A Mobile Contactless Point of Sale Enhanced by the NFC and Biometric Technologies

Vincent Alimi, Christophe Rosenberger, Sylvain Vernois

A mobile contactless point of sale enhanced by the NFC and biometric technologies

Vincent Alimi*, Christophe Rosenberger and Sylvain Vernois

Normandie University,
6 Boulevard Maréchal Juin, 14050 Caen CEDEX 4, France
and
UNICAEN,
GREYC, F-14032 Caen, France
and
ENSICAEN,
GREYC, F-14032 Caen, France
and
CNRS,
UMR 6072, F-14032 Caen, France
E-mail: vincent.alimi@ensicaen.fr
E-mail: christophe.rosenberger@ensicaen.fr
E-mail: sylvain.vernois@ensicaen.fr
*Corresponding author

Abstract: NFC transactions become very popular as they limit the time needed for a user to pay. The advantage of this technology is often seen by considering the user's point of view. In this paper, we address the use of NFC transactions for the merchant side. We propose different architectures in order to use a mobile phone as a point of sale. We compare different solutions considering some criteria such as the security assessment which is a major concern for e-payment or the facility of integration. We propose an original approach to authenticate users through the use of the touch screen of the mobile phone. The biometric authentication is based on signature dynamics (match-on-card approach) achieving a usable solution for this application.

Keywords: near field communication; mobile point of sale; match-on-card; signature dynamics.

Reference to this paper should be made as follows: Alimi, V., Rosenberger, C. and Vernois, S. (2013) 'A mobile contactless point of sale enhanced by the NFC and biometric technologies', *Int. J. Internet Technology and Secured Transactions*, Vol. 5, No. 1, pp.1–17.

Biographical notes: Vincent Alimi received his PhD in Computer Science from the University of Caen, France. He is occupying a post-doctoral position at the GREYC Laboratory, Caen, France. His research focuses on smart cards, mobile devices and embedded security.

Christophe Rosenberger is a Full Professor at ENSICAEN, Caen, France. He received his Master of Science in 1996 and his PhD in 1999 from the University of Rennes I. He works at the GREYC Laboratory. His research interests include computer security and biometrics. He is particularly interested in authentication methods for secure electronic transactions applications.

Sylvain Vernois received his Master's degree in Computer Science at the National School of Engineering ENSICAEN, Caen, France. He works at the GREYC Laboratory as a Research Engineer. His research focuses on smart cards security.

1 Introduction

Point of sales (POSs) are the electronic devices that allow a merchant to process a payment transaction either with the magnetic stripe card (e.g., in the USA) or the chip smart card (e.g., in Europe) of a cardholder. Since a few years, contactless payment smart cards have made their appearance as well as contactless POSs to handle those specific form factors. Some of the existing solutions are mobile and allow the merchant to accept contactless payment somewhere else than his shop such as itinerant merchants, taxi drivers or commercial airplanes staff. In today's world, 'mobility' has taken an important place in users' life. Nowadays, mobile phones are used as the main vector and the convergence point of mobile services such as internet browsing, e-mails reading, TV, etc. Thus, the mobile phone has become an electronic 'Swiss Army Knife'.

Turning a mobile phone into a secure contactless mobile POS is a topical question. Ingenico® has been a pioneer by delivering such a solution with 'iSMP' (Ingenico, 2011). Ingenico®'s *iSMP* is a certified sleeve on which an iPhone or iPod is connected and that turns it into a contactless mobile POS. It has the advantage to comply with the security standards but has some drawbacks. Indeed, it is available only on Apple's devices and it uses the mobile just like a modem.

In this paper, we present three architectures based on the NFC technology to turn a mobile phone into a mobile POS accepting contactless payments. After giving a technical background on POSs and the NFC technology, we study the related works in the literature and in the field. We then expose and discuss the proposed architectures and explain why we consider the solution combining the baseband processor and the secure element (SE) is the most suitable. Then, we finish with a proposition of a match-on-card signature verification method.

1.1 Point of sale

A POS is an electronic device located at a merchant's place and acting as a point of interaction with the banking system. It handles a payment transaction using either a magnetic stripe card by acquiring the data contained in the magnetic track or with a smart card by sending and receiving application protocol data units (APDU) commands as defined in the ISO7816 standard.

As an important link in the payment chain, the POS must be a very secure device. Therefore, it is tamper-resistant and resistant to many physical and software attacks in order to comply to Payment Card Industry PIN Transaction Security (PCI PTS) (Payment Card Industry, 2011) security standards. For example, the payment applications – called payments kernels – are hosted in a secure memory and the cryptographic keys and certificates are hosted in a secure non-volatile memory or in a secure smart card called secure access module (SAM).

Depending on the country, the card and the terminal, the transaction can be processed offline or online, i.e., by connecting or not to the issuing bank. In case of offline payments, the POS is responsible of checking the integrity of the transaction data with protocols based on asymmetric keys. In case of online payments, this verification is processed by the bank thanks to hardware security modules (HSM).

In the following sections, we would like to give to the readers a brief technical background on what a POS and the NFC are.

1.2 The RFID and NFC technology

In Finkenzeller (2010), the radio frequency identification technology (RFID) is presented as "a contactless transfer of data between the data-carrying device and its reader (...) The power required to operate the electronic data-carrying device would also be transferred from the reader using contactless technology". It operates at different frequencies ranging from 135 kHz to 24 GHz. One of the most known application of RFID systems is the coupling of identification smart cards and is described in several ISO standards such as ISO 14443 (ISO/IEC, 2008) and ISO 15693 (ISO/IEC, 2010). As an illustration, ISO 14443 is used for contactless payment and transit smart cards and ISO 15693 for contactless access control smart cards.

Near field communication is a proximity communication technology based on ISO 14443, and is standardised in ISO 18092 (ISO/IEC, 2004). It operates at 13.56 MHz and allows data transfer up to 424 Kbits/second. NFC devices support three operating modes:

- Reader/writer mode (proximity coupling device, PCD): Operating in this mode, a NFC device can read and alter data stored on a passive tag. Such tags can be found on smart posters, e.g., allowing the user to retrieve additional information by reading the tag with the NFC device.

- Card emulation mode (proximity induce coupling card, PICC): In this mode, a NFC device can emulate a proximity smart card (ISO14443). A reader cannot distinguish a NFC device in emulation mode from a smart card.

- Peer-to-peer mode: The NFC peer-to-peer mode (ISO18092) enables two NFC devices to exchange, through a bidirectional connection, data such as contacts, vCards, pictures, etc.

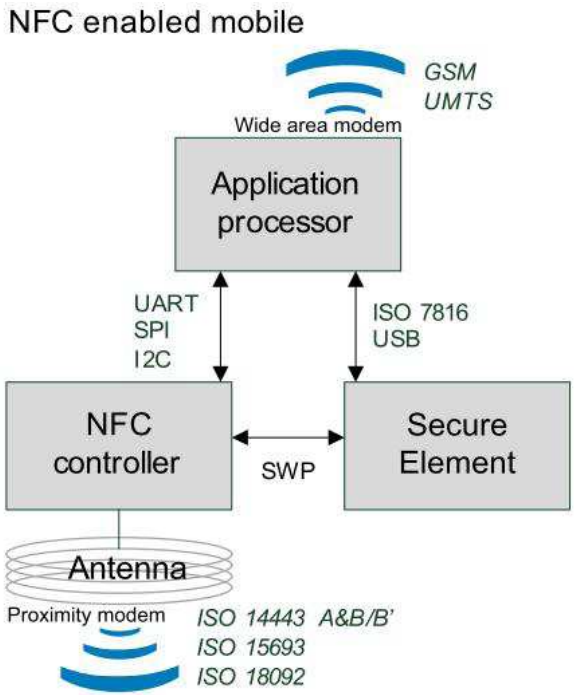
The use of the different NFC modes has been largely experienced in trials such as access control, bus ticketing and parking payment within the European SmartTouch project (Ailisto et al., 2009).

An NFC-enabled device consists of the following logical components: the NFC controller and, optionally, a secure smart card referred to as the SE. They are illustrated in Figure 1. The NFC controller, also referred to as contactless frontend (CLF) within ETSI, is responsible for the analogue/digital conversion of the signals transferred over the proximity connection. The SE, only used in card emulation mode, is a dynamic environment where applications are downloaded, personalised, managed and removed

independently of each other with different life cycles. Four main implementation options for the SE have been identified as promising alternatives at this point (EMVCo, 2007): embedded hardware, UICC, removable hardware, SE in the baseband processor (also called application processor).

It is very likely that NFC will be one of the next step forward for the mobile phone manufacturers. It is expected that the customers can pay with their mobiles. Thus, the POSs will have to evolve in order to adapt to this new next form factor. In the following sections, we present a state-of-the-art of the contactless POS solutions.

Figure 1 Architecture of NFC integrated in a mobile device (see online version for colours)



2 Related research and technology

In this section, we present works in the state-of-the-art on contactless and mobile payment research. We study first the literature, then the industrial field. We show that the academic research on the topic is rare and discuss the different findings. Prior to this, we would like to mention that as contactless and mobile payments are based on the same technology, we include both of them in the study.

Figure 2 Examples of contactless readers and POSs, (a) VivoPay® contactless reader (b) unattended POS (c) integrated POS (Ingenico® i3070) (see online version for colours)

(a) (b)

(c)

2.1 Contactless payment terminals in the literature

Contactless payment terminals are not a topic that is much covered in the literature. In a recent literature review of mobile payment research (2008), Dahlberg et al. (2008) pointed the fact that most of published papers covered very specific technical issues (e.g., security, protocols) and consumer-centric studies (e.g., adoption of the technology). Furthermore, as noticed by Ondrus and Pigneur (2008), there are few papers evaluating the potential of NFC and they provide a very descriptive approach that limits the evaluation (Chen and Adams, 2004; Zmijewska, 2005). This can be explained by the recent emergence of the contactless and mobile payment research and the fact that POSs are often considered as a highly secure piece of hardware on the merchant side and strictly controlled by banks. Thus, it is not likely to be subject to research activities.

Among the few papers dealing with this topic we can quote (Resatsch et al., 2007) in which a mobile phone is turned into a sales assistant, displaying information about a product when tapping its RFID tag. Nevertheless, this scenario, i.e., payment, requires a

more robust architecture as it deals with very sensitive data. Veijalainen et al. (2006) study the use case of a payment transaction in a taxi. The user holds a personal trusted device to return the credit card details to the card terminal over a wireless link (Bluetooth, infrared or RFID). The latter sends the payment data to the payment scheme in order to get the transaction confirmation. In this use case, the communication between the devices does not especially rely on the NFC but the authors highlight the need for security, privacy and trust of such a solution.

2.2 Contactless payment terminals in the industry

The contactless POSs found in the industry come in multiple forms. One can find unattended contactless POS, contactless payment readers to be connected to an existing POS or fully integrated contactless POS. In addition, they can implement a supplementary feature to support mobile payment. Unattended contactless POS can be found on gasoline dispensers, toll road or vendor machines. They deal most of the time with small amount transactions and increase the speed and convenience of the purchase for the consumer.

Contactless payment readers or targets are external devices connected to an existing POS or electronic cash register (ECR) that handle the radio-frequency dialog and the contactless payment transaction. At the end of the transaction, it sends to the associated POS or ECR the data to be sent on the clearing networks. Among available products, one can quote the VivoPay® solutions.

Fully integrated contactless POS are the last generation of POSs. They embed in the same device all hardware and software to handle contactless payments (contactless antenna and micro-controller, contactless payment applications, ...).

2.3 Motivation

The aforementioned solutions present common characteristics such as the ease, speed and convenience of the transaction. Most of them are countertop solutions, i.e., intended to be used in shops. A very few of them are intended to be mobile, for itinerant merchants for example. This can be explained by the necessity to be connected to the bank (depending on the country) and the extra cost it would imply. Another point that needs to be revealed is the lack on the market of POS capable of handling NFC mobile payments, i.e., where the contactless card is emulated by a mobile phone. Those payments differ from standard contactless payments by the fact that, very often, the payment functionality of the mobile would be protected by a passcode or personal code. Thus, this implies an additional interaction with the user to inform him the payment is refused and that he should enter his passcode on his mobile.

The motivations to design mobile NFC POS solutions are the following:

- allows accepting contactless and mobile payments
- suitable for itinerant and outdoor merchants
- can coexist on the same device with other mobile services
- use the existing data plan subscription to connect to the bank or payment gateway
- allows a rich user interface by taking advantage of the mobile device display

- allows a variety of added-value services such as dematerialising the receipt or adding geolocation-based information.

In the next section, we propose three architectures turning a mobile into a mobile contactless POS thanks to the NFC technology. Then, we compare them with objective criteria such as the security offered by the solution and the integration effort for the device manufacturer.

3 Proposed architectures

In this section, we detail three possible architectures for a mobile contactless POS taking advantage of the NFC technology.

3.1 Everything in an external device

This architecture is shown in Figure 3(a). A SE, i.e., a highly secure smart card (e.g., EAL4+ security level), is embedded in a small device that is connected to the mobile's dock. This SE hosts the payment kernels, a software SAM, a toolbox of cryptographic facilities and a dedicated processor. The device is linked to the NFC controller via a digital link and the NFC controller can be accessed from the baseband processor with the classical mechanisms [e.g., JSR 257 (Java Community Process, 2009)]. For the visual interface with the users, i.e., the merchant and the customer, a UI application is ran from the baseband and access the device via an application programming interface (API). When a smart card is detected in the RFID field, the concerned payment kernel (i.e., Visa©, MasterCard©, JCB© or other) communicates with the card and process the payment transaction. The payment transaction data is then sent to the host application for sending an authorisation query over the network. The UI application is used to display the details of the transaction and eventually captures the cardholder signature or PIN code.

3.2 Payment kernels in the baseband and SAM in the SE

In this architecture, the payment kernels and the SAM are placed in two different locations [cf. Figure 3(b)]. The payment kernels are located in the baseband processor while the SAM is securely hosted by the SE along with some cryptographic functions. The SAM is a piece of software code in the SE that is accessed by the payment kernels through an API. It contains the issuer's public keys to validate the card certificates and eventually some symmetric DES keys to secure the communication over the mobile network operator (MNO) network. The payment kernels and the API are built over a trusted execution environment (TEE) (Aarts et al., 1998). TEE's main goal is to offer a two world-based platform: a secure world in which execution of code, access to I/O and devices such as display and keyboard are secured; and the 'normal' world in which applications run in the standard way. Those last can access secure applications, called services, via a secure channel between the two worlds.

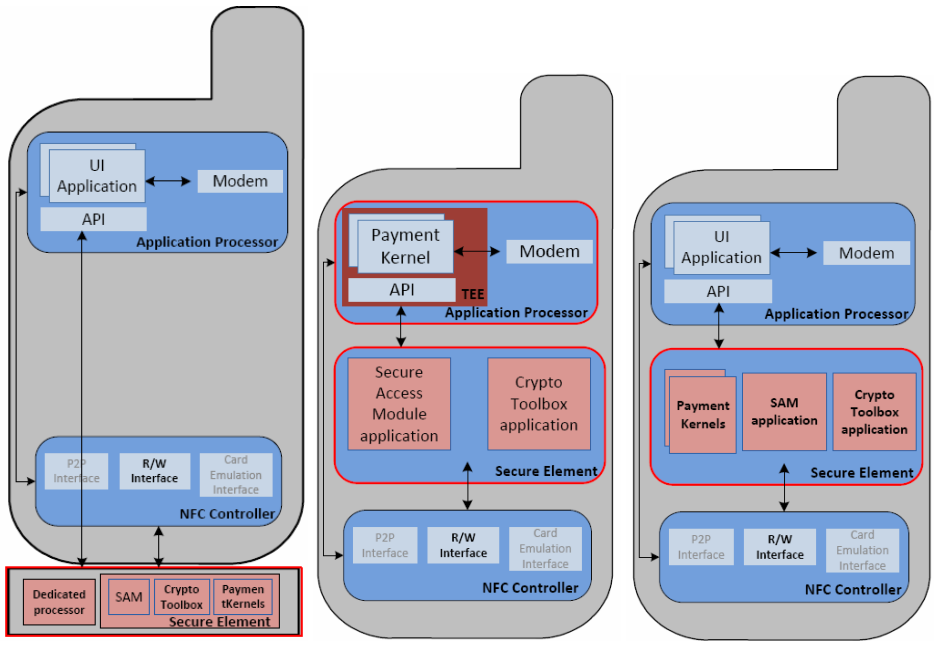
When a card is detected in the field, the payment kernel is informed by the NFC controller. Then, the payment kernel handles the transaction by sending commands from the baseband to the card passing through the NFC controller. This is done via

mechanisms such as JSR 257 in Java-based mobiles. The UI application is placed in the normal world of the TEE, except for 2 operations: the cardholder PIN code entry or signature capture and the confirmation of the amount. Indeed, two of the attacks that are dread in a mobile payment environment are the stealing of the PIN code (e.g., by a key logger) and the falsification of the displayed amount (e.g., display a 10 euros amount while the transaction is processed for 100 euros). For these reasons, those two operations are based on subroutines located in the secure world. This allows what we will call 'Secure mobile PIN' and 'What you see is what you pay'. To ensure of the UI application integrity, its code is hashed and the result is stored in the SE. Every time the application is launched, a subroutine is called from the TEE's secure world and checks the integrity by comparing the computed hash and the one stored.

3.3 *Everything in the SE*

This approach is similar to the first one except that the components are not embedded in an external device but in the SE of the mobile. It is illustrated in Figure 3(c). The payment kernels are securely hosted and executed from the SE as well as the SAM. It allows taking benefits of existing SE architectures such those relying on a GlobalPlatform base (Dahlberg et al., 2008). The payment kernels and the SAM are located in a security domain that keeps them safe from any altering attempts. When a smart card is detected in the field, the SE handles the payment transaction and sends events to the baseband processor to update the display with transaction details.

Figure 3 Proposed architectures, (a) payment kernels and SAM in an external device, (b) payment kernels in the baseband and SAM in the SE, (c) everything in the SE (see online version for colours)



(a) (b) (c)

4 Comparative study

In this section, we discuss the three proposed architectures, compare them with objective criteria and summarise their benefits and limitations. The considered criteria are: the offered security level, the target of security certification and the integration effort needed to integrate the solution in existing devices. Each criteria is rated from 1 to 4 according to the analysis done below.

4.1 Everything in an external device

- *Security*: this solution is very secure as the components are hosted outside of the mobile in a certified add-on. It would obtain a pretty good level of certification as the target of evaluation (TOE) is simple. 'We assign the scores of 4 for the offered security and 4 for the certification level'.

- *Integration*: this solution suffers from difficulties of integration. Indeed, until all mobile phones have the same dock, the device has to be implemented for all models. Furthermore, some additional APIs have to be added to the mobile software stack as well as some hardware modifications to enable the communication between the NFC controller and the SE in the external device. 'We assign the score of 1'.

- *Analysis*: this solution allows to turn a mobile phone into an NFC mobile POS just by plugging an external add-on. It requires an integration effort as it uses a proprietary connector and proprietary access APIs.

4.2 Baseband and SE

- *Security*: this solution inherits the security of the highly secure TEE and SE. The certification seems to be a difficult point as it would consist in certifying the operating system of the mobile. Some initiatives such as aggregation certification are also under investigation to certify complex targets such as operating systems (GlobalPlatform, 2011a). 'We assign the scores of 3 for the offered security and 3 for the certification level and maturity of the solution'.

- *Integration*: the TEE is a very promising secure concept but suffers from a lack of both integration efforts by manufacturers and standardisation efforts by the industry. Regarding the latter, there is a current initiative at GlobalPlatform (2011b) to define an API to access secure services hosted by the TEE, the interface between the TEE and the SE and the secure interface with the keyboard and display. 'We assign the score of 2.5'.

- *Analysis*: combining a trusted operating system and a secure chip, this solution offers a high level of confidence. It should help the adoption of mobile payment in general and the entry of a PIN code on a mobile device. Nevertheless, as it is not mature yet it is not a reliable solution in the short term. But, it is likely to be one of the most reliable solution in the long-term.

4.3 Everything in the SE

- *Security*: in this solution, the components are hosted by the SE, a highly secure by design piece of hardware and software. Thus, the payment kernels and SAM are placed in the most safe place in the mobile and inherits its security properties. 'We assign the scores of 4 for the offered security and 2.5 for the certification level'.

- *Integration*: this approach is very secure but implies a lot of work on integration of the SE-NFC controller link. Indeed, the SE is designed to emulate a smart card. In this mode, it is asked to emulate a terminal, i.e., be the originator of the transaction and to send the commands to the card instead of treating incoming commands, do the card-side processing and respond. This requires to completely change the processing of both the NFC controller and the SE. Another concern is the transaction timing. Indeed, SEs are optimised for performing cryptographic operations such as signing and hashing but not for the inverse operations (signature verification, hash verification). 'We assign the score of 1'.

- *Analysis*: with a further integration effort, this solution could add a great added value for the security of the PIN entry and the display of the transaction amount. Indeed, as the SE is a highly secure and certified component, it could be part of the design of new generation secure mobile phones and help also the adoption of the NFC technology.

4.4 Synthesis

Table 1 compares the three architectures according to the following criteria: the ease of integration in mobile phones, the security of the solution and the ease/feasibility of the certification. In the latter, we include the certification by the PCI security standards. The PCI standards take care of the appropriate use and storage of the cardholder data [as per Payment Application Data Security Standard, PA-DSS (Payment Card Industry, 2012)] as well as the security of the PIN entry [as per PCI PTS (Payment Card Industry, 2011)]. In the proposed solutions, whether a PIN is to be entered by the user, the PCI PTS standard apply. It defines the requirements to ensure the logical and physical security of the POS and the protection of the data between the input component (in our case the mobile keyboard or touch screen) and the secure controller of the device (in our case the SE). An overall mark summarises the evaluation. The marks range from ★ to ★★★★ (the ✯ symbol represents a half-star) and are assigned according to the aforementioned discussion items.

Table 1 Comparison of the proposed mobile POS architectures

	Integration	*Security*	*Certification*	*Overall*
Secure element	★	★★★★	★★✯	★★✯
External device	★★	★★★★	★★★	★★★
BB and SE	★★✯	★★★	★★★	★★★

4.5 Conclusions

Table 1 shows that the integration of the three solutions suffer either from a software or from a hardware standpoint. Indeed, the TEE is not a mature technology yet and the SE found in NFC-enabled devices has not been designed to work as a 'Master'. It also shows that the three solutions are very secure but they differ in the certification level they can achieve. We observe that the two 'monolithic' solutions obtain a high confidence for the certification while the 'combined' solution suffers from difficulties in the OS certification.

Nevertheless, these difficulties are only software related. Indeed, while there exist hardware challenges for the integration of the two monolithic solutions that are to be solved by the manufacturers, the TEE and its certification mobilise of lot of efforts in the standardisation bodies. It is estimated that in the upcoming years (GlobalPlatform, 2011b), a reliable and stable solution will have been designed, published and implemented. Thus, if we refer back to Table 1, we would assign the score of 4 for the integration and the certification of the solution. The combined solution would then become the best solution of the three exposed in this paper.

In the motivations section, we mentioned the ability of using the mobile device display to offer a rich user interface. More and more, the devices on market are equipped with touch-sensitive screens and allow a richer interface with the user. Indeed, in our case, the touch-sensitive screen can be used to capture the cardholder's signature and dematerialise the receipt usually printed. In the next section, we expose a method to verify a signature captured on a touch-sensitive screen in order to enforce the security of the transaction.

5 A match-on-card signature verification algorithm

In order to verify if the user is the real owner of the smart card, we need to process an additional authentication step. The requirements for a contacless face to face payment are:

1 the authenticator needs to be difficult to obtain or to duplicate by an impostor

2 the verification must be fast

3 the authentication solution must be as simple as possible for the user.

Among the different solutions in the state-of-the-art, we make the choice of the authentication method for the proposed application in the next section.

5.1 Authentication solutions

The authentication process can be based on a combination of one or more authentication factors. The four (widely recognised) factors to authenticate humans are:

- Something the user knows: a password, a pass-phrase, a PIN code, the maiden name of his mother…

- Something the user owns: a USB token, a phone, a smart card, a software token, a navigator cookie…
- Something that qualifies the user: a fingerprint, a DNA fragment, a voice pattern, hand geometry…
- Something the user can do: a signature, a gesture…

For an e-payment application, we suppose that the user holds the smart card. Another authentication factor is always used for face to face payments, the most common solutions are: the knowledge of a PIN code or the ability to make the same signature than the one printed at the back of the smart card. The problem is that these authentication methods are not sufficient to guarantee the identity of the user. It is not a difficult task to obtain the PIN code of another user. Moreover, with training, it is rather easy to be able to impersonate the signature of somebody (as the verification is done visually). To overcome all these drawbacks, in this paper, we propose to use a biometric-based solution.

Biometrics is associated to the authentication factors based on what users are or how they do things. The main advantage of biometric systems is the strongest relationship between the authenticator and the associated user. Other user authentication approaches are more related to machine authentication. It is so a priori more difficult to steal or copy the biometric template of an individual compared to a PIN code as for example. The user authentication generally generates some errors that must be of course minimised, that constitutes the main drawback of the authentication methods based on biometrics. There are three categories of biometric modalities: biological (DNA, blood...), behavioural (signature dynamics, keystroke dynamics, voice...) and morphological (fingerprint, face, hand veins...). The most used biometric modality is the fingerprint because of its efficiency and the cost of the sensor. In this paper, we propose to use signature dynamics for many reasons:

- easy for an user to sign
- quick verification
- easy to capture on a smart phone with a touch screen
- difficult to forge the signature dynamics of an user (way of signing).

In the next section, we present a state-of-the-art on signature dynamics to choose the best solution to embed in the proposed POS.

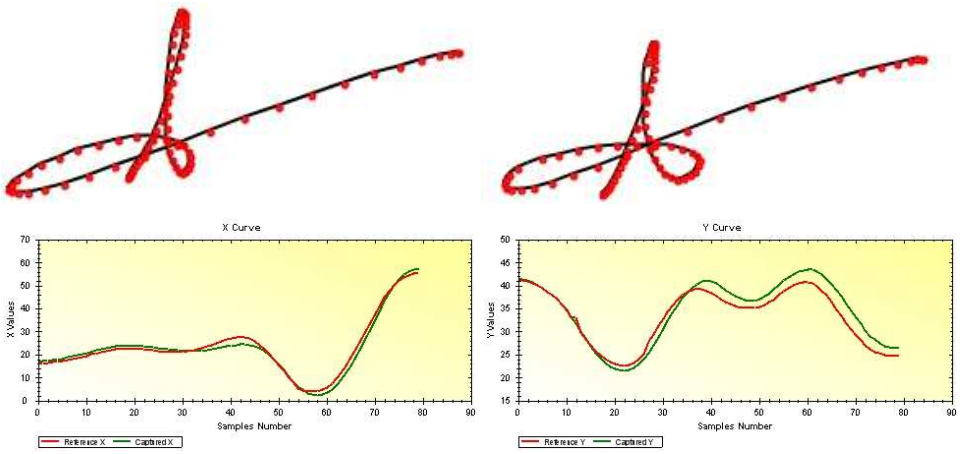
5.2 State-of-the-art in signature dynamics

In our application, we suppose having at each time t, the location of the pencil in the touch screen represented by a vector (x_t, y_t), $t = 1: N$ (N depending of the complexity of the user's signature). Based of this vector, we can measure different features to generate user's template (enrolment step) and to realise the verification step. The problem of the signature dynamics verification can be resolved by computing a complex distance between the reference signature and the capture one based on the features computed on the raw data.

There are two main approaches for the verification of the signature dynamics. The first one is based on a global computation taking into account different features of the signature dynamics such as the average speed, the total duration … (Fierrez-Aguilar et al., 2005; Ketabdar et al., 2005; Yanikoglu and Kholmatov, 2009). This category provides quite poor results. The second category uses a local information for the comparison of two signature dynamics. Some methods compute a descriptor on each acquired point (x_t, y_t) (Jain et al., 2002; Henniger and Franke, 2004; Kholmatov and Yanikoglu, 2005; Ly Van et al., 2007). Another possibility is to compute a descriptor on specific points (where the speed is higher as for example) (Hao and Chan, 2003). The last solution consists in computing some descriptors on each interval on the signature dynamics (Aarts et al., 1998).

One of the most efficient solution [especially when only two measures (x_t, y_t) are used (Garcia-Salicetti and Houmani, 2009)] is based on the elastic distance (Martinez-Diaz and Hangai, 2009). We have chosen this approach as it gives good results and the verification is quick. First, the (x_t, y_t) signals of the signature dynamics can be resampled in order to provide equidistant spacing between points (considering time). Two features are extracted at each point in the signature namely δ_x and δ_y, these features correspond to the change in the x direction and y direction. The feature values are finally normalised. The matching algorithm is based on the string matching technique called dynamic time warping (DTW). The performance of this algorithm has been evaluated on different benchmarks (such as MCYT-100). The equal error rate (EER) value is around 3% meaning that for the compromise configuration (specific setting of the biometric system), 3% of impostors are accepted and 3% of genuine are rejected. As this authentication method is additional to the belonging of the smart card, this is a correct result. We think also this result is much better than a visual verification and more convenient for the merchant. As illustration, Figure 4 presents an example of comparison of two signature dynamics of a genuine user.

Figure 4 Example of two signatures from the same person (see online version for colours)



Note: X and Y curves describing the way of signing are very similar.

5.3 Implementation

We describe in this section the implementation on the signature dynamics verification. We distinguish two steps:

- *Enrolment*: The biometric template of an individual is stored in its smart card. It consists in a vector of dimension 2N where N is the temporal sampling number of the signature dynamics. In our studies, 50 is a good value. In this case, the storage of its personal signature $R = \{(x_t, y_t)\ t = 1{:}50\}$ costs 200 octets (2 octets per value x or y).

- *Verification*: For the authentication process, the user is asked to sign on the touch screen of the mobile phone considered here as a POS. Once the signature dynamics captured (a vector of 50 values $C = \{(x_t, y_t)\ t = 1{:}50\}$), the POS sends to the smart card through a contactless transaction an encrypted message containing the biometric data and a random challenge. The encryption is realised by using the classical RSA algorithm with the public key of the smart card (embedded in its certificate). The smart card decrypts the message and compares C and R with the verification method described in the previous section (match-on-card). The smart card sends back an encrypted message with its private key containing the result of the verification with the challenge previously transmitted by the POS. The POS decrypts the previous message using the public key of the smart card and verifies the challenge (check if it is the same than the one transmitted). The verification result is printed on the screen of the POS. This ends the authentication process.

A proof of concept software has been developed on a Windows™ Platform and is shown in Figure 5. We have implemented a tablet version of the signature dynamics authentication scheme. It is very fast (the answer is given in less than 1 second) and meets operational constraints. We have implemented a low cost version based on correlation computation between signals that can definitely be used on a SE (such as a SIM card).

5.4 Discussion

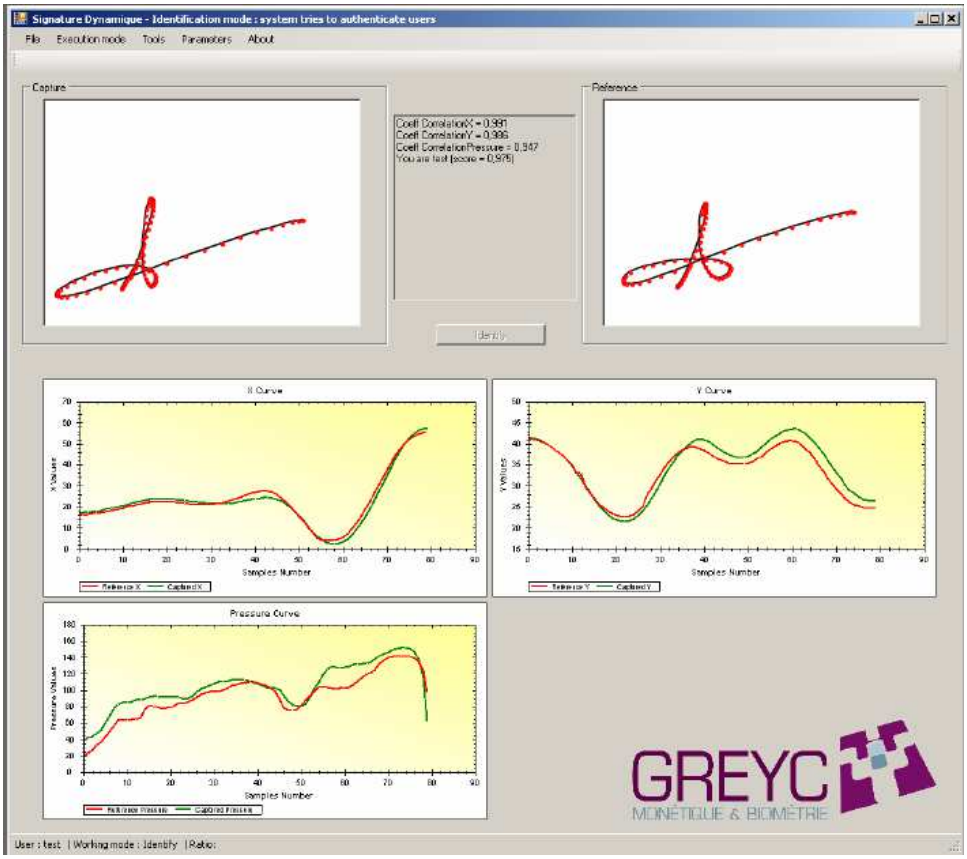
We think this solution is very usable for many reasons:

- The security is achieved through classical cryptography. An attacker cannot retrieve the signature dynamics of another user as it is encrypted. The replay attack is not possible thanks to the use of a challenge by the POS.

- The processing time is low as it consists only on computing a distance between two vectors of integers.

- It is very convenient for the user as anybody is used to sign documents.

Figure 5 Signature verification proof of concept (see online version for colours)



6 Conclusions

We presented in this paper three secure architectures to implement a mobile contactless POS solution that are adapted to the contactless and mobile payment requirements. The three proposed architectures present a very good level of security but require a more or less important work of integration. As it would allow to securely key a PIN code and displays the transaction information, we think that the solution combining a TEE in the Baseband and the SE is the most reliable in the long term. It should help the adoption of mobile payment and the user trust in this technology. We also presented a match-on-card signature verification method. This solution, that dematerialises the usual paper signature, has the advantages to be secure, low-time processing and convenient for both the user and the merchant. Furthermore, it is applicable to the three architectures exposed in this paper.

References

Aarts, E.H.L., Doling, J.G.A. and Van Oosterhout, J.J.G.M. (1998) 'On-line signature verification with hidden Markov models', in *Proceedings of the International Conference on Pattern Recognition*.

Ailisto, H., Isomursu, M., Tuikka, T. and Häikiö, J. (2009) 'Experiences from interaction design for NFC applications', *Journal of Ambient Intelligence and Smart Environments*, December, Vol. 1, No. 4, pp.351–364.

Chen, J.J. and Adams, C. (2004) 'Short-range wireless technologies with mobile payments systems', in *Proceedings of the 6th International Conference on Electronic Commerce, ICEC'04*, ACM, New York, NY, USA, pp.649–656.

Dahlberg, T., Mallat, N., Ondrus, J. and Zmijewska, A. (2008) 'Past, present and future of mobile payments research: a literature review', *Electronic Commerce Research and Applications*, Vol. 7, No. 2, pp.165–181.

EMVCo (2007) 'Emv mobile contactless payment technical issues and position paper', Technical report, EMVCo.

Fierrez-Aguilar, J., Nanni, L., Lopez-Penalba, J., Ortega-Garcia, J. and Maltoni, D. (2005) 'An online signature verification system based on fusion of local and global information', in *Proceedings of 5th IAPR International Conference on Audio and Video-based Biometric Person Authentication, AVBPA*.

Finkenzeller, K. (2010) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 3rd ed., John Wiley and Sons, Inc., New York, NY, USA.

Garcia-Salicetti, S. and Houmani, N. (2009) *Encyclopedia of Biometrics*, Chapter Digitizing Tablet, pp.224–228, Springer Publishing Company, Inc., USA.

GlobalPlatform (2011a) 'Globalplatform defines new certification model for mobile secure elements' [online] http://www.globalplatform.org/mediapressview.asp?id=868 (accessed May 2011).

GlobalPlatform (2011b) 'The trusted execution environment – delivering enhanced security at a lower cost to the mobile market', Technical report, GlobalPlatform.

Hao, F. and Chan, C.W. (2003) 'Online signature verification using a new extreme points warping technique', *Pattern Recognition Letters*, Vol. 24, No. 16, pp.2943–2951.

Henniger, O. and Franke, K. (2004) 'Biometric user authentication on smart cards by means of handwritten signatures', in *Biometric Authentication, chapter Lecture Notes in Computer Science*, pp.1–39, Springer, Berlin/Heidelberg.

Ingenico (2011) 'Mobile Terminal Payment System for iPhone and iPod Ingenico iSMP' [online] http://libertismp.com (accessed August 2011).

ISO/IEC (2004) *ISO/IEC 18092: Information Technology – Telecommunications and Information Exchange between Systems – Near Field Communication – Interface and Protocol (NFCIP-1)*.

ISO/IEC (2008) *ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit(s)cards – Proximity Cards*.

ISO/IEC (2010) *ISO/IEC 15693: Identification Cards – Contactless Integrated Circuit(s)cards – Vicinity Cards*.

Jain, A.K., Griess, F.D. and Connell, S.D. (2002) 'On-line signature verification', *Pattern Recognition*, Vol. 35, No. 12, pp.2963–2972.

Java Community Process (2009) JSR 257: Contactless Communication API.

Ketabdar, H., Richiardi, J. and Drygajlo, A. (2005) 'Global feature selection for on-line signature verification', in *Proceedings of International Graphonomics Society*.

Kholmatov, A.A. and Yanikoglu, B. (2005) 'Identity authentication using improved online signature verification method', *Pattern Recognition Letters*, Vol. 26, No. 15, November.

Ly Van, B., Garcia-Salicetti, S. and Dorizzi, B. (2007) 'On using the viterbi path along with HMM likelihood information for on-line signature verification', *IEEE Transactions on Systems, Man and Cybernetics, Part B, Special Issue on Recent Advances in Biometric Systems*, October, Vol. 37, No. 5, pp.1237–1247.

Martinez-Diaz, J.F.M. and Hangai, S. (2009) *Signature Features*, Springer Verlag, USA.

Ondrus, J. and Pigneur, Y. (2008) 'An assessment of NFC for future mobile payment systems', in *Proceedings of the International Conference on the Management of Mobile Business*, IEEE Computer Society, Washington, DC, USA.

Payment Card Industry (2011) Payment Card Industry PIN Transaction Security.

Payment Card Industry (2012) 'Payment Application Data Security Standard', Technical report, Payment Card Industry.

Resatsch, F., Karpischek, S., Sandner, U. and Hamacher, S. (2007) 'Mobile sales assistant: NFC for retailers', in *Proceedings of the 9th International Conference on Human Computer Interaction with Mobile Devices and Services, MobileHCI '07*, ACM, New York, NY, USA, pp.313–316.

Veijalainen, J., Terziyan, V. and Tirri, H. (2006) 'Transaction management for m-commerce at a mobile terminal', *Electronic Commerce Research and Applications*, Vol. 5, No. 3, pp.229–245.

Yanikoglu, B. and Kholmatov, A. (2009) 'Online signature verification using Fourier descriptors', *EURASIP Journal on Advances in Signal Processing*, January, pp.12:1–12:1.

Zmijewska, A. (2005) 'Evaluating wireless technologies in mobile payments: a customer centric approach', *International Conference on Mobile Business*, pp.354–362.