ELSEVIER

Computer Standards & Interfaces 23 (2001) 367–381

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Integrating SET and EDI for secure healthcare commerce

Duen-Ren Liu *, I-Chin Wu, Sung-Ting Hsieh

Institute of Information Management, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan

Received 19 February 2001; received in revised form 22 March 2001; accepted 20 July 2001

Abstract

Different from conventional online goods purchases, healthcare commerce, such as purchasing prescription drugs, involves transaction steps of insurance coverage inquiries which are required to determine insurance coverage and payments. Without efficient processing of online insurance coverage inquiries, the online healthcare commerce cannot be carried out successfully. This work proposes a novel secure healthcare commerce protocol that incorporates the insurance coverage inquiries into the transaction steps of online purchases. The proposed protocol is designed based on the Secure Electronic Transaction (SET) and healthcare Electronic Data Interchange (EDI). Efficient ASC X12N interactive EDI messages are adopted to facilitate online real-time interactions of insurance coverage inquiries. The results have shown that the process of healthcare commerce is streamlined by integrating secure online purchases and online EDI interactions.

Keywords: Secure electronic transaction; EDI; Healthcare commerce; Information security

1. Introduction

The computerization of healthcare information has improved the efficiency and quality of healthcare management. Management costs have also been reduced since a tremendous amount of data is now processed and transmitted via computers, including medical insurance claims, medicine purchase orders and payments for prescription drugs. Moreover, the popularity of the Internet and advances in information technology have made Internet access to healthcare information an inexorable trend. Healthcare organizations are enabling online healthcare transactions on the Internet [8]. However, the open environment of the Internet makes data security and patient privacy crucial. The healthcare commerce needs to provide secure transactions.

This work considers the following network-based healthcare commerce transaction scenarios—Patients purchase prescription drugs and make payments to hospitals or pharmacies on the Internet. The conventional online (goods) purchase mainly adopts Secure Electronic Transaction (SET) [21] to conduct online interactions among the customer, merchant, credit card issuer and acquiring bank. Unlike in traditional online purchases, the purchase order of prescription drugs is determined by doctors' prescriptions. Furthermore, the amount of a payment should be determined based on the patient's insurance coverage. As a result, the pharmacy (hospital) and the insurance company need to exchange insurance benefit inquiries and responses. Such requirements necessitate the healthcare commerce (e.g., prescription drug purchases) to adopting healthcare Electronic Data Inter-

* Corresponding author. Tel.: +886-3-572-3792; fax: +886-3-571-2121.

E-mail address: dliu@iim.nctu.edu.tw (D.-R. Liu).

0920-5489/01/$ - see front matter
PII: S0920-5489(01)00088-5

change (EDI) to process the insurance coverage inquiry. Consequently, healthcare commerce not only includes online interactions as those in conventional online purchases, but also additional online *EDI interactions* (i.e., data interchange via EDI standards) required to determine the purchase. The main participants in such healthcare commerce include the patient, pharmacy, hospital, insurance company, credit card issuer and acquiring bank. The participants' roles in healthcare commerce are more complicated than in the conventional online purchases. The result is more complex transaction interactions in the prescription drug purchases.

This work proposes a novel secure healthcare commerce protocol that can be applied to healthcare environments to support online healthcare commerce, such as online purchases of prescription drugs. The proposed protocol is capable of integrating the processing of online purchases and online EDI interactions. This integration is necessary for online insurance coverage inquiries to determine the payment amount. Notably, without integrating online purchases and insurance coverage inquiries, the patient needs to pay the pharmacy full price without any deduction, and then files a claim application to the insurance company. The process of healthcare commerce (e.g., purchasing prescription drugs) consists of two separate transactions—the online purchase and the claim application. This results in inconvenience for the patient, since the patient needs to conduct two separate transactions. In contrast, by integrating online purchases and insurance coverage inquiries, the whole process of healthcare commerce is streamlined. The patient only needs to conduct one transaction.

Furthermore, if the integration is ineffective to support real-time interactive processing, the online healthcare commerce may fail due to long waiting time on insurance coverage inquiries. Herein, we adopt the SET protocol and healthcare EDI to design the proposed protocol. Security technologies and the approach of SET are employed to ensure secure transactions of healthcare commerce. Moreover, the interactive healthcare EDI messages, which are designed by ASC X12N for real-time interactive processing [1], are used to facilitate online real-time transaction interactions. Adopting interactive EDI enables effective integration of online purchases and online insurance coverage inquiries. The proposed protocol extends online purchases to include online EDI interactions for supporting secure and effective online healthcare commerce.

1.1. Related work

The privacy and security aspects of healthcare information are important issues [12,17,23–25]. To protect personal healthcare information and ensure secure access, user authentication and data encryption are needed to provide secure transactions. Section 2 illustrates some relevant security technologies, including encryption methods, digital signatures and digital certificates. The developments of healthcare EDI standards for healthcare systems have been discussed [5,14]. Those work mainly focus on information interchange among organizations without considering how to support online purchases for patients. In addition, a smart card and IP-based healthcare system infrastructure has been proposed to support insurance-related procedures [22]. However, the issues of integrating online purchases with EDI interactions are not addressed. Furthermore, various Internet payment systems have been proposed [6,15,16,21]. Credit card payment systems extend general credit card transactions to make secure transactions on the Internet, including SET [21], CyberCash [6], etc. SET was originally developed by the international credit card organizations, VISA and MasterCard. Enhancements to the basic protocol have also been suggested [11].

Two main open technical standards for EDI exist [7], namely ANSI ASC X12, proposed by the American National Standards Institute (ANSI), and EDIFACT, which is adopted by the United Nations (UN). The popular EDI standards in healthcare include ANSI X12N [10], used in North America, and Technical Committee 251 (TC 251) [9], promoted by the European Standardization Committee (CEN). ANSI X12N, a subcommittee of X12, is responsible for establishing standards for medical insurance EDI, and CEN TC251 also defines EDI standards for healthcare. The Internet healthcare commerce protocol proposed herein is based on SET, while the interchange of healthcare information is based on ANSI X12N EDI.

The rest of this paper is organized as follows. Section 3 describes SET in detail. Meanwhile, Section 4 illustrates ANSI X12N in greater depth. Next, Section 5 presents a healthcare commerce protocol that integrates Secure Electronic Transactions and healthcare EDI, while Section 6 outlines a prototype system to demonstrate that the process of healthcare commerce is streamlined via integrating online purchases and online EDI interactions among organizations. The work presented in Sections 5 and 6 supplements the standards by providing a useful application of the integration of SET and healthcare EDI. Section 7 then discusses the merits of the proposed healthcare commerce protocol, while possible future research directions are finally pointed out in Section 8.

2. Security technology

Two major approaches to encryption are symmetric cryptography (such as DES and IDEA) and asymmetric cryptography (such as RSA) [20]. Symmetric cryptography uses a single key to encrypt and decrypt the message, while asymmetric cryptography, also known as public key cryptography, uses a pair of keys comprising of a public and private key. The message encrypted with the public key (private key) can only be decrypted with the corresponding private key (public key). The digital signature approach [18,20] uses public key cryptography to encrypt and decrypt the message digest, as follows: The sender uses a one-way hash function to generate a message digest and then encrypts the message digest by using the sender's private key to generate a digital signature. Upon receiving the digital signature (encrypted message digest) and the message, the recipient can obtain the received message digest by using the sender's public key to decrypt the digital signature. By using the same hash function the recipient can also generate a message digest for the received message. If the two message digests are identical, the recipient is ensured that the message really does originate from the sender. Digital signatures can be used to achieve authentication, integrity and non-repudiation [20]. The dual signature approach [21], digitally signing two related messages with a single signature, is similar to the digital signature approach except that two message digests are concatenated for signing together. The dual signature approach uses similar methods as those of the digital signature approach to match digests and authenticate dual-signed messages.

Symmetric cryptography is generally used to encrypt and decrypt message transmitted via the Internet. The digital envelope approach [20] uses a symmetric key to encrypt the message and then uses the recipient's public key to encrypt the symmetric key. The encrypted key is sent to the recipient along with the encrypted message. The recipient uses his own private key to decrypt the encrypted symmetric key, then uses the symmetric key to decrypt the encrypted message. The ITU-T proposed X.509 protocol [13] uses public key certificates to convey a subject's public-key information along with his (the subject's) identity information. User authentication and digital signatures can, thus, be conducted on the basis of the X.509 public key certificates.

3. Secure Electronic Transaction

SET accomplishes transactions by exchanging purchase and payment information online, along with fund transfers between banks. Fig. 1 shows the participants in SET. The Cardholder is a customer with a legal credit card issued by the Issuer, while the Issuer is the financial institution that issued an account and a credit card to a Cardholder. Meanwhile, the Merchant is the store that accepts the credit card issued by the Issuer, and the Acquirer is the financial institute that cooperates with the Merchant.

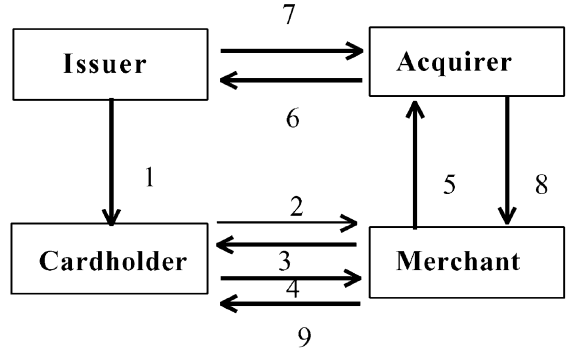


Fig. 1. Transaction interactions in SET [21].

SET uses the digital envelope to ensure data confidentiality and uses the digital signature to verify data integrity. Identity authentication and non-repudiation is accomplished by using the digital signature and certificates issued by the Certificate Authority (CA). The dual digital signature is used to ensure that the Merchant cannot obtain the Cardholder's payment instructions, but can verify the linkage between the order information and payment instruction [21].

The steps of transaction interactions in SET are the following [21].

(1) The issuer issues a credit card to the Cardholder.

(2) The Cardholder sends an initial request to the Merchant.

(3) The Merchant generates a response message, digitally signs it and then sends it along with public key certificates of the Merchant and Acquirer to the Cardholder.

(4) The Cardholder creates the Order Information (OI) and Payment Instruction (PI). The transaction identifier assigned by the Merchant is placed in the OI and PI to link the OI and PI together. Notably, the OI does not contain the order data (e.g., description of goods). The Cardholder then transmits its certificate along with the following messages to the Merchant: OI, a digest of PI, a dual signature of OI and PI, encrypted cardholder credit card number (CreditCNo) and a digital envelope of payment information for the Acquirer. The payment information comprises PI, digest of OI and the dual signature of OI and PI. Notably, the CreditCNo and the symmetric key used to encrypt the payment information are encrypted via using the Acquirer's public key.

(5) The Merchant verifies the integrity of the dual signature on OI. The Merchant generates an authorization request message, digitally signs it and then sends it along with the certificate of the Merchant to the Acquirer. The following messages received from the Cardholder are also forwarded to the Acquirer for payment authorization: the certificate of the Cardholder, encrypted CreditCNo and the digital envelope of payment information.

(6) The Acquirer obtains the authorization request message and verifies the Merchant's signature. The Acquirer then decrypts the digital envelope to obtain PI, the digest of OI and the dual signature of OI and PI; verifies the integrity of the dual signature on PI; and decrypts the encrypted CreditCNo of the Cardholder. Finally, the Acquirer transmits the Cardholder's data to the Issuer to confirm the Cardholder's identification, expiration date and credit line.

(7) The Issuer confirms the verification and notifies the Acquirer.

(8) The Acquirer generates and digitally signs an authorization response message and then transmits it to the Merchant.

(9) The Merchant obtains the authorization response message and verifies the Acquirer's signature. The Merchant then generates and digitally signs an order response message and transmits it to the Cardholder. If the authorization is correct, the Merchant can proceed to deliver the ordered merchandise to the Cardholder.

4. Healthcare EDI

ASC X12N [10] defines standards for the format of healthcare messages to be exchanged between a Provider and a Payer. A provider is a hospital, medical institution or pharmacy that provides healthcare treatment services, while a Payer is an organization (e.g., an insurance company) which administrates and provides insurance coverage. The 837 Health Care Claim [2] is used by the Provider to issue healthcare claim billing to the Payer. The Payer uses the 835 Health Care Claim Payment/Advice [4] to conduct Electronic Fund Transfer (EFT) transactions. Meanwhile, the Provider uses the 270 Health Care Eligibility/Benefit Inquiry [3] to query patients' insurance coverage for benefits. Payers use the 271 Health Care Eligibility/Benefit Information [3] to reply to the Provider's inquiry. Generally, the 837 and 835 transaction sets are processed in a batch mode, while the 270 and 271 transaction sets can be used with processing in a batch mode or online processing in a real-time environment.

ASC X12N transmits information using the interchange envelope. Every interchange envelope is composed of several functional groups, and every functional group is composed of similar transaction sets. Every transaction set comprises several segments. Each segment consists of multiple data elements to convey predefined information regarding

the ASC X12N transaction set, such as 270/271/837/835. For example, the NM1 segment defines the type of entity, name and identification code. The EQ (Eligibility or Benefit Inquiry) segment in 270 specifies the detail of the eligibility/benefit inquiry, while the EB (Eligibility or Benefit Information) segment in 271 conveys the service and the coverage of benefits being inquired upon. ASC X12N implementation guides describe detailed formats and fields for the implementation of 270/271 and 835/837 [2–4].

To support real-time interactive processing requirements, ASC X12N has also developed the following interactive UN/EDIFACT message standards, Interactive Health Care Eligibility/Benefit Inquiry (IHCEBI) and Interactive Health Care Eligibility/Benefit Response (IHCEBR) [1]. The IHCEBI is used to inquire the eligibility/benefit information and the IHCEBR is used to respond with the inquiry. The IHCEBR conveys detailed information regarding the benefits, copayments, deductible amounts, limitations, remaining visits, etc. The IHCEBI/IHCEBR generates shorter messages by using a single conversation identifier for ongoing messages instead of including identifying data with each message. As a result, the IHCEBI and IHCEBR are more efficient transaction sets for interactive processing. The 270/271 can also be used interactively, but more information will need to be exchanged. Both the 270/271 and IHCEBI/IHCEBR support the functional capability of allowing the Pharmacy to inquire the benefit information of the insured (patient). They both are suitable to support effective integration with SET and can be adopted to design the proposed healthcare commerce protocol. Owing to that IHCEBI and IHCEBR are more efficient than 270 and 271, we adopt them to design the proposed protocol.

The IHCEBI and IHCEBR were developed to accommodate interactive processing according to the UN/EDIFACT interactive message design guideline [1]. The IHCEBI/IHCEBR message is embedded in a message structure as follows, UIB UIH IHCEBI/IHCEBR UIT UIZ. The UIB and UIZ are the interchange header and trailer, respectively, while the UIH and UIT are the interactive message header and trailer, respectively. Table 1 describes the general information content of some of the IHCEBI and IHCEBR segments. See the ASC X12N IHCEBI/IHCEBR implementation guide for more information [1].

The Eligibility Request (ELR) segment in IHCEBI (EQ segment in 270) specifies the inquired eligibility or benefit information in regard to the classification of service (service type) and benefit coverage level of the insured. The Eligibility Response (ELG) segment in IHCEBR (EB segment in 271) supplies eligibility/benefit information and is composed of several data elements, including eligibility status/benefit category, benefit coverage level, service type, benefit amount, benefit percentage, etc. Various benefit categories are defined, including active coverage, inactive, copayment, deductible, unlimited, etc. The benefit coverage level indicates the level of coverage, such as “family”, “individual” or “employee only”, being provided for the insured. Meanwhile, the service type represents the category of healthcare service, including medical care, surgical,

Table 1
The IHCEBI and IHCEBR segments [1]

Segment	Description
MSP (Message purpose)	Identifies the message—e.g., a request for IHCEBI or a response for IHCEBR; specifies a unique message reference number to provide the linkage of IHCEBR and IHCEBI
PVD (Provider)	Supplies the information about the provider submitting inquiry
SUB (Subscriber)	Specifies information about the health plan subscriber
PTT (Patient)	Identifies the patient if the individual is different from the subscriber in SUB
ELR (Eligibility request)	Specifies the detail of eligibility/benefit inquiry (only in IHCEBI)
ELG (Eligibility response)	Provides specific eligibility or benefit response information—e.g., copayment, deductible (only in IHCEBR)
PVD/SUB/PTT could be omitted from IHCEBR if the information is the same as was on the IHCEBI.	

dental care, hospital, pharmacy, mail order prescription drug, generic prescription drug, etc. For example, the ELG segments may supply that the benefit information of the insured is active coverage with family coverage level under the dental care service, while the amount of copayment for pharmacy service is 10 dollars.

5. Healthcare commerce protocol

The proposed Internet-based healthcare commerce protocol can deal with the following transactions. (1) Patient purchases of prescription drugs and payments to the Pharmacy. (2) Pharmacy inquiries to the insurance company (Insurer) to obtain information of the patient's insurance coverage and healthcare billing claims. Notably, we use "Pharmacy" to denote a pharmacy or a hospital with a pharmacy department.

The proposed protocol adopts SET to provide secure purchase transactions. The efficient ASC X12N IHCEBI/IHCEBR messages are adopted to enable the integration with SET to support real-time message exchanges between the Pharmacy and the Insurer. This integration is necessary for online insurance coverage inquiries to determine the payment amount. The protocol can also integrates with ASC X12N 835/837 sets to conduct the transactions of healthcare payment claims and electronic fund transfers as the following. The Pharmacy sends a healthcare claim request, encoded using 837, to bill the Insurer for the healthcare claim. The Insurer makes the actual transfer of funds for the healthcare payment via using 835 ERA (Electronic Remittance Advice), EFT and FDN (Funds Deposit Notification) [4]. The 837 and 835 are processed in a batch mode. The batch process is not our focus and, thus, the detailed discussion of 835/837 is omitted from this paper.

Verification of doctor's prescriptions: Prescription drug purchases are regulated by prescriptions digitally signed by doctors. The situation differs from general goods purchases, where customers make the decisions. The Pharmacy needs to determine the purchased prescription drugs based on the digitally signed prescriptions (i.e., doctor's prescriptions and digital signatures). Moreover, the prescription itself must be verified with the digital signature to confirm its integrity and authenticity. Various scenarios are possible to convey the digitally signed prescriptions to the Pharmacy. One possible scenario is that the Patient uses a smart/healthcare card to store the digitally signed prescriptions. The digitally signed prescriptions can then be retrieved from the smart/health card and transmitted to the Pharmacy during online interactions. The other scenario is that the digitally signed prescriptions are stored in the Hospital. The Patient requests the digitally signed prescriptions from the Hospital and then transmits them to the Pharmacy, while the alternative is for the Pharmacy to obtain proof of authorization from the Patient to request the digitally signed prescriptions from the Hospital.

Overview of healthcare commerce protocol: The protocol contains six phases: initial transaction request, prescription verification, payment determination, purchase request, payment authorization and purchase confirmation. The *prescription verification phase* mainly involves steps to acquire and verify the digitally signed prescriptions and determine the order list of prescription drugs. After deciding the list of prescription items, *payment determination phase* is conducted through online interactions with the Insurer to acquire the Patient's insurance coverage. During the *purchase request phase*, the Patient places orders according to the prescription drug and payment information supplied by the Pharmacy. The Patient then transmits order information and payment instructions to the Pharmacy. Next, the *payment authorization phase* includes steps to request payment authorization according to the Patient's payment instructions and encrypted credit card number. The Acquirer then communicates with the Patient's Issuer to verify the Patient's identity, expiration date and credit line and, thus, decides whether or not to authorize payment. Finally, the Patient's purchase is confirmed in the *purchase confirmation phase*.

Table 2 lists security functions defined herein that are necessary to clearly and concisely explain the proposed transaction protocol. The protocol uses the digital envelope to ensure data confidentiality and uses the digital signature to verify data integrity. Meanwhile, identity authentication and non-repudiation of origin is accomplished by using the digital signature and public key certificates.

Table 2
Explanation of security functions

$Cert_{Role}$: Role's Public key certificate.
Digest(M): Generates a message digest of M through a one-way hash function.
Encr(M,K): Encrypts message M with key K.
DigSig(M,SK_{Sender}): Generates Digest(M) and then encrypts Digest(M) with *Sender*'s private key SK_{Sender}, i.e., Encr(Digest(M),SK_{Sender}).
VerifyDigS(DigSig(M,SK_{Sender}),M,PK_{Sender}): Uses *Sender*'s public key PK_{Sender} to decrypt the signature DigSig(M,SK_{Sender}) and obtain Digest(M); then applies the same hash function to generate a message digest using the received message M. If the two message digests are identical, *Recipient* can ensure that message M really originates from *Sender*.
DigEnv(M,$PK_{Recipient}$): Message M is encrypted using a randomly generated symmetric encryption key K_i to generate a cipher text E_i; and a digital envelope D_i is created by using *Recipient*'s public key to encrypt the symmetric key K_i. The function returns both E_i and D_i, where $E_i = Encr(M,K_i)$ and $D_i = Encr(K_i,PK_{Recipient})$.
DecrDigEnv(DigEnv(M,$PK_{Recipient}$),$SK_{Recipient}$): *Recipient* decrypts the digital envelope D_i by using *Recipient*'s private key to obtain the randomly generated symmetric key K_i; and then uses the key K_i to decrypt the cipher text E_i and obtain the original message M.
DualSig(M_1,M_2,SK_{Sender}): Generates Digest(M_1) and Digest(M_2); generates the dual digest, Digest(Digest(M_1) · Digest(M_2)); and encrypts the result dual digest with *Sender*'s private key SK_{Sender}, i.e., Encr(Digest(Digest(M_1) · Digest(M_2)),SK_{Sender}).
VerifyDualS(DualSig(M_1,M_2,SK_{Sender}),M_1,Digest(M_2),PK_{Sender}): Uses *Sender*'s public key PK_{Sender} to decrypt the dual signature DualSig(M_1,M_2,SK_{Sender}) to obtain Digest(Digest(M_1) · Digest(M_2)); applies the same hash function to generate a dual digest using the received message M_1 and Digest(M_2). If the two dual digests are identical, *Recipient* can ensure that message M_1 really originates from *Sender*.

5.1. Transaction steps of the protocol

The transaction scenario involves the Patient, Pharmacy, Hospital, Issuer, Acquirer and Insurer. During the transaction, the Pharmacy issues an inquiry regarding the Patient's insurance coverage to the Insurer to determine the amount of payment due for Patient. In the protocol presented herein, the inquiry and reply for insurance coverage information are conducted by deploying healthcare EDI (ASC X12N IHCEBI/IHCEBR) to exchange messages between the Pharmacy and Insurer. To make a concise discussion of the protocol, the doctor's prescriptions and digital signatures are assumed herein to be stored on the smart/health card. The protocol can also be easily modified to handle the scenario in which the digitally signed prescriptions are stored in the Hospital. Section 5.3 presents two alternatives to acquire digitally signed prescriptions stored in the Hospital. Fig. 2 illustrates the transaction steps of the protocol.

Step 1. The Patient carries the smart/health card containing doctor's prescriptions and digital signatures.

5.1.1. Initial transaction request phase

Step 2. The Patient sends an initial transaction request to the Pharmacy.

Step 3. The Pharmacy generates a response message Resp and digitally signs it. The Pharmacy then sends the message, DigSig(Resp,$SK_{Pharmacy}$) along with the public key certificates, $Cert_{Pharmacy}$ and $Cert_{Acquirer}$ to the Patient.

Step 4. The Patient verifies the public key certificates.

5.1.2. Prescription verification phase

To determine the order list of prescription drugs, the Pharmacy must obtain and verify the digitally signed prescription. In this transaction scenario, the prescription and the digital signature of the Hospital

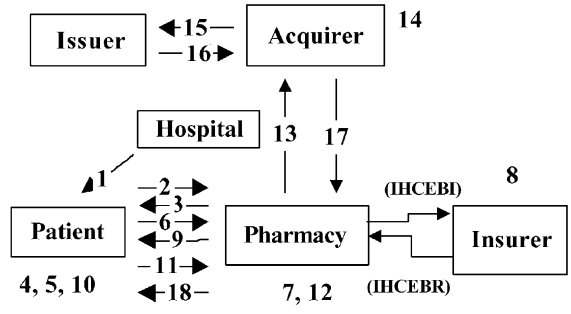


Fig. 2. Healthcare transactions involving online EDI interactions with the Insurer.

are stored on the smart/health card. The Patient sends the digitally signed prescription to the Pharmacy. Upon receiving the digitally signed prescription, the Pharmacy uses the Hospital's public key to verify the integrity and authenticity of the prescription. The prescription verification phase involves Steps 5 to 7, as described below.

Step 5. The Patient retrieves the doctor's prescription Prescr and digital signature DigSig(Prescr, $SK_{Hospital}$) from the smart/health card. The Patient generates an InsurInfo message consisting of the identification of the Insurer as well as the identifications (including member ID no.) of the Patient and the subscriber of the insurance plan.

Step 6. The Patient generates the digital envelope DigEnv([Prescr,DigSig(Prescr,$SK_{Hospital}$),InsurInfo], $PK_{Pharmacy}$) and then sends it to the Pharmacy, along with the public key certificates $Cert_{Patient}$ and $Cert_{Hospital}$.

Step 7. The Pharmacy verifies public key certificates $Cert_{Patient}$ and $Cert_{Hospital}$. The Pharmacy decrypts the digital envelope by DecrDigEnv(DigEnv([Prescr,DigSig(Prescr,$SK_{Hospital}$),InsurInfo], $PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain Prescr, DigSig (Prescr,$SK_{Hospital}$) and InsurInfo, and then the Pharmacy verifies the Hospital's signature by VerifyDigS(DigSig(Prescr,$SK_{Hospital}$),Prescr,$PK_{Hospital}$) to ascertain the integrity of the prescription.

5.1.3. Payment determination phase

Upon obtaining the list of prescription drugs, the Pharmacy determines the payment due from the Patient based on the Patient's insurance coverage information. In this transaction scenario, the Pharmacy interacts online with the Insurer to obtain benefit information on the Patient's insurance coverage.

Step 8. The Pharmacy makes an inquiry to the Insurer to obtain the Patient's benefit information. The IHCEBI and IHCEBR messages are exchanged between the Pharmacy and Insurer to inquire and reply benefit information. The messages are transmitted via using the digital envelope approach to ensure data security. Detailed explanations of Step 8 are presented in Section 5.2.

Step 9. Based on the prescription Prescr and the Patient's benefit information, the Pharmacy generates prescription information PresInfo, including a list of prescription drugs and the payment due. The Pharmacy then digitally signs the PresInfo and sends the digital envelope DigEnv([PresInfo,DigSig(PresInfo,$SK_{Pharmacy}$)],$PK_{Patient}$) to the Patient.

5.1.4. Purchase request phase

The Patient makes purchase request according to the list of prescription drugs and the payment details included in the prescription information. The order information is sent to the Pharmacy, while the payment instructions and encrypted credit card number are forwarded to the Acquirer for payment authorization. Notably, the order information and payment instruction is dual signed using the Patient's private key. The purchase request phase comprises Steps 10 and 11.

Step 10. The Patient decrypts the digital envelope by DecrDigEnv(DigEnv([PresInfo,DigSig(PresInfo, $SK_{Pharmacy}$)],$PK_{Patient}$),$SK_{Patient}$) to obtain PresInfo and verifies the Pharmacy's signature by VerifyDigS (DigSig(PresInfo,$SK_{Pharmacy}$),PresInfo,$PK_{Pharmacy}$).

Step 11. The Patient creates the Order Information (OI) and Payment Instruction (PI) based on the received PresInfo. The Patient then generates a dual signature, DualSig(OI,PI,$SK_{Patient}$), and encrypts the Patient credit card number by using the Acquirer's public key, Encr(CreditCNo,$PK_{Acquirer}$). Finally, the following order-transaction (OrderTrans) information is transmitted to the Pharmacy: DigEnv([OI, Digest(PI), DualSig(OI, PI, $SK_{Patient}$)], $PK_{Pharmacy}$), DigEnv ([Digest(OI), PI, DualSig(OI, PI, $SK_{Patient}$)], $PK_{Acquirer}$), Encr(CreditCNo,$PK_{Acquirer}$).

5.1.5. Payment authorization phase

The Pharmacy verifies the Patient's order information and requests the Acquirer for payment authorization, as described below. The dual signature allows the Pharmacy to verify the linkage between the order information and payment instruction without having to know the Patient's payment instruction. The Pharmacy then requests the Acquirer for payment authorization by providing the Patient's payment instruction and encrypted credit card number. Next, the Acquirer interacts with the Patient's Issuer to verify the Patient's identification, expiration date and credit line and, finally, the result of payment authorization verification is transmitted to the Phar-

macy. The payment authorization phase comprises Steps 12 to 17.

Step 12. The Pharmacy decrypts the digital envelope by DecrDigEnv(DigEnv([OI,Digest(PI),DualSig(OI,PI,$SK_{Patient}$)],$PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain OI, Digest(PI), DualSig(OI,PI,$SK_{Patient}$) and then verifies the integrity of the dual signature of OI by VerifyDualS(DualSig(OI,PI,$SK_{Patient}$),OI,Digest(PI), $PK_{Patient}$). The Pharmacy generates an authorization request message, AuthReq and digitally signs it by DigSig(AuthReq,$SK_{Pharmacy}$).

Step 13. The Pharmacy generates DigEnv ([AuthReq,DigSig(AuthReq,$SK_{Pharmacy}$)],$PK_{Acquirer}$) and transmits the following payment-transaction (PaymentTrans) information to the Acquirer: DigEnv ([AuthReq,DigSig(AuthReq,$SK_{Pharmacy}$)],$PK_{Acquirer}$), $Cert_{Patient}$, $Cert_{Pharmacy}$, Encr(CreditCNo,$PK_{Acquirer}$), and DigEnv([Digest(OI),PI,DualSig(OI,PI,$SK_{Patient}$)], $PK_{Acquirer}$).

Step 14. The Acquirer decrypts the digital envelope via DecrDigEnv(DigEnv([AuthReq,DigSig (AuthReq,$SK_{Pharmacy}$)],$PK_{Acquirer}$),$SK_{Acquirer}$) to obtain the authorization request message and verifies the Pharmacy's signature via VerifyDigS(DigSig (AuthReq,$SK_{Pharmacy}$),AuthReq,$PK_{Pharmacy}$). The Acquirer then decrypts the digital envelope using DecrDigEnv(DigEnv([Digest(OI),PI,DualSig(OI,PI, $SK_{Patient}$)],$PK_{Acquirer}$),$SK_{Acquirer}$) to obtain PI, Digest(OI), DualSig(OI,PI,$SK_{Patient}$); verifies the integrity of PI by VerifyDualS(DualSig(OI,PI, $SK_{Patient}$),PI,Digest(OI),$PK_{Patient}$); and uses the private key of the Acquirer to decrypt the encrypted CreditCNo of the Patient.

Step 15. The Acquirer transmits the Patient's data to the Issuer to confirm the Patient's identification, expiration date and credit line.

Step 16. The Issuer confirms the verification and notifies the Acquirer.

Step 17. The Acquirer generates and digitally signs an authorization response message AuthResp and transmits DigEnv([AuthResp,DigSig(AuthResp, $SK_{Acquirer}$)],$PK_{Pharmacy}$) to the Pharmacy.

5.1.6. Purchase confirmation phase

The Patient's purchase is confirmed when the Pharmacy receives the Acquirer's response regarding payment authorization, after which the Pharmacy notifies the Patient.

Step 18. The Pharmacy decrypts the digital envelope by DecrDigEnv(DigEnv([AuthResp,DigSig (AuthResp,$SK_{Acquirer}$)],$PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain authorization response message and verifies the Acquirer's signature by VerifyDigS(DigSig (AuthResp,$SK_{Acquirer}$),AuthResp,$PK_{Acquirer}$). The Pharmacy then generates and digitally signs an order response message, OrderResp, and transmits DigEnv([OrderResp, DigSig (OrderResp, $SK_{Pharmacy}$)], $PK_{Patient}$) to the Patient.If the authorization is correct,the Pharmacy can proceed to deliver the ordered items to the Patient.

5.2. Eligibility / benefit inquiry and response

Step 8 employs healthcare EDI (ASC X12N IHCEBI/IHCEBR) [1] to process the inquiry and response regarding eligibility/benefit information. The Pharmacy sends an inquiry, which is encoded using ASC X12N IHCEBI, to the Insurer to inquire about the Patient's insurance coverage. The Insurer then replies to this inquiry by sending healthcare eligibility/benefit information encoded using ASC X12N IHCEBR. The benefit inquiry and response comprise Steps 8-a, 8-b and 8-c.

Step 8-a. Based on the InsurInfo and the prescription, the Pharmacy generates a benefit inquiry EDI message BenefitReq and digitally signs it. The BenefitReq message, formatted according to ASC X12N IHCEBI, comprises the member identification numbers of the subscriber (insured) and the patient, the identification of the Pharmacy (provider) and the inquired service and benefit coverage. The Pharmacy then generates and sends a digital envelope DigEnv([BenefitReq,DigSig(BenefitReq,$SK_{Pharmacy}$)], $PK_{Insurer}$) to the Insurer.

Step 8-b. The Insurer decrypts the digital envelope via DecrDigEnv(DigEnv([BenefitReq,DigSig (BenefitReq,$SK_{Pharmacy}$)],$PK_{Insurer}$),$SK_{Insurer}$) to obtain the BenefitReq message; verifies the Pharmacy's signature via VerifyDigS(DigSig(BenefitReq, $SK_{Pharmacy}$),BenefitReq,$PK_{Pharmacy}$); and then decodes the IHCEBI formatted BenefitReq message to obtain the inquiry. Based on the requested information, the Insurer then generates a benefit response message BenefitResp and digitally signs it. The BenefitResp message contains the specific eli-

gibility/benefit information for the Patient and is formatted according to ASC X12N IHCEBR. The Insurer generates and sends a digital envelope DigEnv([BenefitResp,DigSig(BenefitResp,$SK_{Insurer}$)], $PK_{Pharmacy}$) to the Pharmacy.

Step 8-c. The Pharmacy decrypts the digital envelope via DecrDigEnv(DigEnv([BenefitResp,DigSig (BenefitResp,$SK_{Insurer}$)],$PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain the BenefitResp message; and further verifies the signature via VerifyDigS(DigSig(BenefitResp, $SK_{Insurer}$),BenefitResp,$PK_{Insurer}$). The Pharmacy then decodes the IHCEBR formatted BenefitResp message to obtain the Patient's benefit information conveyed in the ELG segment.

The digital signature and digital envelope approaches are used to authenticate the inquiry/response and prevent impersonation attacks. The benefit inquiry/response message is digitally signed and then transmitted via the digital envelope approach. Notably, to improve the efficiency of interactive processing, the benefit inquiry and response messages may be transmitted via the digital envelope approach without being digitally signed.

The ASC X12N IHCEBI/IHCEBR transaction sets are deployed to request the Patient's simple eligibility status, deductible amounts or copayment amounts. Table 3 illustrates an example of eligibility/benefit inquiry and response via IHECEBI and IHCEBR messages. Please refer to Ref. [1] for detailed descriptions of the segments and data elements. The benefit inquiry information of the Patient regarding the prescription drugs being requested by the Pharmacy is identified in the IHCEBI in the Eligibility Request (ELR) data segment. The benefit reply information, such as the copayment amounts of the prescription drugs, is contained in the IHCEBR in an Eligibility Response (ELG) data segment.

5.3. Acquiring digitally signed prescriptions

The protocol presented in Section 5.1 assumes the scenario in which the digitally signed prescriptions are stored on the smart/health card. The other possible scenario is that the digitally signed prescriptions are stored in the Hospital. The following discussion illustrates two transaction scenarios of acquiring the digitally signed prescriptions from the Hospital. We only present the transaction steps necessary to acquire the digitally signed prescriptions. They can be easily incorporated into the prescription verification phase of the protocol and, thus, the complete descriptions of the modified protocol are omitted.

5.3.1. Scenario 1

Patient requests the digitally signed prescriptions from the Hospital, as described in the following.

Table 3
An example of eligibility/benefit inquiry and response

Segments	Description
IHCEBI message	
MSP + 13 + + 12300007:2I ~	13: Request; *12300007:2I*: tracking reference number
PVD + P2 + P100001:D3 ~	P2: Pharmacy (type of provider); D3: national association of boards of pharmacy number P100001
SUB + 12300022:1W ~	1W: Member identification number 12300022
PTT + 01 + + + 12300022-01:1W ~	01: Spouse (relationship to subscriber) 1W: member identification No. 12300022-01
ELR + 88 + 472:010201:D3 + + FAM ~	88: Pharmacy (service type); 472: service date 2001/02/01; FAM: Family (coverage level)
IHCEBR message	
MSP + 11 + + 12300007:2I ~	11: Response; *12300007:2I*: tracking reference number (same as in MSP in IHCEBI)
ELG + 1 ~ ELG + B:27:10 + + 88 + + + FAM + MP ~	1: Active coverage (benefit category); B: Copayment (benefit category); *B:27:10*: Copayment amount US$10/per visit 88: Pharmacy (service type); FAM: Family (coverage level); MP: Medicare primary (insurance type)

Notably, the Provider, Subscriber and Patient information are the same as those conveyed in the IHCEBI PVD, SUB and PTT segments; thus, they can be omitted from the IHCEBR to increase the efficiency.

Step a. The Patient generates a prescription request message PresReq and digitally signs it. The PresReq message contains the identification of Patient. The Patient then sends DigEnv([PresReq,DigSig(PresReq,$SK_{Patient}$)],$PK_{Hospital}$) to the Hospital.

Step b. The Hospital decrypts the digital envelope via DecrDigEnv(DigEnv([PresReq,DigSig(PresReq,$SK_{Patient}$)],$PK_{Hospitak}$),$SK_{Hospital}$) to obtain PresReq; and verifies the Patient's signature via VerifyDigS(DigSig(PresReq,$SK_{Patient}$), PresReq, $PK_{Patient}$). The Hospital then digitally signs the prescription Prescr and sends a digital envelope DigEnv([Prescr,DigSig(Prescr,$SK_{Hospital}$)], $PK_{Patient}$) to the Patient.

Step c. The Patient decrypts the digital envelope by DecrDigEnv(DigEnv([Prescr,DigSig(Prescr, $SK_{Hospital}$)],$PK_{Patient}$),$SK_{Patient}$) to obtain Prescr and DigSig(Prescr,$SK_{Hospital}$).

5.3.2. Scenario 2

The Pharmacy first obtains proof of authorization from the Patient to request the doctor's prescription from the Hospital. The Hospital then verifies the Pharmacy's request via the authorization proof and sends the digitally signed prescription to the Pharmacy, as described below.

Step a. The Patient generates and digitally signs a prescription authorization message PresAuth and an authorization notification message AuthNotify, respectively. The PresAuth message contains the authorization identifier as well as the identifications of the Patient, Pharmacy and Hospital. Meanwhile, the AuthNotify message contains the authorization identifier as well as the identifications of Patient and Hospital. The following messages are transmitted to the Pharmacy: DigEnv([PresAuth,DigSig(PresAuth, $SK_{Patient}$)], $PK_{Hospital}$),DigEnv([AuthNotify, DigSig (AuthNotify,$SK_{Patient}$)],$PK_{Pharmacy}$).

Step b. The Pharmacy decrypts the digital envelope using DecrDigEnv(DigEnv([AuthNotify,DigSig (AuthNotify,$SK_{Patient}$)],$PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain AuthNotify and its signature; and verifies the Patient's signature by VerifyDigS(DigSig(AuthNotify,$SK_{Patient}$),AuthNotify,$PK_{Patient}$). The Pharmacy generates a prescription request message PresReq and digitally signs it. The PresReq message contains the authorization identifier and identifications of Patient and Pharmacy. The Pharmacy then sends the following messages to the Hospital: DigEnv([PresReq,DigSig(PresReq,$SK_{Pharmacy}$)],$PK_{Hospital}$) and DigEnv([PresAuth,DigSig(PresAuth,$SK_{Patient}$)],$PK_{Hospital}$).

Step c. The Hospital decrypts the digital envelope via DecrDigEnv(DigEnv([PresReq,DigSig(PresReq,$SK_{Pharmacy}$)],$PK_{Hospitak}$),$SK_{Hospital}$) to obtain PresReq; verifies the Pharmacy's signature via VerifyDigS(DigSig(PresReq,$SK_{Pharmacy}$),PresReq, $PK_{Pharmacy}$); then decrypts the digital envelope by DecrDigEnv(DigEnv([PresAuth,DigSig(PresAuth, $SK_{Patient}$)],$PK_{Hospital}$),$SK_{Hospital}$) to obtain PresAuth; and verifies the Patient's signature via VerifyDigS(DigSig(PresAuth,$SK_{Patient}$),PresAuth, $PK_{Patient}$). The pharmacy's request for prescriptions can, thus, be verified using the contents of the PresReq and PresAuth message. After verifying that the Pharmacy is authorized by the Patient to obtain the prescription, the Hospital digitally signs the prescription Prescr and then sends a digital envelope DigEnv([Prescr,DigSig(Prescr,$SK_{Hospital}$)], $PK_{Pharmacy}$) to the Pharmacy.

Step d. The Pharmacy decrypts the digital envelope by DecrDigEnv(DigEnv([Prescr, DigSig(Prescr, $SK_{Hospital}$)],$PK_{Pharmacy}$),$SK_{Pharmacy}$) to obtain Prescr and DigSig(Prescr,$SK_{Hospital}$).

6. System implementation

A prototype system for healthcare commerce is implemented to demonstrate the merits of the proposed protocol. Various security functions are implemented based on RASEURO release 1.04 [19], including digital signature, dual signature, digital envelope, etc. The online EDI interactions between the Pharmacy and Insurer are implemented following the ASC X12N IHCEBI/IHCEBR implementation guide. Meanwhile, Borland Delphi 3.01 is used to implement the subsystems of the Patient, Hospital, Pharmacy, Pharmacy's Bank (Acquirer) and Insurance Company (Insurer). Furthermore, the protocol is simplified to carry out the implementations necessary to demonstrate the main idea presented herein. For example, the public keys of all participants are stored in each participant in advance; patient's credit-line information is assumed "Verified" to omit the interactions between the Issuer and Acquirer; and

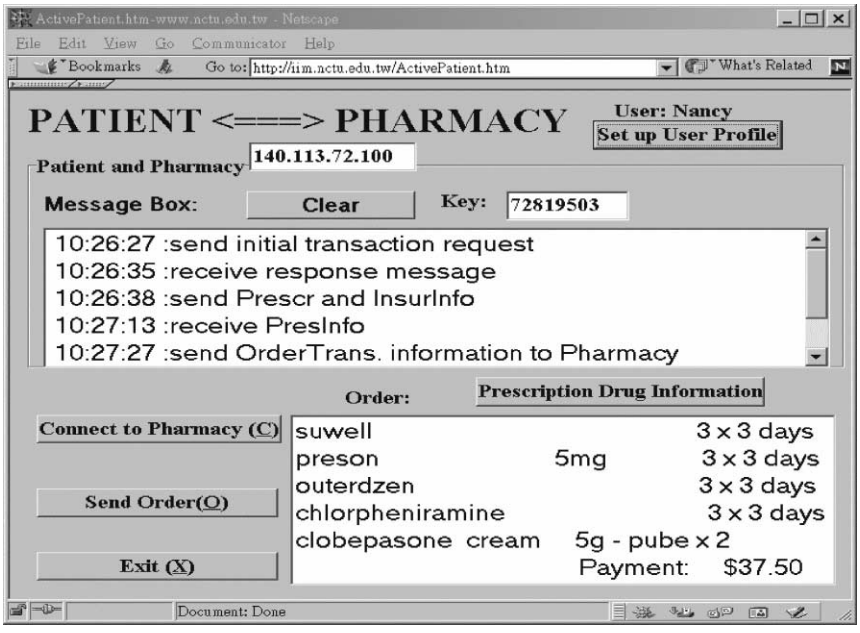


Fig. 3. Patient subsystem for interactions with the Pharmacy.

only some required segments and data elements in IHCEBI/IHCEBR are implemented.

The demonstration presents the transaction scenario of prescription drug purchases via online interactions with the Insurer. During the transaction, the Pharmacy issues an inquiry regarding the Patient's

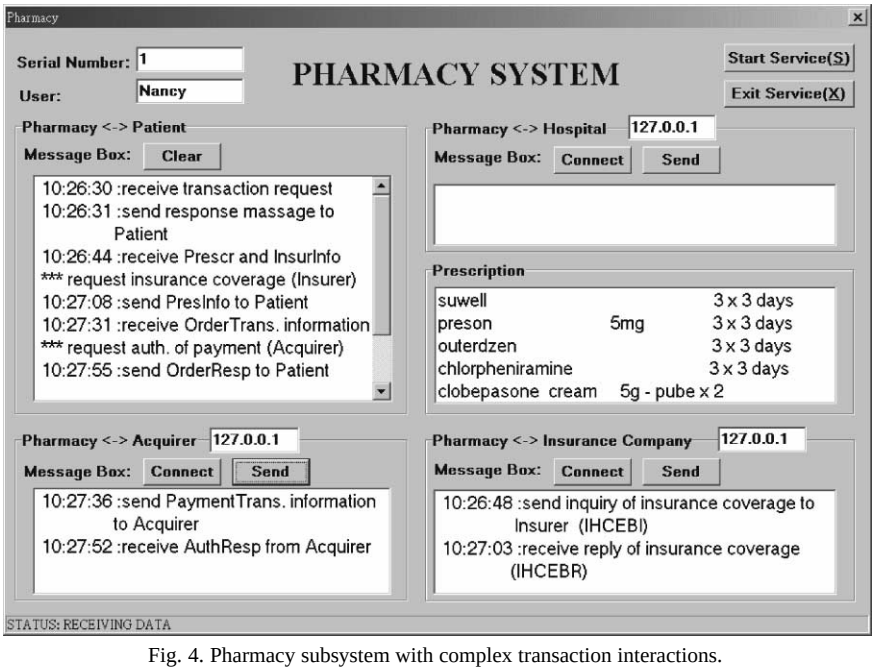


Fig. 4. Pharmacy subsystem with complex transaction interactions.

insurance coverage to the Insurer to determine the amount of payment for the Patient. Additionally, the scenario in which the digitally signed prescriptions are stored on the smart/health card is presented. Fig. 3 shows the Patient subsystem that is mainly responsible for transaction interactions between the Patient and the Pharmacy, including transaction request, prescription verification, purchase request, etc. The pharmacy subsystem, displayed in Fig. 4, controls both online purchases and online EDI interactions. The subsystem conducts data interchange with the Insurer by transmitting encrypted ASC X12N IHCEBI/IHCEBR EDI messages.

The transaction interactions between the Patient and the Pharmacy are based on the secure healthcare protocol described in Section 5. Fig. 4 shows the complex interactions among the Pharmacy, Patient, Hospital, Acquirer and Insurer. The message boxes display the interactions of Pharmacy with Patient, Insurer and Acquirer, respectively. The prototype system demonstrates that the process of healthcare commerce is streamlined by integrating secure online purchases (Patient-to-Pharmacy) and online healthcare data (e.g., benefit inquiry/reply) interchange (Pharmacy-to-Insurer).

7. Discussion

This work has designed integrated protocols that can be applied to healthcare applications to effectively integrate the processing of online purchases and online EDI interactions. The conventional online purchase mainly adopts SET to conduct online interactions among the Customer, Merchant, Issuer and Acquirer. Our work has extended online purchases to include online data interchanges among the Merchant and other associated organizations, in which further information is required to determine the purchase. The proposed healthcare commerce protocol differs from the conventional online (goods) purchase in several aspects.

- *Participants:* Besides the participants considered in conventional online purchase, additional participants are involved in the healthcare commerce. The Hospital is responsible for providing digitally signed prescriptions, while the Insurer may need to provide insurance coverage information and determine healthcare payment claims. This results in more complex transaction interactions than in conventional online purchases.
- *Confirming orders:* The purchase of prescription drugs is restricted by the digitally signed prescriptions. The contents of orders (prescription drugs) must be verified according to the Hospital (doctor) prescriptions and digital signatures. The Patient (Customer) cannot alter the prescriptions. The situation differs from the conventional online purchase, where Customers make the decisions.
- *Determining payment:* In the conventional online purchase, the Merchant determines the amount of payment according to the Customer's order. However, in healthcare commerce protocol, the Pharmacy may need to make a further inquiry to the Insurer regarding the insurance coverage of the Patient and then decide the payment due.

The designed protocol for prescription drug purchases successfully integrates online purchases and online EDI interactions necessary for online insurance coverage inquiries to determine the payment amount. The integration is achieved via adopting the efficient IHCEBI/IHCEBR EDI messages, which are designed by ASC X12N for real-time interactive processing requirements. This approach opens a whole new perspective on designing secure transactions for online commerce.

Besides healthcare commerce applications, other Internet commerce applications may also need to integrate online purchases with online EDI interactions. Consequently, the design of secure online purchases is raised to the level of integrated applications involving online EDI interactions. The results of the present work have shown that the process of healthcare commerce is streamlined by integrating secure online purchases and online EDI interactions.

8. Conclusions and future work

This work has investigated online healthcare transactions (e.g., online purchases of prescription drugs) that involve more participants and more complex transaction interactions than those in conventional online purchases. Such healthcare transaction scenarios necessitate the integration of Secure Electronic Transactions and online EDI interactions to

streamline the commerce process. The results presented herein have demonstrated that the novel approach supports secure and effective online healthcare commerce.

This work supplements the standards to provide a useful application of the integration of SET and healthcare EDI. We have adopted efficient interactive healthcare EDI messages (ASC X12N IHCEBI/IHCEBR) to enable the integration and, thus, facilitate efficient online real-time transaction interactions. The protocol presented herein opens new approaches to designing Secure Electronic Transactions for applications when the integration of online purchases and online EDI interactions is required to streamline the commerce process. Future works will explore the application of the novel design to other Internet commerce applications. Currently, the proposed protocol is more suitable for applications that allow EDI interactions to be processed in an online real-time mode. The integrated processing of online purchases and EDI interactions can be effectively conducted online in such applications. However, EDI interactions for some applications may need to be processed in a batch mode, in which the interactions cannot be processed immediately online to exchange the required data. Further work is necessary to design secure transaction protocols with EDI interactions in a batch mode.

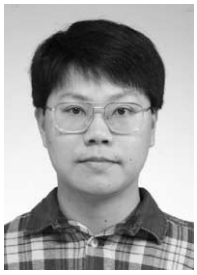
Acknowledgements

The work was supported in part by National Science Council of the Republic of China under the grant NSC 89-2416-H-009-041.

References

[1] ANSI ASC X12N Healthcare Implementation Guide, IHCEBI/IHCEBR: Interactive Health Care Eligibility/Benefit Inquiry and Response (003070X007—Sept. 1998), Washington Publishing (WPC), http://www.wpc-edi.com.
[2] ANSI ASC X12N Healthcare Implementation Guide, 837: Health Care Claim: Pharmacy (003070X081—Jan. 1997), Washington Publishing (WPC), http://www.wpc-edi.com.
[3] ANSI ASC X12N HIPAA Implementation Guide, 270/271: Health Care Eligibility/Benefit Inquiry and Information Response, (004010X092—May 2000), Washington Publishing (WPC), http://www.wpc-edi.com.
[4] ANSI ASC X12N HIPAA Implementation Guide, 835: Health Care Claim Payment/Advice, (004010X091—May 2000), Washington Publishing (WPC), http://www.wpc-edi.com.
[5] B. Blobel, M. Holena, Comparing middleware concepts for advanced healthcare system architectures. International Journal of Medical Informatics, 46, (1997) 69–85.
[6] CyberCash, http://www.cybercash.com/.
[7] EDI Standards, ANSI ASC X12 and UN/EDIFACT, Data Interchange Standards Association (DISA), http://www.disa.org/.
[8] G. Gillespie, Online managed care transactions gain some ground. Health Data Management, 9, (3) (2001) Mar.
[9] Health Informatics Standards- CEN, European Committee for Standardization, Technical Committee for Health Informatics, CEN TC 251, http://www.centc251.org/.
[10] Health Informatics Standards- X12N, Accredited Standards X12, Accredited Standards Committee (ASC), X12N Insurance subcommittee, http://www.x12.org/x12/x12n.
[11] J.-J. Hwang, S.-C. Hsueh, Greater protection for credit card holders: a revised SET protocol. Computer Standards and Interfaces, (19) (1998) 1–8.
[12] S. Immonen, Developments in health care, the increasing role of information technology: security issues. International Journal of Bio-Medical Computing, 43, (1996) 9–15.
[13] ITU-T Recommendation X.509|ISO/IEC 9594-8, Information Technology-Open Systems Interconnection—The Directory: Authentication Framework, ITU-T SG/7|ISO/IEC JTC1/SC21/WG4.
[14] B.J. Love, Developing national standard clinical EDI messages. Computer Methods and Programs in Biomedicine, 48, (1995) 79–83.
[15] G. Medvinsky, Clifford Neuman, NetCash: a design for practical electronic currency on the internet. Proceedings of the 1st ACM International Conference on Computer and Communication Security. ACM Press, New York, 1993, pp. 102–106.
[16] B. Clifford Neuman, Security, payment, and privacy for network commerce. IEEE Journal on Selected Areas in Communications, 13, (8) (1995) October.
[17] T.C. Rindfleisch, Privacy, information technology, and health care. Communications of the ACM, 40, (8) (1997) 93–100, August.
[18] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21, (2) (1978) Feb.
[19] RSAEuro release 1.04, http://www.rsaeuro.com/products/RSAEuro/.
[20] B. Schneier, Applied Cryptography. 2nd edn., Wiley, 1996.
[21] SET Secure Electronic Transaction Specification, Version 1.0, Book1: Business Description, MasterCard, VISA, May 31, 1997. http://www.setco.org/download/set_bk1.pdf.
[22] D. Trcek, R. Novak, G. Kandus, M. Suselj, Slovence smart card and IP based health-care information system infrastructure. International Journal of Medical Informatics, 61, (2001) 33–43.

[23] D.A. Tribble, The health insurance portability and accountability act: security and privacy requirements. American Journal of Health-System Pharmacy, 58, (9) (2001) 763–770, May.
[24] C.P. Waegemann, Industry in focus: developing a security policy for health care providers. Computer Security Journal, XI, (1) (1995).
[25] B. Wright, Security concerns of computer-based health care information. Computer Security Journal, X, (1) (1994).



Duen-Ren Liu received the BS and MS degrees in Computer Science and Information Engineering from the National Taiwan University, Taiwan in 1985 and 1987, respectively, and the PhD degree in Computer Science from the University of Minnesota in 1995. He is currently an Associate Professor of the Institute of Information Management, National Chiao Tung University, Taiwan. His research interests include database systems, information systems, electronic commerce, workflow systems and Internet applications. Dr. Liu is an associate member of the IEEE and a member of the ACM.

I-Chin Wu received the BS degree in Computer and Information Science from the Soochow University, Taiwan in 1999. She is now a masters student of the Institute of Information Management, National Chiao Tung University, Taiwan. Her research interests include electronic commerce, knowledge management and medical informatics.

Sung-Ting Hsieh received the BS degree in Statistics from the National Cheng Kung University, Taiwan in 1996 and the MBA degree in Information Management from the National Chiao Tung University, Taiwan in 1998. Currently, he is an Engineer at the System Development Department of TSMC. His research interests include electronic commerce, information systems, information security and medical informatics.