New Technology Reports

Fair Electronic Voucher Exchange Technology for Mobile Terminals

Masayuki Terada, Kensaku Mori,
Kazuhiko Ishii and Sadayuki Hongo

To realize safe electronic commerce, it is necessary to guarantee transaction fairness. We established a method for safe and fair transactions involving currency, tickets and other such items of value implemented in the form of electronic vouchers. We also evaluated practicality of the method with a prototype system.

1. Introduction

A mobile terminal "electronic wallet" service called "Osaifu-Keitai" in Japanese launched in 2004. It is an epoch-making service for mobile terminals that goes beyond the exchange of phone calls and e-mail.

Osaifu-Keitai offers users the convenience such as not requiring small change when paying for goods at stores that are equipped with specific terminals. While the scenario for using Osaifu-Keitai has so far been limited to settlement of over-the-counter store purchases, the application range will broaden and provide even greater convenience to users if it can also trade other kinds of valuable items such as tickets and coupons, by using network function of mobile terminals.

For the future of Osaifu-Keitai, we have been conducting R&D on technology for safe transactions among mobile terminal users via a network. Such transactions will not be limited to money, but will extend to various kinds of electronic vouchers.

This technology allows users to use their mobile terminals to buy, sell and exchange electronic vouchers that can represent money including local currency, incentive point cards and other forms of currency, tickets or coupons including admission tickets, gift certificates, discount coupons, and digital rights including access rights to digital music, movies and books. Since most commerce transactions can be mapped onto exchanges of vouchers representing the item to be traded, the integration of transactions on these various kinds of vouchers will transform the mobile electronic wallet into a "mobile electronic market." That is to say, implementing a unified platform for trading electronic vouchers will bring forth a new electronic marketplace making the mobile terminal a more intimate part of our lifestyle.

In this article, we introduce key technology to realize secure and fair transactions of vouchers in the form of an optimistic fair exchange protocol for trading electronic vouchers [1]. This protocol enables users to trade arbitrary vouchers stored in their smartcards (e.g. SIM cards in mobile terminals) without the risk of illegal activities such as fraud and swindles. Chapter 2 describes design goals, Chapter 3 presents a technical overview, and Chapter 4 describes a performance evaluation of a prototype smartcard that confirms the efficiency of this protocol.

2. Design Goals

The purpose of this technology is to make it possible for anyone to safely trade diverse kinds of vouchers including tickets, coupons, access rights and value as well as money. Electronic data that represents such a voucher is called an "electronic voucher."

A system that implements electronic vouchers must possess diversity, security and practicality [2][3]. Diversity is the ability to handle many different types of rights and value that involve various kinds of content in a unified manner. Security means that those rights and value cannot be forged or copied during the distribution process. Practicality means that the system shall have at least the convenience of exchange that is currently offered by cash and paper tickets, yet suffer no degradation in performance in response to increases in the number of users and the frequency of transactions.

In addition to these requirements, we found that another requirement, fairness, is also important to realize an environment in which users can safely trade electronic vouchers. Fairness means that, for both of the two parties involved in the transaction, each party does not lose its voucher unless they receive the voucher to be received in the transaction from the other party. This point is described with an example below.

Consider that a user possesses an electronic voucher that represents an electronic coupon that is redeemable for 1,000 yen worth of product and chooses to use that voucher to purchase content access rights that are sold by a store for 1,000 yen over a network. This is an exchange transaction of the electronic coupon and the content access rights between a customer and a shop.

Now, which party should send its voucher first in this transaction, the customer or the shop? In contrast to a face-to-face transaction involving a product and cash that takes place in an actual store, it is difficult to send and receive data "simultaneously" in a transaction over a network. If one party sends its voucher before receiving the voucher from the other party, there is a risk for the former party that the other party will "run away with the voucher." Even if the customer goes ahead and sends the correct coupon, the store (or an impostor of the store) might be able to break the transaction without sending the access rights to the customer, and be out of touch.

As mentioned above, the state in which one party in a transaction has absconded with a received voucher without the other party receiving the voucher to be received is defined as an unfair state. Safe and care-free transactions between mutually unknown persons or businesses via a network require a guarantee for both parties that a transaction cannot be ended in an unfair state. In other words, it is necessary to guarantee transaction fairness.

This technology implements transaction fairness in addition to the three basic requirements for electronic vouchers (diversity, security and practicality), thus providing an environment for the safe use and trade of diverse kinds of electronic vouchers.

3. Technical Overview

This technology provides a means of conducting safe and fair exchange transactions of electronic vouchers that are stored in the smartcards of mobile terminals. In this system, electronic vouchers are a form of electronic information that includes "issuer ID" and "the contents of the rights (or value)". When this electronic information is stored in a smartcard, the possessor of the card has the authority to use the rights or value designated by the issuer. That is to say, that user possesses an electronic voucher.

The transactions in this technology are conducted in an optimistic manner [4]. By optimistic, we mean that the transaction is attempted to be conducted by mutual communication between the trading parties at first, and a Trusted Third Party (TTP) is involved to restore the fairness of the transaction only in case that the mutual communication cannot be ended successfully. Since the transaction is completed by the two parties alone and the TTP is not involved in the transaction at all in normal (errorless) cases, this approach allows a large number of mobile terminals to conduct transactions simultaneously and in parallel without degrading performance.

When a transaction by mutual communication is interrupted in an unfair state such as in the example of Chapter 2, transaction fairness is restored by using a TTP. This restoration process does not require any interaction with the other party, so the transaction can be always ended fairly even if the other party has absconded.

3.1 Main Protocol

Transactions in this system are executed by the exchange of messages between the smartcards of mobile terminals. This exchange process is called the main protocol (**Figure 1**). The main protocol adopts digital signatures and secure hash functions[*1] to prevent forgery or copying of vouchers and guarantees fairness in transactions. Taking electronic vouchers v1 and v2 stored in the smartcards of user A and user B, respectively as an example, for a transaction involving these vouchers, successful completion of the main protocol results in the transfer of v1 to the smartcard of user B and the transfer of v2 to the smartcard of user A. This means that each electronic voucher is deleted from the smartcard in which it was originally stored, and stored in its destination smartcard.

3.2 Restoration of Fairness

If the mutual communication during the main protocol is interrupted and reconnection is not possible, there is a possibility of the transaction breaking in an unfair state. In the resolvable period shown in Fig. 1, user A has lost electronic voucher v1, but has not yet received electronic voucher v2. In the abortable period, user B has lost v2, but has not yet received v1.

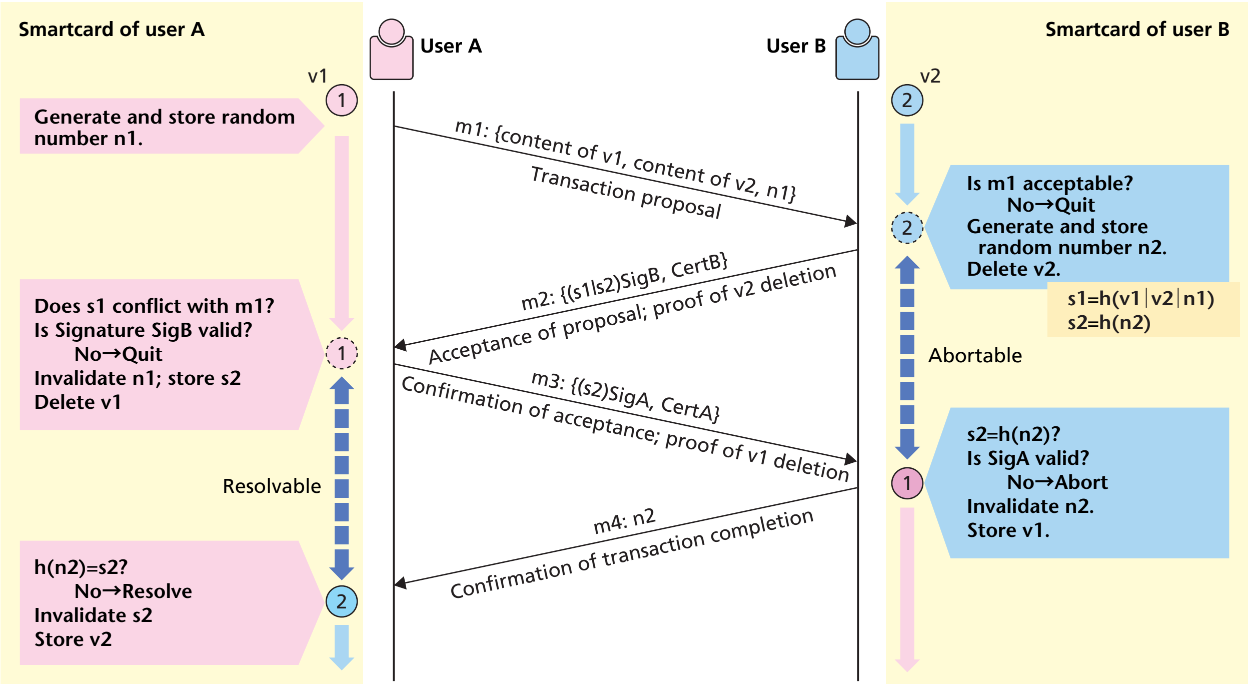
Our system provides a means of restoring transaction fairness when it becomes impossible for the main protocol to continue while in an unfair state. That is accomplished by a single round-trip message exchange with a TTP on the network through the use of restoration protocols as described below. When restoring transaction fairness with this protocol, there is no need for communication with the other party in the transaction; the unfair state can be cancelled only by communicating with the TTP.

3.3 Restoration Protocols

The restoration protocols consist of a resolve protocol that allows user A to request transaction resolution (**Figure 2**) and an abort protocol that allows user B to request that the transaction be aborted (**Figure. 3**).

When user A executes the resolve protocol, the TTP verifies if the transaction has already been aborted (i.e., whether or not execution of the abort protocol with user B for that transaction has been already conducted). If the abort protocol has not

[*1] A secure hash function is a collision-resistant one-way function that outputs data of fixed length calculated from the input data. A typical example is the SHA-1 algorithm.



v1, v2: The electronic vouchers to be exchanged
CertA, CertB: The respective public key certificates of A's smartcard and B's smartcard
h(m): The hash value of m by the secure hash function
(m)SigX: Signed text obtained by appending the signature of X to m

Figure 1 Flow of the main protocol

been conducted yet, the TTP permits the transaction resolution for user A and stores the electronic voucher that was to be received, v2, in the smartcard of user A. If the abort protocol has been already conducted, an indication of the aborting of the transaction is sent instead of the permission for resolution and the original v1 is restored in the smartcard of user A. In either of these two cases, the unfair state of user A is eliminated. The same is true for user B abort protocol. If the result of the test for resolution completion (i.e., whether or not the resolve protocol has been conducted) is 'not resolved yet,' electronic voucher v2 is restored in the smartcard of user B by the permission to abort message. If the result is 'resolution already completed,' v1 is stored by the resolution indication message.

In the event that both the resolve protocol and abort protocol are executed, priority is given to the one that is first executed. This guarantees restoration of the fair state for both users while preventing inconsistency in the transaction results.

4. Performance Evaluation

To verify the practicality of this protocol, we implemented it in a mid-range commercial smartcard (CPU clock: 15 MHz, EEPROM: 32 kB, RAM: 5 kB) and evaluated its performance [5].

The times required to process each message in the main protocol from the beginning of the transaction to the end of the

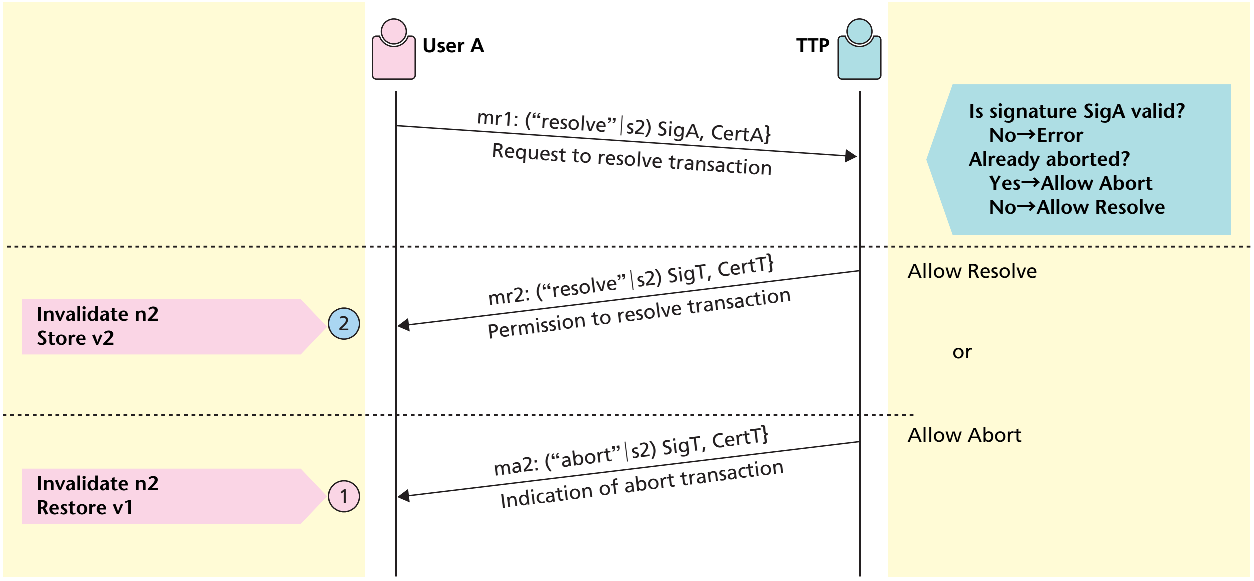

User A
TTP
mr1: ("resolve"|s2) SigA, CertA}
Request to resolve transaction
Is signature SigA valid?
No→Error
Already aborted?
Yes→Allow Abort
No→Allow Resolve
Allow Resolve
mr2: ("resolve"|s2) SigT, CertT}
Permission to resolve transaction
Invalidate n2
Store v2
2
or
Allow Abort
ma2: ("abort"|s2) SigT, CertT}
Indication of abort transaction
Invalidate n2
Restore v1
1

Figure 2 Resolve protocol flow

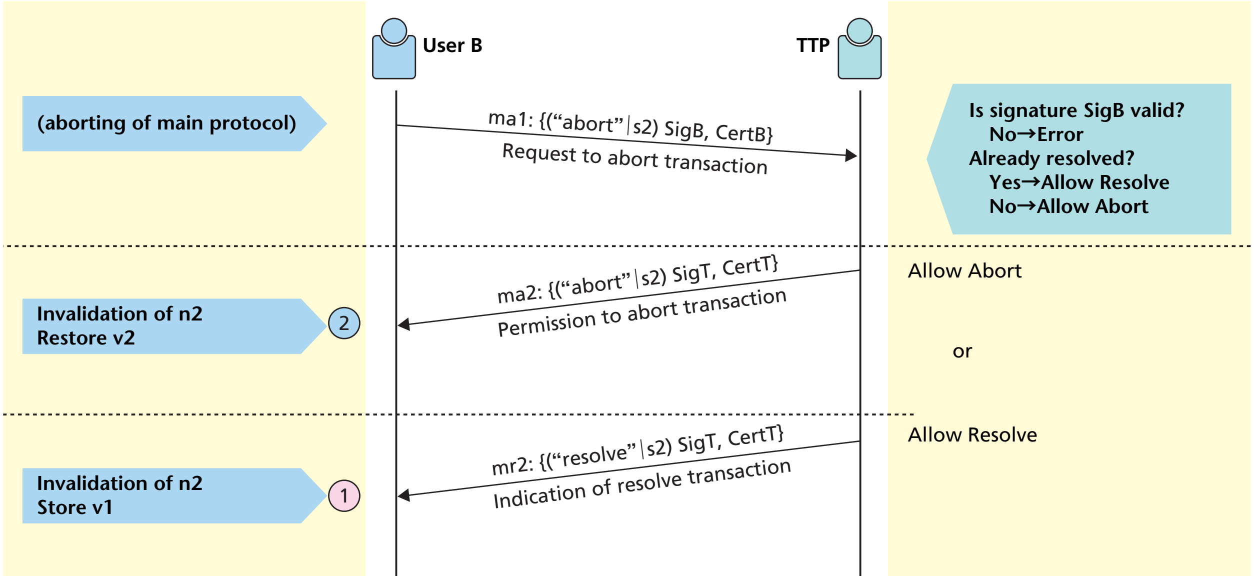

User B
TTP
(aborting of main protocol)
ma1: {("abort"|s2) SigB, CertB}
Request to abort transaction
Is signature SigB valid?
No→Error
Already resolved?
Yes→Allow Resolve
No→Allow Abort
Allow Abort
ma2: {("abort"|s2) SigT, CertT}
Permission to abort transaction
Invalidation of n2
Restore v2
2
or
Allow Resolve
mr2: {("resolve"|s2) SigT, CertT}
Indication of resolve transaction
Invalidation of n2
Store v1
1

Figure 3 Abort protocol flow

Table 1 Results of the performance evaluation

Description of processing	Internal computations	Smartcard I/O	Total
Transaction proposal (m1 generation)	50ms	129ms	179ms
Transaction acceptance (m1 processing)	191ms	153ms	344ms
Transaction consent (m2 processing)	553ms	153ms	706ms
Transaction confirmation (m3 processing)	402ms	91ms	493ms
Transaction completion (m4 processing)	24ms	42ms	66ms
Entire transaction	1,220ms	568ms	1,768ms

transaction are listed in **Table 1**. These times include the time required for smartcard I/O, but do not include that for transferring the messages between the terminals via the network.

The evaluation results confirm that a smartcard that has about the same memory capacity and processing power as the one used in this evaluation can be used to implement this protocol and can exchange vouchers in less than two seconds, excluding the time required for network communication.

5. Conclusion

We have given a brief technical description of protocols that allow users to exchange diverse kinds of electronic vouchers safely and fairly with anyone over a network. We also presented performance evaluation results of the protocol implemented in a smartcard. The results confirmed that the proposed protocol is sufficient for achieving practical electronic voucher transactions with current smartcards.

The smartcard specifications and Java™[*2] Application Program Interface (API) specifications for using this technology from a mobile terminal have been completed. These specifications have been adopted as standard specifications by the T-Engine Forum, which is a standardization organization for embedded computers [6]. The standardization activities in that forum will accelerate adaptation of this technology not only in mobile terminals but also in the area of PDAs, information appliances and other embedded products.

In the future, we plan to rigorously analyze the security of this technology and investigate its applicability to new applications and services.

[*2] Java™: Java and all Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

References

[1] M. Terada, M. Iguchi, M. Hanadate and K. Fujimura: “An Optimistic Protocol for Trading Electronic Rights,” Proc. 6th intl. conf. Smart Card Research and Advanced Applications (CARDIS2004), pp. 255–270, 2004.

[2] K. Fujimura and D. Eastlake: “RFC3506: Requirements and Design for Voucher Trading System (VTS),” Internet Society, 2003.

[3] M. Terada, H. Hanadate, K. Fujimura and J. Sekine: “Copy Prevention Scheme for Rights Trading Infrastructure,” Journal of the Information Processing Society of Japan, Vol. 42, No. 8, pp. 2017–2029, 2001.

[4] N. Asokan, V. Shoup and M. Waidner: “Asynchronous Protocols for Optimistic Fair Exchange,” Proc. 1998 IEEE Symposium on Security and Privacy, pp. 86–99, 1998.

[5] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: “TENeT: A Framework for Distributed Smartcard,” Proc. 2nd intl. conf. Security in Pervasive Computing (SPC2005), LNCS 3450, Springer-Verlag, pp. 3–17, 2005.

[6] T-Engine Forum, TENeT Standard Specifications, 2005.

Abbreviations

API: Application Program Interface