ELSEVIER

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*

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.
© 2004 Elsevier B.V. All rights reserved.

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).

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
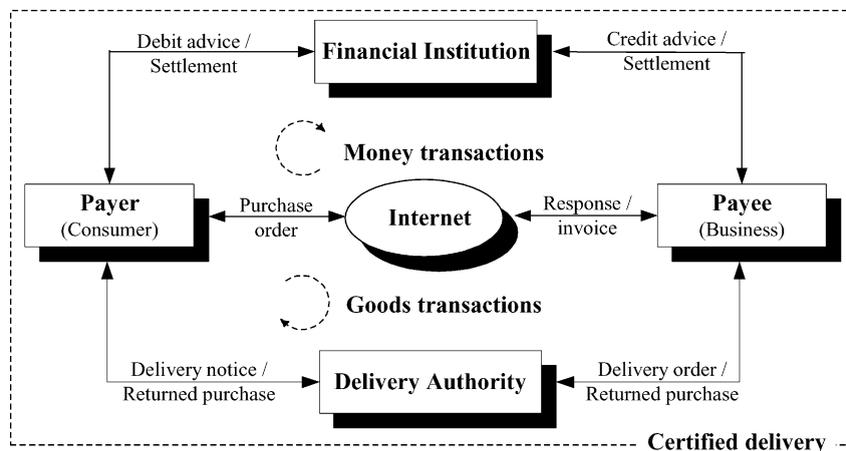

Fig. 1. A typical business-to-consumer transaction cycle.