32

Trading among Untrusted Partners via Voucher Trading System

Ko Fujimura and Masayuki Terada
NTT Information Sharing Platform Laboratories

Abstract: To provide highly usable electronic commerce systems at lower cost, it is important to utilize and co-ordinate the function-specific application service providers (ASPs) that are distributed throughout the Internet such as those providing matching, payment, and delivery services. In order to coordinate independent services that have not yet established trust among each other, this paper proposes to use electronic "vouchers" to link untrusted trading partners. A voucher is a digital representation of rights to claim goods or services and can be securely transferred between trading partners using the Voucher Trading System (VTS). This paper clarifies the basic functionalities that VTS should provide for coordinating untrusted trading partners.

1. INTRODUCTION

Electronic commerce (e-commerce) is generally conducted in three phases: (1) the marketing/matching phase in which consumers search for merchandise they want to purchase and negotiate with vendors, (2) the contract/payment phase in which the desired merchandise are ordered and purchased, and (3) the delivery/service phase in which the purchased merchandise are delivered or services are rendered.

Many e-commerce systems now provide all of the three phases mentioned above, but their level of usability is limited because of their excessive development costs. A recent trend is the establishment of highly usable and low-priced Application Service Providers (ASPs) that provide services restricted to a specific phase. Recently, product manufacturers and service providers have started constructing marketing channels to consumers by coordinating component ASPs (Figure 1). The reason for this is that this type of direct channel can reduce the costs of the value chain, and each of the three phases can be flexibly combined to satisfy the consumers' diverse requirements. On the other hand, in this form, the delay of

each phase becomes significant as described below. Technology that co-ordinates these dispersed independent services is a key goal for realizing the next generation of e-commerce.

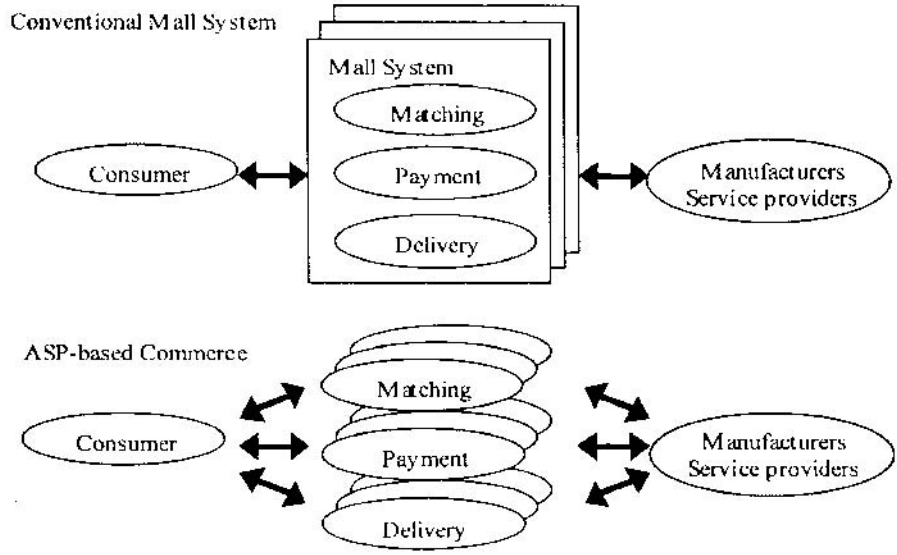

Figure 1. Transition in e-commerce

Specialization. When the three phases are provided by different, autonomous organizations, completion of service provision demands that the physically separated organizations must be able to co-operate with each other. In general, though the term is e-commerce, not all the phases are electronic. Searching for merchandise and negotiating in the matching phase are performed on the Internet, but the payment for and the delivery of merchandise will often be conducted at convenience stores or convention halls in the real world.

Time dispersion. There is no delay between the payment and delivery phases when the merchandise is exchanged for money. However, in the transportation or entertainment industry, payments are generally made for future services. For example, a passenger purchases a ticket before riding on a train. By collecting the money from the consumers beforehand, the number of cancellations can be reduced and important resources such as seats on a train or in a theater can be better utilized. In these cases, the time between payment and delivery can range from several minutes to several months.

Throughout history, physical “slips of paper” called tickets or coupons have been used for coordinating these spatially and temporally dispersed processes. The tickets or coupons are considered to be a physical representation of rights to claim goods and services. In other words, as the result of the payment transaction, the generic

value represented by "money" is exchanged for specific rights represented by "slips of paper" and these slips of paper are used to confirm prior payment at the time the goods or services are delivered. These slips of paper representing rights do not just fill the gap between payment and delivery, they also represent a medium that fills the gap between the matching and payment phases. A discount coupon that represents the right to purchase items at certain price, or a queuing ticket that represents the right to purchase certain goods are examples of such use.

We believe that the trend towards dispersed e-commerce demands the creation of a new digital medium that can take the place of slips of paper. We call such a digital medium *voucher* in this paper. Unlike electronic money, vouchers exhibit a wide diversity in terms of the types of rights involved and issuers. Vouchers may be issued by individuals or companies, and the contents will vary widely. For this reason, if each specific voucher required a dedicated system, the implementation costs would be excessive. We, therefore, believe that a generic Voucher Trading System (VTS) capable of trading a wide variety of vouchers in which a large number of issuers can participate and share costs is essential.

This paper proposes a generic VTS model that can be implemented in several ways. We use application examples in discussing how independent dispersed trading partners who have not yet established trust amongst each other can be coordinated through VTS intermediation.

The rest of the paper is organized as follows. Section 2 provides a survey of related works. Section 3 describes the model of the proposed VTS. Section 4 describes a synopsis and the characteristics of typical implementation models. Section 5 presents application examples and discusses the benefits of the VTS. Section 6 discusses standardization issues and proposes a wallet architecture that achieves interoperability without sacrificing implementation flexibility. In this section, the trust model assumed in the architecture is also presented. Section 7 concludes the paper.

2. RELATED WORK

There are several previous studies that provide technologies useful for VTS implementation. Since the 1980s, hundreds of schemes have been proposed for implementing "electronic cash" [17]. Some of them can also be applied for implementing VTS, especially for preventing double-spending. This paper thus does not intend to propose a new/particular method for preventing double spending. Instead, this paper clarifies the basic functionalities that VTS should provide for coordinating untrusted trading partners.

TEDIS, EDIBOL [14], and Mandate [12] address the technical, business, and legal issues of circulating financial instruments, e.g., electronic checks and Bill of Lading. They also made many suggestions collected through their experience with

pilot systems. The main focus of these works is large scale B2B transactions in which PKI or trustworthy identifiers of trading partners can be assumed. To the contrary, this paper focus on B2C or C2C transactions in which cost sharing is essential, and PKI cannot be assumed.

SEMPER [11] provides a generic payment service framework that allows users to handle several payment schemes in a flexible way. Its approach is comparable to ours, but our goal is to provide a more simple solution by assuming the VTS model.

Ricardo System [8] and SOX [10] provide a payment platform that enables a wide-range of financial instruments to be traded. Their system introduces a value description system called Ricardian Contract, which specifies two separate issuer entities, i.e., legal issuer and technical issuer. The legal issuer is responsible for backing the value of the instruments and the technical issuer is responsible for managing the instruments. This separation is also a key concept of this paper and we present a formal model.

We have also developed an implementation of VTS called FlexTicket and presented some techniques in previous papers. [6][7] are early studies that address the language needed to define diverse types of rights. In [13][15], we presented protocols that assured the "genuineness" of vouchers that were circulated. However, none of the previous papers focused on the business aspects of VTS.

This paper is based on a discussion within the IETF trade WG[48] and presents details of background and implementation models, in addition to the requirements, terminologies, and standardization interfaces presented in [4][5].

3. RIGHTS TRADING MODEL

3.1 Vouchers

A voucher[49] is a digital representation of the right to claim goods or services. A voucher is generated by an issuer when the issuer (e.g., manufacturer or service provider) makes a certain promise to a holder (e.g., consumer). This paper thus defines a voucher as follows:

> **Definition.** Let *I* be a voucher issuer, *H* be a holder, *P* be the issuer's promise to the holder. A *voucher* is defined as the 3-tuple of <*I, P, H*>.

Vouchers differ from electronic cash since *I* and *P* can represent a wide variety of issuers and contents, respectively. Contents can cover a wide range: one voucher may state that it can be exchanged for a hamburger, another may state that it can be

[48] The IETF trade WG mainly addresses B2C payment protocols and has developed IOTP [1] which encapsulates and supports diverse types of payment systems.

[49] The previous studies often call this concept "ticket," "right," or "bearer instrument [9]."

exchanged for one night's lodging, while a third may state that it can be exchanged for 2 dollars worth of train travel. The contents of a voucher can even represent some monetary value; the voucher may indicate that it can be exchanged for 100 dollars worth of merchandise. (Note: *P* does not need to be described in terms of a natural language provide the contents of the vouchers are specified. For example, the contents can be defined by XML to facilitate machine processing, and the identifier or hash value of the XML document can be used to specify *P*.)

3.2 Participants

In this paper, the VTS consists of four participants: the issuer, the holder (or user), collector, and VTS provider. The roles of each participant are as follows:

Issuer: Creates and issues a voucher. Guarantees the contents of the voucher.

Holder (or user): Owns the voucher. Transfers and redeems the voucher to other users or collector.

Collector (or examiner): Collects the voucher: generally accompanied by the transfer of goods or the rendering of services. Note that the roles of collector and issuer can be done by the same entity.

VTS provider: Provides the VTS and guarantees that there are no duplicate assignments or multiple use of vouchers.

The issuer generates the voucher, $< I, P, H >$, and the vouchers are circulated among users in the VTS until finally they are collected. The VTS provider provides the trading system to the issuer, user, and collector, and is assumed to be trusted by the other participants (Figure 2).

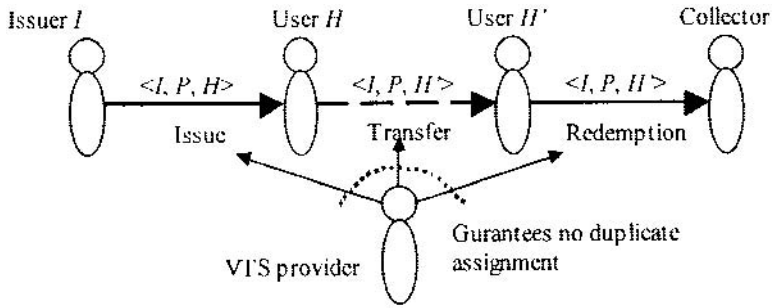

Figure 2. Participants and roles

3.3 Voucher Trading System

The purpose of the VTS is to provide a means of circulating issuer-generated vouchers among the users. The system must satisfy the three requirements described below:

Prevention of forgery: It must be impossible to counterfeit vouchers. Only the issuer generates vouchers.

Prevention of alteration: It must be impossible to alter vouchers during circulation.

Prevention of reproduction: It must be impossible to reproduce or copy vouchers during circulation. Multiple transfers or duplicate redemptions are to be prohibited.

A formal definition of a system that satisfies these requirements is given below.

Definition. A *Voucher Trading System* is a system that logically manages a set of valid vouchers $R \subset \{<I, P, H> \mid I \in I, P \in P, H \in H>\}$ where I is the set of issuers, P is the set of promises, and H is the set of holders; VTS prevents the vouchers from being modified or reproduced except as part of the three transactions of issue, transfer, and redemption. The initial state of R is an empty set.

Issue: An *issue transaction* is the action that creates the tuple $<I, P, H>$ and adds it to R to reflect the issuer's intention.

Transfer: A *transfer transaction* is the action that rewrites the tuple of $<I, P, H>(\in R)$ as $<I, P, H'>(H \neq H')$ to reflect the original holder *H*'s intention.

Redemption: There are two redemption transactions: presentation and consumption. A *presentation transaction* is the action that shows the tuple of $<I, P, H>(\in R)$ to reflect the holder's, *H,* intention. In this case, the ownership of the voucher is retained when the voucher is redeemed, e.g., redemption of licenses or passports. A *consumption transaction* is the action that deletes the tuple of $<I, P, H>(\in R)$ to reflect *H*'s intention. In this case, the ownership of the voucher may be voided or the number of times it is valid reduced when the voucher is redeemed, e.g., redemption of event tickets or telephone cards.

4. IMPLEMENTATION MODELS

The Voucher set, R, described in Section 3, is logical, and management can be centralized on a network server or it can be dispersed across portable devices (e.g., smart cards) maintained by the users. This section gives a synopsis and the characteristics of these implementation styles.

(1) Server storage type

In this model, the VTS provider manages a centralized server in which sets of 3-tuple $<I, P, H>$ entries is stored. The issuing of a voucher in this model is done by authenticating *I* and storing a new entry, $<I, P, H>$, in the server. The transfer of a voucher is done by authenticating user *H* and rewriting the entry contained in the server with $<I, P, H'>$, where *H'* is the new holder of the voucher. The consumption of a voucher is done by authenticating user *H* and deleting the entry contained in the server (see [13] for an example).

A key feature of this model is that the center's cost for development and operation can be shared among the many participating issuers.

(2) Portable storage type

In this model, the VTS provider supplies each user *H* with portable devices (e.g., smart cards) that store sets of 2-tuple <*I, P*> entries. A voucher is issued in this model by authenticating *I* and storing a new entry, <*I, P*>, in the tamper-resistant storage of a portable device managed by user *H*. The transfer of a voucher is conducted by generating the digital signature that proves entry <*I, P*> was erased from the tamper-resistant storage of *H'*s portable device (this authenticates the sender's portable device) and sending it to the recipient's portable device. The receiving portable device then verifies the digital signature and stores entry <*I, P*> in its tamper-resistant storage. The consumption of a voucher is done by generating the digital signature that proves entry <*I, P*> was erased from the tamper-resistant storage of *H'*s portable device and sending it to the collector (see [15] for an example).

This model is similar to (1) above in the sense that the smart cards issued by the VTS provider can be shared by multiple issuers resulting in a decrease in the costs of card issuance and program development. Furthermore, since the redemption of vouchers can be done offline, this model is superior to the server storage type model in terms of communication cost and availability. However, since a smart card reader/writer is required at the user terminal, this model is not so popular at this moment.

The above two models are typical implementation examples of the VTS proposed in this paper. In many existing types of digital ticket systems, the issuer himself manages the issued tickets or vouchers. These types are also supported by VTS; the roles of issuer and VTS provider are merged. Typical implementation examples of such existing systems are given below and comparisons of these types are made.

(3) Issuer-managed server storage type

In this model, a set of 2-tuple <*P, H*> entries is stored on a server managed by the issuer. Vouchers are issued, transferred, or consumed in this model by authenticating *H* and adding, rewriting, or deleting the entries on the server database, respectively. One difference of this model from (1) above is that authentication of the issuer is unnecessary since the issuer is also the debtor. Moreover, on the user side, user authentication can be easily established by using a credit card or ID card. For these reasons, many instances have been developed such as the ticket-less service of airlines and a concert ticket system.

(4) Issuer-managed portable storage type

In this model, each issuer of vouchers supplies users with portable devices (e.g., smart cards) that store sets of promise *P* entries. The assumption is that a user must have one smart card from each issuer. Vouchers are issued, transferred, or consumed in this model by authenticating *H* (the validity of the card is

authenticated) and adding, rewriting, or deleting the entries in the tamper-resistant storage of the portable device, respectively. Since this method is easy to implement and enables high-speed processing, it has spread throughout the transportation industry in the form of the smart-card-based passenger ticket. Most current systems, however, do not have transfer functionality nor do they allow transfer over the Internet.

In the models where the issuer is the manager of the voucher ((3) and (4) above), the system is not fair from the user's point of view since the issuer can illegally erase the voucher from memory or repudiate the existence of the voucher. Therefore, as an application requirement, the user must trust the issuer as in the case with transportation companies. Additionally, as described in Section 1, each user in this model must develop a system capable of issuance, examination, etc., even though it is difficult for a small business to create an operation center or to issue smart cards independently. For these reasons, we believe that the model in which the tasks of voucher administration are delegated to the VTS provider is superior. One high priority goal is to minimize the trading cost of inexpensive tickets and coupons such as meal and prepaid tickets. For these applications, the portable storage type seems to be most suitable. Table 1 shows the relationships among the features of the different models.

Type \ Characteristics		Non-Repudiation	Cost sharing (Card issuance, Center operation)	Offline capability (Low communication cost)
Third party management	Server	Yes	Yes	No
	Portable device	Yes	Yes	Yes
Issuer management	Server	No	No	No
	Potable device	No	No	Yes

Table 1. Characteristics of voucher management methods

5. APPLICATION EXAMPLES

This section describes, using a typical e-commerce example involving matching, payment, and delivery, how vouchers are traded using the proposed VTS, and why VTS is effective for coordinating untrusted trading partners.

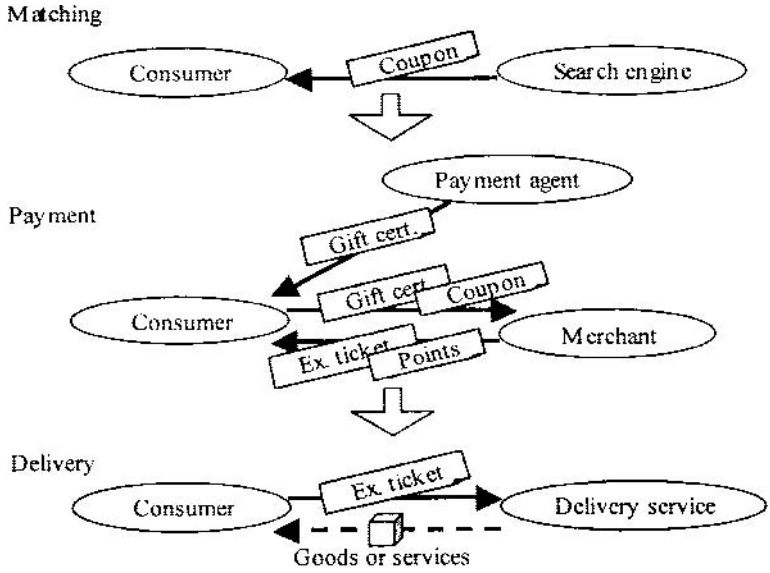

Figure 3. Typical transaction example of using vouchers

Figure 3 shows a typical e-commerce example of a consumer searching for merchandise and making a purchase:

Matching: A consumer uses a search engine to locate the desired merchandise and acquires a coupon that represents rights to purchase that merchandise at a discounted price.

Payment: The consumer purchases gift certificates from a payment agent site since "real" cash is not suitable for transferring credit. When cash is used to pay for gift certificates at a publicly accessible terminal such as an ATM terminal, the gift certificates are stored on a smart card in exchange for the cash. After getting the gift certificates, the consumer redeems the coupon and gift certificates at the merchant site; in exchange he/she acquires an exchange ticket for the merchandise and loyalty points.

Delivery: The consumer transfers the exchange ticket to the delivery service site and specifies the address to which the merchandise is to be sent.

In this example, the coupon coordinates the matching and payment phases while the exchange ticket coordinates payment and delivery phases. In particular, note that the exchange ticket ensures the cooperation of the mutually independent entities of consumer, merchant, and delivery service. In other words, there is no need to exchange contracts among the consumer, delivery service, and the merchant beforehand. The merchant exchanges the merchandise for the exchange ticket from the delivery service and the delivery service exchanges the merchandise for the exchange ticket from the consumer (Figure 4). This is possible even though the

participants involved in the transactions may not directly trust each other; all trust the vouchers themselves. For example, even if the delivery service does not trust the consumer, the merchant that issued the exchange ticket is trusted, and if the VTS guarantees that there is no duplication of the exchange ticket, there is no problem in exchanging the exchange ticket for the merchandise. In the same way, even if the merchant does not trust the delivery service, the issuance of the exchange ticket can be verified, and if the VTS guarantees that there is no duplication of the exchange ticket, there is no problem in exchanging the exchange ticket for the merchandise. In other words, if there is trust in the issuer and the VTS, the trust of the user is not an absolute necessity. In general, it is difficult to manage the trust of individuals, so this characteristic of the VTS is especially effective in B2C or C2C transactions.

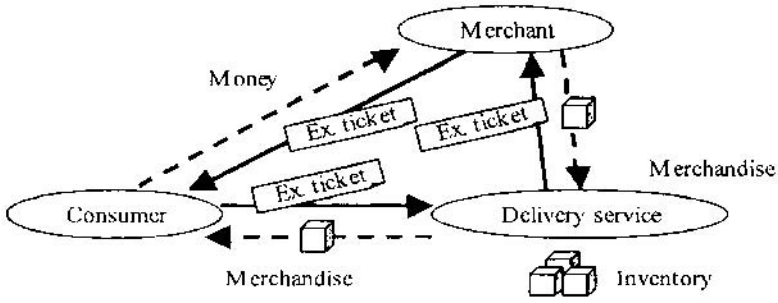

Figure 4. Trading with untrusted trading partners

Moreover, the transactions that involve vouchers have other desirable features such as privacy protection. For example in the above exchange ticket scenario, the consumer can contact the delivery service by himself, the merchant does not even need to know any personal information such as the delivery address. Furthermore, by designating a publicly accessible site such as a convenience store as the receiving point, the delivery service is prevented from learning the address of the consumer.

6. WALLET ARCHITECTURE

6.1 Processing Model

In order to realize the full benefits of VTS described in the above sections, a common VTS should be shared among a large number of consumers and services. A single VTS provider, however, is also impractical, because security level and performance requirements differ with the application. For discount coupons or event tickets, for example, the portable storage type VTS is often preferred, whereas for bonds or securities, the server storage type VTS is preferred. Moreover, each issuer

must have the right to specify the trusted VTS providers delegated to circulate the vouchers, because if the VTS provider illegally copies the vouchers, the issuer would incur a loss due to the illegal copying.

Multiple VTS, however, will rise the issue of interoperability and may force consumers to install a "digital wallet" for each VTS. For these reasons, we believe some standard specifications should be developed to achieve interoperability. As shown in Section 4, however, there are several ways of implementing the VTS and technologies are continuously changing. It is impractical to define standard protocols for issuing, transferring, or redeeming voucher at this moment.

To provide implementation flexibility, we propose a modular wallet architecture that allows additional VTSs to be added as modules. In this architecture, instead of specifying a standard voucher transfer protocol, two specifications, i.e., Voucher Component and VTS API specifications, are standardized (Figure 5) [4] [5].

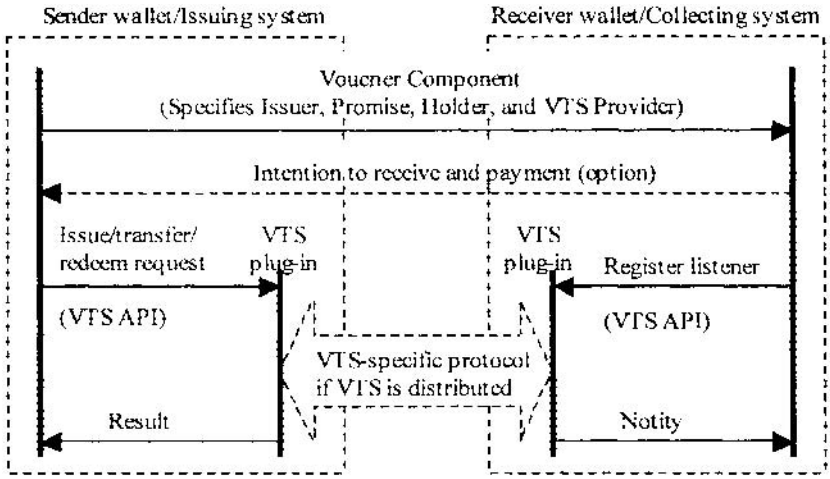

Figure 5. Wallet architecture with VTS plug-ins

The Voucher Component is an XML component that contains branding information for letting the receiver know which VTS plug-in can be used for receiving the voucher. The component also contains standard properties needed to display the entities in the wallet, e.g., name of the issuer and the title of the voucher.

After sender and receiver agree on what vouchers are to be traded and which VTS is to be used, the issuing system or wallet system requests the corresponding VTS plug-in to permit the issue, transfer, or redeem transactions to be performed via the standard VTS API. The VTS then rewrites the ownership of the voucher using a VTS-specific protocol. Finally, a completion result/notify is sent to the wallet systems or issuing/collecting systems.

6.2 Trust Model

A voucher is trusted if the Issuer and VTS Provider are trusted, since the Issuer is responsible for the contents of the voucher and the VTS Provider is responsible for preventing ownership from being assigned to multiple users. The trust level required for Issuer and VTS Provider depends on the type (or Promise) of the voucher. To provide the information needed for verification, we propose to specify the conditions of Issuer and VTS Provider in the Voucher Component and given as input to the verifier, which is provided as a function of the wallet system. The trust in a voucher is thus verified through the Voucher Component. This model enables trading partners to verify their trust in the voucher regardless of the trust in the partners.

In this model, the Voucher Component is the root of trust and must be delivered securely, since a forged voucher could be verified as valid if a malicious user could alter the Voucher Component. Delivery of the Voucher Component exceeds the scope of this paper, since existing technologies, such as XML digital signature [2] SSL [3], or IPSEC [16], can be used. Note that the Voucher Component does not have to be sent from the sender of the voucher. It can be directly delivered from the issuer or trusted third party using SSL. Note also that a set of trusted Voucher Components can be pre-downloaded before conducting a transaction.

7. CONCLUSION

E-commerce systems on the Internet are becoming increasingly complicated and diverse. Against this backdrop, technologies that coordinate multiple e-commerce services are becoming more important. This paper proposed a Voucher Trading System (VTS) for coordinating transactions conducted among untrusted trading partners, such as consumers, and matching, payment, and delivery services. This approach enables companies or individuals to trade goods or services via the Internet without demanding trust in the identity of trading partners. All that is needed is trust in the vouchers themselves, just like the paper-securities-based transactions of the real world.

This paper proposed a VTS model and showed that it can be realized in several ways. This paper also discussed the importance of standardization and proposed an architecture that achieves interoperability without sacrificing implementation flexibility. We are currently developing Voucher Component and VTS API specifications in the IETF trade WG to establish voucher trading as the infrastructure of e-commerce.

8. ACKNOWLEDGEMENT

This work is based on discussions within the IETF trade WG. I would like to thank all active members of the WG, especially Donald E. Eastlake 3rd, Ian Grigg, and Renato Iannella for providing encouragement and helpful comments.

9. REFERENCES

[1] D. Burdett, “Internet Open Trading Protocol – IOTP Version 1 .0," RFC 2801, IETF, 2000.

[2] D. Eastlake, J. Reagle, D. Sole, et al., "XML-Signature Syntax and Processing," W3C Candidate Recommendation, W3C, <http://www.w3.org/TR/xmldsig-core/>, 2000.

[3] A. Freier, P. Karlton, and P. Kosher, "The SSL Protocol Version 3.0," IETF Internet Draft, <http://home.netscape.com/eng/ssl3/draft302.txt>, 1996.

[4] K. Fujimura, "Requirements for Generic Voucher Trading," IETF Internet Draft, draft-ietf-trade-drt-requirements-02.txt,2001.

[5] K. Fujimura and M. Terada, "XML Voucher: Generic Voucher Language," IETF Internet Draft, draft-ietf-trade-voucher-lang-0 1 .txt, 2001.

[6] K. Fujimura and Y. Nakajima, "General-purpose Digital Ticket Framework," *3rd USENIX Workshop on Electronic Commerce,* pp. 177-186, 1998.

[7] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine, "Digital-Ticket-Controlled Digital Ticket Circulation," *8th USENUX Security Symposium,* pp. 229-238, 1999.

[8] I. Grigg, "Financial Cryptography in 7 Layers," *Pre-proceedings of the Fourth Annual Conference of Financial Cryptography,* 2000.

[9] R. A. Hettinga, "A Market Model for Digital Bearer Instrument Underwriting," <http:llwww.philodox.com/modelpaper.html>, 1998.

[10] G. Howland, "Development of an Qpen and Flexible Payment System," Systemics Ltd., <http://www.systemics.corn/docs/sox/overview.html>

[11] G. Lacoste, B. Pfitzrnann, M. Steiner, and M. Waidner (Eds.), "SEMPER - Secure Electronic Marketplace for Europe," LNCS 1854, Springer-Verlag, 2000.

[12] MANDATE II Consortium, "MANDATE final report," Draft version 2.0, 1998.

[13] K. Matsuyama and K. Fujimura, "Distributed Digital-Ticket Management for Rights Trading System," *1st ACM Conferences on Electronic Commerce,* pp. 110- 118, 1999.

[14] A. Schmidt’ "TEDIS II - EDICON final report," 1997.

[15] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Right Trading Infrastructure," *4th Smart Card Research and Advanced Application Conference (CARDIS),* IFIP 52, Kluwer Academic Publishers, 2000.

[16] R. Thayer, N. Doraswamy, and R. Glenn, "IP Security Document Roadmap," RF62411, IETF, 1998.

[17] P. Wayner, "Digital Cash," Academic Press Ltd., 1997.