Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

ELSEVIER

Information & Management 42 (2005) 607–618

INFORMATION & MANAGEMENT

www.elsevier.com/locate/dsw

A transactional-cycle approach to evidence management for dispute resolution

Min-Hua Shao[a], Jing-Jang Hwang[b,*], Soushan Wu[c]

[a]Institute of Information Management, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan
[b]Department of Information Management, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 333, Taiwan
[c]Department of Business Administration, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 333, Taiwan

Received 25 February 2003; received in revised form 25 August 2003; accepted 24 April 2004
Available online 8 July 2004

Abstract

Dispute resolution, a necessary function in electronic commerce, must rely on evidence that includes mechanisms to ensure non-repudiation of actions by the participants. In open systems comprising computer networks, this ‘‘non-repudiation service’’ is one type of security service defined in the ISO/IEC standards. These, as well as other literature, have defined a system framework for such a service. Evidence management is the central part. We propose a new methodology for evidence management with a model using a transactional cycle in which evidence is collected in compliance with the legal concept of chain-of-evidence. Evidence then exists as a set of relevant pieces instead of an atomic item. A case study involving credit-card-over-SSL transactions was used to demonstrate how the model works. Our aim was to present a new approach and show that evidence accountability can be better ensured.

Keywords: Chain of evidence; Accountability of evidence; Non-repudiation services; Value transfers; On-line payment; Information security

1. Introduction

Disputes are inevitable in business, and their resolution is necessary in electronic commerce just as it is in any other form of business. But disputes cannot be legally resolved unless the evidence underlying them has been previously recorded. A non-repudiation service establishes evidence and is one type of security service for open systems [6]. We reviewed the literature on information security and found that these services have been less discussed than others, such as authentication. Pertinent international standards on non-repudiation include ISO/IEC 10181-4 [7], 13888-1 [8], 13888-2 [9], and 13888-3 [10], which deal mainly with general concepts of evidence and define the system framework and some mechanisms for non-repudiation. The goal of this type of service is to generate, collect, maintain, make available, and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence of the event or action.

Due to evidence accountability, evidence management is a critical part of the security framework. Previous research [3,15,18–20] dealt with evidence management as a unit of evidence involving a particular event or action; but this fails to pick up the

[*] Corresponding author. Tel.: +886 3 2118018;
fax: +886 3 2118020.
E-mail address: jjhwang@mail.cgu.edu.tw (J.-J. Hwang).

0378-7206/$ – see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.im.2004.04.002

complete context. Given that no business activity is atomic, we must consider a series of activities formed onto a complete transaction, rather than an isolated unit. It follows that evidence does not exist as an atomic piece but as a chain-of-evidence. This concept was originally introduced in law-enforcement. However, we integrate the concept with evidence management to trace accountability of each event or action into the overall transaction.

2. Value transfers in a cyclic model of a transaction

2.1. A business-to-consumer transaction cycle

Business-to-consumer (B2C) activities are an important type of electronic commerce involving: (i) the buyer/payer; (ii) the seller/payee; (iii) the financial institution; and (iv) the delivery authority. Only if money flow and logistics operate in coordination can the activity complete successfully. Tygar [16] discussed atomic transactions in electronic commerce and defined three levels: money, goods, and certified delivery. Money transactions deal with the transfer of funds. Goods transactions cover money paid and the transfer of goods for money. Certified delivery involves both money and goods and further allows the business and consumer to prove exactly what goods were delivered. The treatment of certified delivery is the focus of this paper.

A typical model of a B2C transaction, including exchanges between actors, is illustrated in Fig. 1. The series of activities presents a transaction cycle, and its closing produces a concluded transaction. Two events—payment in monetary terms and delivery of goods—form a minimum cycle, although it normally involves a longer series of events. The first half of the figure deals with monetary transactions, while the other involves goods, where ownership is transferred.

2.2. Value transfers

A business transaction is not complete until a series of activities involving value transfers has been successfully conducted. For money transactions, Pfitzmann and Waidner [13] defined the properties of general payment systems and indicated that one of their major distinctions is the point at which money is transferred between the payment initiator and the receiver. Moreover, Abad Peiro et al. [1] indicated that the basic function of these payment models was to provide value transfer among different players, but that between the issuer and the acquirer occurs in proprietary banking systems, which are outside the scope of the generic payment services.

In the study of on-line payment and dispute resolution, the word bank often signifies various financial institutions. For the purpose of dispute expression about transfers between payer or payee and bank, Asokan et al. [2] defined three types of value transfers: (i) value subtraction; (ii) payment; and (iii) value

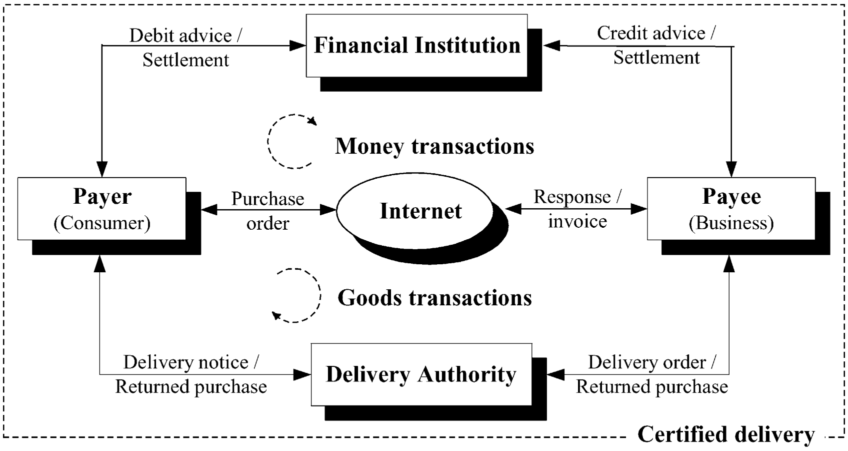

Fig. 1. A typical business-to-consumer transaction cycle.

claim. These, taken together, give the profile of the payment service in a transaction. A partial view involves a subset of the players, and their interaction is an instance of a 'primitive transaction.' This, for value subtraction, is the conversion of 'real value' into electronic value. Normally, a bank and a payer engage in value subtraction: the payer authorizes the bank to remove real value from his or her account. In a payment, the players involved are a payer and a payee. The payer moves electronic value to the payee and the payee requests the bank to convert electronic value into real value.

However, these three primitive transactions of monetary value transfer portray only a part of a usual composite transaction. Recently, the development of global B2C markets has been slowed by insufficient support of distribution channels. Business transactions have been conducted on-line but with inadequate logistics services. Many disputes have arisen from the product-delivery service. To help overcome consumer concern over delivery, business alliances between Internet retailers (especially 'pure' virtual stores) and off-line distributors can be effective. The 'click-and-brick' alliance and a solution called 'B2B2C' to logistics problems have been initiated [11].

No activity in business is independent of others. A series of successful activities usually brings about a completed business transaction, resulting in a transaction cycle. In Fig. 2, a solid line represents the movement of monetary value whereas a dotted line shows the delivery of purchased-object value. For the delivery of purchased-object value, an intermediary agent, called a delivery authority (DA), is usually involved. One or more DAs, trusted by both seller and buyer, provides delivery services in accordance with the terms of the sale and the nature of the purchased object. The delivery may precede, follow, or accompany the exchange of monetary value.

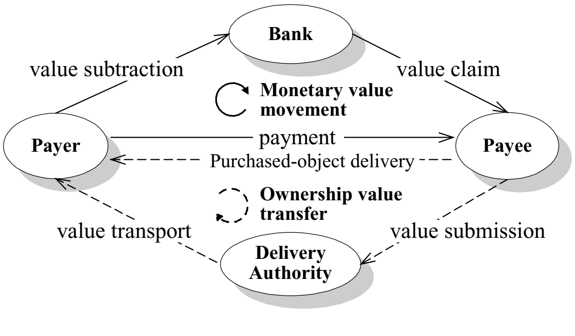

Fig. 2. Value transfers in a cyclic model of a typical B2C transaction.

Considering the overall distribution process, we define three types of transfers: (i) value submission; (ii) value transport; and (iii) purchased-object delivery. These constitute ownership value transfer. The purchased-object delivery is initiated by the buyer specifying shipping method along with payment, but the object is normally transferred, after payment, from the seller to the buyer. The players involved in a value submission are the payee and a DA. The DA is responsible for delivery to the intended recipient on time.

3. Evidence management

The primary types of consumer problems, according to a report of the OECD Committee on Consumer Policy [4], can be divided into: "I didn't do it" (unauthorized transactions), "I didn't receive it", and "I don't want it." Irrespective of the approach taken to settle disputes, the important first step is to establish evidence. Non-repudiation services deal with this and its accountability is a key factor in examining the details and context of a claim. Therefore, we have defined a general framework that provides a chain of evidence when accountability is a requirement.

3.1. Non-repudiation services

The transfer or receipt of messages during exchanges between actors in a commercial transaction can be regarded as a commitment and recorded as evidence of the transaction. The protection of digital evidence against injury depends on cryptographic techniques. Either symmetric (secret-key) or asymmetric (public-key) cryptographic techniques can be used for non-repudiation. Technically speaking, there are three forms of evidence in the ISO/IEC 10181-4 standard: (i) digital signatures (using a public key); (ii) secure envelopes (using a secret key), and (iii) security tokens (using a secret key). Functionally speaking, the ISO/IEC 13888-1 standard defines four types of document demanded for non-repudiation, all related to the transfer of messages between the two communicating parties: (i) proof of origin; (ii) proof of delivery; (iii) proof of submission; and (iv) proof of transport.

The proof of origin: The Non-Repudiation of Origin (NRO), is intended to prevent foul play on the part of the sender in denying being the creator and sender of the message.

The proof of delivery: Non-Repudiation of Delivery (NRD), contains both proof of receipt and of knowledge. The first is the Non-Repudiation of Receipt (NRR) intended to prevent a recipient's denial of having received a message. The Non-Repudiation of Knowledge (NRK) shows that the recipient was aware of the content of the message.

The proof of submission: Non-Repudiation of Submission (NRS), shows that an intermediary party was commissioned to transmit the message for the sender but was not generally aware of its contents. The intermediary party is the Delivery Authority.

The proof of transport: Non-Repudiation of Transport (NRT), is intended to prevent the Delivery Authority's denial of having delivered the message to the recipient.

The NRS and NRT cover cases in which one or more DAs are involved. If two or more DAs participate in a message delivery, NRS and NRT also provide evidence that proves the transmission of the message between them.

More importantly, the role of the DA bears a meaning different from the ISO standard definition of non-repudiation services. The DA in the ISO documents are a third party trusted by the sender to deliver digital data to the receiver—as is the case of Internet service providers, B2B exchanges, and e-marketplaces. In contrast, the DA in value transfers provides services in the delivery of physical or information goods. The service of FedEx is an example.

For entities involved in phases of non-repudiation in the ISO/IEC 10181-4 document, there is an evidence subject, evidence generation requester, evidence user, evidence generator, evidence verifier, and one or more trusted third parties in generation, transfer, storage/retrieval, and verification phases. There are also plaintiff, defendant, and agreed adjudicators in any dispute-resolution phase. Generally, the role played by the various entities depends on the cryptographic techniques employed. In the case of an asymmetric cryptosystem, the evidence is usually generated by the evidence subject and verified by the evidence user, whereas, in a symmetric cryptosystem, the evidence generator and verifier can be one or more trusted third parties. In the case of B2C market transactions, the possibility of involving trusted third parties in existing application systems is decreased by transaction costs and difficulties in implementation efficiency. Also, to satisfy legal restraints and the validity of the evidence, most application systems employ digital signature techniques to ensure the truth of the evidence. The evidence subjects, for the most part, act as the evidence generators, and the evidence users are also evidence verifiers.

3.2. Chain of evidence

In the literature, non-repudiation services establish one part of the evidence about a particular event or action. It offers information that can be used to prove its occurrence or non-occurrence, but does not necessarily establish truth. Once each piece of evidence is generated, the next step is to provide for its accountability within the transaction. *Evidence accountability* is the conjunction of technical and managerial factors. On the technical side, the validity of each piece of evidence can be ensured through cryptography. For management factors, the key point is to tie together every piece of evidence, in order to draw a map which allows accurate assessment of a situation for the dispute-resolution phase. Only by clarifying the causal relation between cause and effect can the truth be ascertained. Evidence generation usually follows execution of a specific event or action. So, a set of gathered evidence will reflect a sequence of business activities (value transfers in a transaction cycle). Consequently, the map of evidence here is defined as a 'chain of evidence.' This was described by Welch [17] as tracing accountability by law-enforcement agencies in the conduct of criminal investigations. The detailed items involved: who obtained the evidence, where and when it was obtained, who secured it, and who had control or possession of it.

A chain of evidence in a business transaction can be obtained from the transactional-cycle model. Any event or action can trigger business activities or value transfers at any time. These value-transfer activities are significant in establishing the context of the dispute. Thus, to identify value transfers during a

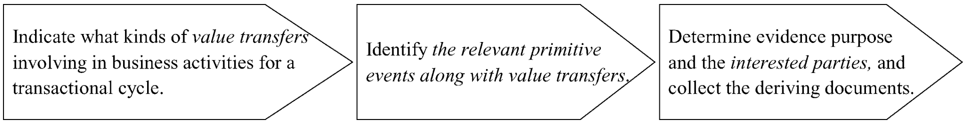
Indicate what kinds of *value transfers* involving in business activities for a transactional cycle.
Identify *the relevant primitive events along with value transfers.*
Determine evidence purpose and the *interested parties,* and collect the deriving documents.

Fig. 3. The procedures for establishing a chain of evidence.

transaction, it is first necessary to identify the relevant event or action. Here, we consider a specific set of events or actions; all of them are related to specific non-repudiation services in connection with evidence purpose, the derivative documents, and the interested parties. Generally, a specific set of events or actions is common to similar properties or functions of many electronic transaction systems. We therefore define a ‘primitive event’ as an abstract of a specific set of events or actions for a general B2C transaction. The procedure of establishing a chain of evidence is summarized in Fig. 3. This acts as a ‘clue map’ to provide a guide to necessary information in order to indicate context of pertinent occurrences.

The detailed treatment of the primitive events is according to value transfers in a transaction cycle. There are three primitive events abstracted from input interface—pay, receive, and allow. The *pay* event is initiated by a buyer in making a payment; the *receive* event is an input by the merchant who responds to the pay event from the buyer; the *allow* event is an input by the buyer’s bank, which checks the account to ensure that there is enough balance to make the electronic payment. The major output events are deduct, add, paid, and received. The *deduct* event gives the buyer’s bank notice to remove the authorized money from the account; the *add* event notifies the merchant’s bank to put the authorized money into the merchant’s account; the *paid* and *received* events indicate to the participants that an authorized payment has been fulfilled. In effect, the paid event is the successful culmination of the *allow* and *deduct* events. The *received* event must take another event into consideration: the *liquidate* event, in which the merchant makes a ‘capture’ request to the merchant’s bank. Thus the received event is not complete until both the *liquidate* and *add* events have been accomplished. Therefore, “paid” and “received” are not primitive events, and we do not include them in Table 1.

With respect to the composite event of purchased-object value delivery, we define six basic primitive events for the overall distribution process; all are concerned with the generation of evidence during the purchased-object delivery: (i) the submit event (in which the merchant commissions the delivery authority to provide shipment service); (ii) the undertake event (which signals the DA to accept the commission); (iii) the shipping-to event (an input by the buyer that chooses shipping method and preference); (iv) the shipping-from event (which is input by the merchant); (v) the delivery event (by which the DA transports the purchased object to the recipient); and (vi) the obtain event (which signals that the buyer has received the purchase). Table 1 provides a summary.

Evidence is generated by the data describing the event along with value transfers. Therefore, the primitive events are the key intermediaries in linking a series of business activities with every piece of evidence. Interested parties in a chain of evidence take account of the evidence subject and user. The role of the event claimant is often the opposite of that of the event initiator, and thus the possession of evidence regarding the event is on the side of the claimant. This shows that a chain of evidence must be identified in order to trace the accountability of each event along the cycle.

Table 1
The relation between the primitive events and value transfers

Type of value transfers	Value transfers	Primitive events
Monetary value movement	Value subtraction	Allow Deduct
	Payment	Pay
		Receive
	Value claim	Liquidate
		Add
Ownership value transfer	Value submission	Submit
		Undertake
	Purchased-object delivery	Shipping-from
		Shipping-to
	Value transport	Deliver
		Obtain

Table 2
A chain of evidence associated with monetary value movement

Primitive event	Derivative document	Evidence purpose	The interested parties	
			Event initiator	Event claimant
Allow	Payment instruction	NRO_Value Subtraction	Payer	Bank
Deduct	Payment authorization	NRR_Value Subtraction	Bank	Payer
Pay	Purchase order	NRO_Payment	Payer	Payee
Receive	Confirmation and invoice	NRR_Payment	Payee	Payer
Liquidate	Capture claim	NRO_Value Claim	Payer	Bank
Add	Capture acceptance	NRR_Claim	Bank	Payer

In order to distinguish the notation about evidence purpose in ISO/IEC 13888-1 from our method, the chain of evidence for a typical business-to-consumer transaction is shown in two tables: Table 2 shows the evidence chain associated with monetary value transfers, while the chain associated with ownership value transfers is depicted in Table 3. The notation about evidence purpose is according to specific non-repudiation service and this, in conjunction with value transfers, is linked to the primitive event that occurred. ''NRO_Value Substraction'' for example, is one of the notations linking the primitive event ''Allow'' with the document for ''Payment Instruction.''

Monetary value movement uses two types of non-repudiation evidence—NRO and NRR—in the ISO/IEC 13888-1 standard. Both NRO and NRR are related to the transfer of messages over the network.

In addition to NRO and NRR adopted from the ISO/IEC 13888-1, we introduce a new notation NRPD, Non-Repudiation of Purchased-object Delivery. We believe that the proof of purchased-object delivery provides a proof of evidence for ownership value transfer. We further identify three evidence purposes—NRPD_Value Submission, NRPD_Purchased-object Delivery, and NRPD_Value Transport—to support the proof for ownership (purchased goods) value transfer. The interested parties, derivative document, and primitive events associated are listed in this table.

We define nine types of evidence and their derivative documents as follows:

- The payment instruction prepares non-repudiation evidence of a value subtraction primitive transaction, the NRO_Value Subtraction. It indicates the occurrence of an *allow* event. The initiator of the event is the payer and the claimant is the bank.
- The payment authorization offers non-repudiation evidence of a value subtraction primitive transaction, the NRR_Value Subtraction. It proves the occurrence of the *deduct* event. The initiator is the bank and the payer is the claimant.
- The purchase order offers non-repudiation evidence of a payment primitive transaction, the NRO_Payment. It gives the accountability of the *pay* event. The payer is the initiator and the payee is the claimant.
- The confirmation and invoice offers non-repudiation evidence of a payment primitive transaction, the NRR_Payment. It traces the occurrence of the

Table 3
A chain of evidence associated with ownership value transfer

Primitive event	Derivative document	Evidence purpose	The interested parties	
			Event initiator	Event claimant
Submit Undertake	Consignment receipt	NRPD_Value submission	Delivery authority	Merchant
Shipping-to Shipping-from	Shipping agreement	NRPD_Purchased-object Delivery	Buyer Merchant	Merchant Buyer
Delivery Obtain	Acknowledgement receipt	NRPD_Value Transport	Buyer	Delivery authority/merchant

receive event. The payee is the initiator and the payer is the claimant.

- The capture claim document offers non-repudiation evidence of a value claim primitive transaction, the NRO_Value Claim. It aims to account for the *liquidate* event. The payee is the initiator and the bank is the claimant.
- The capture acceptance document offers non-repudiation evidence of a value claim primitive transaction, the NRR_Value Claim. It testifies that the *add* event has taken place. The bank is the initiator and the payee is the claimant.
- The consignment receipt provides for non-repudiation evidence of a value submission primitive transaction, the NRPD_Value Submission. It occurs when the delivery authority provides evidence to the merchant. The initiator is the delivery authority and the claimant is the merchant.
- The shipping agreement for product delivery, such as the shipping method and preference, provides non-repudiation evidence of a primitive transaction of ownership transfer. Due to the exchange of the agreement between the buyer and the merchant, this, the NRPD_Purchased-object Delivery, can be used to account for both shipping-to and the shipping-from events. For the shipping-to event, the buyer is the initiator and the merchant is the claimant; further, as regards the shipping-from event, the merchant is the initiator and the buyer is the claimant.
- The acknowledgement receipt provides non-repudiation evidence of a value transport primitive transaction, the NRPD_Value Transport. It happens when the buyer acknowledges to the DA and, indirectly, to the merchant that the purchased object has been received; the initiator is the buyer and the claimant is the DA or the merchant.

4. Case study: credit-card payment over SSL

A survey of consumer shopping over the Internet, conducted by ActiveMedia Research and reprinted in [12], shows that most credit card transactions utilize systems based on a Secure Sockets Layer (SSL), which is software incorporated in browsers to protect communication security. However, some (27% in the year 2000) Internet shoppers preferred off-line payment. The implication of this is discussed in [14]; apart from security, consumers had misgivings about follow-up processes after payment—packaging, shipment, and delivery, and after-sales services. Preventive measures were thus essential.

4.1. The SSL-based payment system

SSL is a general-purpose security protocol; it was developed by Netscape Corporation in late 1994 [5] to protect privacy and data integrity between two communicating applications, and provide a way to prevent eavesdropping, tampering, and message forgery. As SSL is a general protocol for secure exchange, the use of credit cards over SSL is, strictly speaking, not a complete payment system, because it deals only with exchanges between consumers and merchants. The SSL-based payment system was developed to transfer credit-card details securely across the network, in much the same way as a mail or telephone order. In contrast, the Secure Electronic Transaction (SET) protocol developed by Visa and MasterCard was exclusively for bank card transactions. Fig. 4 illustrates messages exchanged in a 'credit-card-over-SSL' system for business-to-consumer transactions. An SSL-based system is not concerned with interaction with other entities in the payment transaction. Nor is it concerned with the details of the content, etc. In other words, a 'credit-card-over-SSL' system provides no security to safeguard credit-card information after it is delivered to the merchant and collected in the database. The merchant generally interacts with the corresponding bank, an acquirer, by traditional media (such as leased lines).

4.2. Non-repudiation for SSL-based purchase activities

The first step in establishing a chain of evidence is to identify the value transfers involved in each phase of the transaction. Our analysis revealed that the major service was to provide value transfers of payment from the payer to the payee. The message flows, in Fig. 4, are marked as solid lines (2 and 5). Queries about the catalogue and initial negotiation (during the pre-purchase phase, number 1) generally proceed in an open manner outside the SSL-based payment system for business-to-consumer transactions.

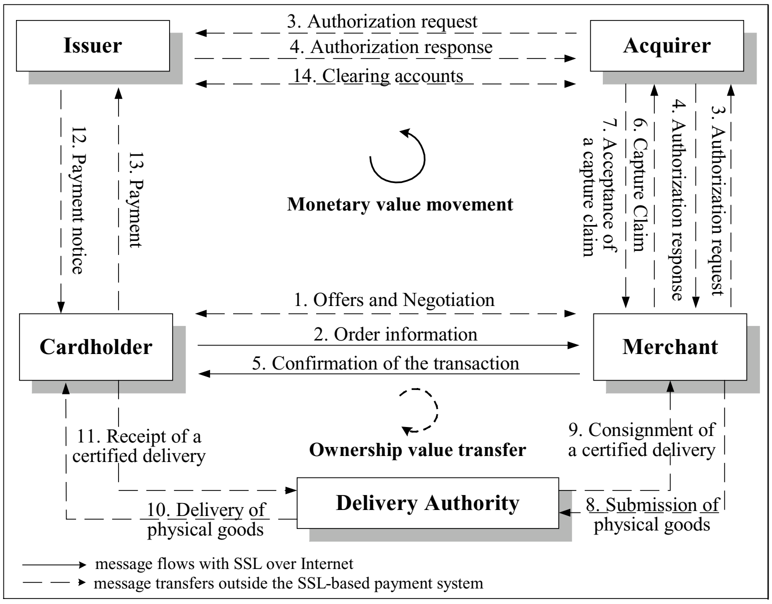
Issuer
Acquirer
Cardholder
Merchant
Delivery Authority
3. Authorization request
4. Authorization response
14. Clearing accounts
12. Payment notice
13. Payment
Monetary value movement
7. Acceptance of a capture claim
6. Capture Claim
4. Authorization response
3. Authorization request
1. Offers and Negotiation
2. Order information
5. Confirmation of the transaction
Ownership value transfer
11. Receipt of a certified delivery
9. Consignment of a certified delivery
10. Delivery of physical goods
8. Submission of physical goods
message flows with SSL over Internet
message transfers outside the SSL-based payment system

Fig. 4. Message flows for a 'credit-card-over-SSL' transaction.

The next step involves discovery of the primitive events relevant to value transfers. There are two primitive events for value transfers of payment. The *first* is the pay event during the purchase request; in this the cardholder acts as the pay initiator and in it the merchant is the pay claimant. The merchant might hold evidence about the pay event, the NRO_Payment. The *second* is the receive event during the transaction response; in it the merchant plays the receive initiator and the cardholder plays the receive claimant, possessing evidence of the NRR_payment. Finally, the relevant documents and the interested parties can be determined, based upon the events.

4.3. The chain of evidence in a 'credit-card-over-SSL' transaction

Primitive events in a credit-card-over-SSL transaction deal only with value transfers of payment, rather than a full cycle formed as a business transaction. A chain of evidence is derived from the transaction cycle and consequently it can trace the accountability of each event or action. Non-repudiation services possessing only a portion of evidence never results in success. Because of this, we must examine all phases of the business transaction, in order to establish the evidence chain. In general, there are eight phases:

- *The pre-purchase phase*: It deals with information query and negotiations regarding sales between the buyer (cardholder) and merchant.
- *The purchase request phase*: Here the cardholder makes a request (including the shipping agreement and purchase order) to the merchant. The primitive events are shipping-to and pay, and the related value transfers include ownership transfer and payment. In ownership transfer, the cardholder acts as an initiator of the shipping-to event and the merchant is the claimant who holds the NRPD_Purchased-object Delivery evidence. In payment, the cardholder acts as an initiator of the pay event and the merchant is the claimant and possesses the NRO_Payment evidence.
- *The authorization request phase*: It assures that the transaction amount to the merchant has been authorized by the bank. Specifically, because an SSL-based transaction is treated as a transaction over the Internet, the merchant takes the place of the cardholder in making a payment instrument to the corresponding bank and deals with responses about the payment request from the bank. The term

Table 4
The chain of evidence in a 'credit-card-over-SSL' transaction

Transaction phases	Relevant documents	Value transfers	Non-repudiation roles of the interested parties			
			Cardholder	Merchant	Banks	Delivery authority
Pre-purchase	Catalog		Information query and negotiation			
Purchase request	Purchase order, shipping agreement	Payment, purchased-object delivery	*Pay* initiator, *Shipping-to* initiator	*Pay* claimant (NRO_Payment) *Shipping-to* claimant (NRPD_Purchased-object delivery)		
Authorization request	Payment instruction	Value subtraction		*Delegated-Allow* initiator	*Delegated-Allow* claimant (NRO_Value Subtraction)	
Authorization response	Payment authorization	Value subtraction		*Delegated-Deduct* claimant (NRR_Value Subtraction)	*Delegated-Deduct* iitiator	
Purchase response	Confirmation and invoice, consignment receipt	Payment, purchased-object delivery, value submission	*Receive* claimant (NRR_Payment) *Shipping-from* claimant (NRPD_Purchased-object delivery)	*Receive* initiator, *Shipping-from* initiator, *Submit* initiator, *Undertake* claimant (NRPD_Value Submission)		*Submit* claimant, *Undertake* initiator
Distribution	Acknowledgement receipt	Value transport	*Deliver* claimant, *Obtain* initiator	*Obtain* claimant (NRPD_Value Transport)		*Deliver* initiator, *Obtain* claimant (NRPD_Value Transport)
Capture request	Capture claim	Value claim		*Liquidate* initiator	*Liquidate* claimant (NRO_Value Claim)	
Capture response	Capture acceptance	Value claim		*Add* claimant (NRR_Value Claim)	*Add* initiator	

delegated is used to describe these two events, including the delegated-allow event in the authorization request phase and the delegated-deduct event in the authorization response phase. For the delegated-allow event of value subtraction, the merchant is the initiator and the bank is the claimant, possessing the NRO_Value Subtraction evidence.

- *The authorization response phase*: The bank verifies the cardholder's credit line and then makes an authorization response to the merchant. The delegated-deduct event corresponds to value subtraction. The bank is the initiator and the merchant is the claimant, who retains the payment authorization as NRR_Value Subtraction evidence.
- *The purchase response phase*: The merchant gives the purchase confirmation (including shipping agreement) and invoice to the cardholder after obtaining authorization from the bank. This indicates the occurrence of the receive event in payment and the shipping-from event in the purchased-object delivery. For the receive event, the merchant is the initiator and the cardholder is the claimant, possessing the NRR_Payment evidence; for the shipping-from event, the merchant is the initiator and the cardholder is the claimant, who therefore possesses NRPD_Purchased-object Delivery evidence. After that, the merchant submits the purchased object to the delivery authority. Its corresponding event is the submit related to value submission, while the merchant is the initiator and the DA is the claimant. By undertaking the delivery work the delivery authority must give the consignment receipt to the merchant as the NRPD_Value Submission evidence. For the undertake event, the delivery authority is the initiator and the merchant is the claimant.
- *The distribution phase*: While delivering the goods to the recipient, the cardholder provides the acknowledgement receipt as the NRPD_Value Transport evidence to the delivery authority and/or the merchant. It triggers the deliver and obtains events in value transport. For the deliver event, the delivery authority acts as the initiator and the recipient (the cardholder) is the claimant; and further, the cardholder acts as the initiator of the obtain event and the delivery authority and/or the merchant is the claimant.
- *The capture request phase*: The merchant makes a capture request to the bank, and triggers a value transfer—value claim. The corresponding primitive event is the liquidate event. The merchant is the initiator and the bank is the claimant, possessing the capture claim document as the NRO_Value Claim evidence.
- *The capture response phase*: The bank gives a response to the merchant after acting on the merchant's request; its corresponding event related to the value claim is the add event. The bank is the initiator and the merchant is the claimant, who possesses the capture acceptance document as the NRR_Value Claim evidence.

These are summarized in Table 4.

5. Conclusions

A new evidence-management methodology and its associated establishing procedures were discussed and then applied to a credit-card-over-SSL transaction case. The concept of chain-of-evidence and the transactional-cycle approach were integrated into the evidence-management methodology. Once each piece of stored evidence was generated, a map could be drawn to trace back the accountability of each event or action along the transactional cycle. We presented a systematic treatment of evidence accountability for non-repudiation services; this is a supplement to single pieces of evidence, which are quite limited when attempting to learn the context.

Essentially, the non-repudiation service overlaps the functions of security audits and alarms. Both aim to record events or actions that have occurred. Recording the event in the audit trail might require support from non-repudiation services, and vice versa. That is, the audit recorder can be used to store and utilize non-repudiation evidence. Moreover, the analytical works about these are essentially different approaches to achieve the same purpose.

Acknowledgements

The authors would like to thank the anonymous referees for their helpful comments on an earlier manuscript of this paper, and to thank Prof. Edgar

H. Sibley, the Editor-in-Chief, for his excellent editing work and revisions that substantially improved the quality of this paper. Part of this research was funded by the National Science Council of Taiwan under the contracts of NSC 90-2213-059 and NSC 91-2416-H-182-009; the former contract was conducted by the corresponding author (J.J. Hwang) while he was working at National Chiao Tung University. A related article of this paper was published in the Proceedings of the 18th IFIP International Information Security Conference. The major contribution of this paper beyond that conference article includes a complete description about the theoretical model and a verification of the model through a case study.

References

[1] J.L. Abad Peiro, N. Asokan, M. Steiner, M. Waidner, Designing a generic payment service, IBM Systems Journal 37 (1), 1998, pp. 72–88.

[2] N. Asokan, E.V. Herreweghen, M. Steiner, Towards a framework for handling disputes in payment systems, in: Proceedings of the Third USENIX Workshop on Electronic Commerce, Boston, MA, September 1998, pp. 187–202.

[3] T. Coffey, P. Saidha, Non-repudiation with mandatory proof of receipt, Computer Communication Review 26 (1), 1996, pp. 617.

[4] DSTI/CP (Directorate for Science, Technology and Industry/ Committee on Consumer Policy), Report on consumer protection for payment cardholders, OECD, June 14, 2002.

[5] A.O. Freier, P. Karlton, P.C. Kocher, The SSL protocol version 3.0, Netscape Communications Corporation, November 18, 1996.

[6] ISO/IEC, ISO/IEC 10181-1, Information technology—open systems interconnection—security frameworks for open system: overview, 1996.

[7] ISO/IEC, ISO/IEC 10181-4, Information technology—open systems interconnection—security frameworks for open system: non-repudiation framework, 1997.

[8] ISO/IEC, ISO/IEC 13888-1, Information technology—security techniques—non-repudiation part 1: general, 1997.

[9] ISO/IEC, ISO/IEC 13888-2, Information technology—security techniques—non-repudiation part 2: mechanisms using symmetric techniques, 1998.

[10] ISO/IEC, ISO/IEC 13888-3, Information technology—security techniques—non-repudiation part 3: mechanisms using asymmetric techniques, 1997.

[11] T.P. Liang, H.J. Lai, Effect of store design on consumer purchases: an empirical study of on-line bookstores, Information & Management 39 (6), 2002, pp. 431–444.

[12] National Credit Card Center of R.O.C., Market report on electronic commerce, 5 April 2000, Retrieved June 30, 2000 from the world wide web: http://www.nccc.com.tw/plan/news/newsg3.htm.

[13] B. Pfitzmann, M. Waidner, Properties of payment systems: general definition sketch and classification, IBM Research Report RZ 2823 (#90126), June 1996, pp. 1–28.

[14] C. Ranganathan, S. Ganapathy, Key dimensions of business-to-consumer web sites, Information & Management 39 (6), 2002, pp. 457–465.

[15] S. Schneider, Formal analysis of a non-repudiation protocol, in: Proceedings of 11th IEEE Computer Security Foundations Workshop, 1998, pp. 54–65.

[16] T.D. Tygar, Atomicity in electronic commerce, Mixed Media, April/May 1998, pp. 32–43.

[17] T. Welch, Computer crime investigation and computer forensics, in: M. Krause, H.F. Tipton (Eds.), Handbook of Information Security Management, Auerbach, Boca Raton, Fla, 1999.

[18] C.H. You, J. Zhou, K.Y. Lam, On the efficient implementation of fair non-repudiation, Computer Communication Review 28 (5), 1998, pp. 50–60.

[19] J. Zhou, Evidence and non-repudiation, Journal of Network and Computer Applications (20:3), July 1997, pp. 267–281.

[20] J. Zhou, D. Gollmann, An efficient non-repudiation protocol, in: Proceedings of 10th IEEE Computer Security Foundations Workshop, 1997, pp. 126–132.

Min-Hua Shao is a candidate for doctorate degree at National Chiao Tung University in Taiwan. She received her MBA degree in 1998 with major in information management from National Chengchi University, Taiwan. Her current research interests include information security management and financial services such as Internet banking and payment systems in electronic commerce.

Jing-Jang Hwang began his academic career in 1976 as an instructor at National Chiao Tung University (NCTU) in Taiwan. He worked at NCTU for more than 25 years until the summer of 2002, and is now a Professor of Chang Gung University. Given leave of absence from NCTU, he studied Business Administration at the University of Cincinnati, and then studied Computer Science at the University of Florida. He received his PhD degree from the University of Florida in 1987. In addition to teaching, he has designed several computerized information systems, which include the administrative and the library systems of NCTU itself, the business system of a securities brokerage firm, and the office automation system of the judicial courts in Taiwan. Since 1990, he has also been involved in research on subjects of cryptography, information security, and electronic commerce, and has contributed research articles, in the English language as well as in the Chinese language, to various magazines and journals. He is now an editor of Computer Standards & Interfaces, a journal published by North-Holland.

Soushan Wu received his PhD in Finance from the University of Florida in 1984. He is currently a Chair Professor and Dean of College of Management, Chang-Gung University, Taiwan. He is also a visiting scholar in Clemson University, Hong Kong Polytechnic University now. His research interests include Management Science, Investment Science, Capital Markets and Information Systems. He has published more than 90 articles in Research in Finance, Financial Management, Asia-Pacific Journal of Finance, International Journal of Accounting and Information Systems, etc. He is now an editor of several academic journals, including Journal of e-Healthcare, Taiwan Management Review, and Journal of Financial Studies.