CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59

Albert Levi
Information Security Lab
Electrical and Computer Engineering Dept.
Oregon State University,
Corvallis, Oregon 97331
levi@ece.orst.edu

Çetin Kaya Koç
Information Security Lab
Electrical and Computer Engineering Dept.
Oregon State University,
Corvallis, Oregon 97331
koc@ece.orst.edu

Abstract

The security of electronic payment protocols is of interest to researchers in academia and industry. While the ultimate objective is the safest and most secure protocol, convenience and usability should not be ignored, or the protocol may not be suitable for large-scale deployment. Our aim in this paper is to design a practical electronic payment protocol which is both secure and convenient.

ANSI X9.59 standard describes secure payment objects to be used in electronic payment in a convenient and secure way. It has many useful convenience features for large-scale consumer market deployment, the best being the elimination of consumer certificates. Consumer public keys are stored in account records at financial institutions; the digital signatures issued by consumers are verified by financial institutions. Encryption is deliberately not provided by X9.59.

In this paper we propose a new Internet e-payment protocol, namely CONSEPP (CONvenient and Secure E-Payment Protocol), based on the account authority model of ANSI X9.59 standard. CONSEPP is the specialized version of X9.59 for Internet transactions (X9.59 is multi-purpose). It has some extra features on top of the X9.59 standard. X9.59 requires merchant certificates; in CONSEPP we propose a lightweight method to avoid the need for merchant certificates. Moreover, we propose a simple method for secure shopping experience between merchant and consumer. Merchant authentication is embedded in the payment cycle. CONSEPP aims to use current financial transaction networks, like VisaNet, BankNet and ACH networks, for communications among financial institutions. No certificates (in the classical sense) or certificate authorities exist in CONSEPP. Convenience is not traded for security here; basic security requirements are fulfilled in the payment authorization cycle without extra messaging and significant overhead.

1. Introduction

One of the most important components of an electronic commerce (e-commerce) application is a digitally secure means of electronic payment (e-payment). E-payment may be treated as a protocol among the payer, the payee and their respective Financial Institutions (FIs). We will follow e-commerce terminology and refer to the payer as "consumer" and the payee as "merchant". All e-payment systems involve transfer of funds and monetary instruments. Thus, FIs are irreplaceable players in e-payment systems.

There are several e-payment methods proposed, but only a few are being used successfully. CyberCash [1], which is based on payment-card transactions, is one. Electronic money systems [2] are not as successful as credit-card methods. Secure Electronic Transaction (SET) [3] is another payment-card based protocol. Although it is not specifically designed for electronic payment, Secure Socket Layer (SSL) [4] based e-payment methods are at present the most widely used. Combinations of these methods are also possible. For example, a system might use SSL between the consumer and merchant, and SET between the merchant and FIs.

The security of an e-payment method is very important for all parties involved in a transaction, but security alone does not guarantee success in the marketplace. An e-payment system must also be convenient. This requirement has different meanings for different parties. From the consumer's point of view, "convenience" means to pay quickly and without an additional cost or too much effort. From the FI's point of view, "convenience" means low deployment and operational cost. The "convenience" requirement is generally ignored by security developers whose aim is to make the system as secure as possible. However, the aim should be to design a system which is both "secure" and "convenient".

* *Proceedings, The 17th Annual Computer Security Applications Conference*, pages 286-295, New Orleans, Louisiana, IEEE Computer Society Press, Los Alamitos, California, December 10-14, 2001.

1.1. Contribution of the paper

SET is a good example of a protocol that ignores "convenience". SSL-based methods, on the other hand, are ignoring important "security" requirements. In this paper we propose a new e-payment protocol for Internet based transactions. Our aim is to balance the trade-off between security and convenience. This protocol, named CONSEPP (CONvenient and Secure E-Payment Protocol), is based on ANSI X9.59 [5] standard. This standard describes secure payment object to be used in electronic payment. It is not restricted to Internet-based payment; same idea could be applied to Point-of-Sale terminals, Mail-Order and Telephone-Order payments. However, CONSEPP is for Internet transactions only. In CONSEPP, we add some more features on top of the X9.59 standard to make it more specific for Internet based payments. We solve the existing merchant certificate problem of X9.59 with dynamic public key transfers embedded in authorization messages. We propose a secure method for shopping experience in which merchant authentication is embedded in payment cycle. These extra features are light methods and do not create a significant burden on transactions. As a result, we end up with a certificate-free and convenient Internet e-payment method that satisfies the security requirements of all parties.

In the rest of this section the trade-off of security vs. convenience will be detailed using two applications, SSL and SET. Section 2 discusses the basic characteristics of the X9.59 model. CONSEPP is explained in Section 3. The advantages of CONSEPP are the subject of Section 4. Some further discussions are given in Section 5. Conclusions are in Section 6.

1.2. SSL, SET and their disadvantages

SSL [4] is a protocol that provides a private, encrypted session between the client and the server. The protocol and its related certificates are widely used in web browsers. The server authenticates itself to the client using the server certificate, but the authentication of the client to the server is optional. In electronic payment terminology, server means merchant; client means consumer. In a basic electronic payment protocol based on SSL, a consumer sends account information and the transaction amount over an SSL protected connection. The merchant also sends the acknowledgment over the same channel. The authorization for the transfer of funds from the consumer's account is done as in classic Mail-Order/Telephone-Order transactions. This step is transparent to the consumer. Such a protocol is not only easy to implement but also minimally changes the traditional business model. Therefore it is very "convenient". The consumer does not need to register and obtain another account or card for electronic payment. The merchant and the FIs will make only slight modifications to the traditional authorization and settlement procedures. Some new interfaces may need to be implemented in order to provide automated responses to the consumer.

An SSL based protocol provides privacy, integrity and authentication of merchant to consumer. However, it does not guarantee the authentication of consumer to merchant and consumer non-repudiation. The consumer may deny making the payment and the merchant may not be able to prove the fact even if the transaction was legitimate. This causes a "charge-back" cost for honest merchants due to dishonest consumers. The SSL based methods may also work for dishonest merchants to make illegal money. The merchant has to see the consumer's account information in order to initiate the authorization process after receiving the payment order from the consumer. The merchant could intentionally or unintentionally disclose this sensitive account information. Furthermore, since the consumer's FI has no way to check the intent of the consumer to make the payment, a dishonest merchant is also able to use this account information later to make charges without the consent of consumer. Of course, the consumer can rightfully repudiate this bogus transaction. However, transactions that are overlooked would be to the benefit of the dishonest merchant.

Another class of electronic payment methods involves the FIs in the protocol. The most well-known example is the Visa and MasterCard joint effort, the *Secure Electronic Transaction* (SET) protocol [3]. The interaction among FIs in the settlement network is not a part of SET. Communication between FIs and consumer/merchant is defined in the protocol. The authentication and non-repudiation requirements require the use of digital signatures and consequently of digital certificates for each message. Privacy and integrity are also attained. Each SET cardholder must have a digital certificate issued by a trusted Certificate Authority (CA). The cardholder's public key is certified via a digital certificate. This is necessary, because otherwise no one can be sure of the legitimacy of a cardholder's identity or of the public key. SET provides all necessary security requirements, unfortunately by sacrificing "convenience". Currently, SET is not widely deployed and we believe that it will not be in the near future. We also believe that the FIs are less than eager to deploy SET, for reasons discussed below.

1. SET requires the registration of consumers by their FIs. They need to have certificates in order to use the protocol. However, SSL based solutions do not require such registration.
2. SET requires a PKI (Public Key Infrastructure) that is defined in [3]. A PKI is a complete system for

certificates. The FIs, the payment brands and the end users come together in a hierarchical manner in this PKI. The certificates are issued by independent CAs. We think that this PKI, as all other distributed and large CA-based PKIs, is unlikely to be used, because the implementation and maintenance cost of this PKI, which is to be paid to CAs, would be an extra expense for the FIs.

3. SET is only for payment-card (credit or debit) based transactions. Account based transactions, like electronic check (e-check), are not included in SET.

1.3. Motivation behind X9.59

SSL based protocols are convenient but have some authentication and non-repudiation problems. SET and other payment-card based protocols, which require either intermediary agents or CA-based PKI, are secure, but not so convenient, particularly for FIs. X9.59 standard tries to find a middle ground in the security-versus-convenience trade-off.

The Account Authority Digital Signature (AADS) model was first introduced by Lynn and Anne Wheeler [6] in 1997 as the part of the ANSI X9.59 "Electronic Commerce for Financial Services Industry" standardization efforts. The Wheelers and ANSI X9A10 working group shaped the AADS idea and used it in the X9.59 standard. As of this writing, X9.59 is in DSTU (Draft Standard for Trial Use) status. Some prototype implementations are being developed. In the rest of this paper, the terms AADS model and X9.59 model will be used interchangeably.

The Wheelers tried to eliminate the requirement of a Certificate Authority (CA), and consequently a CA-based PKI, in order to verify a public-key based digital signature, because they strongly believe that the existence of a CA-based certification system has no part in business models for the financial services industry. They use the name "Certificate Authority Digital Signature (CADS)" to describe the classical way to obtain a public key using certificate(s) and to verify a digital signature using this certificate. They name their method AADS, since the public key necessary for the verification does not come from a CA in their method. The public key is stored and used by the account authority (i.e., the FI) of the entity.

2. Basic characteristics of the X9.59 model

The basic idea behind the AADS model as proposed by the Wheelers for the X9.59 standard is to avoid the necessity of consumer certificates. However, to verify the signatures issued by the consumer, a public key is still necessary. The merchant verifies the digital signature of the consumer in most of the electronic payment protocols. However in X9.59, the Consumer's FI (CFI) is the authority who verifies the consumer's digital signature. The consumer's public key is stored in the consumer's account record held by the CFI. Therefore, no consumer certificate is necessary. Having verified the signature of the consumer on the payment order, the CFI sends an acknowledgment to the merchant via the Merchant's FI (MFI).

Since the account information of the consumer is already held in the CFI's site, it would not be difficult to hold the consumer's public key as another field of this account record. Moreover, the transaction should be forwarded to the CFI in order to allocate enough funds for the authorization. An acknowledgment should also be sent to the merchant for this fund authorization. In X9.59, these authorization and acknowledgment messages contain the digital signature and its verification information as well. The X9A10 committee believes that this payment method does not require changing the existing settlement infrastructure tremendously. A few addenda fields in the current messages would solve the problem. Furthermore, the business model remains the same.

Another important characteristic of the X9.59 model is that messages transmitted among the consumer, merchant and FIs are not encrypted. However, the X9.59 draft standard [5] states that encryption could be provided by some other means outside the scope of X9.59 standard. Justifications for this challenging characteristic are as follows.

1. X9.59 uses Payment Routing Code (PRC) instead of consumer and merchant account/card numbers. This is an FI-assigned account number that internally identifies a consumer or a merchant. PRCs are X9.59 specific and are not used elsewhere. FIs assign and pass PRCs to their customers when they are registered for the first time. This is part of the account setup procedure. Consumers and merchants use their PRCs for all X9.59 transactions, instead of regular account/card numbers. PRCs are not one-time, their holders use the same value for all their X9.59 transactions. The FIs keep the mappings between the PRCs and conventional account numbers in order to process an X9.59 transaction, but they do not reveal this mapping. In this way, the binding between a PRC and its holder becomes a secret between the holder and its FI. A PRC is not valid unless there is an accompanying digital signature issued by its owner. Any third party cannot take advantage of knowing PRC, since it cannot produce a digital signature. Thus, PRCs need not be encrypted.
2. The strong authentication that X9.59 claims to provide is sufficient to prevent the majority of consumer and merchant frauds. Using the PRC concept and strong authentication make encryption a luxury in X9.59. The

X9.59 group believe that strong privacy via encryption is one of the reasons behind the failure of SET [3], since such an approach slows down the transaction processing and creates extra key distribution problems.

3. Having no encryption makes the system suitable for consumers who use wireless devices. Processing speed and power consumption are important problems of wireless devices. End-user wireless devices can save some time and power by having no encryption.
4. X9.59 is not an Internet-only standard. Implementation is possible in existing point-of-sale networks where the consumer/merchant transaction occurs at a physical box located on the merchant's premises. The encryption requirement is minimal in such a classical transaction.

Integrity is inherently supplied by the digital signature scheme in X9.59. Replay attacks are avoided by supplying a unique "nonce" called Locally Unique IDentifier (LUID).

The X9.59 model tries to take full advantage of the current payment infrastructure and business model. It is not restricted to a specific payment method and infrastructure. It defines secure payment objects that can be applied to any payment method. The credit/debit card, wire transfers and e-check methods are immediate candidates that can be adopted into the X9.59 model with minor changes in the current infrastructure.

Initial registration of both consumer and merchant to their respective FIs is necessary. The public-private key pairs are created and the public keys are deposited in their FIs. Moreover, merchant and consumer learn the public keys of their respective FIs. The registration process is outside of the scope of X9.59 standard.

The shopping experience until the payment step is not a part of the X9.59 standard. In other words, it is assumed that the consumer knows the PRC of the Merchant (PRCM) and the order details.

The interchange protocol among the FIs is also out of the scope of the X9.59 standard. This protocol might be updated in order to carry some addenda fields (e.g. the signature of the consumer over the payment object).

Authorization request and response messages are assumed to be a part of the existing infrastructure and they are not defined by the X9.59 standard.

3 .CONSEPP: CONvenient and Secure Electronic Payment Protocol

CONSEPP is based on X9.59 standard, but there are some add-ons. CONSEPP is for Internet based payments and defines most of the features that are excluded in X9.59 because of its general-purpose characteristic. Thus CONSEPP must be considered as an instantiation of the X9.59 standard. The basic CONSEPP payment cycle as described by the X9.59 standard is given in Section 3.1.

CONSEPP also defines the following features that are excluded in the core X9.59 standard:

- merchant authentication that is embedded in the payment cycle,
- a method for secure shopping experience,
- authorization request and response messages,
- a lightweight method for merchant's public key transfer from MFI to consumer.

These features are detailed in Sections 3.2, 3.3, 3.4 and 3.5.

3.1. Basic payment cycle

A generic CONSEPP payment cycle as described in the X9.59 standard [5] is given in Figure 1. First we start by explaining the payment infrastructure and trust relationships among the consumer, merchant and FIs. Then the protocol is detailed.

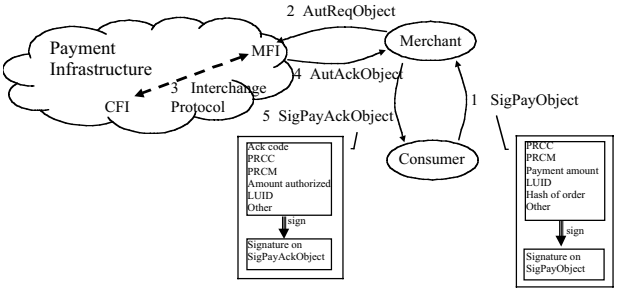

Figure 1. Payment cycle

3.1.1. Payment infrastructure and trust relationships

Payment Infrastructure is the existing payment network among financial institutions and the related payment mechanism it supports. Automated Clearing House (ACH) networks [8] are interconnected networks for electronic check clearing and direct fund transfers. VisaNet and BankNet are two such infrastructures for credit card transactions operated by Visa [10] and MasterCard [11] respectively. The topology of these networks is hierarchically interconnected local star networks. There are local transaction hubs (transaction centers) where local transactions are completed. National and international transactions pass through higher-level hubs.

There are well-defined security policies and trust relationships within the payment infrastructure. Each pair of entities communicating with each other also trust each other and have enough information and resources to

send/receive authenticated and secured information. Therefore, once a transaction has reached the MFI its security and integrity are guaranteed within the financial network. Security and authentication are provided via leased lines and hardware devices based on public key cryptography like the ones produced by Zaxus [12]. ISO 8583 standard defines the messaging among FIs and transaction centers for credit card payments, but security and authentication are above this layer. "Interchange protocol" is the general name for messaging within a financial network and is not a part of CONSEPP.

CONSEPP assumes that consumer and merchant ultimately trust all FIs involved in the payment cycle. This trust is explicit between consumer and CFI, and between merchant and MFI as there are agreements between them. Consumer-MFI and merchant-CFI trust relationships are implied by the protocol. Merchant trusts CFI since the consumer's signature is verified by CFI. Consumer trusts MFI since it plays an important role in merchant authentication. The consumer-MFI and merchant-CFI trust relationships are actually results of transitive trust among the FIs. For example, consumer knows and trusts only CFI. CFI trusts MFI due the inter-FI trust relationships within the payment infrastructure. Consequently consumer trusts MFI.

In certificate based e-payment protocols CAs are the trusted third parties. FIs replace CAs in CONSEPP. We believe that trusting an FI is much better than trusting a CA. Some justifications of this proposition follow.

- We already trust FIs since we deposit our funds there. The level of trust that we assign to FIs in CONSEPP is not more than controlling our savings.
- FIs are already business partners of all merchants. CONSEPP just opens a new area of partnership.
- FIs have a well-established legal base with responsibilities and obligations spelled out by law. There is also a large body of precedent that enforces FIs to behave properly. An FI would not want to destroy its reputation by behaving dishonestly.
- On the other hand, CA companies do not have a long background. Their commercial durability as technological companies is in question in today's market conditions. A business model relying on a CA is prone to fail if that company cannot continue its operations later. Changing a CA is not like changing a server machine. All business models must change tremendously when the CA company is changed.

Now let us briefly analyze the trust relationship between consumer and merchant. They need not know their public keys a priori. Therefore, they do not have any cryptographic trust relationships. The consumer must trust the merchant only commercially. By commercial trust it is meant that the merchant is trusted to send the goods ordered to the consumer in reasonable condition and time. Such a trust also exists in mail-order and telephone-order business models, so it is not a new concept for CONSEPP. Unlike mail-order and telephone order, merchant does not need to trust consumer in CONSEPP, because consumer authentication and payment authorization are taken care of by CFI.

3.1.2. Basic payment steps

Now let us briefly explain the steps of basic payment cycle as shown in Figure 1.

1. ***SigPayObject*:** This object is the payment object created and signed by the consumer to show its intent of payment. It contains
   - consumer's PRC (PRCC),
   - merchant's PRC (PRCM),
   - locally unique transaction identifier (LUID)
   - the hash of the order details,
   - payment amount and
   - other payment, transaction and protocol details.
2. ***AutReqObject*:** The merchant does not perform any signature verification over *SigPayObject*. It forwards *SigPayObject* to MFI as the authorization request *AutReqObject*. *AutReqObject* is nothing but the *SigPayObject* packed in the format of a standard authorization request. The consumer signature on *SigPayObject* is also packed in *AutReqObject*. This object is not part of the core X9.59 standard since it is assumed that payment infrastructure already has such an interface. Section 3.4 gives more information on *AutReqObject*.
3. **Interchange Protocol:** The MFI transfers the fields of the *SigPayObject* and the consumer signature over it to CFI together with other standard authorization details of the selected payment mechanism. CFI performs two operations: i) fund allocation for the transaction, ii) reconstruction of *SigPayObject* and verification of the consumer signature over it. CFI uses the public key of the consumer stored in the account records for this verification. After that, CFI responds to MFI with positive or negative acknowledgment. The communication between CFI and MFI is a part of the interchange protocol and is outside the scope of X9.59 and CONSEPP.
4. ***AutAckObject*:** MFI forwards the authorization response back to the merchant as Authorization Acknowledgment *AutAckObject*. This object, as *AutReqObject*, is a part of the standard payment infrastructure interface and not described in the core X9.59 standard. Section 3.4 gives more information on this object.
5. ***SigPayAckObject*:** At the final step, the merchant signs the authorization response using its private key and sends it to consumer as Signed Payment

Acknowledgment *SigPayAckObject*. This object contains

- acknowledgment code (approved or rejected),
- PRCC,
- PRCM,
- LUID (the same one used in corresponding *SigPayObject*),
- actual amount authorized,
- other payment, transaction and protocol details.

SigPayAckObject should also bear the certificate of the merchant signed by MFI in order to allow the consumer to check the validity of the merchant's signature over *SigPayAckObject*. The standard X.509 [9] certificate lists are proposed for this purpose in [5]. However, this proposal is vague and the details are missing in [5]. Thus we propose a novel method for merchant's public key transfer from MFI to consumer. This method will be described in Section 3.5.

X9.59 standard also defines a signed object for the consumer to acknowledge the receipt of goods or services. Payment query request and acknowledgment are two other objects defined in X9.59 to allow the consumer to learn about the current status of a payment operation that it initiated. Another signed object is the request for refund that is useful in case the consumer returns the goods to the merchant. The details of these objects can be found in [5] and they can be used in CONSEPP.

3.2. Merchant authentication

In certificate based e-payment methods, merchant authentication is performed by using merchant certificates at the beginning of the payment steps. This authentication is on the binding between the URL and the commercial name of the merchant. CONSEPP does not use classical merchant certificates. The verification of merchant's signature on the *AutAckObject* can provide authentication of merchant's URL, but this is done at the end of the payment cycle. If the merchant's URL is not the correct one, then it is too late for the consumer to realize this fact. Merchant authentication should be performed before the payment authorization. Such an early merchant authentication can be embedded in the payment cycle of CONSEPP as explained below.

First, consumer finds out merchant's URL and commercial name during the shopping experience (Section 3.3). Consumer includes this information in *SigPayObject*. Merchant forwards it to MFI in *AutReqObject*. MFI cross-checks merchant's URL and commercial name that it received in *AutReqObject* with the ones in its account records. If they match, then MFI proceeds the transaction. Otherwise, it rejects the transaction as fraud. The merchant cannot alter the URL and name information before sending to the MFI, because this causes the *SigPayObject* not to be verified at CFI's site.

We rely on the correctness of the MFI's account records for merchant authentication. This is a reasonable assumption since CONSEPP is based on "Account Authority" model. CFIs are in charge for customer signature verification; similarly MFIs are in charge for merchant authentication. Moreover this authentication does not create extra message rounds.

3.3. Secure shopping experience in CONSEPP

In CONSEPP shopping experience and initial data exchange between merchant and consumer might be SSL based. Two modes of SSL are proposed below.

SSL using only merchant certificate: This mode of SSL is the most widely used one in practice. Merchant (server) uses his certificate, but the consumer (client) need not have a certificate. SSL is used for secure communication between them and for initial and conditional authentication of the merchant. Here SSL authentication is one-way, merchant to consumer. The merchant sends its PRCM and they negotiate on the payment details over a SSL protected channel. The consumer finds out merchant's URL and commercial name from this session and believes in its authenticity under SSL protocol rules. However, neither CFI nor MFI are responsible of this authentication since SSL certificates are issued by independent certificate authorities like Verisign. The actual merchant authentication takes place during the payment cycle as explained in Section 3.2. The use of merchant SSL certificate only helps the consumer to feel more secure during the shopping experience.

SSL in Anonymous Diffie-Hellman mode (no certificate): The regular use of SSL explained above requires a CA-signed merchant certificate. This certificate is unnecessary, because the actual merchant authentication is performed during the payment cycle. A*nonymous* Diffie-Hellman mode of SSL [4] can be used instead. No certificates are needed in this mode. Merchant and consumer exchange their Diffie-Hellman public parameters without any signature on them. This mode helps them to decide on a secret encryption key, but does not provide any authentication. This is not a very big problem since actual authentication will be performed by MFI during payment authorization. Another known problem of this mode is being vulnerable to man-in-the-middle attacks where the attacker plays the role of merchant to consumer, and consumer to merchant. Although such an attack is still possible in our scheme, it

can eventually be detected since the attacker cannot continue its attack during the payment cycle. The security of the CONSEPP payment cycle is based on the signatures on the CONSEPP payment messages. Those signatures are created using previously generated private keys, so it is not possible for the attacker to obtain those keys during its man-in-the-middle attack. One may argue that an independent Diffie-Hellman protocol [13] could be used here instead of embedding it into SSL. That would help to save some overhead due to SSL headers. Although this argument is correct, SSL is still preferred since major browsers support it. Embedding an independent Diffie-Hellman protocol within the browsers would not be so easy.

3.4. Authorization request and response messages (AutReqObject and AutAckObject) in CONSEPP

AutReqObject and *AutAckObject* are not defined in X9.59 standard [5], but an annex of the standard explains how to use ISO 8583 messages' addenda records for these authorization messages in X9.59. As an X9.59 based protocol CONSEPP uses the same approach and it is briefly explained here.

Authorization request and response messages between merchant and MFI are parts of the existing payment system. Credit card transactions use ISO 8583 standard as the messaging standard for authorization messages. In order to use those messages in CONSEPP and X9.59, some extra fields, like the consumer's signature on *SigPayObject*, must be included in ISO 8583 authorization messages. ISO 8583 allows "addenda records" to add extra information to authorization messages. The extra information that must be sent to MFI via *AutReqObject* and the extra information that must be sent to merchant via *AutAckObject* can be embedded into these addenda records. In this way the existing interface between MFI and the merchant would not change significantly.

The solution for ACH-based transactions is not so different. Addenda records are also possible in ACH authorization messages. Therefore the extra CONSEPP fields that are not part of the existing ACH authorization messages could be sent/received in addenda records as in ISO 8583 messages.

AutReqObject can be signed by the merchant and *AutAckObject* can be signed by the MFI. These signed objects can be verified by the recipient since both merchant and MFI know each other's public key from the registration phase.

3.5. Merchant certificate problem and its solution

Although the basic idea of X9.59 is to get rid of the certificates and CAs, X.509 based merchant certificates are still referred to as merchant-to-consumer authentication method (*SigPayAckObject* in Figure 1) in the X9.59 standard [5]. Moreover, the FIs are referred to as CAs. It seems that a CA-based PKI would be necessary for merchant certificates, but the merchant certificate management is still obscure in [5]. We think that such a CA-based certificate mechanism does not conform to the "convenience" characteristic of the X9.59 model and the AADS idea. Here we propose an easy solution to the merchant certificate problem in CONSEPP.

Our aim in CONSEPP is to avoid certificates that are pre-generated by CAs, since the idea behind X9.59 is not to have individual CAs. We assumed that each consumer initially registers with a CFI. It is also assumed that they know the public keys of their CFIs.

First consumer includes a request for merchant's public key in *SigPayObject*. This request is transferred to MFI in *AutReqObject*. The merchant's public key is stored at the MFI's site. This public key is returned to consumer using *AutAckObject*, *SigPayAckObject* and the financial network's authorization messages. The protocol is explained below and depicted in Figure 2.

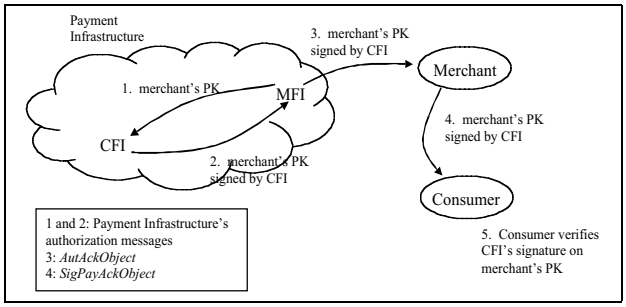

Figure 2. Merchant public key transfer

1. MFI sends the merchant's public key towards the CFI in addenda records of "existing" financial network authorization messages. Since the public key information travels along with the authorization request, no extra messaging rounds are necessary.
2. Upon receipt the merchant's public key, CFI signs it and returns the signed merchant's public key to MFI along with authorization response in the financial network.
3. MFI forwards the CFI-signed merchant's public key to merchant in *AutAckObject*.
4. Merchant forwards the signed public key to the consumer in *SigPayAckObject.* Merchant cannot alter the public key information since it is signed by the CFI.
5. Consumer verifies the signature over the merchant's public key using CFI's public key and, then, use merchant's public key to verify its signature on *SigPayAckObject* (of course the merchant's signature does not cover its public key information).

The method proposed for public-key transfer above does not require extra messages. Public key requests and actual public keys are piggybacked to CONSEPP and financial networks transaction messages. Public key information is transferred in "addenda records" of these existing messages.

Financial networks like ACH, VisaNet and BankNet have their own security, authentication and integrity mechanisms for existing payment authorization requests and responses among the FIs in the interchange protocol. Since the public key information is embedded in these authorization messages, authentication and integrity of the public key transmitted between CFI and MFI in this network are automatically provided. The merchant's public key is signed by CFI only for verification of this public key by the consumer.

There is no direct connection between CFI and MFI in the financial network. There is at least one transaction center to connect these two FIs. In some cases, there might be several transaction centers between them. We assume that the public key information passes through these transaction centers along with other authorization information.

3.6. Object contents

The CONSEPP extensions proposed in Sections 3.2 through 3.5 change the object contents of the basic payment cycle described in Section 3.1. The object contents after those extensions are depicted in Figure 3. Those extensions change only the content and processing of the objects; the flow remains unchanged. *AutReqObject* and *AutAckObject* fields are packed into standard authorization messages as explained in Section 3.4.

4. Advantages of CONSEPP

Consumers generally worry about the theft of their card or account numbers and refrain from using this sensitive information for electronic payments. Although it is possible to send the classical card or account numbers over an encrypted line, the merchant may not be able to hide this private information properly. CONSEPP eliminates the possibility of improper usage of the card and account numbers, because they are not used in CONSEPP transactions. CONSEPP uses specific PRCs instead of account and card numbers. PRCs cannot be used for some other purpose. A CONSEPP transaction that holds the PRC of a consumer must be digitally signed by the same consumer. Therefore, theft of PRC does not cause any problem.

There are three advantages of not having consumer certificates in CONSEPP:

1. There is no need for a CA-based PKI. Implementation of such a PKI would bring some extra cost to FIs and some inconveniences to consumers and merchants.

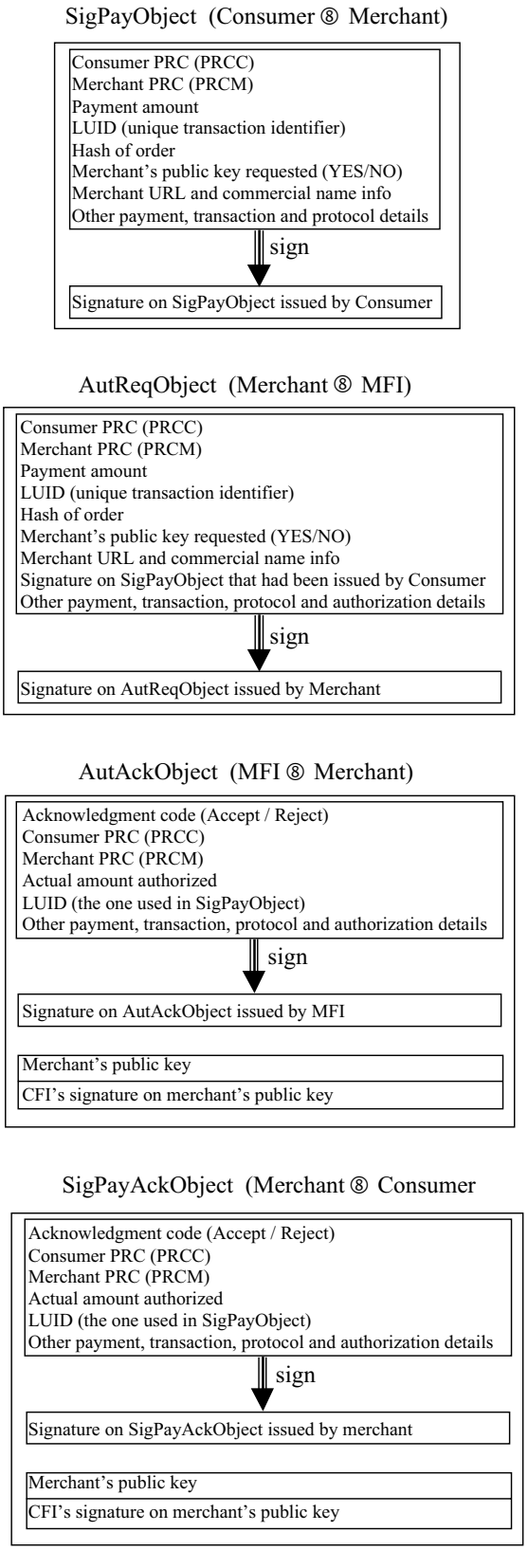

Figure 3. Object contents

2. A certificate revocation mechanism must be implemented for CA-based PKIs in order to check the validity of unexpired certificates. Verifiers must contact an online validation server or periodically download validity lists for revocation control. However, in CONSEPP, there is no such inconvenience for certificate revocation. If the consumer's public key must be revoked or changed, the account records that are held at the CFI's site can be updated. The verifiers should not take any action for revocation control.
3. Certificate-based systems are often criticized since they carry some private information via certificates. In CONSEPP, no private information, such as the name, birth date, account number are revealed to a third party (i.e. merchant), since there are no classical certificates. This protects the consumer's privacy.

CONSEPP offers strong protection against consumer transaction repudiation. This is a very important problem in payment systems that use conventional cards. Merchants are responsible for verifying the consumer's authenticity in these systems. If the merchant does not receive a strong evidence, such as a signature, from the consumer, then the consumer can deny initiating the transaction and the merchant faces a charge-back. On the contrary, in CONSEPP, the merchants are not responsible for authenticating the consumers; CFIs authenticate the consumers by verifying the consumer signature on *SigPayObject*. This signature is created by consumer using his/her public key[1], which is supposed to be known only by the consumer. Since the CFI keeps the consumer's correct public key in its records, this verification serves as strong evidence for the initiation of the transaction by the claimed consumer. The consumer can still dispute it by claiming that his/her private key or the password that is used to unlock the private key is stolen, but this is an issue between the consumer and its CFI. Merchant is not responsible for the outcomes of such a consumer dispute, so its charge-back cost is reduced to zero.

The above advantages result from the characteristics of X9.59 standard. The special CONSEPP extensions over X9.59 that have been explained in Sections 3.2 through 3.5 provide extra flexibility. The proposed secure shopping experience method makes use of common SSL technology, but bypasses its trusted certificate requirements. This method allows merchant authentication to be done by MFI with no significant extra cost.

[1] Since a private key is a long and hard-to-remember string, in practice it is cryptograhically locked using a password, and the key holder uses this password to unlock it when he/she wants to issue a digital signature.

The model that is proposed for merchant public key transfer in Section 3.5 eliminates the need for merchant certificates. This feature uses the existing authorization message rounds and does not put a significant cost on the FIs, merchant and consumer.

Elimination of both consumer and merchant certificates makes CONSEPP totally certificate/CA-free. This is a very important advantage of CONSEPP, since having no CA-based PKI results in fast, cheap and simple transactions.

Cryptographic burden on consumer is minimal in CONSEPP. Excluding the shopping experience, consumer should generate only one (for *SigPayObject*) and verify two digital signatures (one is to learn the merchant's public key, the other is to verify *SigPayAckObject*) for payment processing. Most of the advantages described above also have efficiency improvement aspects. For examples:

- Consumer should not spend time to verify a chain of certificates to find out merchant's public key; only one signature verification is sufficient for this.
- Since no CA-based PKI exists in CONSEPP, there is no need to spend time for certificate revocation control.
- Having no encryption in the payment part of CONSEPP is another speed-up factor.

Secure shopping experience method described in Section 3.3 requires some encryption. However encryption is a standard approach for all e-payment protocols that require confidentiality during shopping experience; CONSEPP does not create an extra burden that does not exist in its rivals. Moreover, an encrypted shopping experience is not a prerequisite for the rest (actual payment part) of the protocol. Consumers may prefer not to have an encrypted shopping experience due to performance concerns.

5. Discussion

Both merchant and consumer should register with their FIs before taking place in CONSEPP. This registration should be offline, because he/she must sign a contract and prove his/her identity. On the other hand, if an FI already knows its customer, it may establish an online agreement page and get the customer's approval by clicking on a "I accept" button at the end of the "terms and conditions". However, it would be difficult for the FI to prove the existence of such an agreement if its customer denies it.

Initial merchant/consumer key generation and distribution can be performed in two different ways.

1. Key pairs may be created by the FIs. Consumers/merchants get their private keys within smart cards issued by their FIs. They may also obtain soft versions of their private keys in order to use it in a computer without a smart card reader.
2. Consumer/merchant may run a program to create a set of keys and send (or take) the public key to FI. Private key may be kept by the owner and be used in software.

The first method is more convenient, but the possibility of FI's access to the private key during its generation may raise some security concerns. The FIs must act honestly and carefully here.

Since the CFI acts as a trusted authority to resolve possible disputes raised by the consumer, the consumer must assign the CFI as a proxy for dispute resolution a priori. This fact may be included in the contract between the consumer and CFI. Moreover, the local laws must endorse such a role to CFI.

CFI or its agent should always be online in order to provide proper service. This is not only for CFI's signature verification responsibility, but also for fund authorization. Indeed such a requirement is not new for payment mechanisms. Traditional authorization responsibility compels the financial institutions to be online all the time. Therefore, signature verification does not cause an extra burden of being online.

6. Conclusions

We proposed a new Internet e-payment system, called CONSEPP (CONvenient and Secure E-Payment Protocol) based on ANSI X9.59 standard [5]. Our aim was to balance the security and convenience features. CONSEPP minimally changes the existing payment infrastructure and business models, thus it is convenient. Moreover, CONSEPP has enough authentication, integrity and confidentiality features to support security.

CONSEPP inherits the basic idea of X9.59, which is to use the Consumer's Financial Institution (CFI), instead of the merchant, to verify the consumer's signature over the payment request. The ultimate aim is to get rid of the need for consumer certificate. However, X9.59 still needs merchant certificates. In CONSEPP we proposed a dynamic and convenient method to transfer merchant's current public key to the consumer using existing authorization messages and payment infrastructure. This does away with the need for merchant certificates. In this way CONSEPP becomes a CA/certificate-free protocol. This results in faster and less costly payment transactions.

X9.59 standard does not rule out encryption, but does not include it in the standard. CONSEPP does not include encryption for the payment messages either. In case of a need for optional encryption and anonymous data transfer between consumer and merchant, a third party anonymizer/privacy wrapper or an extension of SSL protocol could be used.

Acknowledgments

This work is supported by rTrust Technologies. The authors are grateful to Behzad Sadeghi, Anne and Lynn Wheeler and anonymous referees for their valuable comments.

References

[1] CyberCash Inc., http://www.cybercash.com/

[2] P. Wayner, *Digital Cash: Commerce on the Net*, 2nd Edition, Morgan Kaufmann Publishers, March 1997.

[3] MasterCard Inc., *SET Secure Electronic Transaction Specification, Book 1: Business Description*, MasterCard Inc., May 1997.

[4] A. O. Freier, P. Karlton, and P. C. Kocher, *The SSL Protocol Version 3*, Netscape Communications Corp., 1996, available from http://home.netscape.com/eng/ssl3

[5] American National Standard DSTU X9.59, *Electronic Commerce for Financial Services Industry: Account Based Secure Payment Objects*, 2000.

[6] A. Wheeler, and L. Wheeler, *Payment, Security & Internet References*, http://www.garlic.com/~lynn/

[7] ISO 8583, *Financial Transaction Card Originated Messages – Interchange Message Specifications*, 1993

[8] NACHA - The Electronic Payments Association, http://www.nacha.org

[9] ITU-T Recommendation X.509, ISO/IEC 9594-8, *Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks*, 2000 (fourth) edition.

[10] Visa International, http://www.visa.com

[11] Mastercard International, http://www.mastercard.com

[12] Zaxus Limited, http://www.zaxus.com

[13] W. Diffie, and M. E. Hellman, New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644-654, November 1976.