An e-payment Architecture Ensuring a High Level of Privacy Protection

Aude Plateaux[1,2], Patrick Lacharme[1], Vincent Coquet[2], Sylvain Vernois[1], Kumar Murty[3], and Christophe Rosenberger[1]

[1] ENSICAEN, 17 rue Claude Bloch, 14000 Caen, France
{aude.plateaux,patrick.lacharme,sylvain.vernois,
christophe.rosenberger}@ensicaen.fr
[2] BULL SAS, Avenue Jean Jaurès, 78340 Les Clayes-sous-Bois, France
vincent.coquet@bull.net
[3] Department of Mathematics, 40 St. George Street, Toronto, Canada
murty@math.toronto.edu

Abstract. Online shopping is becoming more and more interesting for clients because of the ease of use and the large choice of products. As a consequence, 2.3 billion online clients have been identified in 2011. This rapid increase was accompagnied by various frauds, including stolen smart cards or fraudulent repudiation. Several e-payment systems have been proposed to reduce these security threats and the 3D-Secure protocol is becoming a standard for the payment on the Internet. Nevertheless, this protocol has not been studied in-depth, particularly in terms of privacy. This paper proposes a detailed description and an analysis of the 3D-Secure protocol, through a new privacy-orienting model for e-payment architectures. Some improvements of 3D-Secure protocol, concerning the protection of banking information, are also presented. Then, this article presents and analyses a new online payment architecture centered on the privacy of individuals.

Keywords: Electronic payment, privacy and security.

1 Introduction

In recent years, e-commerce has considerably grown with the democratization of the Internet. Thus, online payments were adopted by 69% of Internet users in 2011. Fraud amount in e-payment has increased with the same regularity and become now a major concern for financial institutions and web clients [20]. Indeed, although the online payment only represents a small percentage of transactions, it concentrates, for instance, 40% of the amount of fraud in France and 54% in United Kingdom [23]. Clients and merchant websites are not always the only actors in the electronic payment architecture. In addition to the two banks, the security problem is sometimes modified by the introduction of another actor, the third-party cashiers, as Paypal or Amazon payment (called Cashier as a Service in [35]), but it is not the scope of this paper.

T. Zia et al. (Eds.): SecureComm 2013, LNICST 127, pp. 305–322, 2013.

Many directives are related to the security of online payments, as for instance, the European Directive 2000/31/EC on e-commerce security [13]. In the same way, the Directive on Payment Services, [14], provides an european wide single market for payments and a legal platform for SEPA (Single Euro Payment Area, [16]). The banking industry strategy is centered on identity spoofing and user authentication. The first protocol proposed to securize electronic transactions was SET (Secure Electronic Transactions, [32]). Standard e-payment protocols are later enhanced by an additional secret, sent by mobile phone, as for the 3D-Secure protocol [33] or an additional device as a CAP reader [25]. However, the results in terms of security of these responses are mitigated [28,18]. Moreover, if the SET protocol has been extensively studied by the academic literacy (for instance [27,8,9,10]), the 3D-Secure protocol is surprisingly overlooked, excepted in the security analysis of Murdoch and Anderson [28] and Pasupathinathan et al. [30] .

Security and authentication in e-business should not be strengthened to the detriment of users' privacy [26]. There are a lot of personal information involved in all steps of a payment on the Internet and these data should be protected. Principles of user centric architecture and *privacy by design* are more and more accepted by numerous organizations and actors of various areas. For example, the European Commision is more and more interested by the privacy protection. Thus, the principle of data minimization has been strengthened in 2010, requiring that the personal data disclosure should be limited to adequate, relevant and non-excessive data [15]. Another important aspect of user's privacy concerns the data sovereignty principle: the personal data belong to an individual, with a control and a consent on the use of data and their purposes. Finally, the data sensitivity principle applies personal data must be considered as sensitive and requires a decentralized structure for their storage. These principles should be applied to e-payment systems.

The e-payment development has strongly modified the traditional relationship between a bank and its clients. During these transactions, a large amount of user's personal information is requested and stored. It is therefore essential to focus on user privacy in online payments and services. Surprisingly, the e-payment industry does not seem concerned by privacy. PCI/DSS is a first step of payment industry into personal data protection [19]. However, this norm is mainly concerned by data security in payment systems. User's privacy protection has completely disappeared in e-payment protocols on the Internet by the transition from SET to 3D-Secure [28]. Some existing publications deal with e-payment protocol generally focused on the security of service providers and users without talking about the user's privacy. The aim of the proposed architecture is to meet all the requirements in terms of security and privacy protection.

Our Contribution. We propose a list of necessary requirements for security and privacy protection of users and merchants during online payments. Then, using these requirements, we analyze the level of privacy protection of the current 3D-Secure protocol and propose an improvement of the protocol in order to enhance some privacy criteria. Our main contribution is the proposition of an e-payment

architecture providing security for the actors and more privacy protection for the users and the service providers. The presented solution allows the users to make a purchase on the Internet, with the generation of an electronic bank cheque. More precisely, the proposed solution ensures the data minimization, sensitivity and sovereignty principles without disclosing any user's banking information.

Organization. The reminder of this paper is organized as follows: Actors of the system and the security and privacy requirements are presented in Section 2. In Section 3, a description of existing e-payment solutions are presented, with a detailed focus on the 3D-Secure protocol, as well as an improvement of this latter. Finally, the context and the new solution are proposed and explained in Section 4, then analyzed in Section 5.

2 Security and Privacy Requirements of e-payment Systems

Four actors are present in electronic payments: The **client** C wants to purchase an online service with a credit card, through the website of a **service provider** SP. These two actors have one payment provider: the **debit account bank** and **credit account bank**, called respectively in this paper *client's bank* and *SP bank*. In most of e-payment architectures, a fifth actor is involved, the trusted party as a third-party cashier or the Directory used in 3D-Secure. The role of this fifth actor is consequenlty various. However, the security analysis of the payment scheme is generally similar and allows to authenticate the banks. The proposed architecture is concentrated on the payment phase. Thus, in the case where the authentication and/or the registration with the SP is required, we assume it is properly conducted. The protocol should securely ensure that the client is debited and the SP is paid, but the SP does not need to know inadequate client's information.

Several personal data are involved during an online payment. These data must be protected against numerous threats. A list of these potential threats has been presented by Antoniou and Batten in [5]. These threats notably concern the information revealed by a client to the SP. In order to ensure the minimization principle, the personal information must be divided in different parts. Indeed, depending on the data owner, the information will be differently protected. However, the data sovereignty and data sensitivity principles must also be applied to any e-payment architecture. In the proposed approach, the personal information is divided in three parts:

1. The identity information Id includes the information allowing to know the client's identity, for instance, his/her name.
2. The order information OI includes the detailed basket and other data linked to the expected service, as the SP name. These data are known by the SP.
3. The banking information BI is, for instance, composed of client's bank name, the personal account number (PAN) or the cryptogram $CVX2$. These data are known by the client's bank. As an indication, it is necessary to take note that the PAN can also allow to identify a client.

A list of fifteen requirements R_i including all privacy principles, as well as the risks raised in the literature, is established. These requirements should be taken into account by the e-payment architectures:

- R_1: The **confidentiality of transactions** requires that each exchanged data must be encrypted in order to protect these data against external entities.
- R_2: The **integrity of transmitted information** allows the accuracy of the content and so the non-alteration of data during transmission or storage.
- R_3: The **confidentiality of client's identity towards the SP** ensures that a client can access to a service without disclosing his/her identity to the SP. This requirement is waived if the customer wants a home delivery service.
- R_4: The **confidentiality of client's identity towards the SP bank** ensures that a client can access to a service without disclosing his/her identity to the SP bank.
- R_5: The **client's authentication** by a trusted party ensures the identity of the client. Depending on the situation, the trusted party can ideally be the client's bank or another trusted party *where the client is registered*.
- R_6: The **SP authentication** by the client or by a trusted party ensures the identity of the SP.
- R_7: The **banks authentication** by a trusted party ensures the identity of SP bank and client's bank.
- R_8: The **non-reusability** of transmitted information (banking or other) allows to have unique and non-reusable transactions.
- R_9: The **confidentiality of order information** OI ensures that only authorized persons have access to order information. This requirement includes that the client's basket is unknown to the client's bank.
- R_{10}: The **confidentiality of banking information** BI (or client's data minimization principle) ensures that only authorized persons have access to banking data. This requirement includes the fact that the SP does not know the client's banking information.
- R_{11}: The **client's anonymity** is ensured if the requirements R_3, R_4, R_9 and R_{10} are fulfilled. Indeed, OI or BI partially allows to identify the client.
- R_{12}: The **SP's data minimization** principle includes the fact that the client does not know the SP bank. This condition is very important when the SP is a very small organisation, for instance one person. Indeed, in this case, the SP bank is the same bank than the manager's personal bank. Moreover, the SP's data minimization principle includes the requirement R_4. The SP bank does not need to know the client.
- R_{13}: The **data sovereignty** principle involves the uses of personal data associated to the client with his/her control and consent.
- R_{14}: The **data sensitivity** principle involves that the personal data are considered as sensitive and requires a de-centralized structure for data storage.
- R_{15}: The **ownership of a certificate** for the client **should not be required** in order to facilitate the e-payment. This last requirement concerns the usability of payment systems.

3 Existing e-payment Architectures

3.1 Introduction and Related Works

An online service generally begins with an authentication and a secure connection between the client and the SP website, using a protocol such as SSL/TLS [22,17]. This protocol involves the client trusting in the SP to keep this payment information and is aware of known published browser attacks [34,24,3]. However, the client can use a trusted partyner, such as Paypal. This service implies the creation of a Paypal account for the client and, consequently, a large amount of personal data is registered: name, email, address, PAN, $CVX2$ and expiration date. Then, the client can send and receive online payments without providing new data, through the Paypal platform. Nevertheless, although Paypal specifies *not sell or rent this information*, its privacy policy [31] adds it can *share some of your personal information with third parties* in the world. If the client does not use a trusted partyner, he/she must supply the SP bank, through the SP website, his/her banking information: PAN, $CVX2$ and expiration date. Client's banking information is so directly sent to the SP.

Several payment schemes have been recently proposed. For instance, a secure payment protocol managing different aspects such as smart card with network capabilities or the multiplicity of entities is proposed in [11]. However, these scenarios do not manage user's privacy. Antoniou and Batten are interested in enforcing trust in e-commerce systems [5]. They propose four models with four levels of privacy protection. However, these protocols are centered around one deliverer which knows all stakeholders of the process. Another scheme is suggested by Ashrafi and Ng in [6], by using a non-reusable password based authentication. The process ensures the client's privacy and minimizes the SP business risks. This protocol uses the card company with an optional payment gateway and has the same complexity as the 3D-Secure protocol. However, all the security is based on the card company which stores all the client's payment details in a local centered database.

The SET protocol [32] was developed by a consortium of credit card companies, such as VISA [1] and MasterCard [2], and software corporations. It is a protocol for securing e-payment transactions by credit card which runs in two steps: registration and purchase. This protocol ensures the data confidentiality and integrity and provides a mutual authentication between the SP and the client, through a trusted third party, the SP bank. This secure protocol has many advantages considering client's and SP privacy. The SP does not know the client's banking information. The client bank does not see the contents of the order. And finally, the client does not know the identity of the SP bank. However, in terms of client's privacy, the client does not necessarily trust the SP bank which authenticates him/her. Therefore, the SP bank knows the client's identity. In addition, although the client's bank does not know the contents of the client's order, it knows the SP identity. SET has been extensively analyzed in the begining of the 2000s and improved [8,7,21]. Thus, the client's consent to send his/her credit card details cannot be proved [9]. Moreover, this protocol is

complex from the client perspective and expensive for the SP. Indeed, a specific software must be installed by the client in order to prove card detention with an electronic signature. In addition, card readers and distribution of certificates by the SP are inevitable. Consequently, the successor of the SET protocol is the 3D-Secure protocol where the few parts concerning privacy of SET are simply deleted. The Fig.1 quickly analyses this protocol.

3.2 Description of the 3D-Secure Protocol

The 3D-Secure protocol [33] is the commonly used two-factors authentication system for e-payment, developed by VISA in 2001. Other financial organizations also developed their own implementations of VISA's 3D-Secure licensed architecture, such as MasterCard with its MasterCard SecureCode, American Express with SafeKey [30]. In order to use the 3D-Secure protocol, a dedicated module called MPI (Merchant Plug In) is implemented into the SP website. Moreover, a dedicated server (the Directory) is made available for this system. This scheme works as specified below (see Fig.4 in the Section Annexes):

A. The client sends to the SP his/her purchase intention, with his/her banking information: PAN, expiration date and $CVX2$.
B. MPI queries the Directory server with the VEReq (Verify Enrollment request) message.
C. The Directory server checks the SP identity, the card number and the client's bank. The Directory recovers the ACS (Access Control Server) managing the card and transfers the VEReq message. The PAN allows the Directory server to identify the ACS.
D. The ACS checks if the client's card is enrolled in the 3D-Secure program and sends the cardholder authentication URL to the MPI through the VERes (Verify Enrollment Result) message.
E. MPI sends the PAReq (Payer Authentication Request) message to the previous URL. This message contains the details of the authorized purchase and requests the ACS to authenticate the cardholder. The authentication protocol depends on the cardholder's bank.
F. The client provides the necessary information for authentication to the bank.
G. ACS sends to MPI a confirmation of client's authentication through PARes (Payer Authentication Responses) message.
H. MPI records PARes message as confirmation of client's authentication by ACS.
I. SP authenticates to the bank. The bank checks the nature of the transaction from the client's bank and confirms the payment authorization from the SP. The SP gets his/her payment and the client's bank stores payment information to ensure non-repudiation of the transaction.

The main security flaw of 3D-Secure implementations, underlined in [28], has been corrected by many banks. The client authentication with his/her date of birth or other trivial secrets is consequently replaced by an One Time Password

sent to user's mobile phone. As an indication, the complete payment phase is not described. Thus, the entire payment system using 3D-Secure protocol contains more than nine steps.

3.3 Privacy Analysis and Improvements of 3D-Secure

In a first step (step A), the client sends his/her banking information to the SP bank. However, this information can identify him/her. Consequently, the requirements R_3 and R_{10} can not be guaranteed. The requirements R_4 and R_{12} are also not respected given that the client's bank knows the SP identity and the SP bank knows the client's identity. Then, even if the client's authentication is realized by his/her bank, this authentication is also realized by the Directory server (step C). Consequently, R_5 is partially ensured. Similarly, the SP authentication is not realized by the client or by a client's trusted party (step C. and I.), and R_6 is not respected. In addition, the order information is contained in the $PAReq$ message sent to ACS (step E.), these data are consequently not confidential (R_9). Thus, the requirements R_3, R_4, R_9 and R_{10} are not ensured, the requirement of anonymity R_{11} cannot be respected. Finally, R_{13} is only partially respected. Indeed, the client has not total control over these data which passes through many entities. In addition, in terms of privacy, the sensitivity of exchanged information is not enough taken into account. Therefore, R_{14} is not ensured. The 3D-Secure protocol ensures therefore only six of the fifteen requirements. However, the privacy protection of 3D-Secure can easily be improved by using the SP bank certificate. Indeed, in the 3D-Secure protocol, *CVX2* and the expiration date are not necessary. These data are only used for the compatibility with classic existing payment systems. Thus, given that the client's authentication from his/her bank is strong, these two elements are unnecessary. The SP bank certificate contains the standard information, as well as the Directory public key. Only two steps must so be modified (the other seven steps are the same as above):

A. The SP **provides the SP bank certificate to the client**. Thus, the client sends to the SP his/her purchase intention, **with only his/her** PAN **encrypted by the Directory public key**. These data are intended for a dedicated module MPI implemented into the SP website.

C. The Directory server **decrypts the PAN with its private key** and checks the SP identity, the card number and the client's bank. The Directory recovers the ACS managing the card and transfers the VEReq message.

These small changes do not involve significant modifications in the 3D-Secure architecture. Moreover, these improvements involve none of the client's banking information is visible by the SP and thus ensure R_{10}. Indeed, through the SP bank certificate, the encryption of PAN is possible and use of *CVX2* is avoided. In addition, only relevant data and useful data pass through the Directory server. The requirement R_{14} can be taken into account, as well as R_5. Indeed, the client is only authenticated by his/her bank. The Fig.1 shows the increase of the privacy protection level thanks to these modifications.

R_i	**Properties**	**3D-Secure**	**3D-Secure Modified**	**SET**
R_1	Confidentiality of transactions	Yes	Yes	Yes
R_2	Integrity	Yes	Yes	Yes
R_3	Confidentiality of client's identity for SP	No	No	No
R_4	Confidentiality of client's identity for SP bank	No	No	No
R_5	*Client*'s authentication	Partial	**Yes**	No
R_6	SP authentication	No	No	No
R_7	Banks authentication	Yes	Yes	Partial
R_8	Non-reusability	Yes	Yes	No
R_9	Confidentiality of OI	No	No	Partial
R_{10}	Confidentiality of BI	No	**Yes**	Yes
R_{11}	*Client*'s anonymity	No	No	No
R_{12}	SP data minimization	No	No	No
R_{13}	Data sovereignty	No	No	Partial
R_{14}	Data sensitivity	No	**Partial**	Partial
R_{15}	Ownership of certificate not necessary	Yes	Yes	No

Fig. 1. Properties of the 3D-Secure protocols and comparison with SET

Nevertheless, this improved protocol does not fulfill all requirements described in Section 2. The minimization principle, specially R_9, is not respected. For example, the client's bank knows the purchases of the client or at least the merchant category. The bank is so able to deduce the purchases type. Consequently, the anonymity principle is not respected. Moreover, as often in the existing e-payment architectures, the fifth actor always takes place in the middle of the transaction, for instance, the Directory server in 3D-Secure or the card company in the Ashrafi and Ng's model [6]. Thus, the privacy is always exposed to an impossibility of complete protection.

4 The New e-payment Architecture

The proposed architecture combines the advantages of electronic cheque systems and easy-of-use of online payment systems described in Section 3.1. However, the architecture is not considered as an electronic cheque scheme [4] which are often difficult to use for the average user. Indeed, these systems lead to the use of client's certificate and an electronic checkbook card. Many computations and storages by the client's bank are also required, even if [12] proposes a small improvement. Finally, these schemes do not generally take into account privacy protection, excepted in [29].

Thus, our new architecture involves five actors: the client, the merchant SP, both banks and an additional entity, the interbank system IS. The goal of this interbank trusted third party is detailed later. Each bank generates a key pair, where the public key is certified by the IS. This latter publishes these certificates which contain the following: its name; its public key; the hash function

algorithm; the signature algorithm and the name of certification authority. Similarly, the SP has a key pair, where the public key is certified by the trusted third party contractualized with, for instance the interbank system. These certificates are composed by the following data: its name; its public key; the hash function algorithm; the signature algorithm; the name of certification authority and the parameters describing the payment scheme recognizing the SP and allowing to secure the future payment (American Express, VISA, MasterCard,..). In addition, as explained in the sequel, the new architecture allows the SP not to reveal the identity of its bank. Thus, in order to add privacy for the SP, the generation of the SP certificate by a trusted party different from the SP bank is preferable. For instance, the interbank trusted party could play this role.

Notations: The notations for the proposed e-payment protocol are:

- $Sign_X(m)$: Signature of message m by the actor X with message recovery;
- $[m]_{K_{PU_X}}$: Encryption of message m by the public key K_{PU} of the actors X;
- $[m]_{K_{S_X}}$: Encryption of message m by the session key K_S of the actors X;
- N_i: Random number i used to guarantee the freshness of messages;
- $H(m)$: Hashing of message m.

The online payment architecture respecting the users' privacy proposed in this article is based on the generation of two documents: a contract between the SP and the client, and another electronic bank document, called electronic bank cheque or cheque to simplify. As explained in the beginning of this section, this latter document is different from the cheque generated in the electronic cheque architecture. The interbank system IS plays the role of a trusted third party. It enables communication between banks without revealing information about the other actors. As explained in the following section, the fifth actor can not be excluded. However, IS has the smallest possible role for managing authentificaitons banks and prevent money laundering. The new solution is summarized in Fig.2. First, the client creates his/her basket and sends it to the SP with a random number N_1, as well as a session key K_{S_1} (Step 1). N_1 ensures the freshness of message and K_{S_1} encrypts data between the client and the SP. In the case where the client has a certificate, the session key is replaced by his/her public key.

$$Client \rightarrow SP : [Basket, N_1, K_{S_1}]_{K_{PU_{SP}}} \quad (1)$$

The SP then generates a contract with its client (Step 2), containing:

- The total amount $Amount$ of purchases;
- A random order number $Order$ generated by the SP. This number should not link to the SP identity;
- A symmetric random key K_{S_2} encrypted by the public key of the SP bank $K_{PU_{Bank_{SP}}}$;
- The beneficiary's name $Benef$ encrypted by the previous symmetric key K_{S_2};
- The URL of the SP in order to return to the payment page;
- The detailed shopping list $Basket$, such as quantity or unit price.

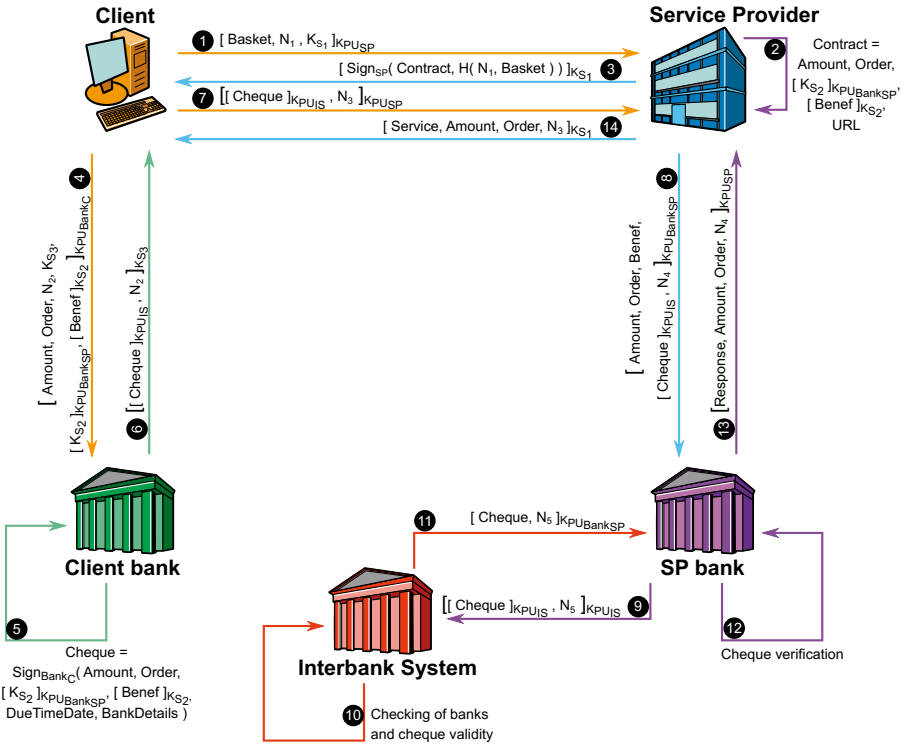

Fig. 2. The proposed e-payment architecture

$$SP : Contract = \{Amount, Order, [K_{S_2}]_{K_{PU_{Bank_{SP}}}}, [Benef]_{K_{S_2}}, URL, Basket\} \tag{2}$$

To avoid the non-repudiation and ensure the SP authenticity, the SP signs the contract. It is then sent to the client with the hash of $Basket$ and N_1 (Step 3).

$$Client \leftarrow SP : [Sign_{SP}(Contract, H(N_1, Basket))]_{K_{S_1}} \tag{3}$$

Then, the client connects to his/her bank, using a macro of its Internet browser (Step 4). The macro establishes the HTTPS connection and sends a filtered contract. The authentication protocol depends on the client's bank. But, a strong authentication is recommended. The filtered contract only contains the necessary information of the contract for the client's bank: the whole amount, the currency, the encrypted symmetric key, the encrypted beneficiary's name and the random order number. Thus, the client's bank does not know the SP identity. Moreover,

a random number N_2 ensures the freshness of messages. The client has no public key certificate, his/her bank will consequently use the session key K_{S_3} to encrypt the messages with his/her client. To encrypt the beneficiary's name, a session key is favoured in order to reduce the computation complexity.

$$Client \rightarrow Bank_C : [Amount, Order, [K_{S_2}]_{K_{PU_{Bank_{SP}}}}, [Benef]_{K_{S_2}}, N_2, K_{S_3}]_{K_{PU_{Bank_C}}} \quad (4)$$

Then, if the authentication is successful and the client is creditworthy, the bank positively responds to the client's request. The bank generates an electronic bank cheque to the SP (Step 5). This electronic cheque includes: the total; the currency; the random order number; the encrypted beneficiary's name; the encrypted symmetric key; the information of the client's bank and the signature of the client's bank. Thus, the cheque does not contain client's banking information.

$$Bank_C : Cheque = Sign_{Bank_C}(Amount, Order, [K_{S_2}]_{K_{PU_{Bank_{SP}}}}, [Benef]_{K_{S_2}}, DueTimeDate, BankDetails) \quad (5)$$

The client's bank signs the cheque and encrypts it with the interbank system public key. Thus, IS could check the banks identities and the cheque validity. The cheque is sent to the client (Step 6) who forwards it to SP (Step 7). N_2 and N_3 ensure the freshness of transactions. N_2 also gives the identity of the request. The result being encrypted, the SP cannot know client's banking information.

$$Client \leftarrow Bank_C : [[Cheque]_{K_{PU_{IS}}}, N_2]_{K_{S_3}} \quad (6)$$

$$Client \rightarrow SP : [[Cheque]_{K_{PU_{IS}}}, N_3]_{K_{PU_{SP}}} \quad (7)$$

Then, the SP obtains $[Cheque]_{K_{PU_{IS}}}$ and N_3 thanks to its private key. So, the SP authenticates to its bank (Step 8) and provides its filtered contract, the signed and encrypted electronic bank cheque. As previously, the authentication protocol depends of the SP bank. However, a strong authentication is recommended. The SP filtered contract contains: the whole amount, the currency, the beneficiary's name and the random number N_4.

$$SP \rightarrow Bank_{SP} : [Amount, Order, Benef, [Cheque]_{K_{PU_{IS}}}, N_4]_{K_{PU_{Bank_{SP}}}} \quad (8)$$

In order to validate the banks identities and the cheque, the SP bank authenticates to the interbank system and transfers the cheque (Step 9), using N_5 for the freshness of the transaction.

$$Bank_{SP} \rightarrow IS : [[Cheque]_{K_{PU_{IS}}}, N_5]_{K_{PU_{IS}}} \quad (9)$$

The interbank system checks the identity of the SP bank and decrypts the electronic cheque with its private key (Step 10). The validity of this cheque, its signature, and consequently the identity of the client's bank, are checked. Then, if the verifications are correct, the interbank system re-encrypts the cheque with the public key of the SP bank and the cheque is transferred to this bank (Step 11). N_5 is reused to identify the request.

$$Bank_{SP} \leftarrow IS : [Cheque, N_5]_{K_{PU_{Bank_{SP}}}} \tag{11}$$

The SP bank decrypts the cheque with its private key (Step 12). It firstly checks that the cheque amount and currency are similar to those provided by the SP in the filtered contract. Then, the bank decrypts the symmetric key with its private key. Thanks to this symmetric key, the SP bank decrypts the beneficiary's name. Afterwards, the bank compares the beneficiary's name of the filtered contract with the decrypted name of the electronic cheque. As indication, the verification of the client's bank signature by the SP bank is optionnal. Indeed, the interbank system has processed to this verification. The SP bank can use directly the client's bank information.

Finally, if one verification fails, the transaction is cancelled. However, if all verifications are correct, the SP bank contacts SP and validates the cheque as being authentic; that allows the SP to deliver service for its client (Step 13, 14). The random numbers N_3 and N_4 allow to identify the requests and to guarantee the freshness of transactions.

$$SP \leftarrow Bank_{SP} : [Response, Amount, Order, N_4]_{K_{PU_{SP}}} \tag{13}$$
$$Client \leftarrow SP : [Service, Amount, Order, N_3]_{K_{S_1}} \tag{14}$$

The SP bank also contacts the client's bank, located through the electronic cheque. The debit/credit process between banks completes this payment architecture in using the electronic cheque as payment proof.

5 Analysis of the Architecture

Most of security and privacy requirements are ensured by the first eight steps of the proposed architecture. Moreover, the proposed protocol has no more steps than 3D-Secure as the described steps of 3D-secure are not as detailed as our protocol. In addition, the last five steps allow to ensure the banks authentication by the interbank system (R_7) and so to avoid the money laundering.

5.1 Data Security and Authentication

The secure channel between actors and the encryption schemes ensure the confidentiality of exchanged data during the protocol. Consequently, the requirement R_1 is ensured. The use of random numbers garantees the freshness of messages, avoids the linkability and ensures the data integrity respecting R_2 and R_8. Entities authentication is realized through certificates, the first one for the SP and

the second one for each bank. Thus, contrary to the SET protocol, the trusted third party is not one of banks. The banks own certificates issued by IS. The SP certificate is provided by IS or another trusted autority. These documents allow to sign, encrypt and decrypt information and to prove the validity of the SP and banks. The interbank system manages the bank certificates and authenticates the SP bank and the client's bank. Moreover, IS checks information contained in the signed electronic cheque and gives a validation of cheque for the SP bank. The contract signed by the SP then allows client to obtain his/her service with indicated conditions. Finally, validation of the client's bank identity by IS and verification of transaction information by the SP bank ensure the SP to be paid once the service provided. Thus, the requirement R_7 can be ensured. Moreover, these verifications by IS also allow to avoid money laundering by malicious SP and malicious SP bank.

5.2 Privacy Analysis

The proposed architecture is more respectful of the users' privacy than the SET protocol and 3D-Secure protocol. The SP authentication by the client and then the SP bank, ensures the SP validity and the client does not provide personal order data as long as he/she is not certain to use a service. The requirement R_6 is thus respected. Moreover, the client's identity is never disclosed and the SP bank does not know the client. This authentication is realized by the client's bank. Thus, R_3, R_4 and R_5 are respectively ensured. More precisly, in order to respect the client's privacy during the transfer of data to different banks, the order number, used in Step (3), should not contain SP information, such as the business number. Consequently, it must be random or unidentifiable. As an indication, in the case where the two banks would be the same, all requirements would be preserved except that the bank could know the SP and the client. Moreover, the client's bank knows neither contents of the basket, nor the SP with whom his/her client deals. The requirement R_9 is consequently ensured. This new proposition also solves the other privacy problems of 3D-Secure protocol. The client's banking information is preserved against the SP ensuring the requirement R_{10}. The encrypted cheque with IS public key allows the SP not to have knowledge of the client's bank. Moreover, contrary to all the existing e-payment architecture, the client's banking information is never disclosed to the SP. Thus, the requirements R_3, R_4, R_9 and R_{10} are respected. Consequently, the client can be anonymous and the requirement R_{11} can be ensured. Finally, the cheque encrypted with IS public key prevents the client to know the SP's bank. Consequently, the protection of some SP personal information, representing the requirement R_{12} is also ensured by this protocol. This requirement is important when the SP is a small organisation and consequently, when the SP bank is the same bank than the manager's personal bank.

The most sensitive data of client and SP are protected. The requirement R_{14} is ensured and the client only provides the necessary, appropriate and relevant information (minimization and sensitivity principles). In addition, contrary to the existing protocol, the fifth part performs at the end of the architecture. Thus,

the privacy is not always exposed to an impossibility of complete protection. Once the SP has signed the contract, the client should click two times to accept it: one for the confirmation of his/her basket and one for the validation of the payment. Thus, the client has read two times the similar information. These two clicks are used to ensure the client's consent and, consequently R_{13}. These clicks could be replaced by a client's signature based on a certificate. In the future, the certificate will be possibly present in the client's identity card or his/her passport. Finally, the ownership of certificate by the client is not necessary (R_{15}), contrary to SET protocol. Figure 3 summarizes the analysis of the proposed architecture compared to the existing protocols 3D-Secure and SET protocol.

R_i	**Properties**	**3DS**	**SET**	**Our protocol**
R_1	Confidentiality of transactions	Yes	Yes	Yes
R_2	Integrity	Yes	Yes	Yes
R_3	Confidentiality of client's identity for SP	No	No	**Yes**
R_4	Confidentiality of client's identity for SP bank	No	No	**Yes**
R_5	C's authentication	Partial	No	**Yes**
R_6	SP authentication	No	No	**Yes**
R_7	Banks authentication	**Yes**	Partial	**Yes**
R_8	Non-reusability	**Yes**	No	**Yes**
R_9	Confidentiality of OI	No	Partial	**Yes**
R_{10}	Confidentiality of BI	No	**Yes**	**Yes**
R_{11}	C's anonymity	No	No	**Yes**
R_{12}	SP data minimization	No	No	**Yes**
R_{13}	Data sovereignty	No	Partial	**Yes**
R_{14}	Data sensitivity	No	Partial	**Yes**
R_{15}	Ownership of certificate not necessary	**Yes**	No	**Yes**

Fig. 3. Properties of the 3D-Secure, SET and the proposed protocols

6 Conclusion

A lot of sensitive information are transferred during current online payment transaction, introducing strong privacy problems. Current e-payment systems, such as 3D-Secure, are not designed to ensure user's privacy. Moreover, even if its proposed improvement is more respectful of the privacy, several underlined requirements are not ensured. The proposed architecture allows to overcome these weaknesses by respecting the client's privacy against the banks and the SP, as well as the SP privacy. This solution is mainly based on the generation of an electronic bank cheque associated with certificates.

This architecture is fully compliant with the data minimization, data sovereignty and data sensitivity principles. More particularly, the payment transaction never discloses any client's banking information. Moreover, the client does not need to have particular knowledge or cryptographic devices. The non-repudiation could be improved by supplying the client with a certificate.

Moreover, in order to prove the practicability of the proposed solution, a proof of concept and a statistical study are currently conducted (see Annexes).

Acknowledgment. The authors would like to thank Gabriel Frey and Arnaud Gouriou for their project concerning the implementation of our proof of concept, Roch Lescuyer for his proofreading, as well as the BULL company and the ANRT organization for their financial support.

References

1. Visa corporate (1958), `http://corporate.visa.com/index.shtml`
2. Mastercard worldwide (1966), `http://www.mastercard.com/`
3. Aciiçmez, O., Schindler, W., Koç, Ç.K.: Improving brumley and boneh timing attack on unprotected ssl implementations. In: Proceedings of the 12th ACM Conference on Computer and Communications Security, pp. 139–146. ACM (2005)
4. Anderson, M.: The electronic check architecture. In: Financial Services Technology Consortium (1998)
5. Antoniou, G., Batten, L.: E-commerce: protecting purchaser privacy to enforce trust. Electronic Commerce Research 11(4), 421–456 (2011)
6. Ashrafi, M.Z., Ng, S.K.: Enabling privacy-preserving e-payment processing. In: Haritsa, J.R., Kotagiri, R., Pudi, V. (eds.) DASFAA 2008. LNCS, vol. 4947, pp. 596–603. Springer, Heidelberg (2008)
7. Bella, G., Massacci, F., Paulson, L.: Verifying the SET purchase protocols. Journal of Automated Reasoning 36(1), 5–37 (2006)
8. Bella, G., Massacci, F., Paulson, L.C., Tramontano, P.: Formal verification of cardholder registration in SET. In: Cuppens, F., Deswarte, Y., Gollmann, D., Waidner, M. (eds.) ESORICS 2000. LNCS, vol. 1895, pp. 159–174. Springer, Heidelberg (2000)
9. Bella, G., Paulson, L., Massacci, F.: The verification of an industrial payment protocol: The set purchase phase. In: ACM CCS, pp. 12–20. ACM (2002)
10. Brlek, S., Hamadou, S., Mullins, J.: A flaw in the electronic commerce protocol set. Information Processing Letters 97(3), 104–108 (2006)
11. Carbonell, M., Torres, J., Izquierdo, A., Suarez, D.: New E-payment scenarios in an extended version of the traditional model. In: Gervasi, O., Murgante, B., Laganà, A., Taniar, D., Mun, Y., Gavrilova, M.L. (eds.) ICCSA 2008, Part II. LNCS, vol. 5073, pp. 514–525. Springer, Heidelberg (2008)
12. Chen, T.H., Yeh, S.C., Liao, K.C., Lee, W.B.: A practical and efficient electronic checkbook. Journal of Organizational Computing and Electronic Commerce 19(4), 285–293 (2009)
13. European Commission. Directive 2000/31/ec of the European parliament and of the council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('directive on electronic commerce') (2000)
14. European Commission. Directive 2007/64/ec of the European parliament and of the council of 13 November 2007 on payment services in the internal market amending directives 97/7/ec, 2002/65/ec, 2005/60/ec and 2006/48/ec and repealing directive 97/5/ec (2007)
15. European Commission. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions (2010)

16. European Payments Council. Sepa - single euro payment area (2007), http://www.sepafrance.fr/
17. Dierks, T.: Rfc 5246: The transport layer security (tls) protocol version 1.2 (2008)
18. Drimer, S., Murdoch, S.J., Anderson, R.: Optimised to fail: Card readers for online banking. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 184–200. Springer, Heidelberg (2009)
19. PCI DSS. Payment card industry data security standard (2006), https://www.pcisecuritystandards.org/
20. Espelid, Y., Netland, L.–H., Klingsheim, A.N., Hole, K.J.: A proof of concept attack against norwegian internet banking systems. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 197–201. Springer, Heidelberg (2008)
21. Fioravanti, A., Massacci, F.: How to model (and simplify) the set payment phase for automated verification (2001)
22. Freier, A., Kocher, P., Karlton, P.: Rfc 6101: The secure sockets layer (ssl) protocol version 3.0 (2011)
23. Frenkiel, M.: Cybercriminalité et crime organisé (2009), http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/24583/Cybercriminalite-et-crime-organise.aspx
24. Gabrilovich, E., Gontmakher, A.: The homograph attack. Communications of the ACM 45(2), 128 (2002)
25. MasterCard International. Chip authentication program functional architecture (September 2004)
26. Katsikas, S.K., López, J., Pernul, G.: Trust, privacy and security in E-business: Requirements and solutions. In: Bozanis, P., Houstis, E.N. (eds.) PCI 2005. LNCS, vol. 3746, pp. 548–558. Springer, Heidelberg (2005)
27. Meadows, C., Syverson, P.: A formal specification of requirements for payment transactions in the SET protocol. In: Hirschfeld, R. (ed.) FC 1998. LNCS, vol. 1465, pp. 122–140. Springer, Heidelberg (1998)
28. Murdoch, S.J., Anderson, R.: Verified by visa and masterCard secureCode: Or, how not to design authentication. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 336–342. Springer, Heidelberg (2010)
29. Pasupathinathan, V., Pieprzyk, J., Wang, H.: Privacy enhanced electronic cheque system. In: Seventh IEEE International Conference on E-Commerce Technology, CEC 2005, pp. 431–434. IEEE (2005)
30. Pasupathinathan, V., Pieprzyk, J., Wang, H., Cho, J.Y.: Formal analysis of card-based payment systems in mobile devices. In: The 2006 Australasian Workshops on Grid Computing and e-research, vol. 54, pp. 213–220. Australian Computer Society, Inc. (2006)
31. Paypal. Privacy policy for paypal services (2012)
32. S.E.T. Secure electronic transaction specification. Book 1: Business Description. Version, 1 (2002)
33. Visa. 3d secure protocol specification, core functions, July 16 (2002)
34. Wagner, D., Schneier, B.: Analysis of the ssl 3.0 protocol. In: The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 29–40 (1996)
35. Wang, R., Chen, S., Wang, X.F., Qadeer, S.: How to shop for free online security analysis of cashier-as-a-service based web stores. In: IEEE Symposium on Security and Privacy (S&P 2011) (2011)

Annexes

3D-Secure Protocol

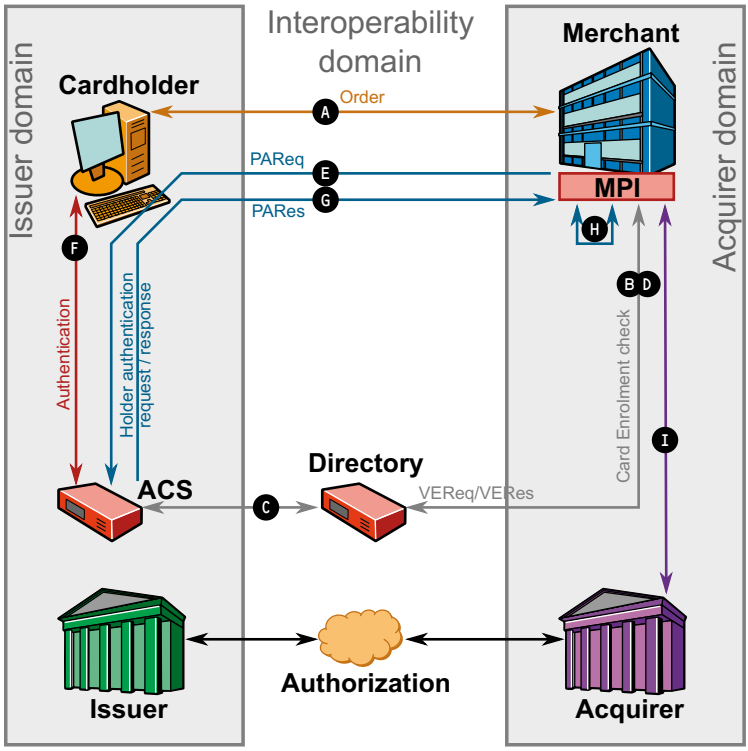

Fig. 4. The 3D-Secure protocol

Statistical Study

In order to justify the importance of the privacy protection issues during an online payment, a statistical study was conducted on a sample of 354 individuals. In particular, for the question "Are you concerned by the issues of privacy protection on the Internet?", 87% of responses are positive and 69% of individuals have apprehensions during this transaction.

Patent

There is a provisional application for patent cover sheet.

The docket number is 61/712616.

A U.S. patent deposit has been made with the patent number: US 04097.

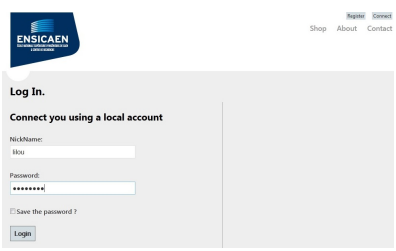

Fig. 5. After the registration of the client with only the storage of one pseudonym and one password, the client logs in to the SP

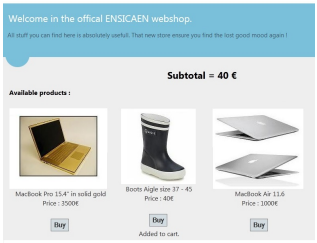

Fig. 6. The client fills his/her basket

Fig. 7. The recap chart is processed

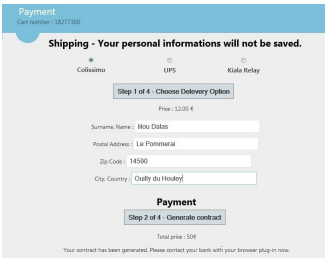

Fig. 8. The client chooses his/her delivery option and the contract is generated

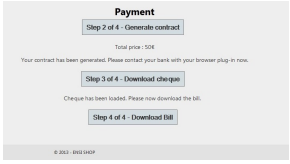

Fig. 9. After the contract uploaded and the cheque has been generated, the cheque is transmitted to the SP bank through the SP

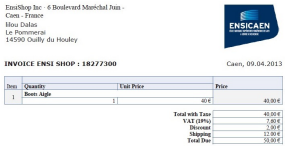

Fig. 10. The transaction is concluded and the bill is sent to the client

Perspectives

A proof of concept has been developed to demonstrate the feasibility of the proposed protocol. The Figures 5, 6, 7, 8, 9 and 10 provide an overview of the current implementation.