ESTABLISHING CHAIN OF EVIDENCE AS A BASE FOR NON-REPUDIATION SERVICES

Jing-Jang Hwang[a], Min-Hua Shao[b], Soushan Wu[c]
[a]*Department of Information Management, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan 333, R.O.C.*
[b]*Institute of Information Management, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan 300, R.O.C.*
[c]*College of Management, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan 333, R.O.C.*

Abstract: Disputes are inevitable in business. Disputes in the real world are resolved in various ways. Similarly, in the virtual world, there is a variety of non-repudiation services as defined in the ISO/IEC standards [5, 6, 7, 8]. Whatever actions are taken, evidence is the key to the successful conduct of these services. These previous works usually define the concept of non-repudiation services using a single piece of evidence, which fails to describe the causality of an event completely. In business, no activity is atomic, and evidence therefore does not exist as an atomic piece. Rather, evidence exists in the form of a series of relevant pieces of evidence. That is, we must consider a series of activities—formed onto a cycle of value transfers. This paper introduces a chain-of-evidence concept to electronic commerce as a basis for the refinement of the pertinent international standards. The chain of evidence can be analyzed and derived from the cyclic model of value transfers. From information security and information processing perspectives, this paper aims to provide a better evidence-management methodology as the first step to be taken in settling any disputes. As a result, we expect that the research will contribute a theoretical basis for non-repudiation services in the practical world.

Key words: evidence management, cycle of value transfers, non-repudiation services, disputes resolution, electronic commerce

1. INTRODUCTION

Disputes are inevitable in business, and the resolution of such disputes is necessary in electronic commerce just as it is in any other form of commerce. Disputes cannot be resolved unless the evidence underlying the dispute has

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

been previously recorded. Non-repudiation services establish evidence. Non-repudiation services for open systems such as the Internet are one type of security services defined in ISO/IEC standards. Pertinent standards include ISO/IEC 10181-4 [5], 13888-1 [6], 13888-2 [7], and 13888-3 [8], which deal with general concepts of evidence and which define the system framework and some mechanisms for non-repudiation services. The goal of non-repudiation services 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. As stated in the standards themselves, and in the academic literature [3, 10, 12, 13, 14], they define the concept of using a single piece of evidence according to a particular event or action. Given that in business, and in electronic commerce in particular, no activity is atomic, we must consider a series of activities, rather than an isolated instance. It follows that evidence does not exist as an atomic piece. Rather, it exists in the form of relevant pieces of related evidence. In this paper, we take the chain-of-evidence concept, as originally conceived for law-enforcement purposes, and adapt it to non-repudiation services, with a view to supplementing the above-mentioned international standards, which are, as noted above, based on the presumption of a static state of evidence. A chain of evidence must be identified and organized, such that each piece of evidence stored in a computer somewhere can be traced, and its accountability established in any given event or action. Evidence accountability is the future basis on which disputes can be resolved.

Since a composite transaction consists of a sequence of events, the evidence chain derived from these events will be helpful in gaining a clear picture of what has transpired. A business transaction is not complete until a series of activities involving value transfers has been successfully conducted. The series of activities presents a cycle of value transfers, and the closing of the cycle simultaneously produces a concluded transaction. Two events—payment in monetary terms and delivery of goods—form a minimum value-transfers cycle, although the cycle normally involves a longer series of events. Asokan et al. [2] defined the concept of value transfers in a general payment model, which was proposed by Pfitzmann and Waidner [9]. However, Asokan et al.'s works put much emphasis on movement of monetary value only. Recently, under pressure from the need for cost reductions in business-to-consumer (B2C) transactions, other types of value transfers (for example, the delivery of goods or services) have come under scrutiny. But, it appears that most electronic payment systems cannot be tightly coordinated with logistic activities, which must be conducted through separate distribution channels. Therefore, a complete transaction cycle must combine movement of monetary value with separate delivery of purchased-object value. In summary, the main purpose of a chain of evidence is to enhance evidence accountability by examining the series of activities formed as a value-transfer cycle.

The remainder of this paper is organized as follows. Section 2 clarifies disputes resolution in a non-repudiation process. Section 3 provides a redefinition of the transactional cycle. Based upon this cycle, the concept of chain-of-evidence is developed in Section 4. Finally, Section 5 concludes the paper with a discussion of our approach.

2. DISPUTES-RESOLUTION PHASE IN A NON-REPUDIATION PROCESS

To illustrate how the concepts of the chain of evidence and the value-transfer cycle assist dispute resolution, Fig. 1 presents a procedure for handling the dispute-resolution phase of a non-repudiation process. Discussion on that is outside the scope of the pertinet standards [5]. The procedure consists of four steps: (i) stating the claim; (ii) collecting evidence; (iii) arbitrating in the dispute; and (iv) deciding on the fact. First, the claim-stating step indicates what activities are investigated and who may get involved. Value transfers associated with these activities can be determined. These value-transfer activities are significant in establishing the context of the dispute. The next step is evidence collection. The primary challenge of this task is how to collect all relevant evidence effectively. The chain of evidence acts as a 'clue map' to provide a guide to necessary information. The map indicates events, interested parties, relevant documents, and the time and place of pertinent occurrences. By analyzing the interested parties, the ISO/IEC 10181-4 document defines some roles involved in a non-repudiation system, including the evidence subject, the evidence generation requester, the evidence user, the evidence generator, the evidence verifier, and one or more trusted third parties in the evidence-generation phase; and the plaintiff, the defendant, and the agreed adjudicators in the dispute-resolution phase. Generally, the type of role played by various entities depends on the cryptographic techniques employed. 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. In addition, to accord with legal restraints and the validity of evidence, most application systems employ digital signature techniques to provide non-repudiation evidence. The evidence subjects, for the most part, act as the evidence generators, and the evidence users are also the evidence verifiers. Third, in the dispute-arbitration step, the arbitration criterion is determined by the non-repudiation policy. The policy can include the following items [5]: (i) rules for the generation of evidence; (ii) rules for the verification of evidence; (iii) rules for the storage of evidence; (iv) rules for the use of evidence; and (v) rules for adjudication. After arbitration, the last step is to announce the decision, indicating the truth or existence of something.

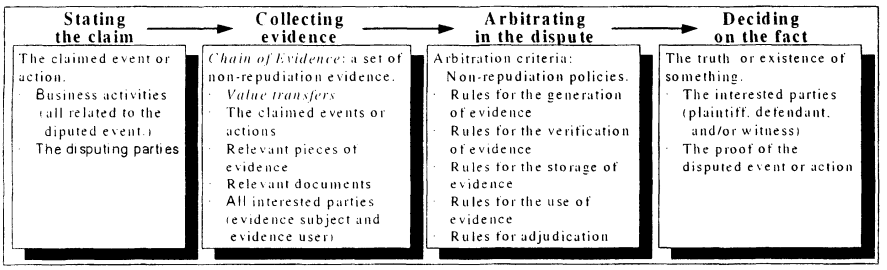

Figure 1. Dispute-resolution procedure

3. VALUE-TRANSFER CYCLE

The section demonstrates value transfers in a business transaction and shows how to form a whole cycle of value transfer. Pfitzmann and Waidner [9] indicated that one of the major distinctions among payment systems is the point at which there is money transfer between the payment initiator and the receiver. The basic function of these payment systems is to provide value transfer among different players. Generally, the basic set of players involved in the payment transaction is made up of the payer, the payee, and the financial institutions (including the issuer interacting with the payer and the acquirer interacting with the payee). Value transfers between the issuer and the acquirer occur in proprietary banking systems, which are outside the scope of the generic payment service [1]. In the study of on-line payment and that of dispute resolution, the word *bank* often signifies various types of 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 based upon the work of Pfitzmann and Waidner. These three types of value transfer are: (i) value subtraction; (ii) payment; and (iii) value claim. The three value transfers, taken together, fully sketch the profile of the payment service in a transaction. A partial view of the payment service involves a subset of the players, and their interaction is an instance of what is defined as a 'primitive transaction'. The 'primitive transaction' of *value subtraction* is to convert 'real value' into electronic value. Normally, a bank and a payer engage in a value subtraction. In other words, the payer allows the bank to remove real value from the payer's account. In a *payment*, the players involved in the transaction are a payer and a payee. The payer moves electronic value to the payee. Then the payee requests the bank to convert electronic value into real value in the primitive transaction of a *value claim.*

However, these three primitive transactions of monetary value transfer portray only a part of a usual composite transaction. In the past few years, the development of global B2C markets has been held up by insufficient support of distribution channels. Business transactions are conducted online, but with inadequate logistics services. Many disputes arise from the product-delivery service. Due to this, customers can be more or less reluctant to

proceed to the purchase phase and complete a transaction on the Internet. According to a survey of the means of on-line payment polled by ActiveMedia research group, a majority (56 percent) of Internet shoppers prefer off-line payment (such as telephone, fax, or account transfer) to on-line payment. To help overcome the challenge of consumer concerns regarding delivery, business alliances between Internet retailers (especially 'pure' virtual stores) and off-line distributors, so-called 'click-and-brick' alliance or 'B2B2C', can be very effective to support the overall transaction—including payment and delivery services. No activity in business is independent of others and the successful conducting of a series of activities usually brings about a completed business transaction. The series of business activities thus also involve a cycle of value transfers. The cyclic model should comprise at least two types of value—the movement of monetary value and the ownership of purchased-object value transfer form the essence of a value transfer cycle (as illustrated in Fig. 2). In Fig. 2, a solid line represents the movement of monetary value whereas a dotted line shows the delivery of purchased-object value, with the direction of the arrowhead reflecting the direction of value transfers between parties. The movement of monetary value is defined in the work of Asokan et al. [2] as noted above. With regard to the delivery of purchased-object value, an intermediary agent, called a delivery authority (DA), is usually involved in the distribution process. One or more DAs, trusted by the seller and the buyer, provide delivery services in accordance with the terms of the sale and the nature of the purchased object. The delivery can precede, follow, or accompany the exchange of monetary value. Considering the overall distribution process, we define three type of value transfers—(i) value submission; (ii) value transport; and (iii) purchased-object delivery. These three constitute the ownership value transfer. The *purchased-object delivery* is initiated from the buyer as specifying shipping method along with payment, but is transferred from the seller to the buyer often later than the successful transfer of monetary value. The players involved in a *value submission* are the payee and a DA. That is, the payee consigns goods or services to the DA in accordance with the sales agreement. The DA is responsible for delivery to the intended recipient on time. The players involved in a *value transport* are a DA and a payer.

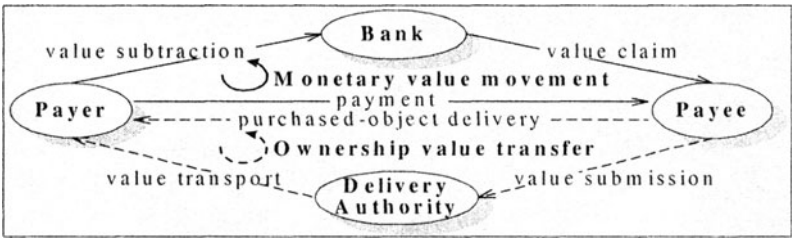

Figure 2. A cycle of value transfers for a typical business-to-consumer transaction

4. EVIDENCE MANAGEMENT

The section introduces the concept of a chain of evidence to reinforce evidence accountability in ISO/IEC standards. Particularly, we show how to begin from a cycle of value transfers and then obtain the evidence chain.

4.1 Non-repudiation services

There are four types of exchanges between the buyer and the seller in a typical commercial transaction. These are: (i) information enquiry and response; (ii) agreement on the terms and conditions of the sale and payment; (iii) payment instructions provided by the buyer; and (iv) shipment and delivery of the items acquired done by the seller. The transferring or receiving of messages during these exchanges can be regarded as a commitment, and can be recorded as evidence. The protection of such digital evidence against injury depends on cryptographic techniques. Both symmetric (secret-key) and asymmetric (public-key) cryptographic techniques can be used for non-repudiation. Technically speaking, there are three particular forms of evidence [5]: (i) digital signatures using public key techniques; (ii) secure envelopes and (iii) security tokens both using secret key techniques. Functionally speaking, the ISO/IEC 13888-1 standard defines four main types of document demanded for non-repudiation services, all related to the transfer of messages between the two communicating parties. They are: (i) proof of origin; (ii) proof of delivery; (iii) proof of submission; and (iv) proof of transport. The *proof of origin*, notated as Non-Repudiation of Origin (NRO), is intended to prevent foul play on the part of the sender in the form of denial of being both the creator of a message and the sender of that message. The *proof of delivery*, notated as Non-Repudiation of Delivery (NRD), itself contains (a) proof of receipt and (b) proof of knowledge simultaneously. The first of these, proof of receipt, is notated as Non-Repudiation of Receipt (NRR), and is intended to prevent a recipient's foul play in the form of denial of having received a message. The second of these, proof of knowledge, is notated as Non-Repudiation of Knowledge (NRK), and means that the recipient is aware of the content of the message. The *proof of* submission, notated as Non-Repudiation of Submission (NRS), means that the delivery authority was commissioned to transmit the purchased object for the seller but, in most case, wasn't well aware of the content of the object. The *proof of transport*, notated as Non-Repudiation of Transport (NRT), is intended to prevent the delivery authority's false denial of having delivered the purchased object to the intended recipient. The last two proofs, NRS and NRT, cover the cases in which one or more delivery authorities are involved in transfer of the purchased object between a sender and a recipient. Furthermore, if two or more delivery authorities participate in a delivery order, NRS is also suitable for evidence that proves the transmission of the object between them.

As a whole, there are at least four roles involved in a non-repudiation system during a cycle of value transfers: (i) the payer; (ii) the payee; (iii) banks; and (iv) the delivery authority. The role of the delivery authority (DA) in this paper is rather different from that in the ISO standards defined for non-repudiation services. DA in these ISO documents is a third party trusted by the sender who delivers digital data from the sender to the receiver—as in the cases of Internet service providers, B2B exchanges, and e-marketplaces. Furthermore, the DA in a value-transfer cycle provides services in the delivery of physical or information goods. FedEx is a classic example.

4.2 Chain of evidence

Non-repudiation services establish one piece of evidence regarding a particular event or action. One piece of evidence offers information that can be used to prove the occurrence or non-occurrence of an event or action, but does not necessarily establish the truth of that event or action. Once each piece of evidence is generated, the next step is to provide for its accountability of each event or action 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 examined or ensured through cryptography techniques. With respect to management factors, the key point is how to make a conjunction with every piece of evidence stored in a computer somewhere, in order to draw a map of the evidence. A map of evidence presents clues as to the overall truth of a situation, and is therefore useful in evidence collection in the dispute-resolution phase. Only by clarifying the causality of an event can the truth be ascertained. Evidence generation usually goes along with a specific event or action that has taken place. So, a set of gathered evidence will reflect a sequence of business activities named a cycle of value transfers. Consequently, the map of evidence in this paper is defined as a 'chain of evidence'. The chain-of-evidence concept was originally introduced by Welch [11], where it served as a means of tracing accountability by law-enforcement agencies in their conduct of criminal investigations. The detailed items in the chain of evidence include such matters as who obtained the evidence, where and when the evidence was obtained, who secured the evidence, and who has control or possession of the evidence.

A chain of evidence, as applied to a business transaction, must be obtained from a cycle of value transfers. Any event or action can trigger various business activities, or value transfers, at any given time. To identify value transfer in every phase of the transaction, it is first necessary to identify the relevant event or action. In the following, we consider a specific set of events or actions, all of which 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 for electronic commerce. We now define a 'primitive event' as an abstract of a specific set of events or actions for a general B2C transaction. The above procedure of establishing a chain of evidence is depicted in Fig. 3.

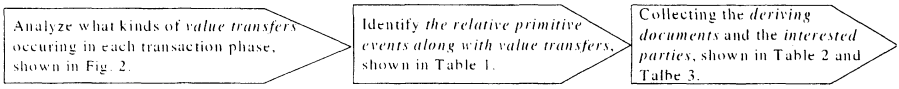

Figure 3. The procedures for establishing a chain of evidence

The detailed treatment of the primitive events is according to a cycle of value transfers. With respect to the primitive events for monetary value movement, Pfitzmann and Waidner [9] have defined some interface events for digital payment systems. Although interface events and primitive events are not identical in views, we will make their efforts fit for our works. In particular, there are three standard input interface events—*pay*, *receive*, and *allow*. The pay event is initiated, or consented to, by a buyer in making a payment; the receive event is an input by the merchant who responds to the pay event from a buyer; the allow event is an input by the buyer's bank which checks his or her account of external money to ensure that there is enough to make an electronic payment. In addition, the major output events are the following: *deduct*, *add*, *paid*, and *received*. The deduct event gives the buyer's bank notice to deduct the authorized money from his or her account; the add event notifies the merchant's bank to add the authorized money to the merchant's account; the paid event and the received event indicate to the buyer and the merchant, respectively, that an authorized payment has been fulfilled. In effect, the paid event is the successful culmination of the allow event and the deduct event. The received event must take another event into consideration. This is 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 event and the add event have been accomplished. Therefore, we do not consider "paid" and "received" as primitive events, and do not include these in Table 1.

With respect to the composite event of purchased-object value delivery, we define six basic primitive events according to the overall distribution process. These six events are all concerned with the generation of evidence during the ownership of purchased-object delivery. They are: (i) the *submit* event (in which the merchant commissions the delivery authority to provide shipment service of the purchased object); (ii) the *undertake* event (which signals the delivery authority to accept the commission); (iii) the *shipping-to* event (which is an input by the buyer that chooses shipping method and preference for the purchased objects, e.g. goods or services); (iv) the *shipping-from* event (which is the corresponding input by the merchant); (v) the *delivery* event (by which the delivery authority transports the purchased object to the intended recipient); and (vi) the *obtain* event (which signals that the buyer has received the purchased object). By analyzing these primitive events, we clarify the relation of value transfers further, as shown in Table 1.

*Table 1.*The relation between the primitive events and 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

As far as monetary value movement is concerned, either the deduct event or the allow event can launch a primitive transaction of value subtraction. A primitive transaction of payment is connected with either the pay event or the receive event. A primitive transaction of value claim is related to the liquidate event or the add event. With respect to ownership value transfer, a primitive transaction of value submission is related to the submit event or the undertake event. A primitive transaction of purchased-object delivery is in connection with the shipping-from event or the shipping-to event. Either the delivery event or the obtain event can launch a primitive transaction of value transport. In particular, depending on the specific situation some primitive events will turn into a composite event, which is formed with other primitive events. For example, in view of monetary value transfer by means of credit card, the pay event and the receive event, respectively, is a composite event; the pay event is the successful fulfillment of the allow event and the deduct event, and further, the receive event is the successful fulfillment of the liquidate event and the add event. By contrast, the pay event and the receive event are primitive events as payment by remittance or credit transfers.

Evidence is generated on the data describing the occurrence 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. Documents derived from these events can be classified as various types of evidence, according to the purpose of each. In the meantime, the interested parties in a chain of evidence take most account of the evidence subject and the evidence user. The evidence subject whose involvement in an event or action is established by evidence [5], and the entity is also the event initiator. The evidence user, who uses non-repudiation evidence, is usually in opposition to the evidence subject, and the entity is also the event claimant. Therefore, the interested parties engaging in the event—consisting of the event initiator and the event claimant—are recognized. This shows a chain of evidence must be identified in order to trace the accountability of each event along the cycle. In order to distinguish the notation about

evidence purpose defined by ISO/IEC 13888-1 standard from our suggestion, the chain of evidence for a typical B2C transaction is divided into two tables upon value transfers. Table 2 shows the evidence chain associated with monetary value transfers, and the other one—ownership value transfer—is depicted in Table 3. These primitive events are continued from table 1, and each of their derivative documents is a general name of transactional information. The notation about evidence purpose is according to specific non-repudiation service and then in conjunction with value transfers upon the primitive event occurred. Specifically, the non-repudiation services all related to the transfer of messages over network in the pertinent standards [4, 5, 6, 7]. Considering monetary value movement is covered in the case, a part of notation for evidence purpose uses two types of non-repudiation evidence—NRO and NRR—in the ISO/IEC 13888-1 standard.

Table 2. A chain of evidence associated with monetary value transfers.

Primitive Event	Derivative Document	Evidence Purpose (Defined by ISO/IEC 13888-1)	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

As regards the ownership of purchased-object, especially physical object, value transfers, non-repudiation evidence can be filled in with moderate difficulty given previous standards or other literature. In view of this, we suggest the *proof of purchased-object delivery*, notated as Non-Repudiation of Purchased-object Delivery (NRPD), as a solution of evidence purpose for ownership value transfer. The non-repudiation of purchased-object service covers the case regarding the product, such as the possession of goods or services, shipping preference, and so on. For example, the service is intended to protect against a holder's false denial of having agreed shipping method and/or possessed the product.

Table 3. A chain of evidence associated with ownership value transfer.

Primitive Event	Derivative Document	Evidence Purpose (Suggested by the authors)	the Interested Parties	
			Event Initiator	Event Claimant
Submit	Consignment Receipt	NRPD_Value Submission	DA	Payee
Undertake				
Shipping-from	Shipping Agreement	NRPD_Purchased-object Delivery	Payee	Payer
Shipping-to			Payer	Payee
Delivery	Acknowledgement Receipt	NRPD_Value Transport	Payer	DA / Payee
Obtain				

In the case of an electronic transaction environment, we define nine main types of evidence and their derivative documents from the primitive events in a cycle of value transfers. The descriptions are as follows: (i) The document of *payment instruction* prepares non-repudiation evidence of a value subtraction primitive transaction, notated as NRO_Value Subtraction. It indicates the occurrence of the allow event. The initiator of the allow event is the payer, and the allow event claimant is the bank. (ii) The document of *payment authorization* offers non-repudiation evidence of a value subtraction primitive transaction, notated as NRR_Value Subtraction. It proves the occurrence of the deduct event. The event initiator is the bank, and the payer is the event claimant. (iii) The *purchase order* offers non-repudiation evidence of a payment primitive transaction, notated as NRO_Payment. The document is toward the accountability of the pay event. The payer is the event initiator and the payee is the event claimant. (iv) The *confirmation and invoice* offers non-repudiation evidence of a payment primitive transaction, notated as NRR_Payment. It traces the occurrence of the receive event. The payee is the event initiator and the payer is the event claimant. (v) The *capture claim* document offers non-repudiation evidence of a value claim primitive transaction, notated as NRO_Value Claim. It aims to account for the liquidate event. The payee is the event initiator and the bank is the event claimant. (vi) The *capture acceptance* document offers non-repudiation evidence of a value claim primitive transaction, notated as NRR_Value Claim. It testifies that the add event has taken place. The bank is the event initiator and the payee is the event claimant. (vii) The *consignment receipt* provides for non-repudiation evidence of a value submission primitive transaction, notated as NRPD_Value Submission. In the case in which the delivery authority provides evidence to the merchant (payee), the event initiator is the delivery authority and the event claimant is the merchant. (viii) The *shipping agreement* regarding the product delivery, such as 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 (payer) and the merchant, this document, as notated NRPD_Purchased-object Delivery, can be used to account for two events—the shipping-to event and the shipping-from event. For the shipping -to event, the buyer is the event initiator and the merchant is the event claimant; and further, as regards the shipping-from event, the merchant is the event initiator and the buyer is the event claimant. (ix) The *acknowledgement receipt* provides non-repudiation evidence of a value transport primitive transaction, notated as NRPD_Value Transport. In the case in which the recipient acknowledges to the delivery authority and the merchant that the purchased object has been duly received, the event initiator is the recipient and the event claimant is the delivery authority and the merchant.

5. CONCLUSIONS

Even if a transaction is concluded successfully, there can be subsequent disputes about what happened during the transaction. Having observed that it is a common practice to operate non-repudiation services in traditional markets, but not in the electronic marketplace, we have attempted to propose a better evidence-management model as an appropriate basis for disputes resolution in electronic commerce. In reviewing previous research efforts, including the international standards, it is apparent that non-repudiation services deal essentially with single pieces of evidence. Each piece of evidence can provide information to account for a claimed event or action, but it is quite limited in attempting to learn about the total context. Only if evidence is viewed in conjunction with business activities will the context of the occurrence of the event be clarified. For this purpose, we introduce the chain-of-evidence concept into the idea of a non-repudiation service, in order to associate it with a series of activities. We also show a cycle of value transfers that presents a series of activities to form a whole business transaction. Consequently, a chain of evidence can trace accountability of each event along the cycle. The main contribution of the present paper is to establish chain of evidence in order to work for the betterment of non-repudiation services for electronic commerce.

ACKNOWLEDGEMENTS

Part of this research was funded by the National Science Council of Taiwan under the contract of NSC 91-2416-H-182-209-, while the first author of this article was working at National Chiao Tung University.

REFERENCE

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

[2] Asokan N., Herreweghen E.V., Steiner M., Towards a framework for handling disputes in payment systems, *3rd USENIX Workshop on Electronic Commerce*, Sep. 1998, pp. 1– 28.

[3] Coffey T. and Saidha P., Non-repudiation with mandatory proof of receipt, Computer Communication Review (26:1), Jan. 1996, pp. 6– 14.

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

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

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

[7] ISO/IEC 13888-2. *Information technology—security techniques—non-repudiation part 2: mechanisms using symmetric techniques*, 1997.

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

[9] Pfitzmann B., Waidner M., Properties of payment systems: general definition sketch and classification, *IBM Research*, Research Report RZ 2823, May 1996, pp. 1– 28.

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

[11] Welch T., *Handbook of information security management*, In M. Krause and H.F. Tipton (Eds.), Boca Raton, Fla.: Auerbach, 1999.

[12] You C.H., Zhou J. and Lam K.Y., On the efficient implementation of fair non-repudiation, *Computer Communication Review* (28:5), Oct. 1998.

[13] Zhou J., Evidence and non-repudiation, *Journal of Network & Computer Applications*, Jul. 1997.

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