Enhancing Security of Terminal Payment with Mobile Electronic Signatures

Evgenia Pisko[1]

Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe-University Frankfurt, Germany

Abstract. With the growing number of debit card transactions, security issues have arisen correspondingly. By applying the latest technical innovations, criminals are using more and more effective methods of card fraud. They are exploiting security weaknesses of existing debit card payment rules. For instance, if a criminal has acquired the complete card data, he will be then able to use it to withdraw money until the card is blocked. To authorize each payment and to guarantee the integrity of payment information, we have developed a service architecture for mobile signature secured payments at the POS, which we present in this paper. To support the proposed architecture we suggest service subscription and payment protocols.

1 Introduction

Debit card payments performed at the point of sale (POS) have gained in customer acceptance over the last years. The proportion of debit card payment transaction (PIN-secured debit (or electronic cash) and signature debit) rose to almost 27% of all purchases in 2005 in Germany [1]. The card usage trend in the USA is similar [2]. With the growing number of debit card transactions, security issues have risen correspondingly. According to statistics from the Federal Criminal Police Office of Germany (in German: Bundeskriminalamt or BKA) signature debit frauds reached 48143 acts and PIN-secured debit frauds reached 32232 acts in 2005 [3]. Weaknesses of existing debit card payment rules are successfully used by criminals to get access to the bank accounts of card holders. Signature falsification is one of the easiest methods for signature debit fraud. Similarly PIN-secured transactions are not safe from misuse if criminals get known PIN and card data. This is possible through communication eavesdropping at manipulated cash points and POS terminals. This manipulation very often occurs at the ignorance of shop or bank personnel. For example, one of the recent schemata introduced in some European countries is shown in Figure 1.

Special chips have been installed in POS terminals by criminals. Physical access to a POS terminal without the assistance of shop or petrol station keepers, who themselves are often victims of these manipulations, is sufficient for this purpose.

[1] Supported by Deutsche Telekom Stiftung

Pisko E. (2007).
Enhancing Security of Terminal Payment with Mobile Electronic Signatures.
In *Proceedings of the 1st International Joint Workshop on Wireless Ubiquitous Computing*, pages 13-22
DOI: 10.5220/0002430900130022

These chips can intercept the card code and PIN and send this data via wire phone channel or via SMS to criminals. The "card mafia" acts mostly internationally. Customer card data eavesdropped in a petrol station in Italy will be send to criminals in Romania and will then be used at a cash point in Spain. This provides additional difficulties for police investigations and consequently for refunding money to the account owner [4].

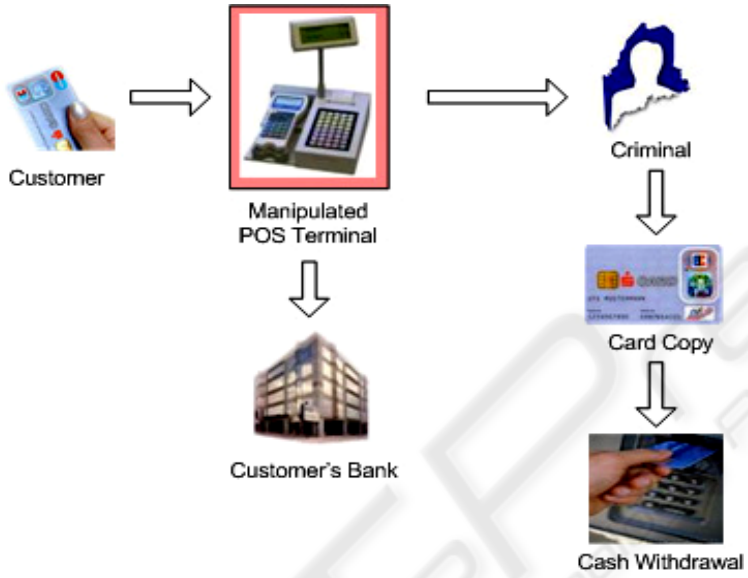

Fig. 1. Card misuse schema.

In addition to the technical security problems of debit cards [5], the main problem is the payment protocol itself. Once known, card data allows endless amounts of payments or cash withdrawals until the card is blocked. Also, TAN usage for payments at the POS would not necessarily bring success because of missing customer acceptance.

Card payment procedure has to meet the following **security requirements**:

- authentication of customer and merchant;
- authorization of payment request;
- integrity and
- confidentiality of payment information (e.g. sum, date and target account);
- availability and
- reliability of payment service.

Application of electronic signatures instead of handwritten ones may enhance existing payment practices to meet the authentication, authorization, integrity and confidentiality requirements. Mobile versions of electronic signatures will facilitate the service availability and an appropriate service design and implementation – the service reliability. To be equated to handwritten signatures, electronic signatures have to meet the legal requirements of the countries in which they are applied. In Europe, legally binding signatures have to be qualified as defined in the European Directive[6]. This implies the use of a smart card as Secure Signature Creation

Device. The most widespread smart cards are the SIM[2] cards already used in mobile phones, which bring the next advantage of signature usage without additional investment in special hardware. Suitability of these mobile smart cards for qualified electronic signatures was argued in [7].

In this paper we suggest mobile service for signature secured payment at the POS. In the next section we discuss related works in mobile payment development. Section 3 presents the service architecture and mobile service specific architecture parts. In sections 4 and 5 we propose the subscription and payment protocols for developed payment architecture. In the last sections we analyze the possible vulnerabilities of the proposed protocols and conclude our presentation.

2 Related Works

Advantages of mobile phone use for payment handling – mobile payment - have engaged mobile commerce research and development very intensely. Numerous mobile payment research and development projects as well as driving initiatives have not achieved hoped-for results: mobile payment transaction volumes have been leaving more to be desired.

A very good classification of mobile payment services is given in [8]. The key distinguishing characteristic of these services is the significant role of an intermediary – it can be a Mobile Network Operator (MNO), a financial institute or a specialized mobile payment provider. [9] presents a generic mobile payment workflow between the customer, merchant, payment service provider and trusted third party (TTP), shown in Figure 2.

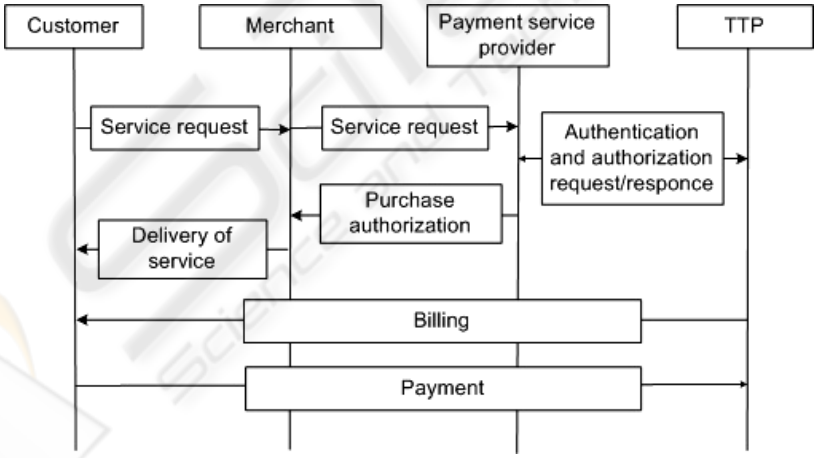

Fig. 2. Mobile payment workflow [9].

In this mobile payment schema, the purchase operation takes place after a circuitous interaction procedure. Our payment schema takes this a step further while

[2] SIM – Subscription Identification Module

only requiring a substitution for one step of the existing payment practice – card usage authorization. However we consider the research results in the mobile payment area as relevant to our work, especially in regard to questions of market acceptance and development trends.

3 Payment Handling at a Point-of-sale with Mobile Signatures

We propose the following payment schema. A customer paying with a debit or credit card has to authorize card usage with his/her signature. The POS terminal reads the card data as usual from a card magnet stripe or integrated chip and generates an electronic receipt. This receipt will be sent to the mobile device of the customer, who signs this receipt on his/her mobile device and sends it back to the POS terminal. The POS terminal verifies the signature and confirms the payment according to payment protocol described in the section 5. Then the signed electronic receipt will be forwarded to the customer bank, which handles it under the terms of its own security policy.

The payment handling described above implies signature service architecture, presented in Figure 3, which consists of the following interacting parts:

- Mobile Signature Application (MSA) on mobile device
- POS terminal application
- Financial Institute (e.g. credit card institute, bank)
- Mobile Signature Service Provider (MSSP)

Fig. 3. Mobile signature service for payment handling at a point-of-sale.

We will discuss the functionality of Mobile Signature Application and MSS Provider in more detail.

3.1 Mobile Signature Application

The core of the MSA is a **cryptographic module** consisting of a Cryptographic Engine (**CryptoEngine**) on the smartcard (SIM or UICC[3]) integrated in the mobile device and a CryptoEngine Interface on the mobile device itself. The **CryptoEngine** provides following cryptographic functions:

- key generation and storing
- signer authentication
- signature calculation

[3] UICC - Universal Integrated Circuit Card

The **CryptoEngine Interface** provides access for additional application components to the cryptographic functions on the smart card. The hash value calculation operation should also be outsourced to the CryptoEngine Interface because of the resource constraints of smart cards. The secret key, stored in smart card memory, can only be accessed via the CryptoEngine after a successful user authentication.

These main components interact with the "outside world" via a set of interfaces: the user interface, the communication module, and the service provider interface. The **User interface** displays the electronic receipt and signature request received from the POS terminal, converts the electronic receipt to an appropriate format for the CryptoEngine, and provides for dialog between the CryptoEngine and user, e.g. signer authentication characteristic input: - PIN and/or biometric authentication. The **Communication module** supports interconnection with the POS terminal according to the hardware facilities of the mobile device and communication protocol.

3.2 Mobile Signature Service Provider

Mobile signatures can be applied not only for payment authorization, but also for Mobile Brokerage [10] or remote enterprise network access [11]. In most cases collaboration with an MSSP is required. Commonly, the MSSP as an intermediary institution offers the following functions: data to be signed and signed data converting, communication interposition and signature verification, as well as access to certificate lists and application component download. For the use case described in this paper, the MSSP acts as a cooperation partner for the other interacting player:

- *Financial institutes* request signature verification from the MSSP for the electronically signed checks they've received
- *Merchants* would require technical and organizational support from the MSSP to offer mobile signature based payment;
- *Customers* subscribe to this service either at the MSSP directly or at the dialer, where they will be eventually redirected to the MSSP cooperating with the merchant to get required software for their mobile devices.

This constellation requires a reliable unified design of interaction workflows. We specify these workflows as service subscription and payment protocols described in the next sections.

4 Service Subscription

Mobile signature service can be offered for a certain special use case or can be shared with other electronic services, e.g. Mobile Banking or E-Government. In both cases service subscription requires a more complex way of service invocation as well as service component distribution and installation. We suggest the following schema shown in Figure 4.

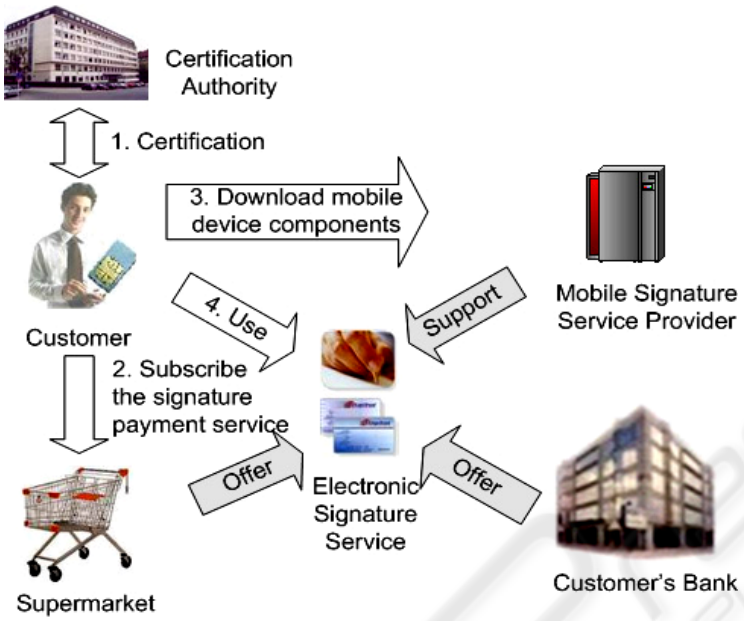

Fig. 4. Signature service subscription.

A user U has an account at a bank B and is accustomed to doing his/her shopping at a certain supermarket chain A, which supports the usage of electronic signatures at their POSs for payments with the debit cards of B. U decides to subscribe this service. The core signature components CryptoEngine and CryptoEngine Interface are already pre-installed on his/her smart phone by an MNO. Using UMTS, U decides to fulfill the service subscription via the mobile device. If U has never used mobile signatures before, at first he/she has to get a signature certificate according to a certification protocol, for example, as described in [7]. Next U goes to the web site of the supermarket chain A and transmits his/her signature certificate. A proofs the certificate via the MSSP and signs it with its own secret key. This signed certificate will be stored on the mobile device and will serve as the *authorization record for U* for further communication with the POSs of A. Then the web site redirects U to an appropriate MSSP, where U can download the needed application components for his/her mobile device. After successful installation, U can sign his/her checks at the POSs of A.

In our service subscription schema we place merchant A as the contact partner for the service subscriber, though it may seem to be more preferable to subscribe to signature service at the bank – the card issuer. However, we consider the presented succession as more effective because of the higher involvement of the merchant in the payment service support.

5 Payment Protocol

The payment protocol describes communication rules and operations between the customer's mobile device and the POS terminal. The protocol operates with following objects:

- PlainRcpt: data to be signed;
- SignedRcpt: signed data;
- SubsrAuth: authorizing characteristic assigned to the customer after service subscription;
- NoRepl: negative answer;
- YesRepl: positive answer;
- SrvRefuse: the payment service will be refused;
- PosPK: public key (PK) of key pair used by the POS terminal.

These objects are used by protocol functions:

- Send(): send message;
- ENCR(): encrypt message with recipient's public key;
- GetSign(): requests signature;
- SendSign(): signature reply;
- GetAuth(): request for service subscriber characteristic;
- SendAuth(): send service subscriber characteristic;
- ProveCert(): prove whether customer's certificate corresponds to the authorization record.

The prerequisite for communication via payment protocol is the successful connection establishment between a POS terminal and a mobile device. The selection of communication carrier (Bluetooth, WLAN, NFC, GSM/UMTS or Infrared) defines, eventually, additional requirements for communication security, e.g. data integrity and confidentiality as well as sender authorization. We suggest Near Field Communication (NFC) [12] as the communication carrier. The NFC provides up to a 424 kBit/s transfer rate at 13.56 MHz within the range of some centimetres. To enable communication, the mobile device should be placed directly next to the POS terminal. In this case, communication data interception and manipulation is almost impossible, and sender authorization will be fulfilled visually by both the customer and the POS terminal operator themselves. This is especially important for the public key exchange procedure. Additionally we assume that secret keys (SKs) of all payment participants are stored securely and can not be shared with a potential attacker.

The positive payment operation has following workflow. After the input of customer card data, POS terminal T has to prove whether mobile device M is allowed to use mobile electronic signatures for card payment by the merchant. After a successful customer authorization, T sends its PK to M, generates the receipt, encrypts it with customer's PK and sends it to M, which decrypts it with own SK stored on the SIM card and displays the received receipt. Then the customer proves the receipts visually on his/her M, whether the card data and payment sum are correct, and signs the electronic receipt. If the signature calculation was successful, M sends the signed receipt back to T. The back communication is also secured by encryption with the PK of T. T encrypts the signed receipt with its SK and then with the PK of M. If the encryption result and original receipt are identical, the payment will be accepted. Then the receipt will be encrypted again and stored at T or transmitted to the merchant's central terminal for continued processing.

Figure 5 presents the full protocol workflow including negative operation variations.

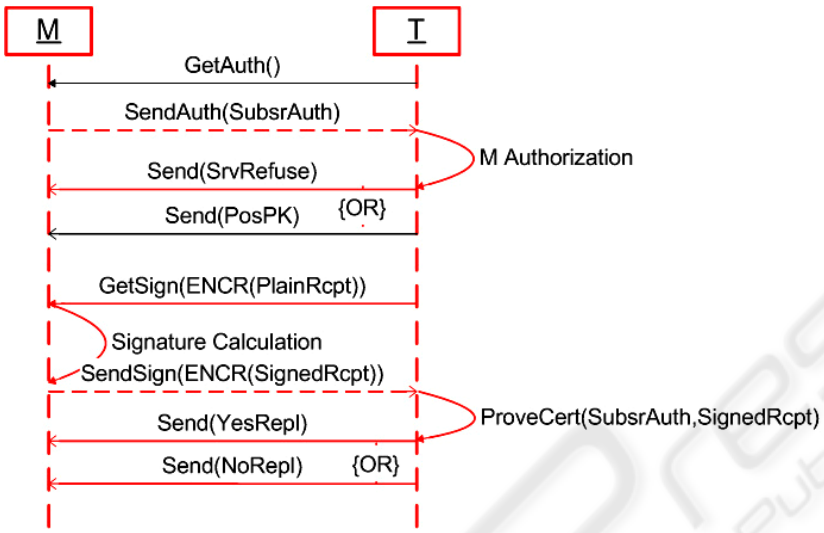

Fig. 5. Payment protocol.

6 Vulnerability Analysis

In this section we present potential attacks on the proposed payment service which are aimed at breach of payment confidentiality, authorization or integrity. Possible vulnerability points of the payment service are the subscription and payment procedures. For our analysis we use following notations:

- Attacker A;
- Customer C;
- Payment service provider P;
- SK_X, PK_X : key pair assigned to each participant;
- $Receipt$: electronic receipt to be signed
- $SK_X(Receipt)$: signed receipt,
- $SK_P(PK_C)$: authorization record, generated for the C during subscription by the P.

Attack scenario 1. A succeeded to get a copy of authorization message $SK_P(PK_C)$, generated for a C by payment service provider P, and stores it on his/her mobile device. At POS of P the A authorizes with this message and then signs the receipt with his/her SK_A. P tries to decode $SK_A(Receipt)$ with PK_C, fails and does not accept payment.

Attack scenario 2. *A* succeeded to get the mobile device of the *C*, containing the authorization message $SK_P(PK_C)$. However the access to signature application and to SK_C on the mobile device is protected via PIN, password or biometric authentication. Therefore *A* can not use the mobile device for payment.

Attack scenario 3. *A* manipulates POS terminal application so the application sends all payment data to *A*. Since the receipt transmission and storing are secured via public key encryption, the interception will not break data confidentiality. This break would only succeed if the interception were to occur during the signature prove operation when the POS terminal processes plain payment data. However the interception will not archive its main goal – receipt manipulation. Also if *A* gets the payment data, he will no be able to change the receipt to get it accepted.

Our analysis shows that the proposed payment architecture and supporting protocols guarantee the payment information integrity that makes customer account misuse impossible. The problem of payment confidentiality that will not be provided for by the proposed payment protocol in its existing form can be solved by an additional operation: after successful authorization, the POS terminal sends a dummy message to the mobile device and asks for a signature; so the POS terminal will get $SK_A(dummy)$ or $SK_C(dummy)$, which it will decrypt with PK_C. This redundant authorization operation may reduce the risk of confidentiality break, but will increase payment processing time.

7 Conclusion and Further Work

SIM-based mobile qualified signatures offer promising features for securing card payments. Payment authorization, always controlled by a customer, and guaranty of payment information integrity may reduce number of debit card frauds significantly. Additionally, the advantages of mobile services - operational availability, flexibility and usability – can stimulate usage of electronic signatures for payment operations. For the suggested service architecture and protocols presented in this paper, we showed integration possibilities for existing payment and mobile infrastructures.

This paper discussed security advantages of the proposed architecture. In our future work we intend to address economic implications of the presented payment architecture. This will cover questions of key parties' interests and implementation possibilities.

References

1. Kartengestützte Zahlungssysteme im Einzelhandel – Jahreserhebung 2005 des Euro-Handelsinstituts, EHI (2005)
2. Lubasi V.: Debit card competition: signature versus pin. In: Chicago Fed Letter, Issue December. Federal Reserve Bank of Chicago (2005). http://www.chicagofed.org/publications/fedletter/cfldecember2005_221.pdf
3. Polizeiliche Kriminalstatistik 2005. Bundeskriminalamt, Kriminalistisches Institut (2005). http://www.bka.de/pks/pks2005/index2.html
4. EC-Karte: Betrüger lauern an der Ladenkasse. http://www.daserste.de/plusminus/beitrag_dyn~uid,taia8kb6z9kn3oda~cm.asp
5. Anderson, R., Bond, M., Murdoch, S.J.: Chip and Spin: Examining the technology behind the "Chip and PIN" initiative (2006). http://www.chipandspin.co.uk/
6. Directive 1999/93/Ec Of The European Parliament And Of The Council of 13 December 1999 on a Community framework for electronic signatures, European Union (1999)
7. Rossnagel, H.: Mobile Qualified Electronic Signatures and Certification on Demand. In: Proceedings of the 1st European PKI Workshop - Research and Applications, LNCS 3093, Springer (2004)
8. Kreyer, N., Pousttchi, K., Turowski, K.: Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce. In: Proceedings of the Third International Conference on E-Commerce and Web Technologies, LNCS, Vol. 2455, Springer (2002)
9. Nambiar, S., Lu, C.T.: M-Payment Solutions and M-Commerce Fraud Management. In: Hu, W.-Ch et al (eds), Advances in Security and Payment Methods for Mobile Commerce, pp. 192-213, Idea Group, Inc. (2005)
10. Muntermann, J., Rossnagel, H., Rannenberg, K.: Mobile Brokerage Infrastructures - Capabilities and Security Requirements. In: Proceedings of the 13th European Conference on Information Systems (ECIS 2005)
11. European IST Project 'Wireless Trust for Mobile Business' (WiTness) (2004)
12. NFC Forum. http://www.nfc-forum.org/home