt.fi/smarttouch/www/?info=intro