A Comparative Study of Card Not Present E-commerce Architectures with Card Schemes: What About Privacy?

A Plateaux, P Lacharme, S Vernois, V Coquet, Christophe Rosenberger

A Comparative Study of Card Not Present E-commerce Architectures with Card Schemes: What About Privacy?

A. Plateaux P. Lacharme S. Vernois V. Coquet

C.Rosenberger

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

christophe.rosenberger@ensicaen.fr

October 5, 2018

Abstract

Internet is increasingly used for card not present e-commerce architectures. Several protocols, such as 3D-Secure, have been proposed in the literature by Card schemes or academics. Even if some of them are deployed in real life, these solutions are not perfect considering data security and user's privacy. In this paper, we present a comparative study of existing solutions for card not present e-commerce solutions. We consider the main security and privacy trends of e-payment in order to make an objective comparison of existing solutions. This comparative study

illustrates the need to consider privacy in deployed e-commerce architectures. This has never been more urgent with the recent release of the new specifications of 3D-secure.

1 Introduction

E-commerce has developed significantly in recent years, with 1.4 billion of online shoppers are counted in the World in 2016 [1] for a total amount of transactions near 2.7 billions dollars. In 2016, the fraud amount in electronic payments increases with the same regularity. Today, it becomes an important preoccupation for both financial institutions and users, and a problem of trust between the different actors [25]. Despite the fact that personal data is exchanged with e-commerce websites during an online payment, the banking industry mainly focuses on identity spoofing and user authentication. The electronic transaction security should not be strengthened at the expense of privacy protection, and a consumer centric privacy system should ensure data privacy with a possible control by users over their personal information [36].

Four actors are necessarily involved in electronic payments during a *Card-Not-Present transaction*. The *client* (also called the cardholder) browses on the website of the merchant, called *service provider* (or SP), to buy an online service. These two actors have a payment provider, respectively called the issuer bank and the acquirer bank. Nevertheless, in most online payment schemes, other actors are involved. They are generally employed as trusted third party, with various roles. For example, it can be an interoperability system, such

as in 3D-Secure, or an identity provider operated by the banks themselves, such as the BankID system [20]. In addition, an authentication system for payment providers is required for fraud resistance but is generally not described in these protocols. Finally, alternative payment systems such as the three-party model PayPal are out-of-scope of this paper. Indeed, we focus in this paper on e-commerce architectures involving banks (representing a large proportion of e-payments).

During an online purchase (card not present transaction), the client sends various banking information such as the PAN (Primary Account Number), the expiry date of the card and the secure cryptogram $CVX2$ (Card Verification Value/Code). This online service generally uses a secure connection between the client and the SP website, using a protocol such as SSL/TLS, ensuring the confidentiality and the integrity of the transaction on the Internet. But, in the same time, neither the client's authentication, nor the confidentiality of the data, on the merchant and bank parts, is granted. In basic systems, the client authentication is realized with the knowledge of these banking information (particularly the CVX2), whereas with *advanced* systems, such as 3D-secure, the authentication is strengthened by an additional data (in complement to banking information), as described below. This additional data is generally an OTP sent by SMS on the mobile device of the user, even if the NIST has recently warned against this system for payments [29].

Historically, many architectures have been defined for client authentication during a Card-Not-Present transaction such as SET (Secure Electronic Trans-

actions [35]). SET is quickly replaced by 3D-secure, that is widely used for many transactions [37]. In addition, alternative protocols have been proposed in the academic literature [4, 10, 3], in order to strengthen the lack of privacy in 3D-secure. Nevertheless, there is no real comparison between these protocols in term of architecture, security and privacy objectives. Finally, two new specifications have been recently published, with a tokenization approach [19] and a new version of 3D-secure (v 2.0) [17, 15, 16, 18]. These specification are described with a special target on mobile devices, providing a new architecture for these electronic payments, where user's privacy has been totally abandoned in favor to fraud detection by the banks. Another EMV-compliant payment system using tokenization, where the security is based on the secure element of a mobile has also been recently proposed in [11].

The objective of this paper is to make a comparative study of existing architectures for e-commerce. As many main papers in the literature [28, 12, 23], we focus on security trends an architecture must fulfill within this context. We also consider privacy trends to analyze the benefit of the architecture proposed in the state of the art, we think this issue is becoming more and more important nowadays as big data is operational in many applications. The machine learning capabilities are able, for example, to identify an individual by analyzing its e-commerce behavior. Finally, we also propose a comparative study on the new specification of 3D-secure with a particular attention on electronic payment with mobile platforms.

Section 2 presents the context of online payments and defines the require-

ments for user's privacy and data security. Existing card payment architectures in the literature are detailed in Section 3. Section 4 presents a comparative study of architectures in the state of the art by considering security and privacy trends. Finally, conclusions and perspectives are given in Section 5.

2 Security and privacy protection requirements

This section establishes a set of security and privacy requirements for an authentication protocol for online payments (with a usability requirement), complementing previous works presented in [13, 3, 34]. Personal data involved in online payments should be divided in several parts (three parts in the present paper), because these data are shared between several entities, that have no operational requirements for access to all these data (except maybe for fraud detection):

1. The identity information are the data linked to the client's identity, such as a name, a home phone (or mobile) number, an email address, a billing address or a special ID number.

2. The purchase information are the data linked to the expected service, as the SP name, purchase details, purchase currency, purchase date and time.

3. The banking information include the issuer bank name, the personal account number (PAN), the card expiry date and the cryptogram CVX2.

Additional information on the client's browser can also be captured at each transaction (typically to determine the ability to support authentication in 3D-

secure) as the IP address, the browser language and time zone, browser screen information or also geolocalization data (particularly in the case of a mobile device).

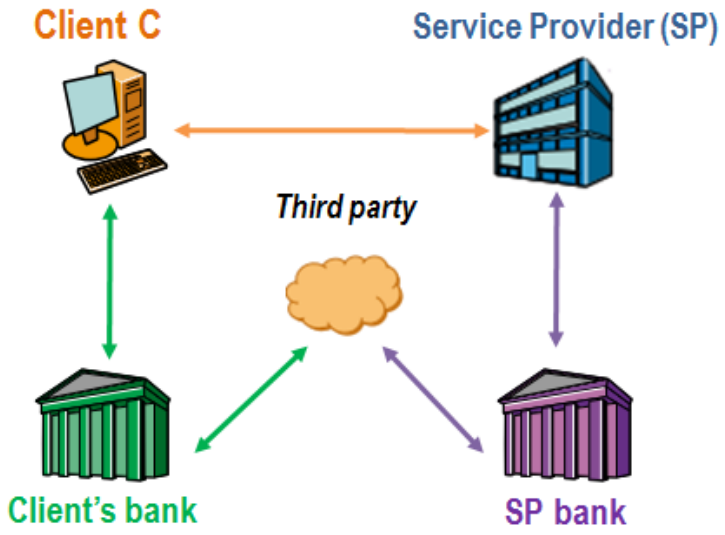

Figure 1: Actors involved in e-commerce architectures.

Four actors are present in electronic payments: The client wants to purchase an online service with a payment card, through the website of a service provider SP. These two actors have each one payment provider: the issuer and the acquirer 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 consequently, various and strongly depends of the architecture.

Independently to the transaction, the issuer bank knows identity information

of the client (maybe not all this information) and their related banking information. During the transaction, the merchant knows all purchase information, but does not necessary knows the identity of the client who realize this transaction (and particularly his/her banking information). More generally, it is suitable that in the case of an architecture with a fifth actor, this actor does not acquire more information than necessary (and ideally no personal information, as in a honest-but-curious model).

A list of security and privacy requirements, including risks raised in the literature [23, 8], is established. It also includes a necessary requirement on deployability of the architecture (for example describing if the system is realistic or user-friendly). These requirements have been determined after a security and privacy audits on authentication protocols on common e-payment architectures, as those described in the next section:

- S_1: The **confidentiality of transactions** requires that each exchanged data must be encrypted against external entities.
- S_2: The **integrity of transmitted information** ensures that the content of messages have not been altered.
- S_3: The **SP authentication** by the client or by a trusted party ensures the identity of the SP.
- S_4: The **banks authentication** by a trusted party ensures the identity of acquirer and the issuer bank.
- S_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 issuer bank or another trusted party *where the client is registered*.

- P_1: 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 (it is waived if the customer wants a home delivery service).

- P_2: The **confidentiality of client's identity towards the acquirer bank** ensures that the SP can deliver a service to the client without disclosing his/her identity to the acquirer bank.

- P_3: The **confidentiality of purchase information** ensures that only authorized persons have access to order information. This requirement includes that the client's purchase is unknown to the issuer bank.

- P_4: The **confidentiality of banking information** 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.

- P_5: The **confidentiality of acquirer bank** includes the fact that the client does not know the acquirer bank.

- U_1: The **deployability** ensures the credibility of use of the proposed e-commerce architectures, particularly for fraud detection aspect that should decrease the deployability of privacy compliant architectures.

Remark: the requirement P_5 could be important, in term of privacy, in the case of small service provider, for example reduced to only one person.

3 Comparative study

In this section, we review the most important authentication protocols in non card present e-commerce architectures involving banks (with a particular attention on authentication flow). We do not review the authentication solution of the client, but the connection of this authentication with the different domains (issuer, acquirer, ..) involved in the architecture. We have chosen past and present solutions used in the industry and academic ones. For example, the SET protocol was marginally used (but widely studied in academic literature), whereas the 3D-secure deployment for merchants is currently widely deployed (for example in 2014, the deployment rate was in 57% in Germany and was 47% in Great Britain [30]).

3.1 The Secure Electronic Transaction (SET) protocol

Several companies, including VISA and MasterCard, developed the SET protocol, [35], for secure electronic payment transactions by credit card. Surprisingly, the SET protocol ensured some SP and client's privacy protection, while its successor (3D-secure) was specified without notion of privacy.

This protocol is partially described in Figure 2 and has been analyzed in detail in the early 2000s, with some improvements. The most important point is the authentication of the client is realized with a certificate, verified by the service provider, allowing client's information to be partially partitioned before the authorization step (i.e. the issuer bank is only requested for authorization). We refer the reader to the abundant literature for more details on the SET

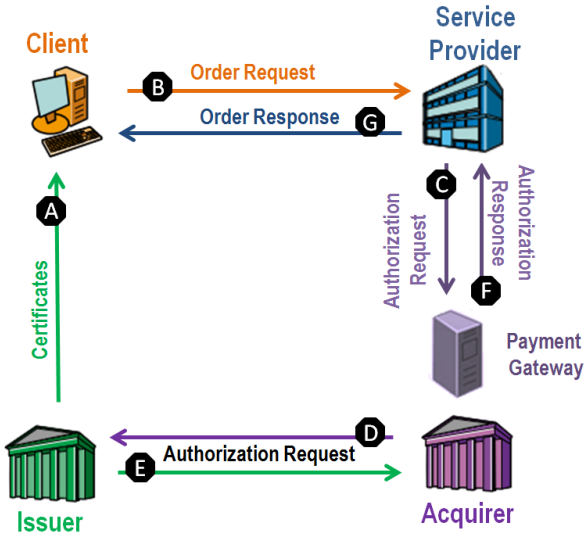

Figure 2: The SET protocol (adapted from [31])

protocol [26, 7, 5, 6, 9, 21].

3.2 The 3D-Secure protocol (3DS)

The 3D-Secure protocol is an authentication protocol developed by Visa in 2001 [37] for electronic transactions. Other financial institutions had also developed their own implementations, such as MasterCard with MasterCard SecureCode and American Express with SafeKey (a comparison between them is given in [32]). Security limitations of 3D-secure are underlined in [32, 27, 14]), particularly on the client authentication solution (realized by the issuer bank, generally through a pop-up window on the client's browser).

This protocol is commonly used for electronic payments over the Internet, through nine steps exchanged among five actors in the system (or three domains

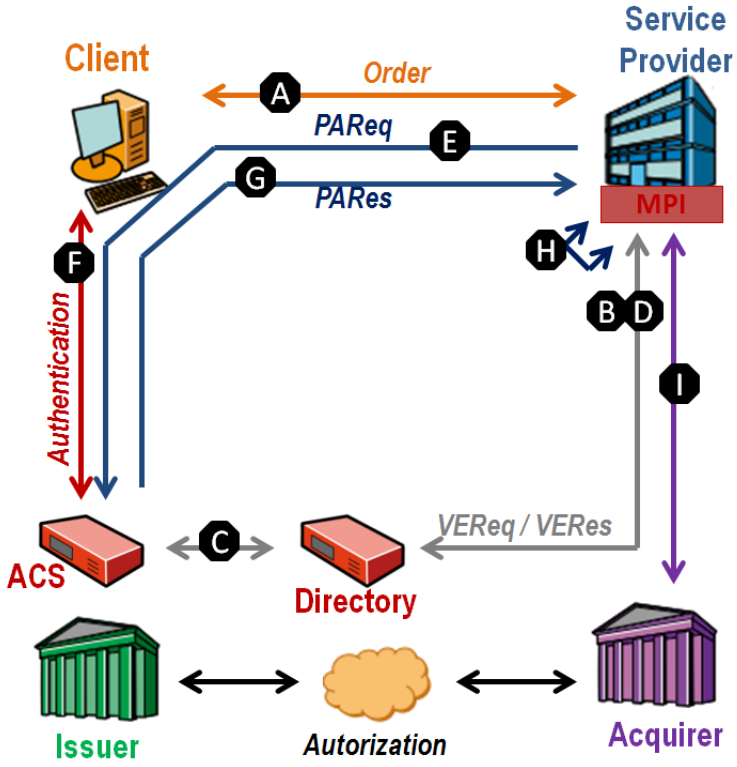

Figure 3: The 3D-Secure protocol [37]

: the issuer, the acquirer and the interoperability domains). As shown in Figure 3, the fifth actor is the Visa server, called Directory, used as a gateway between the issuer and the acquirer bank. A dedicated module called MPI (Merchant Plug In) must be imported to the site of SP.

3D secure protocol has for objective to transfer the transaction responsibility (i.e. client authentication) from the merchant to the issuer bank. The client's authentication is realized for this reason by the issuer bank. The main security flaw of 3D-Secure implementations (weak client's authentication), as underlined

in [27], has been corrected by many banks. The client's authentication with his/her date of birth date or other trivial secrets is generally replaced by an OTP (One Time Password) sent to user's mobile phone. Nevertheless, the NIST has recently deprecated this type of two-factors authentication with SMS (called out-of-band) [29].

3D-secure only describes the authentication protocol in online payments: the complete payment phase is not described with an authorization request for settlement. Thus, the entire transaction system using 3D-Secure protocol contains more than nine steps:

A The client sends his/her purchase intention to the service provider, accompanied by banking information required for the payment.

B The service provider contacts the Directory server for client's authentication (VEReq message).

C The Directory checks the service provider identity and recover the issuer bank (the ACS for Access Control Server) from the client's PAN.

D The ACS verifies the client's card and sends a cardholder authentication URL to the service provider (VERes message).

E The service provider requests the cardholder authentication, accompanied by the details of the authorized purchase, from the ACS,

F The issuer bank authenticates the client.

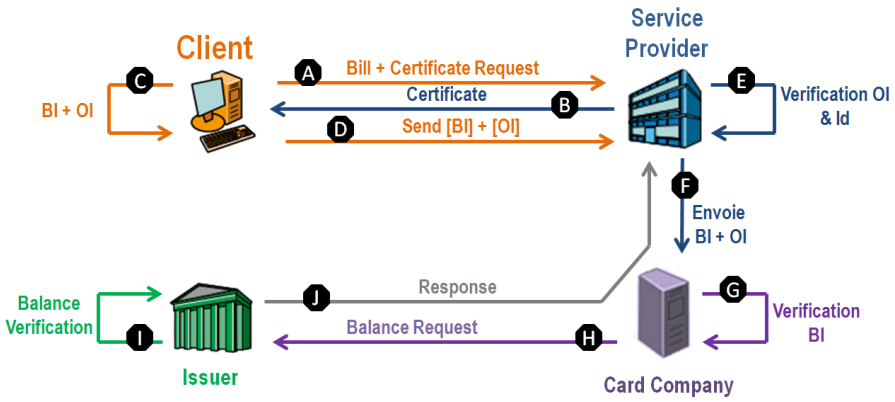

Figure 4: The Ashrafi et Ng's protocol [4]

G The ACS sends a confirmation of the client's authentication to the service provider (PARes message).

H The service provider records this PARes message.

I The service provider is authenticated by the acquirer bank. The bank checks the transaction and realizes a transaction authorization with the issuer bank (not described in the 3D-secure specifications).

3.3 The Ashrafi and Ng's protocol (AN)

Ashrafi and Ng in [4] proposed a payment scheme, ensuring a good level of privacy for the client. This protocol uses an optional third party payment gateway (not developed in this paper), and takes place as shown in Figure 4:

A The client requests the SP's public key and the credit card issuer's public key,

B The SP sends the SP's certificate and the credit cards company's certificate (with a transaction login), to the client,

C These two certificates are checked and the client generates two packages:

- Payment information: the hash of the card details, of the password and of the order information, the timestamps and validity period. This package is encrypted with the public key of the card company.
- Purchase information: the transaction identifier, the transaction amount, the timestamp and the validity period. This package is encrypted with the SP's public key.

D The two packages sent to the SP.

E The SP decrypts the second package with its private key. If the verification is correct, the SP generates a unique payment identifier.

F The two packages are sent to the cards company.

G The card issuer decrypts the payment information with its private key. The company checks the time stamp and expiration date. The hash of the customer data is also checked thanks to the hash locally stored by the company.

H The card issuer sends the message to the issuer bank for checking the client's balance.

I The issuer bank checks the client's balance.

J The issuer bank accepts or rejects the transaction and informs the card company. This latter sends the response to the SP.

At high level, the design of this protocol splits personal information in two types (payment information (BI in Figure 4) and purchase information (OI in Figure 4)) and encrypts them with two different keys, one for each actor. The main drawback of this scheme is that all payment information, used to identify the client and the issuer bank, are known by the card company (the issuer bank is only requested for authorization). That implies a centralized database of information, at the scale of the card company and not only at the scale of the issuer bank.

3.4 Improved 3D-Secure (3DS Imp)

The 3D secure protocol could be improved as presented in [34] for more privacy protection. The first observation involves banking information (CVX2 and the expiration date), that are not necessary information to the service provider. Secondly, one acquirer bank's certificate (with standard information, as well as the Directory public key) could be used for authentication. This protocol only modifies the two following steps:

A The acquirer bank's certificate is sent to the client by the service provider. The client encrypts banking information with the Directory public key and sends these encrypted data to the service provider.

C The Directory server decrypts these information with its private key and

checks SP's identity, the card number and the issuer bank. The Directory recovers the ACS and transfers the VEReq message.

The public key of the Directory server, easily available to the service provider, can be used to protect banking information of the merchant part. Clearly the service provider does not need these information to be paid for the purchases. Nevertheless, these simple privacy improvements have never been considered and deployed in real-world electronic payment architectures.

3.5 Improved Ashrafi and Ng's protocol (AN Imp)

One modification in the Ashrafi and Ng protocol allows to avoid the storage of all client's bank information at the card company level. This improved version is presented in [33], where the card company acts as a relay and does not make more numerous audits of client's data. The verification are delegated to the issuer bank that already has knowledge of banking information. Only three steps are then required to be changed (the other steps being the same as above):

C The client generates two packages. The purchase information is encrypted with the SP public key, and payment information is composed of:

- the hash of card details, the hash of client's password and the hash of order details are encrypted with the issuer bank public key ;
- the issuer bank name, the timestamp and the validity period are encrypted with the public key of the card company.

G The card company decrypts the first part of banking information and checks

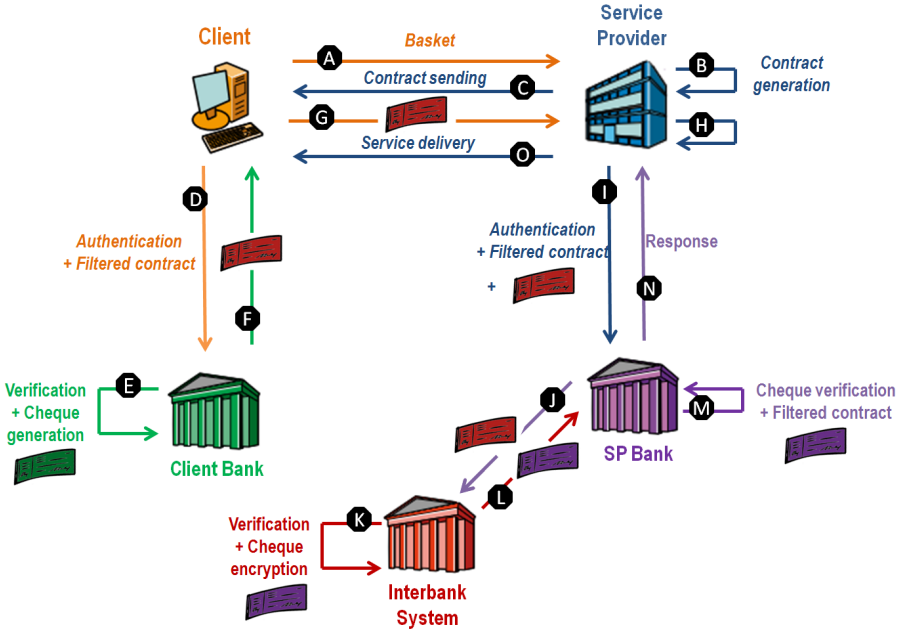

Figure 5: A privacy preserving online payment architecture.

the timestamp, the validity period, and the issuer bank name. The package is encrypted with the issuer bank public key.

I The issuer bank decrypts and checks the banking information, as well as the client's balance.

3.6 Plateaux et al. protocol (PLVCMR)

Data security and privacy during this protocol is related to the generation of two documents: a contract between the SP and the client, and an another bank document, called cheque [34]. Note that the architecture cannot be seen as an electronic cheque scheme in the classical sense of [2].

This architecture involves an interbank system IS at the end of the protocol, ensuring that only relevant information are revealed to the actors of the system. It is also used to check the authentication of the two banks and thus prevents money laundering. The service provider, the issuer and the acquirer bank have a pair of public key/private key, where the public key is certified by the interbank system. This architecture is composed of fourteen steps illustrated in Fig. 5 and detailed below. The last five steps are used to provide the banks authentication through the interbank system and thus prevent money laundering.

A The client sends purchase information and a session key K_{S_1} to the SP, encrypted using the public key of SP.

B The service provider create a contract including the amount of the transaction, a random number *order*, a symmetric key K_{S_2} encrypted by the public key of the acquirer bank, the beneficiary's name encrypted with K_{S_2}, Purchase information and the URL of the SP.

C The SP signs the contract and the hash of purchase information with his/her private key. This latter is sent to the client.

D Client's authentication is realized by the issuer bank (not described in this paper). The client also sends to the issuer bank the filtered contract (without URL and purchase information), encrypted with a session key generated between these both entities.

E The issuer bank generates a bank cheque (for the SP). It includes the amount of the transaction, the random number *order*; the encrypted beneficiary's

name; the symmetric key K_{S_2}, encrypted with the acquirer public key, information of the issuers bank.

F The issuer bank signs the cheque and encrypts it with the interbank system public key (thus, IS will be able to check the banks identities and the cheque validity at the end of the protocol). The cheque is sent to the client.

G The client forwards this cheque to SP. The result being encrypted, the SP cannot know client's banking information.

I The SP is authenticated to the acquirer bank and provides its filtered contract, the signed and the encrypted electronic bank cheque. This filtered contract contains: the amount of the transaction, the beneficiary's name, the order number.

J In order to validate the banks identities and the cheque, the acquirer bank authenticates to the interbank system and transfers the cheque.

K The interbank system checks the identity of the acquirer bank and decrypts the electronic cheque with its private key. The cheque (and its signature and consequently the identity of the client's bank) is verified.

L After verification, the interbank system re-encrypts the cheque (with the public key of the acquirer bank) and sends it to the bank.

M The acquirer bank is able to decrypt this cheque with its private key. The bank verifies that the cheque amount is similar to the filtered contract

provided by the SP. Then, the bank decrypts the symmetric key with its private key. In a second time, the acquirer bank decrypts with this key the beneficiary's name and compares it with the name of the filtered contract. Finally, the acquirer bank verifies the electronic cheque.

N The acquirer bank authorizes the SP to deliver service for its client.

3.7 3D-secure v2 (3DS v2)

The new specification of 3D-secure supports two versions for authentication: one application-based authentication for mobile devices and one browser-based authentication [17, 15, 16, 18]. The first authentication protocol uses a 3DS application requestor that initiates the authentication with the use of a 3DS SDK (integrated in the mobile device of the client). As in the previous version, payment request and authorization are not part of these new 3D-secure specifications. This new specification also introduces biometrics as solution for client's authentication but it is not mandatory.

At high level, the data flow has not really been changed since the previous version. The main modifications are the confirmation of practices which are generally already in place (dynamic authentication, risk management), some change of names in the flows (VAReq/VARes and PAReq/PARes messages are deleted and AReq/ARes and RReq/RRes messages are created with adapted roles), the introduction of elliptic curves in a key agreement procedure and the inclusion of mobile platforms in the protocol. In the following, we concentrate the discussion on application-based authentication in 3D-secure (i.e. with a mobile

device) because, from a privacy point of view, the browser-based authentication of 3D-secure version 2 is similar to the previous version.

In the case of a payment realized from a mobile authentication, a lot of personal data are added in the communications. It typically includes the IMEI number, geolocalisation data, hardware data, OS version, mobile phone number, Wifi and Bluetooth network indicators, indication if the device is jailbroken ... Actually, a security requirement of the SDK technical guide checks that the device is not jailbroken [16]. These data are directly encrypted by the mobile and are decrypted by the Directory Server (with a shared key) before a forward to the ACS for risk management (fraud detection).

Some collected information depend to the OS of the mobile (Android, iOS, windows phone), whereas some other collected information are common to all devices. Nevertheless, specifications only described information that should be collected. As specified in the beginning of section 2 of [16], *the implementer shall ensure that the 3DS SDK collects as many device-platform-specific parameters as possible*. This data collection is motivated by fraud detection. Finally, the SDK technical guide requires that SDK binaries need to be obfuscated [16], so it will be hard to know the precise nature of collected data. An interesting anecdote is the absence of the term *privacy* during all the 227 pages of the EMV 3-D Secure Protocol and Core Functions Specification [17].

3.8 EMV Tokenization

Tokenization was introduced by Mastercard, Visa and American Express and is now specified in [19]. The objective is to replace the PAN by a pseudo random number, called token. More precisely, a tokenization process uses the PAN for the generation of a payment token (including a token expiry date). The de-tokenization process uses these values to recover the original PAN. These two processes are realized by the token service provider, via the token requestor. In most cases, the cardholder is unaware of the use of a payment token. Tokenization has not been envisaged for user privacy, but only to reduce fraud in card-not-present and emerging transactions. Nevertheless, in the case of a data breach, it is clearly better for the cardholder than payment tokens are exposed, instead of PANs. Several usecases are envisaged in the specification, including Mobile NFC (at POS), e-commerce using a mobile or a digital wallet and e-commerce on a merchant site (called card-on-file).

In the case of a token request initiated by the cardholder, the PAN is sent to the merchant site. The PAN is successively transferred to the token requestor, then to the token service provider. The token service provider generates the payment token, realizes an identification and verification (IDV) with the issuer bank, and returns the token to the merchant via the token requestor. This token is stored on the merchant side (card-on-file) and the PAN is deleted. In others usecases (NFC, mobile/digital wallet), the token is stored on the device of the user.

During the transaction, the mercant sends the token to the acquirer bank

and this token is transferred to the payment network. The payment network contacts the token service provider to recover the PAN from the token. These data are finally sent to the issuer bank for authorization. Token request requires token assurance data for the IDV phase. These data are not specified but some examples are given as a cryptogram, or a billing address. Moreover, in usecases with NFC/mobile, device information as MAC address or operating system version are expected. In addition, authentication of the cardholder can also uses password or biometrics, depending to the required assurance level.

EMV tokenization is not compared with other protocols, in the next section, because privacy and data security strongly depends to the usecase and to the implementation. In the card-on-file scenario, the merchant does not store the PAN but he has access to it during the token request phase. In the other scenario, numerous personal data could be sent to the issuer bank, but it depends to the implementation of the corresponding application.

4 Discussions

In this section, we analyze the different e-commerce architectures detailed in the previous section by considering the security and privacy requirements presented in Section 2.

4.1 Analysis of SET

Data confidentiality (S_1) and integrity (S_2) are respected, and the protocol provides a mutual authentication between the SP and the client, based on cer-

tificates (but the client is not directly authenticated), where the SP bank is the trusted authority (S_3 and partially S_5). Bank authentication is not specified but can be realized outside of the protocol (S_4). Concerning privacy requirements, the SP does not know the client's banking information (P_4) and the client's bank does not know the purchase information (P_3), but knows the SP identity. Moreover, the client does not know the identity of the SP bank (P_5). Alternately, the SP and the SP bank know the client's identity (P_1 and P_2 are not verified).

Nevertheless, the installation of a specific software by the client, as well as the distribution of card readers and certificates by SP, makes the protocol complex, hard for the customer. Thus, as stated in [27], all these constraints have led to the abandonment of the SET protocol, with its relative user's privacy respect, for 3D-Secure.

4.2 Analysis of 3DS

Data confidentiality and data integrity are respected and authentication of different entities is ensured. Note that in this paper, we do not consider the authentication solution for client authentication. Moreover, as for SET, bank authentication is not specified but can be realized outside the protocol.

From a privacy point of view, none requirement is respected: the banking information of the client are sent to the service provider at the beginning of the protocol, the issuer bank knows the SP identity and the SP bank knows the client's identity. Moreover, the purchase information are contained in the

PAReq message sent to ACS. For these reasons, 3D-Secure is clearly not a privacy preserving scheme.

4.3 Analysis of the 3DS Imp

The improvement of 3D-Secure minimizes the knowledge of SP concerning the banking information of the client (CVX2 and expiration date of the card) because these data are encrypted by the customer's bank (R_9). In addition, whereas the PAN is known to the directory server, the client's authentication is handled by a single relying party, (the issuer bank). Consequently, the requirement R_3 is partially respected. Finally, with these improvements, the data sensitivity is taken more into account and therefore the requirement R_{11} is partially granted. Nevertheless, the issuer bank knows the client's purchases (R_8). Moreover, in general, the *client* is not anonymous for the fifth actor (the directory server) that is required to authenticate the banks.

4.4 Analysis of AN

The data encryption, the signature and the timestamp allows to guarantee the requirements S_1 and S_2. Moreover, the client authenticates the card company and the SP, thanks to their certificate (S_3 and S_4). The client's authentication is only implicit and partial because it is realized by the card company, instead of the issuer bank (S_5). For privacy requirements, identity information are not sent by the client (P_1 and P_2), but the banking and purchase data confidentiality (P_3 and P_4) are not totally respected, because the card company has many

information thanks to the second package, transferred by the service provider.

4.5 Analysis of AN Imp

The modifications of Ashrafi and Ng's protocol allow to ensure three additional requirements fully. The client's authentication is realized by the issuer bank with a password (S_5). Furthermore, banking information need not be stored by the card company because it is already known by a trusted party, the client's bank (P_4). Finally, the creation of a database containing all the details of customer's payments is avoided, the principle of data sensitivity can be ensured.

4.6 Analysis of PLVCMR

The confidentiality and the integrity of exchanged data during the communications of the protocol (requirement S_1 and S_2) is ensured by the establishment of a secure channel between actors. The client is authenticated by the issuer bank (requirement S_5) with a strong authentication process, whereas other entities authentication is realized through certificates, one for the SP and one for each bank. The SP is authenticated by the client at the beginning of the protocol (S_3), with the signature of the first contract.

Moreover, the client is anonymous for the SP and the acquirer bank and only the issuer bank knows the identity of the client and authenticates him (P_1 and P_2). In addition, the issuer bank knows neither contents of his/her client's purchases, nor the SP with which its client processes (P_3). The client's banking information is also ignored by the SP and by the acquirer bank (requirement P_4),

because these data are encrypted. Moreover, the SP does not know the issuer bank (P_4), because, the cheque is encrypted with the IS public key. Finally, the encrypted cheque with the IS public key prevents the customer to know the acquirer bank (requirement P_5). In addition, the acquirer bank does not know the customer with whom the SP deals.

4.7 Analysis of 3DS v2

The second specification of 3D-secure is rather easy to analyze because the security requirements are clearly taken into account in the specifications with strong cryptography and authentication between all entities, whereas the privacy requirements are voluntary abandoned for fraud detection. As explained above, the collection of personal data have been increased, in the application-based protocol, from the previous version. The objective of the protocol is clear, the collection of all available personal data in the mobile phone. For example, possibilities of fingerprinting on real-world iOS mobile devices has been analyzed in [24] and a very accurate success rate has been obtained. In these conditions, the term *privacy requirements* is not really adequate to analyze this protocol. This specification clearly means the end of privacy in mobile payments (if it had been envisaged one time).

4.8 Summary

Table 1 presents a summary of studied real-world and academic authentication protocols used in e-payment architectures, considering the security and privacy

requirements. As detailed above, many privacy requirements are not covered, especially for protocols used in current transactions.

Contrary to 3D-Secure protocol where all actors know all exchanged data, a privacy preserving architecture is possible, based on reciprocal knowledge of actors. Moreover, the identifier of the transaction can be used by the IS to retrieve the client of the associated transaction in case of litigation. Another important point concerns the deployability of studied architectures. Fraud detection is an important issue in e-commerce. Currently, the issuer has a lot of information and uses it for fraud prevention. A privacy preserving system may interfere with such security techniques. Indeed, many banks use transaction information to detect fraud. Nevertheless, does a bank should know all parameters of your mobile device or what you bought on a website for this reason? Many recent works showed that it is possible to process many data from the users that could be useful for authentication or fraud detection without any privacy leakage [22].

5 Conclusion and perspectives

Personal and sensitive information are exchanged in card-not-present payment systems on the Internet as 3D secure. This protocol is presented as extremely secure but is not intended to provide privacy protection principles. In other side, several others payment schemes improving user's privacy have been recently proposed. Nevertheless, characteristics of all these scheme are not exactly identical, which leads to a difficult comparison between all these systems. A comprehen-

sive list of requirements in terms of security and privacy protection is presented and several systems, with some improvements, are compared with respect to these requirements. Thus, the proposition of [34] is fully compatible with privacy principles.

Nevertheless, the new specification of 3D-secure suggests that data privacy is not taken into account in these card not present payment architectures, because actors involved in these systems (particularly the issuer bank) does not want of it for fraud detection. The variety of collected data by the issuer bank has never been so important. Until recently, it was usual (but inexact) to balance between user's privacy and user's security, but in this last case, that only means in the reduction of user's privacy to fraud detection, not for an enhanced data security system.

Acknowledgments

The authors would like to thanks BULL SAS Company and ANRT (grant number 435/2010) for their financial support to this work.

References

[1] J. Abraham. Global b2c e-commerce report 2016. Technical report, E-Commerce Foundation, 2016.

[2] M. Anderson. The electronic check architecture. *Financial Services Technology Consortium*, 1998.

[3] G. Antoniou and L. Batten. E-commerce: protecting purchaser privacy to enforce trust. *Electronic commerce research*, 11(4):421–456, 2011.

[4] M. Ashrafi and S. Ng. Enabling privacy-preserving e-payment processing. In *Database Systems for Advanced Applications*, pages 596–603. Springer, 2008.

[5] G. Bella, F. Massacci, and L. Paulson. Verifying the SET purchase protocols. *Journal of Automated Reasoning*, 36(1):5–37, 2006.

[6] G. Bella, F. Massacci, L. Paulson, and P. Tramontano. Formal verification of cardholder registration in SET. *Computer Security - ESORICS 2000*, pages 159–174, 2000.

[7] S. Bella, L. Paulson, and F. Massacci. The verification of an industrial payment protocol: The SET purchase phase. In *Proceedings of ACM CCS*, pages 12–20. ACM, 2002.

[8] Anthony Bouch. 3-d secure: A critical review of 3-d secure and its effectiveness in preventing card not present fraud. *University of London, Londra, erişim: http://www. 58bits. com/thesis/3-D_Secure. pdf, erişim tarihi*, 8:2014, 2011.

[9] S. Brlek, S. Hamadou, and J. Mullins. A flaw in the electronic commerce protocol set. *Information Processing Letters*, 97(3):104–108, 2006.

[10] M. Carbonell, J. Torres, A. Izquierdo, and D. Suarez. New e-payment scenarios in an extended version of the traditional model. *Computational Science and Its Applications–ICCSA 2008*, pages 514–525, 2008.

[11] Véronique Cortier, Alicia Filipiak, Saïd Gharout, and Jacques Traoré. Designing and proving an emv-compliant payment protocol for mobile devices, 2017.

[12] Tomi Dahlberg, Niina Mallat, Jan Ondrus, and Agnieszka Zmijewska. Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, 7(2):165–181, 2008.

[13] Linda Delamaire, HAH Abdou, and John Pointon. Credit card fraud and detection techniques: a review. *Banks and Bank systems*, 4(2):57–68, 2009.

[14] S. Drimer, S. Murdoch, and R. Anderson. Optimised to fail: Card readers for online banking. *Financial Cryptography and Data Security*, pages 184–200, 2009.

[15] EMV. 3-D secure : Protocol and core functions specification, 2017.

[16] EMV. 3-D secure : SDK - device information, 2017.

[17] EMV. 3-D secure : SDK technical guide, 2017.

[18] EMV. 3-D secure SDK specification, 2017.

[19] EMV. Payment tokenisation specification v 2.0, 2017.

[20] Y. Espelid, L.H. Netland, A. Klingsheim, and K. Hole. A proof of concept attack against norwegian internet banking systems. *Financial Cryptography and Data Security*, pages 197–201, 2008.

[21] A. Fioravanti and F. Massacci. How to model (and simplify) the SET payment phase for automated verification. In *IJCAR'01*, 2001.

[22] Julien Hatin, Estelle Cherrier, Jean-Jacques Schwartzmann, and Christophe Rosenberger. Privacy preserving transparent mobile authentication. In *ICISSP*, pages 354–361, 2017.

[23] Changsu Kim, Wang Tao, Namchul Shin, and Ki-Soo Kim. An empirical study of customers perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1):84–95, 2010.

[24] A. Kurtz, H. Gascon, T. Becker, K. Rieck, and F. Freiling. Fingerprinting mobile devices using personalized configurations. In *Privacy Enhancing Technologies (PETS)*, pages 4–19, 2016.

[25] H. Abdou L. Delamaire and J. Pointon. Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4(2), 2009.

[26] C. Meadows and P. Syverson. A formal specification of requirements for payment transactions in the SET protocol. In *Proceedings of Financial Cryptography and Data Sceurity*, 1998.

[27] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. *Financial Cryptography and Data Security*, pages 336–342, 2010.

[28] Eric WT Ngai and Angappa Gunasekaran. A review for mobile commerce research and applications. *Decision Support Systems*, 43(1):3–15, 2007.

[29] NIST. Special publication 800-63b, digital identity guidelines - authentication and lifecycle management, 2017.

[30] Ogone. 3-d secure landscape in europe. Technical report, Ogone, 2014.

[31] M. Pasquet, C. Rosenberger, F. Cuozzo, et al. Security for electronic commerce. *Encyclopedia of Information Science and Technology,*, 4:14, 2008.

[32] V. Pasupathinathan, J. Pieprzyk, H. Wang, and JY. Cho. Formal analysis of card-based payment systems in mobile devices. In *Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54*, pages 213–220, 2006.

[33] A. Plateaux. *Solutions opérationnelles d'une transaction électronique sécurisée et respectueuse de la vie privée.* Phd thesis, Université de Caen Basse Normandie, 2013.

[34] A. Plateaux, P. Lacharme, V. Coquet, S. Vernois, K. Murty, and C. Rosenberger. An e-payment architecture ensuring a high level of privacy protection. In *SecureComm*, pages 305–322, 2013.

[35] S.E.T. Secure electronic transaction specification. *Book 1: Business Description*, 2002.

[36] R Smith and J. Shao. Privacy and e-commerce: a consumer-centric perspective. *Electronic commerce research*, 7:89–116, 2007.

[37] Visa. 3-D secure protocol specification - core functions, July 16, 2002.

Table 1: Summary table of the different studied e-commerce architectures considering all requirements defined in section 2 (✓: verified requirement, ∼: partially verified requirement, ✗: not verified requirement)

	Requirements	**SET**	**3DS**	**3DS Imp.**	**AN**	**AN Imp.**	**PLVCMR**	**3DS v2**
S_1	Data confidentiality	✓	✓	✓	✓	✓	✓	✓
S_2	Data integrity	✓	✓	✓	✓	✓	✓	✓
S_3	SP authentication	✓	✗	✗	✓	✓	✓	✓
S_4	Banks authentication	✗	✓	✓	✓	✓	✓	✓
S_5	Client's authentication	∼	✓	✓	∼	✓	✓	✓
P_1	Identity information confidentiality for SP	✗	✗	✗	✓	✓	✓	✗
P_2	Identity information conf. for acquirer bank	✗	✗	✗	✓	✓	✓	✗
P_3	Purchase information confidentiality	∼	✗	✗	∼	∼	✓	✗
P_4	Banking information confidentiality	✓	✗	✓	∼	✓	✓	✗
P_5	Acquirer bank confidentiality	∼	✗	✗	✗	✗	✓	✗
U_1	Decentralized structure	∼	✗	∼	∼	✓	✓	✗
U_2	Deployability	✗	✓	✗	✗	✗	✓	✓