E-PAYMENT SECURITY
Recommendations about the use of a PKI for e-payment security

El Bakkali Hanan
Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes, Rabat, Morocco

Keywords: Electronic Payment, Security, Authentication, Electronic Signature, Certificates, PKI, trust model.

Abstract: The security of the electronic payment requires not only the deployment of cryptographic technologies such as encoding and the electronic signature, but above all, the existence of third parties of confidence whose role is to enable the users of electronic payment applications to have confidence in the use of these technologies. In general, Authorities of Certification belonging to the same infrastructure of management and publication of public keys, commonly called Public Key Infrastructure or PKI, can ensure the role of these third parties of confidence. In this paper, first of all, I will pass in review the various methods of electronic payment. Then, the requirements of the participants of these methods will be presented. Finally, I will introduce some elements of response to the question on which this paper is focused: "Which PKI for the electronic payment security". Indeed, I will present my recommendations concerning both the desirable qualities and the characteristics of such a PKI, namely, the nature of its entities, its trust model and the format of its certificates.

1 INTRODUCTION

No one is unaware of that we start a new era: the era of new information technologies, where Internet occupies an increasing important place, not only in the traditional field of research and teaching, but also in the artistic, medical, media field and lately in that of the businesses and the commerce. This type of commerce via Internet, known under the name of e-commerce, facilitates the access of the customer to the information and the products which are adapted to him, and gives to the companies which adopt it an important competitive advantage and, thanks to its universal aspect, an opening to other markets judged until there inaccessible.

The electronic payment is the most critical part in the deployment of e-commerce. It often requires the authentication of all the parts implied in the payment transaction, the integrity of the exchanged data, the privacy of these data or, at least, the financial or personal ones and, finally, the non-repudiation. The electronic signature, based on public key cryptography, seems being the suitable means to answer these requirements, in particular, the need for authentication. However, without a global and efficient infrastructure for the public keys management and publication, the use of the electronic signature remains vain, even foolish. Indeed, even with the use of reliable cryptographic protocols which are based on electronic signature, the mutual authentication of a transaction actors assumes that each one of them is convinced of the authenticity of the binding between the other actor and its public key. The last requirement is precisely ensured by this type of infrastructure, commonly called Public Keys Infrastructure (PKI), whose role is to allow to the users of e-commerce applications to have `trust' in the use of cryptographic technologies and, particularly, that of the electronic signature. A PKI uses for assuming its role the public keys certificates which make it possible to bind a key to its owner. These certificates are generally signed by certification authorities (CAs) of trust that are the PKI key components. Convinced of the necessity of a PKI for electronic payment security purposes, I will try in this paper to bring some answers to the crucial question: "Which type of PKI is adapted to the needs for electronic payment securisation?". The first section of this paper points out the various methods of electronic payment according to the used payment instrument. The second section is devoted to the requirements of the users of these methods. In the third and last section, I will present my recommendations concerning desirable qualities in a PKI for the electronic payment (PKIEP); then, I will

Hanan Bakkali E. (2004).
E-PAYMENT SECURITY - Recommendations about the use of a PKI for e-payment security.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 317-323
DOI: 10.5220/0001396803170323

translate these qualities of a general nature into terms of some characteristics suggested for this PKIEP.

2 E- PAYMENT METHODS

The electronic payment has the same actors as the conventional payment; thus, it has at least a payer and a paid. Particular financial intermediaries (banks, credit card operators, compensation systems, etc) can intervene according to the used payment instrument. The computerized infrastructure connecting these intermediaries is already set up on a worldwide scale. The e-payment contribution lies in the computerization of the relation between the paid, the payer and the financial universe in general. The figure1 shows the general architecture of an electronic payment system (O'Mahony, 1997) with the various transactions between its participants. The issuer is an organization (in general, the payer bank) which issues to the payer a valid instrument of e-payment whereas the acquirer is an organization (in general, the paid bank) that the paid has charged with checking the validity of the instrument of payment used by the payer at the time of the payment transaction and, then, to credit its account with the transaction amount. The methods of e-payment are generally classified according to the payment instrument on which they are based. Nowadays, we distinguish three types of instruments, which are all inspired by conventional payment means: electronic cheque, electronic money and credit card.

2.1 Payment with e-cheque

An electronic cheque (e-cheque) must contain an instruction addressed to the payer bank to carry out a payment of a specific amount to an identified paid. The fundamental difference with its paper counterpart is that this instruction is in an electronic form and is conveyed via telecommunications networks as Internet. The e-cheque must contain the electronic signature of the issuer as well as a paper cheque contains its handwritten signature. Indeed, in both cases, the signature ensures the paid about the payer identity.
In addition, an e-cheque, contrary to a paper cheque which is supposed to circulate only between few `hands', is brought to cross an open network where the information it contains can be intercepted and misused by bad intentioned people. For this reason, the e-cheque has to be encrypted before being transmitted.
Lastly, the e-cheque is an electronic instrument of payment which is intended to be the equivalent of the paper cheque in the electronic commerce, while decreasing the risks of fraud, the time of transaction and the the cheque handling costs. However, even if it has these advantages as well as indisputable others, its expansion can be made only if there is a global PKI implying a growing number of banks and thus facilitating the use of the electronic signature all over the world. In the absence of this PKI, the solutions implying the e-cheque will have an 'owner' character and thus, their use will be limited as it is the case of NetCheck (Netcheck, 2003).

2.2 Payment with e-cash

E-cash is money under electronic form. It is thus represented by numerical data, which must inform about the value of the electronic money in question and the issuing organization (for checking and money recovery by the paid) and if possible preserve the anonymity of the payer. Like its counterpart in the conventional world, the e-cash must also allow the checking of its authenticity. This authenticity is proven thanks to the electronic signature of its issuer.
The problem which is particular with the e-cash and which is not posed with the ordinary cash is the risk of the sending of the same e-cash on several occasions to carry out different payments (double spending). Some systems of payment by e-cash try to resolve this problem by conserving, in the issuer databases, the coins already used, as well as the association of an expiration date to each coin in order to prevent that these databases do not become too bulky. Other systems are based on the resistance of the chip cards (electronic purse) towards faking attempts to guarantee the use, no more than one time, of the coins stored on this support.
At first sight, the e-cash presents many advantages, in particular, for the micro-payments. However, its practical use remains prone to many challenges. Indeed, unless being satisfied with solutions whose extent is very limited as it was the case of E-cash of Digicash (this solution knew an unhappy failure four years ago), the future of e-cash resides, on the one hand, in vulgarizing the chip cards use in order to proceed in an off-line way without fearing the problem of double spending and, on the other hand, in the adhesion of the e-cash

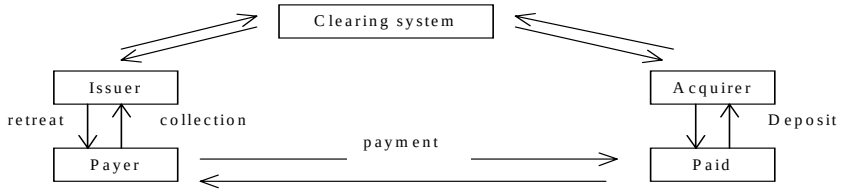

Figure1: Payement system architecture

issuers (generally banks) in a global PKI and this, in order to enable paids to check the issuers signatures by using their certificates and then to be sure about the e-cash authenticity before even the deposit transaction.

2.3 Payment with credit card

In U.S.A and Europe, credit cards are very much used like means of payment, not only for the proximity purchases (great surfaces, hotels and so on), but also for shopping by telephone or via Internet. Indeed, and before even the 'fury' for the e-commerce, credit cards were already used for the payment via the telephone which was used for the transmission of the credit card number and its expiration date, from the cardholder to the merchant. This established fact allows credit cards to become the first means of payment on Internet.
However, in this case and contrary to the conventional one, the payment validation is based only on the credit card number and its expiration date and not on the card itself. Moreover, in absence of a receipt signed by the payer, the paid cannot check if he is the legitimate cardholder. In addition, the payer does not have really any insurance as for the paid identity and also he risks that its credit card number will be intercepted and perhaps misused by an intruder.
It is for these reasons that encryption and electronic signature mechanisms and then certificates are used massively in e-payment methods by credit card. They must ensure the privacy of critical information, the integrity of the transactions, as well as the authentication of the payer, the paid and any other implied part such as a third organization which play the role of the intermediary between the paid and the financial organizations (credit card operator, acquirer & issuer) to carry out the payment authorization and the money deposit in his account, and between the payer and the paid to ensure the privacy of the transaction and the mutual authentication of the two parts.
Credit cards are certainly, at the present time, the favorite means of payment on Internet but that does not prevent that many among the Net surfers still hesitate to cross the step by giving their credit card number to a 'virtual' and completely unknown merchant (especially for the first time). Moreover, many are the countries (as mine) in which the citizens do not have the possibility yet of paying by credit card on Internet because of the not-convertibility of their national currency. For the hesitant ones, the encoding of the credit card number before its sending to the merchant via Internet (as it is possible by using SSL (Freir, 1996)) is far from being sufficient, because if that protects them from the intruders, it does not do the same vis-à-vis the merchant. In this connection, the implication of an intermediate organization of trust makes it possible to ensure the payer for the credibility of the merchant. However, the not-disclosure of the credit card number to the merchant remains always more reassuring. The protocol SET (MasterCard, 1997) that was developed jointly by visa and MasterCard with other partners precisely makes it possible to avoid this disclosure. However, SET supposes the existence of a hierarchical PKI for the certificates management, necessary to the authentication of the paid, the payment gateway (third part of trust) and the payer, which is currently different for each solution of e-payment based on SET.

3 E-PAYMENT REQUIREMENTS

The electronic payment can take a true take-off only if the used methods fulfill the requirements of the various actors. Admittedly, the criteria to be satisfied can vary from a method to another and from an actor to another. Nevertheless, three essential criteria make the unanimity of all the actors, that are: security, conviviality and universality of the payment process.

3.1 Security

Security is the most paramount criterion of a method of e-payment. This security is not however supposed to exceed that usually assured by the conventional payment methods. Indeed, the payment security is not synonymous with impossibility of frauds or conflicts between actors. This criterion of security cannot be filled by a method of e-payment only if it ensures the following points:
-Authentication: It is the process that allows the identity checking of an actor by another. As we've seen, each part implied in a payment transaction (except sometimes the payer) must be able to be authenticated in a sure way by the others. For example, a purchaser must be sure about the merchant identity before the payment transaction.

- Authentication of the instrument of payment: The payment instrument himself must be conceived in such way that the parts concerned can check its validity. As we saw that in the case of a payment by e-cash, the paid must ensure itself of the authenticity of the electronic coins, which he receives, from the payer and this by checking the issuer signature.
-Privacy: The information contained in the transactions of an e-payment method in particular the payment transaction must remain confidential and only readable by its recipient(s). For example, the credit card number must be illegible except for the part(s) which must know it to make succeed the payment transaction.
- Integrity: it makes it possible to prove to the actors of an e-payment method that the information contained in a transactions is authentic in the sense that it was not modified by unauthorized thirds.
- Non-repudiation: It allows to protect the payer against the possible refusal from the paid to deliver the actually paid goods/services and this, while denying to have received the corresponding payment transaction. It also permits to protect the paid against false complaints from the payer.

3.2 Conviviality

A method of e-payment must be easy to use and also to implement particularly on the level of the payer. The response times must be acceptable especially for the on-line methods. It should be noted here that the conviviality of the payment process does not go hand in hand with its security. However, it is necessary that a payment method overcome these problems by finding a compromise between the two so that the satisfaction of the actors requirements as for the payment security does not block the method conviviality.

3.3 Universality

Internet being universal, a method of payment via Internet which can be adopted only by one restricted community on the level of the payers or of the paids, does not offer to the latter all the copetitive advantages of the e-commerce. The e-payment method 'quality' is also measured by the possibility of its adoption by general public.

4 WHICH PKI FOR THE E-PAYMENT (PKIEP)?

The description of the various methods of e- payment as well as the requirements of the actors of these methods, which we have just seen in the preceding sections, show that a global PKI is essential to ensure the security of the electronic transactions between these actors who can a priori not have any pre-established relation between them and even to belong to different legislations. In this connection, we notice that more and more governments become aware of the importance of such a PKI for the e-commerce deployment. The government of Canada is, on this level, pioneer in the implementation of a PKI which aims at satisfying the security requirements of the electronic service of the federal services but also to emphasize Canadian industry on a leader position in the increasingly popular field of the e-commerce (The Government of Canada PKI, 2004). Asia on its side has a forum for the promotion of PKIs and the e-commerce which is called Asia PKI Forum (Asia PKI Forum, 2002). The first forum took place in June 2001 in Tokyo and he knew the participation in more of Japan of many Asian countries like Malaysia and Indonesia. In this paper, I anticipate a little while thinking of qualities and characteristics of a global PKI for the electronic payment (PKIEP) and which would be, I hope that, probably the fruit of such forums.

4.1 Recommended qualities in PKIEP

I present in what follows the qualities that I recommend in this PKI for e- payment PKIEP:
- Global: PKIEP must be able to provide its services to the potential users of e-commerce applications, namely, the community of Net surfers, the companies which are presents (or will become so) on the Web as well as governments, banks, credit card operators, etc.
-Extensible: More the Net surfers number increases more the potential users number of the e-commerce applications increases too. It is thus obvious that PKIEP must be extensible in order to follow the growing number of its users and their corresponding certificates.
- Flexible: PKI basic technologies are various and can moreover know important changes and improvements in the future. PKIEP should not depend closely on technologies which it uses. It must be, on the contrary, flexible in such way that can be adapted to new technologies as they appear.
- Universal: if PKIEP will be 'born', the developed countries will be the countries most implied in its creation. Nevertheless, from its global nature, several governments and organizations with high international notoriety and operating in financial and communications security fields must take part in its development and, once created, participate in its management and maintenance.
-General: A PKI of this scale and inevitably implying a heavy investment on behalf of several participants should not be limited to only one type of use. The various e-payment applications must be concerned as like as those of other e-commerce applications.

-Of trust: CAs of PKIEP must enjoy of notoriety near the end-users. Indeed, the governments implication is more than desirable. Also, it is necessary that the certificate policies of CAs be available to the certificates verifiers so that they can judge of the confidence degree which they will assign to the certificates issued by these CAs. On this subject, it is very useful that these policies are written in a formal way in order to allow an easy and non-ambiguous reading.
- Feasible & convivial: It should not be so much 'perfect' at the point to become impracticable. It should not be forgotten that e-commerce is not supposed being surer than traditional commerce. Moreover, if the e-payment applications must become less convivial to be able to use the PKIEP services, the users naturally will turn aside from these applications.
These qualities are obviously both general and informal; they show, however, the great difficulty of the undertaking task to create this PKI and even the practical impossibility of this task. I believe, in spite of that, that while proceeding in a progressive way this PKIEP-dream can become a reality, especially if there is behind a real determination and if the tendency towards the commerce globalization and the fury towards the e-commerce applications continue.

4.2 Recommendations concerning the PKIEP characteristics

In this section, it is a question of presenting my recommendations concerning the PKIEP characteristics for which I discussed above the general 'qualities'. The PKIEP characteristics, that I consider here, relate to its certificates format, its trust model and its entities.

4.2.1 Certificates format

To remain in conformity with qualities of universality and globality of the PKIEP, there should preferably have one format for the certificates. However, this format must be flexible enough to contain the various types of certificates, that is to say, identity and authorization certificates.
X.509 V3 format (Housley, 1999) could be the format used in PKIEP provided that it undergoes certain improvements. Among those, I suggest that the 'name' field becomes more general in the way that it will contain information not identifying the certificate subject, for example, a nickname (Clarke, 2001).
Moreover, one extension -to be standardized- should be reserved for the attributes, roles or privileges of the certificate subject. Indeed, it is sometimes useless to know the payer identity, but what it is, on the other hand, necessary, it is to know some ones of its attributes. I notice besides that the majority of the individual/payers prefer to keep their anonymity at least with respect to the paid.
At this level, to minimize the risks of frauds, I propose that only the CA, which certifies the payer, takes note of its identity at the time of its first registration. This CA issues then an attributes certificate to him -after checking their attributes-which comprises a 'Nickname' that it will associate to its true identity and this, for example, in a confidential document that the payer should sign. Among the attributes which could be useful to individual/payer, I propose the followings: age, nationality, profession, police record, existence of a valid account for e-cheques, e-cash or credit card, a hash of the account or credit card number, etc.
In addition, I prefer that the paid and the other actors be identified to avoid many frauds. However, I suggest also, for the paids/merchants certificates, that the extension reserved to the attributes contains information which can be useful for the payers, such as: Web site address, references, certifications, trading licence number, jurisdiction, sales turnover, etc.

4.2.2 Trust model and entities of PKIEP

Figure 2 shows the architecture of the trust model that I suggest for PKIEP. As it is illustrated through this figure, I suggest the existence of various types of entities, each one with different functions. Indeed, I make the distinction, on the one hand, as it is often the case in a PKI, between two categories of entities: end entities (EEs) and certification authorities (CAs) and, in addition, between various types of the same category:

a- EEs of PKIEP:

I suggest making the distinction between two kinds of EEs: on a side, the web surfers who will play the role of payers primarily and, more rarely, that of paids; and on the other side, merchants and companies present on the Web which will play the role of paids but also of payers (in the case of B to B).

b- Certification Authorities of PKIEP:

I insist here on the importance owing to the fact that all the CAs of PKIEP must be trustworthy and especially 'approved' by their corresponding governments. Indeed, it is not necessary that the users of e-payment methods, all over the world, be constrained to undergo the monopoly of a private company (like that it seems to be concretized with Verisign (Verisign, 2004)). In addition, I suggest that there are various types of CAs in PKIEP:
- PCAs (Policy Authorities Creation): are CAs ables (and authorizeds) to establish suitable certificates policies to various contexts of e-payment or e-commerce. As it is shown on the figure2, I propose that each country has at least one PCA under the supervision of the government that can be, in its turn, certified and

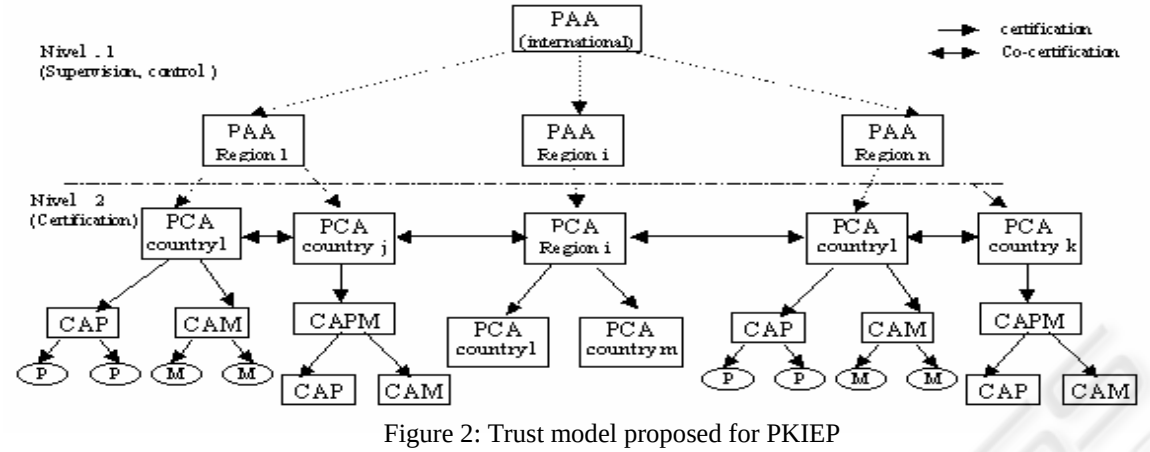

Figure 2: Trust model proposed for PKIEP

'supervised' by a higher level PCA, which would correspond to the 'economic' region of this country.
I encourage, here, co-certification between PCAs which the role is to certify CAs of their country and to check the respect by these CAs of the certificate policies.
- CAMs (CAs for Merchants): are CAs specialized in the certification of merchants and companies present on the Web and which want to adhere to PKIEP.
These CAMs must be equipped with means which enable them to check the attributes of one merchant (society), as those which I mentioned in (4.2.1).
I think that CAMs can be under the supervision of the Chamber of Commerce or the Commerce Ministries.
- CAPs (CAs for Private persons): are CAs which can certify only private persons who want to use applications of e-payment. These CAPs must have trust relationships with these private persons in the real world. The banking organizations are thus very suitable for this role especially that they are already equipped with technical skills in the field of security.
- CAPMs (CAs for Private persons and Merchants): are CAs which can play the role of CAMs and CAPs. These CAPMs can certify in their turn CAMs and CAPs if the number of merchants and private persons wanting to adhere to PKIEP would require it.
Lastly, I suggest that the PKIEP 'initiators' be under the responsibility of several governments, as being, for example, the members of a committee of the United Nations, the World Organization of the Trade or of the International Chamber of Commerce. This committee should start by creating an entity PAA (Policy Approval Authority) that will have, as an initial task, to work out the general directives concerning the PKIEP objectives and the roles of its various entities. Once the PKIEP created, this PAA should approve the certificate policies created by different PCAs, control the respect of these policies by these PCAs and finally supervise co-certifications between PCAs of various countries.
This 'world' PAA could delegate some of its functions to regional PAAs which would be more able to control PCAs of their region. It is advisable to specify here that the PAAs should not issues certificates, in order to avoid the problem having a Root-CA for all the world as well as the limitations raised in (Josang, 2000).

5 CONCLUSION

The e-payment methods are as diversified as the conventional ones. Nevertheless, their use is undeniably more limited and this, primarily because of the insecurity feeling which they inspire to a great number of users.
The security of e-payment methods is thus the key factor of their deployment. In this connection, the existence of a global PKI having precisely as objective, the security of these methods, would allow their expansion and, then, the takeoff of the e-commerce.
In this paper, I presented my recommendations concerning desirable qualities in such a PKI and a part of my vision as-to the nature of its entities, its trust model and the format of its certificates. I thus hope that these recommendations constitute a contribution, though modest, in the emerging of such a PKI.
Lastly, I currently work on other characteristics of this PKI, in particular its certificate policies.

REFERENCES

Clarke, R., 2001. The Fundamental Inadequacies of Conventional Public Key Infrastructure, In ECIS'01.

Freir, A., Karlton, P. and Kocher, P., 1996, The SSL Protocol version 3.0, Internet Draft.

Josang, A., Pedersen, I.G., and Povey, D., 2000, PKI Seeks a Trusting Relationship, in *ASISP 2000*.

Housley, R., Ford, W., and Solo, D., 1999, Internet PKI; Part I: X.509 Certificate and CRL Profile, IETF X.509 PKI (PKIX) Network Working Group, RFC2459.

MasterCard and Visa, *Secure Electronic Transaction (SET) Specifications book 1,2,3*, 1997.

O'Mahony, D., Peirce, M., and Tewari, H., 1997, *Electronic Payment Systems*, Artech House.

Asia PKI Forum, 2002, http://www.asia-pkiforum.org/

Netcheck, 2003, http://www.netcheck.com

The Government of Canada PKI, 2004, http://www.cse.dnd.ca/en/services/pki/pki.html

Verisign Server, 2004, http://www.verisign.com/