

The Technology of Identification and Authentication of Financial Transactions. From Smart Cards to NFC-Terminals.

Sergiy Golovashych, Ph.D.

"Kharkov National University of Radioelectronics", Kharkov city, Ukraine, sgolov@gmail.com,
<http://www.kture.kharkov.ua>

Abstract - In this paper it is performed the comparative characteristics of modern technologies of authentication on the basis of smart cards. There are underlined disadvantages of each considered technology. There is offered the scheme of dynamic authentication, which allows correcting the main disadvantages. Also it is introduced NFC-technology as basis for future systems of authentication, which provide the maximal user security from «abusing on the part of the system».

Keywords – Information Security, Cryptography, Authentication, Smart Card, Near Field Communication (NFC).

I. INTRODUCTION

In modern conditions of intensive automation and computerization of various fields of activity of the society, a necessary condition of construction of viable financial and economic information systems is application of adequate means of information safety. One of the basic requirements showed to financial information systems is maintenance of the control of integrity of the information processed in system, at all stages of its life cycle. The information system can be considered as safe if means used in it and technologies of protection of the information allow preventing or finding out attempts of unauthorized access on the part of any potential malefactor.

For today, the payment (and other information) systems subjects identification and authentication technologies on the basis of plastic cards have received a wide circulation all over the world; however, lots of technologies used today do not meet modern safety requirements any more. Thus last statement is correct even with the reference to the most progressive *smart-technologies* [1].

The purpose of this note is to analyse disadvantages (Achilles' heel) of today technologies of identification and authentication on the basis of smart cards, to define insecure moments and to offer the ways of its protection. We'll concentrate our attention on payment card's systems, as the most attractive object of IT-swindle, however everything described in this article can be applicable to any field where used smart cards identification and authentication systems. Questions of maintenance of confidentiality of the data stored on cards will not be considered in detail since this problem is not so complicated, compare to authentication, and has solutions that satisfy today requirements [2,3].

II. TWO TYPES OF TRANSACTIONS

Now, in payment systems on the basis of plastic cards two basic types of transactions can be supported: *on-line* and *off-line*.

The systems focused on support of only *on-line* transactions assume presence of a constant communication channel between the financial terminal and the issuing bank's server. In this case the protocol of authorization is carried out on the bank server and the sanction to end transaction is also given out by the bank server. Such decision is the most safe (for bank), however shows rigid requirements to quality and reliability of used communication channel. On the other hand, in such systems quite simple terminal equipment and cards with a magnetic strip can be used.

The systems providing support of *off-line* transactions do not require constant communication channel between the financial terminal and the issuing bank servers. In this case protocol of authorization is executed directly on the terminal. Such solution potentially is less safe, however it is more preferable from the point of view of users service efficiency and reduction of an overhead costs for performance of separate transaction. Therefore the support of *off-line* transactions is a necessary condition for construction of modern system of electronic payments. However for realization of such system application of smart cards and more complex terminal equipment is necessary.

III. SYMBOLS

Let's consider the technologies maintaining the integrity control used in both types of systems.

For simplification of the further statement we shall use the following designations:

X – the data stored on a card (and subjects of authentication);

P – personal identification number (PIN) of a card;

I_i – the unique identifier of the system subject;

E_i – a private key of a digital signature algorithm (signing key);

D_i – a public key of a digital signature algorithm (verifying key);

C_i – the certificate of a public key D_i (a public key

signed by the trusted side);

S_i – the digital signature generated on key E_i ;

The basic transformations we shall designate as follows:

$H()$ – the one-way function of hashing;

$F_k()$ – symmetric ciphering on a key k ;

$S_i()$ – formation of the digital signature on the private key E_i ;

$E_i()$ – formation of the digital signature S_i (or certificate C_j of a public key D_i) on the private key E_i ;

$D_i()$ – check of digital signature S_i on the public key D_i (or check of certificate C_j integrity and extraction of the key D_j from it);

(P)RNG – the (pseudo-) random numbers generator.

General structure of the certificate:

$$C_j = E_i(X_j) \quad C_j = \{F_k(X_j) \parallel S_i\} \quad S_i = S_i(X_j)$$

where the key k of symmetric ciphering F_k is fixed (at static authentication) or is formed under the scheme of Diffie-Hellman class (at dynamic authentication).

The subjects of the system we shall designate with the help of the following indexes:

p – a processing center;

e – a cards' issuing bank;

c – a user (a card).

IV. TYPES OF CARD AUTHENTICATION PROTOCOLS

There are two types of card's authentication: static and dynamic.

Static authentication assumes the one-sided control of integrity – only the terminal equipment checks the integrity of a card. In this case cards with a magnetic strip can be used.

Dynamic authentication assumes the two-sided control of integrity – not only the terminal equipment checks integrity of a card, but also the card checks authenticity of the terminal. In this case the basis of cards should be the microprocessor equipped with internal memory and capable to carry out cryptographic transformations. Such cards have received the name of smart cards.

Let's consider both ways of authentication.

V. STATIC AUTHENTICATION

The basis of static authentication in *on-line* systems (and also intrabank (one issuer) *off-line* systems) can be the symmetric crypto algorithms. However, the construction of global (multi-issuer) system of electronic payments with support of *off-line* transactions needs application of asymmetric crypto algorithms to the digital signature. We shall consider more in detail only the second variant of the

static authentication by virtue of its availability.

Asymmetric static authentication

The issuing bank forms a pair of keys of the digital signature: private (E_e) and public (D_e). The private key is kept secret, and the public key is located in payment terminals.

During personification of cards the constant data is stored on them: the number of a card, the term of its action, the information about the owner and possibly other confidential information. In a binary kind, concatenation of this data represents some binary vector X (Fig. 1).

For given vector X and the card owner's PIN-code P , the issuer, with the help of the own private key E_e , evaluates the digital signature of the card $S_c = E_e(H(X \parallel P))$ which is authentication value of the given card. This value is also stored on a card.

At service of the card in a payment point the terminal, having received value X and S_c from the card, carries out the check of the digital signature of issuing bank $D_e(S_c, H(X \parallel P))$. Only if the digital signature is true, the card is considered authentic and is accepted to service.

The advantage of such authentication is its simplicity, and the disadvantage is the complexity of multi-issuer payment systems creation, as public keys of all issuing banks should "know" all payment terminals. Even if it is possible to provide it, at occurrence of the new issuer there are significant difficulties in dispatch of its public key to all terminals. Besides the key of the issuer in this scheme is not certified and that weakens it a little.

Other scheme of static authentication (a Fig. 1) eliminates the last disadvantage, but complicates the protocol a little.

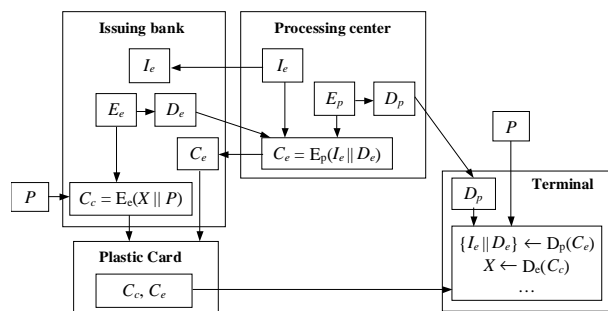


Fig. 1. The static authentication with the certification of the issuer's public key.

The given authentication scheme allows to create multi-issuer payment systems. Each emitter creates the pair of keys (E_e , D_e). Public keys D_e are transferred to the processing center for certification. The processing center

allocates for each issuer identifier I_e which concatenates with a public key of the corresponding issuer, and then the key and the identifier are signed with a private key of the processing center $C_e = E_p(I_e \parallel D_e)$.

The calculated certificate C_e is transferred to the issuer. At personification of cards the issuer signs the data X of given card concatenated with owner's PIN-code P , by means of the private key E_e and then the calculated digital signature of the card S_c places on the card together with the certificate C_e of the public key D_e .

The processing center supplies all terminals with the self public key.

At service of a card the terminal with the help of a public key of the processing center receives the issuer identifier and its public key $\{I_e \parallel D_e\} \leftarrow D_p(C_e)$. Then with the help of the public key of the issuer D_e it checks the digital signature of the issuer $D_e(S_c) = ? = 1$. If the digital signature is true, the terminal accepts the card to service, and otherwise it rejects the card.

Advantages

In the given scheme each of the sides (the issuer, the processing center, the terminal) knows only public keys of other sides. Only owners know self private keys. This property defines the advantages of the given scheme over the systems with symmetric authentication:

1. The possibility of multi-issuer systems construction.
2. The simplicity of addition of new issuers and introduction of new terminal equipment.

Disadvantages:

1. The possibility of the card duplicate creation or unauthorized «repeated transfer» (repeated transaction).
2. The absence of the user protection from the persons serving the terminal equipment abusing.
3. The absence of the user protection from the bank employees abusing.

Reliability of the considered scheme can be increased, if the successfully completed transaction includes the digital signature of the terminal to the information on the executed transaction (subject to sending in bank-assuror).

VI. DYNAMIC AUTHENTICATION

Dynamic authentication increases stability of the protocol of data exchange between the terminal and a card. Dynamic authentication can be based as on symmetric, so asymmetric crypto algorithms. It assumes, that the card possesses a high order of "intelligence". In particular, the card should be able to carry out enciphering with the help of symmetric crypto algorithm and/or to form and check

the digital signature.

The essence of the dynamic authentication is that not only the terminal checks the payment card integrity, but also the user's card can check up the authenticity of the terminal.

A. Symmetric dynamic authentication

In a Fig. 2 and the Fig. 3, are represented schemes of so-called external and internal authentications. In these schemes two cards participate in the protocol of the authentication: the user card and so-called the *master card*. The master card is constantly in the terminal and can be physically inaccessible from the outside.

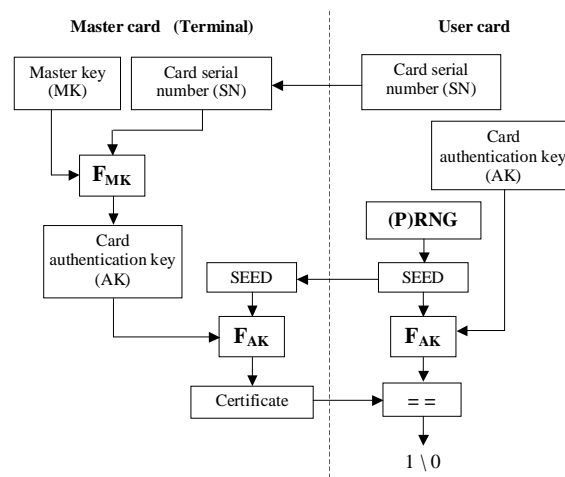


Fig. 2. External authentication. The user card checks the authenticity of the terminal.

The master key, which is inaccessible from the external world, is stored in this card and gets on it at personification. Usually for external and internal authentications various master keys are used.

In the given protocol of the dynamic authentication (a Fig. 2 and the Fig. 3) in the messages exchange between the user card and the terminal is in evidence parameter SEED, which represents random (or pseudo-random) number of necessary length. It allows to make the attack to the protocol, based on listening of a line with the purpose of repeated transfer of reciprocal packages, inefficient as in each session this value will be another. Thus the basic requirement to the parameter SEED is the absence of recurrences in the set ranges of manipulations, therefore for formation of such values the simple pseudo-random number generator (PRNG) constructed on the base of a "counter" can be used.

The given protocol assumes, that the user card "is able" just to cipher according to some symmetric algorithm.

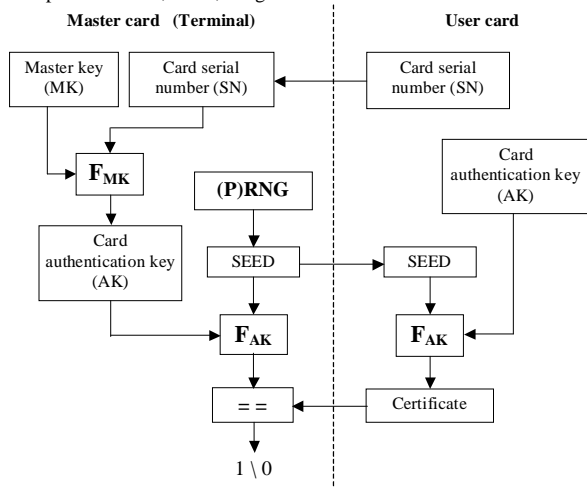


Fig. 3. Internal authentication. The terminal checks the authenticity of the user card.

Advantages:

1. The impossibility (high technological complexity) of the card duplicate creation.
2. The protection against abusing on the part of the personnel serving the terminal equipment.
3. The simplicity and low cost of realization.

Disadvantages:

1. The impossibility of multi-issuer systems construction.
2. The absence of the user protection from abusing on the part of bank employees.

B. Asymmetric dynamic authentication

The cards working on the basis of given protocols (a Fig. 2, a Fig. 3) can be classified as cards of average complexity. The cards of the supreme complexity "are able" to carry out not only symmetric enciphering but also to form / to check the digital signature (and also to carry out the directed enciphering or the key-agreement protocol), i.e. support asymmetric cryptography.

Among similar smart cards the cards, containing hardware random-number generators (RNG), are of considerable interest, since on the basis of such cards it is possible to construct systems with minimal «level of trust» among subjects of the system. For this purpose it is necessary that formation of *all* private keys in the system was carried out by a principle «everyone to itself», i.e. the private key of any card should be formed inside a card and never violate its bounds. For support of the given functionality the card should be able to form a key pair $\{E_j, D_j\}$ (for schemes of ElGamal class this task uses the same mathematics, as procedures of forming / checking of the digital signature, therefore does not demand additional hardware expenses). We shall consider the most

perspective scheme of the authentication subsystem based on the last type smart cards.

The recommended scheme of the dynamic authentication on the basis of smart cards of the second type is given in a Fig. 4.

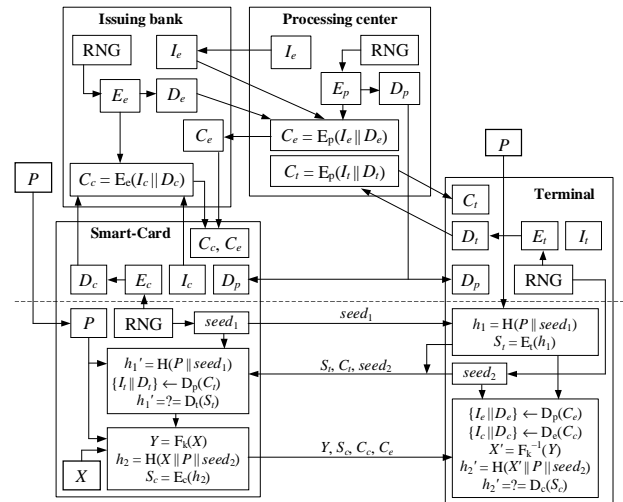


Fig. 4. The scheme of the dynamic authentication on the basis of the cards, supporting the digital signature

In the given figure a dashed line separates the initialization procedure of elements composing the system and authentication procedure of separate transaction. We shall consider each of procedures in detail.

At a stage of system initialization the processing center, responsible for the system support, carries out an initial insertion of both the user cards, and terminal master cards, during which both the unique identifier of a card (I_c or I_t) and a public key of the digital signature check of the processing center D_p are stored in cards.

At the connection of the new issuing bank to the system the processing center appropriates the unique identifier I_e to it and carries out the certification of its signature public key D_e . The corresponding private key E_e is formed by the issuer and does not appear outside of its bounds.

At the addition of a new user to the system, the issuing bank carries out the personification of the user card, during which: the necessary information on the user is stored in the card memory, the information on the owner and the issuing bank is placed on the surface of a plastic card. Then at the special stand the user enters his PIN-code P and initiates the calculation of the card's key pair $\{E_c, D_c\}$, which is formed with the help of built-in random-number generator RNG and is kept in the protected memory of the card together with the PIN-code P . After that the public key of the card D_c will be certified (signed) by the issuing bank private key E_e and as the certificate C_c , together with

the issuer public key certificate C_e is stored in the non-volatile card memory. On it the protocol of the card personification comes to the end.

The forming, certification and loading of the certificate for a terminal card is carried out in similar way.

The cards authentication procedure in the terminal is based on the three-stage protocol:

1. The user card forms a random vector $seed_1$ and transfers it to the terminal.

2. The terminal prompts the card owner PIN-code, combine it with the received vector $seed_1$ and evaluates digital signature S_t from hashing-function h_1 of the combined value on the own private key E_t .

3. The terminal forms a random vector $seed_2$ and together with the evaluated digital signature S_t and the certificate of the own public key C_t , sends it to the user card.

4. The user card takes a public key of the terminal D_t from the certificate C_t and, in case of its integrity, checks the signature S_t generated by the terminal. If the signature is true, the card "considers" the terminal original and passes to the following stage of authentication; otherwise the procedure of authentication interrupts.

5. The user card combine the vector $seed_2$ received from the terminal with the data on the user X stored in the card and the user PIN-code P and evaluates the digital signature S_c from hashing-function h_2 of the combined value by the own private key E_c .

6. The evaluated digital signature S_c together with the certificates of public keys of card C_c and the issuer C_e , and also with the data on user X is transferred to the terminal (data X are transferred in ciphered kind Y ; for encrypting either symmetric algorithm F and a key k , produced under the scheme of Diffie-Hellman class, can be used or the directed encrypting).

7. The terminal extracts from the received certificates first the issuer public key D_e , and then the card public key D_c . If both certificates are authentic, the terminal deciphers the received data X and checks the digital signature of the card S_c . If the signature is true, the terminal "considers" the card original and jumps to the performance of transaction, otherwise the authentication protocol interrupts.

Advantages:

1. The impossibility (high technological complexity) of the card duplicate creation.
2. The user protection against abusing on the part of the personnel serving the terminal equipment.
3. The user protection against abusing on the part of bank employees.
4. An opportunity of arbitration in case of disputed

situations.

Disadvantages:

1. The necessity of application of the specialized (relatively expensive) chips for smart cards.
2. The PIN-code gets in a card through the terminal, which can "be modified" by the malefactor. Besides all the controlling information necessary for the transaction execution is entered and is displayed by means of the terminal. So it can be forged before the transfer on a card.

The given disadvantage is typical for all smart card authentication schemes.

All the considered card technologies of authentication can be realized both on the basis of contact smart cards, and on the basis of non-contact ones. Thus last variant is more preferable, since reduces the card deterioration i.e. promotes the increase of the average term of its service. Besides the use of non-contact communications technologies opens additional prospects of safety increase. We shall consider them more in detail.

VII. USE OF NFC-MOBILE TERMINALS

The last considered disadvantage is an «incurable defect» of the card payment systems since finally the user (the owner of a card) all the same should "trust" the terminal. This disadvantage can be eliminated only in case of the ability to manage a smart card from the user «personal terminal», i.e. such terminal should be equipped with the device of input (the keyboard is desirable) and the device of display. It is natural, that such requirement is practically unrealizable for smart cards. However this requirement is automatically met if a mobile phone, a smart phone or PDA, equipped with Near Field Communication (NFC) means are used as "smart card" (means of identification and authentication). In this case the PIN-code and also the information necessary for transaction initialization gets directly in the *personal* mobile terminal and cannot be compromised or modified. Moreover the absence of electric contact between the terminal and the device of authentication raises the security of the last since the card cannot be damaged by influences of not supported voltage, or other distortion in the interface of an access point.

Last considered scheme (fig. 4) can be used for construction of the reliable protocol of (mutual) dynamic authentication. The only difference from the specified scheme will be absence of necessity to use the PIN-code for the performance of first two steps of authentication, since the PIN-code check is carried out at a stage when the mobile terminal is switched on (or the corresponding

VIII. CONCLUSIONS

Apparently from the considered material, the unique scheme, which allows to secure both the bank from abusing on the user-side and the user from threats of abusing on the part of bank operating personnel and employees, is *asymmetric dynamic authentication with "self-dependent" forming of a card's private keys*. All other considered schemes assume the presence in the bank of all the information, necessary for performing correct authentication of any transaction on the part of the client. I.e. such system allows to secure only the bank from abusing on the part of the client, however it does not secure the client from ill-intentioned actions on the part of the bank. Thus the purpose of ill-intentioned actions aimed at the client can be as the plunder of funds as the discrediting of his name. This fault is especially essential to big clients, because the cost of the damage caused to them "pays back" the "overhead charges".

The possibility to use the personal NFC-terminals [4] for performance of "absolutely secure" transactions deserves especial attention, since in this case the client of the payment system (generally the subscriber of any system of authentication) is as much as possible protected from abusing on the part of the system servicing personnel. In case of personal NFC-terminals use the necessary level of trust to the system from the part of the user is minimal. The unique trusted subject of the system is the processing center forming certificates of the first level. Besides, the integration of functions of identification and authentication, and also functions of electronic commerce in one mobile phone (smart-phone) or PDA, equipped with the function of NFC-access, considerably simplifies and raises the convenience of performance of various payment operations

by the end user. It is connected, first of all, with the ability to perform any payment operations and operations of identification from one device, i.e. there is no need to carry a set of payment cards and certificates for various payment systems and systems of access restriction, and accordingly to remember lots of various PIN-codes or passwords. *The increase of convenience and safety of electronic payments (and identification) systems use due to the integration of the specified functions in one device allows to increase the number of consumers of corresponding services considerably.*

For today all necessary hardware components necessary for realization of the considered systems of «high security» are available on the market. However certain "blank" is observed in the field of the end-user systems satisfying the requirement of "*the maximal user security from the system*". Therefore the realization of similar systems is especially perspective direction today.

The basic advantage of last from the considered schemes is the ability to submit the electronic documents supported by the digital signature to the court (in the states, which have legislatively fixed the electronic documents validity and the digital signature law).

REFERENCES

- [1] Wolfgang Rankl, Wolfgang Effing. Smart Card Handbook. Hardcover 2 Ed edition. John Wiley & Sons, 2000.
- [2] FIPS PUB 201, Federal Information Processing Standards Publication. Personal Identity Verification (PIV) of Federal Employees and Contractors, 2005. http://www.smartcardalliance.org/pdf/industry_info/FIPS_201_022505.pdf
- [3] Government Smart Card Handbook. U.S. General Services Administration, 2004. http://www.smartcardalliance.org/pdf/industry_info/smartcardhandbook.pdf
- [4] NFC Forum. <http://www.nfc-forum.org/home>