Special Articles on Multimedia Information Processing

Electronic Entity Transfer Platform for eTRON-Equipped Mobile Terminals

Kazuhiko Ishii, Masayuki Terada,
Kensaku Mori and Sadayuki Hongo

Although the opportunities for mobile e-commerce via mobile terminals have been steadily increasing in recent years, no widely applicable method of implementation that offers both adequate safety and low system operation cost has not yet been established.
The article reports the realization of a mobile e-commerce environment that can meet those requirements and the design and implementation of a new electronic entity transfer system that adopts the eTRON chip, a tamper-proof IC chip that is equipped with functions for mutual authentication and encrypted communication, and also an evaluation of its feasibility.

1. Introduction

In recent years, the use of mobile e-commerce over mobile terminals has been steadily expanding from the acquisition of charged information and the downloading of ring melodies in the framework of the cyberworld towards services that can be used in relation to the real world, such as electronic money and electronic ticketing. The Electronic Ticket PIA[*1] service allows electronic tickets to be downloaded to mobile terminals and then go through at the admission gate by means of an infrared communication function. Also, mobile terminals that are equipped with the FeliCa[*2], electronic money service system, are also being implemented, allowing the use of mobile terminals to make payments with electronic money or by charging on credit, and the purchasing of train tickets by holding up a

*1 Electronic Ticket PIA: http://t.pia.co.jp/ (Japanese)
*2 FeliCa: FeliCa® is a registered trademark of the Sony Corporation.

mobile terminal at a vending site. The world in which it is possible to store tickets, currency and other such electronic entities in mobile terminals for subsequent use in this way is now becoming a reality.

Differently from conventional paper tickets and currency, however, these mobile e-commerce services do not allow users to freely exchange electronic tickets or electronic money among themselves. With Electronic Ticket PIA, tickets that have been issued to a mobile terminal can be examined by using the mobile terminal and an infrared communication function, but no function for using the infrared mechanism to exchange tickets between mobile terminals has been implemented. With current systems, users that wish to pass tickets among themselves must first return the electronic ticket to a special server, and then transfer the ticket via that server to the other person. For FeliCa as well, implementation of the electronic money exchange among users has not been considered at all.

Taking FeliCa as an example, a major reason that there is no exchange of entities among users is the difficulty in implementing that function safely. In current methods, the exchange of entities with the user's mobile terminal is limited to trusted equipment such as special servers and machines for examining tickets. These trusted machines implement a user terminal authentication process both to prevent unauthorized copying or altering of entities and to guarantee that the entity is not reproduced or lost even if the communication is interrupted.

In peer transactions between users, however, it is not necessarily true that both mobile terminals can be trusted. Under such circumstances, the free exchange of electronic entities in the same way as is possible for conventional paper tickets and currency requires some means by which the electronic entities can be safely exchanged while protecting them from reproduction or alteration.

Towards the purpose of realizing free and safe exchange of electronic entities, we developed the Securely Transferable entity Platform (STeP) [3] using the entity and economy TRON (eTRON) [1] chip, a tamper-proof IC chip that provides functions for mutual authentication and encrypted communication. Here, we briefly explain the eTRON architecture and describe the design policy for the STeP that adopts it in a mobile communication environment and the construction of a specific system. We also present an evaluation of the feasibility of this approach.

2. eTRON

Past e-commerce systems have not been sufficiently tamper-proof with respect to stored entities. In recent years, methods that use IC cards to improve resistance to tampering have been coming into use, and high-speed authentication (touch and go) has been attained with shared key encryption. A problem with shared key encryption, however, is the trade-off between the great damage that would to the entire system if the key were compromised and the huge cost of key management when each user is assigned a unique key. In contrast to that approach, the eTRON architecture [2] adopts an IC chip that is equipped with public key mutual authentication and encrypted communication functions. This approach is not as fast as the shared key method, but it minimizes the damage due to a compromised key while at the same time keeping the key management cost extremely low.

eTRON architecture overview is shown in **Figure 1**. The

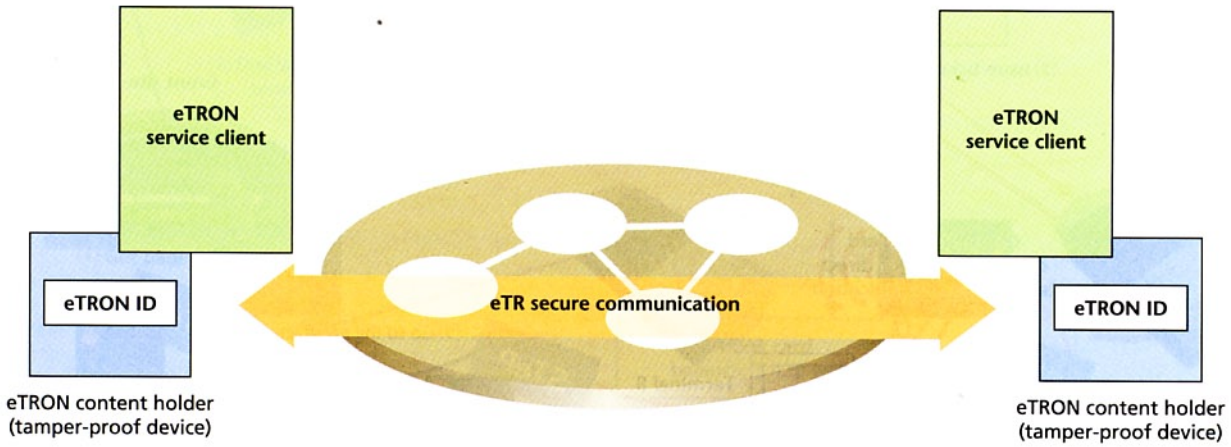

Figure 1 Overview of the eTRON architecture

eTRON architecture consists of the content holder, which serves as a tamper-proof IC chip, and a service client for operating it. The content holder has a unique ID that is referred to as the eTRON ID, and can store electronic entities securely. Content holders use the eTRON ID for mutual authentication and encrypted communication, a kind of secure communication which is referred to as the entity Transfer Protocol (eTP). The service client is a device that manipulates the electronic entities in the content holder and relays secure eTP communication.

3. Securely Transferable entity Platform (STeP) for Mobile Communication

We have applied the eTRON architecture to the mobile environment to develop STeP, a platform that allows the transfer of electronic entities. In this section, we explain the services assumed for this platform. We also describe the requirements of a system for implementing the platform and the design of a system that satisfies those requirements.

3.1 Services Assumed for STeP

We consider the following two cases for electronic entities transfer services.

1) Services for the transfer and consumption of electronic entities in their existing forms
2) Services for the transfer and consumption of sub-divided electronic entities

Here, we take the electronic ticket sales service as an example of the first of the above cases and the e-book billing service as an example of the second case.

1) Electronic Ticket Sales

An electronic ticket sales system represents one kind of assumed STeP service. This system allows users to purchase electronic tickets and freely exchange them among themselves up until the tickets are examined at the site of the event. This entire sequence of actions can be performed using STeP mobile terminals.

Following the overall system flow shown in **Figure 2**, we explain the process from ticket purchase to ticket use.

The user uses the STeP mobile terminal to select and purchase the desired electronic ticket from the Web site of a sales server. Because the electronic ticket can be transferred freely, the user can buy tickets for friends or other persons as well (Fig. 2(1)).

The sales server sends a request to the STeP issuing server to issue the electronic entity (Fig. 2(2)).

The issuing server communicates with the STeP mobile terminal to issue the electronic ticket. That communication with the issuing server is actually performed by the Step chip that is in the STeP mobile terminal. After successful mutual authenti-

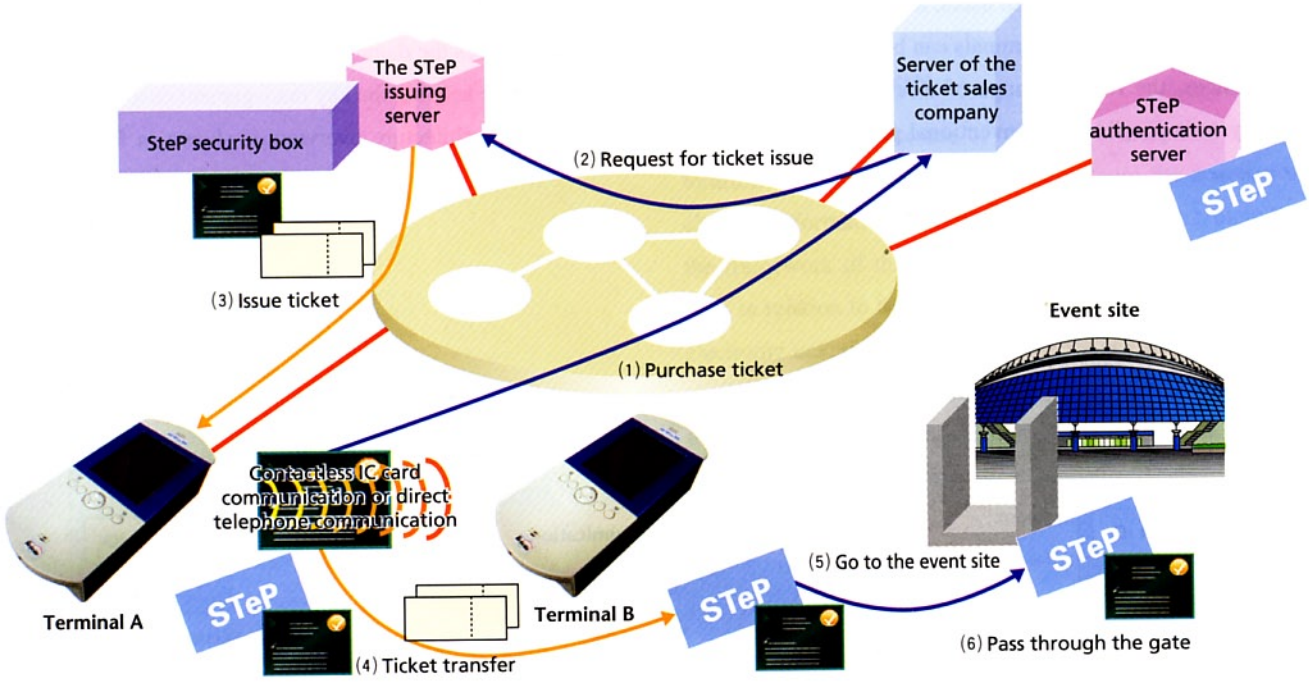

Figure 2 Electronic ticket sales

cation by the STeP chip and the issuing server, the electronic ticket is issued by encrypted communication. The encryption is performed between the STeP chip and the issuing server, so unauthorized access is not possible, even by eavesdropping on the network or the mobile terminal (Fig. 2(3)).

The user transfers an electronic ticket to another terminal that belongs to a friend or other person. The transfer can be accomplished by off-line communication with a contactless interface, etc. Here, also, the communication is done by the STeP chips in the two terminals, so mutual authentication and encrypted communication between chips prevents unauthorized use. Furthermore, the electronic ticket cannot be lost or copied, even if communication is interrupted during transfering (Fig. 2(4)).

The user that has an electronic ticket takes his or her STeP mobile terminal to the site of the event (Fig. 2(5)).

At the ticked gate for the event, the user holds up the STeP mobile terminal. The SteP chips in the ticket gate and in the terminal perform mutual authentication. If the ticket gate finds a valid electronic ticket, it examines the ticket and opens the gate. Once an electronic ticket has been returned or marked as cancelled, it cannot be used again (Fig. 2(6)).

2) e-book Charging System

As the second of the services assumed for STeP, we present the e-book charging system. This system involves the free distribution of e-books in encrypted form and charge them by selling e-book cards as separate entities. The e-book card contains number-of-uses information like a pre-paid card, as well as a key and program for decrypting the e-book. This approach makes it possible to decrypt and read the e-books and charge the user page by page.

The overall system is shown in **Figure 3**. We explain the process from the purchase of the e-book card to the browsing of books.

The e-book server prepares e-books in encrypted form. When the user buys an e-book card, the e-book server requests the issuing of the e-book card by sending the key for decrypting the encrypted e-book and the information on the number of uses that were purchased by the user to the issuing server, (Fig. 3(1)).

The issuing server issues the e-book card, which contains the extent of use information and the key for decrypting the e-book, to the user's STeP mobile terminal. Because the issuing server and the STeP chip perform mutual authentication and

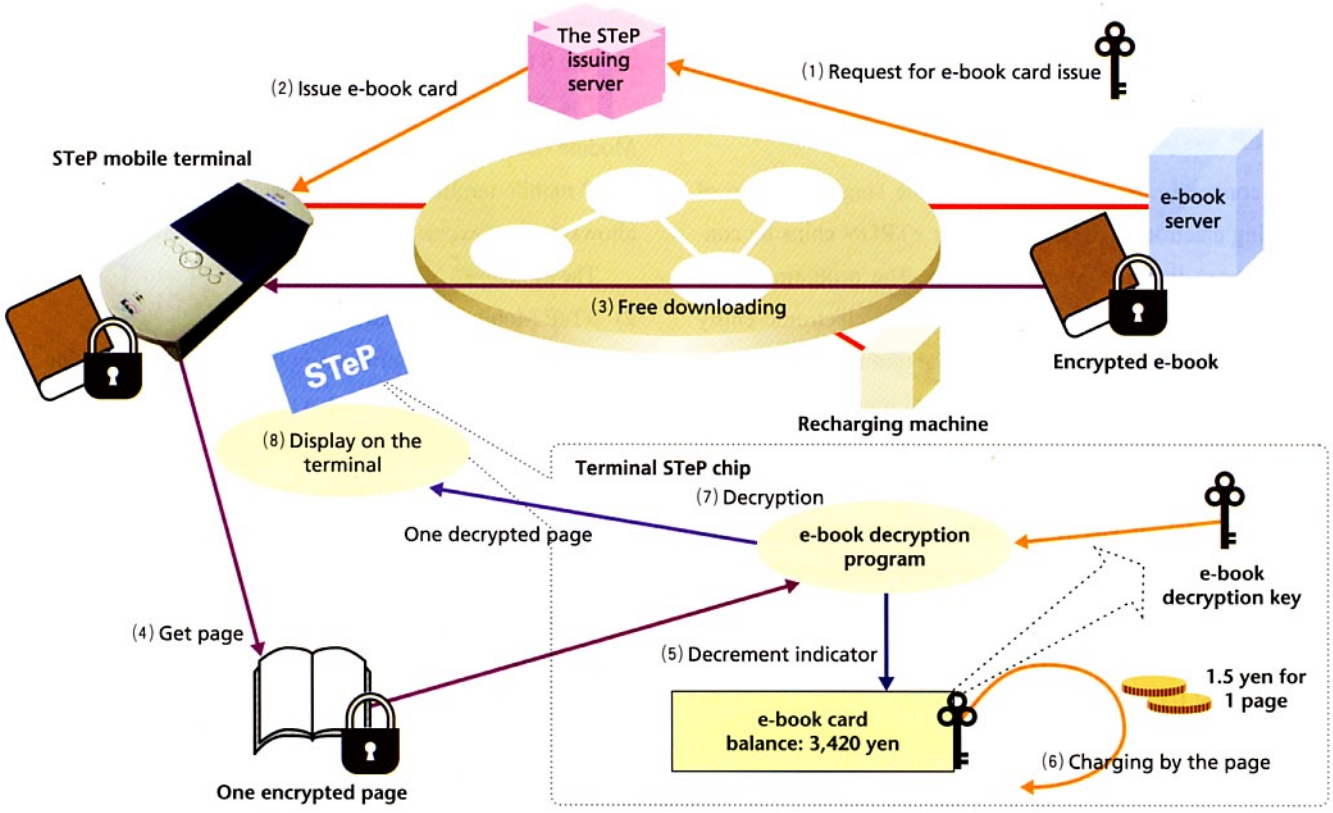

Figure 3 e-book charging system

encrypted communication, the key is transmitted securely even if there is eavesdropping on the STeP mobile terminal or network (Fig. 3(2)).

The user can then freely download encrypted e-books. The possessor of the e-book card is prevented from reading the key for decrypting the e-books that is contained in the e-book card in the STeP chip because an Access Control List (ACL) has been set (Fig. 3(3)).

The user reads the e-book with the e-book reader of the STeP mobile terminal. The terminal can display one page of the book at a time, so data is sent to the STeP chip in units of one page (Fig. 3(4)).

The decryption program in the STeP chip first decrements the number of usage stored in the e-book card and then decrypts the e-book data (Fig. 3(5)).

The number of usage can be reduced in various units, such as by the page or even by a single character (Fig. 3(6)).

After decrementing the number of usage, the decryption program uses the key stored in the e-book card to decrypt and output the e-book data. The process from decrementing the number of usage to decription is performed within the STeP chip, users are not able to perform unauthorized decryption of the data without decreasing the number of usage (Fig. 3(7)). After the above process, a decrypted page is displayed on the terminal (Fig. 3(8)).

3.2 STeP System Requirements

The conventional eTRON chip has the single function of exchanging electronic entities with other eTRON chips by contactless, short-distance communication. The problems listed below must be overcome to achieve flexible electronic entity transfer with the chip mounted in a mobile terminal.

1) It only has a passive contactless IC card interface, electronic entity data can be exchanged with other eTRON cards only via an IC card reader/writer.
2) When transferring electronic entities via the Internet, including the Mopera service, electronic entity transfer is not possible unless the Internet Protocol (IP) address of the receiver (the other party in the eTP session) is known in addition to the eTRON ID.
3) There is no function for controlling access to the electronic entity information, so the data for multiple electronic entities that have different access levels cannot be stored together.

3.3 STeP Design Policy

To satisfy the system requirements described in the previous section, the system was designed by the following policy.

1) Equip the STeP chip with a contact type IC card interface to allow direct communication with the mobile terminal. Equip the mobile terminal with a contactless IC card reader/writer for communication when a contactless card is used.
2) Set up Address Resolution Servers (ARS) on the Internet to provide IP addresses when eTP sessions are established over the Internet. In addition to that, install a cache for eTRON ID and IP address correspondence information (a routing cache) in the mobile terminal to store information previously obtained from the ARS, to reduce both the time needed to establish communication and the load on the ARS.
3) Adding an ACL area to the electronic entity data specifications will allow flexible control of IC card holder access to their own electronic entity information.

3.4 STeP System Design

Based on the design policy described in the previous section, we designed an electronic entities transfer system that applicates eTRON for mobile communication environment (**Figure 4**). The system configuration shown in the figure are as follows.

1) The STeP Chip

The STeP chip is a card of the same size as a User Identity Module (UIM) that has a contact interface. When inserted into a STeP mobile terminal, which is described later in this report, it allows the free exchange of electronic entities between users.

The developed STeP chip is shown in **Photo 1**.

2) STeP Mobile Terminal

The STeP mobile terminal is based on the T-Engine[*3] and has a large LCD equipped with a touch panel and button switches. It has the functions described below.

The developed STeP mobile terminal is shown in **Photo 2**.

i) Electronic Entity Handling Function

This function is used to manipulate the electronic entities within the STeP chip.

It enables the user to store purchased electronic entities, browse the electronic entities that are in the chip, and exchange electronic entities with other STeP mobile terminals.

ii) Mobile Communication Function

This function is used for data communication when a

*3 http://www.t-engine.org/

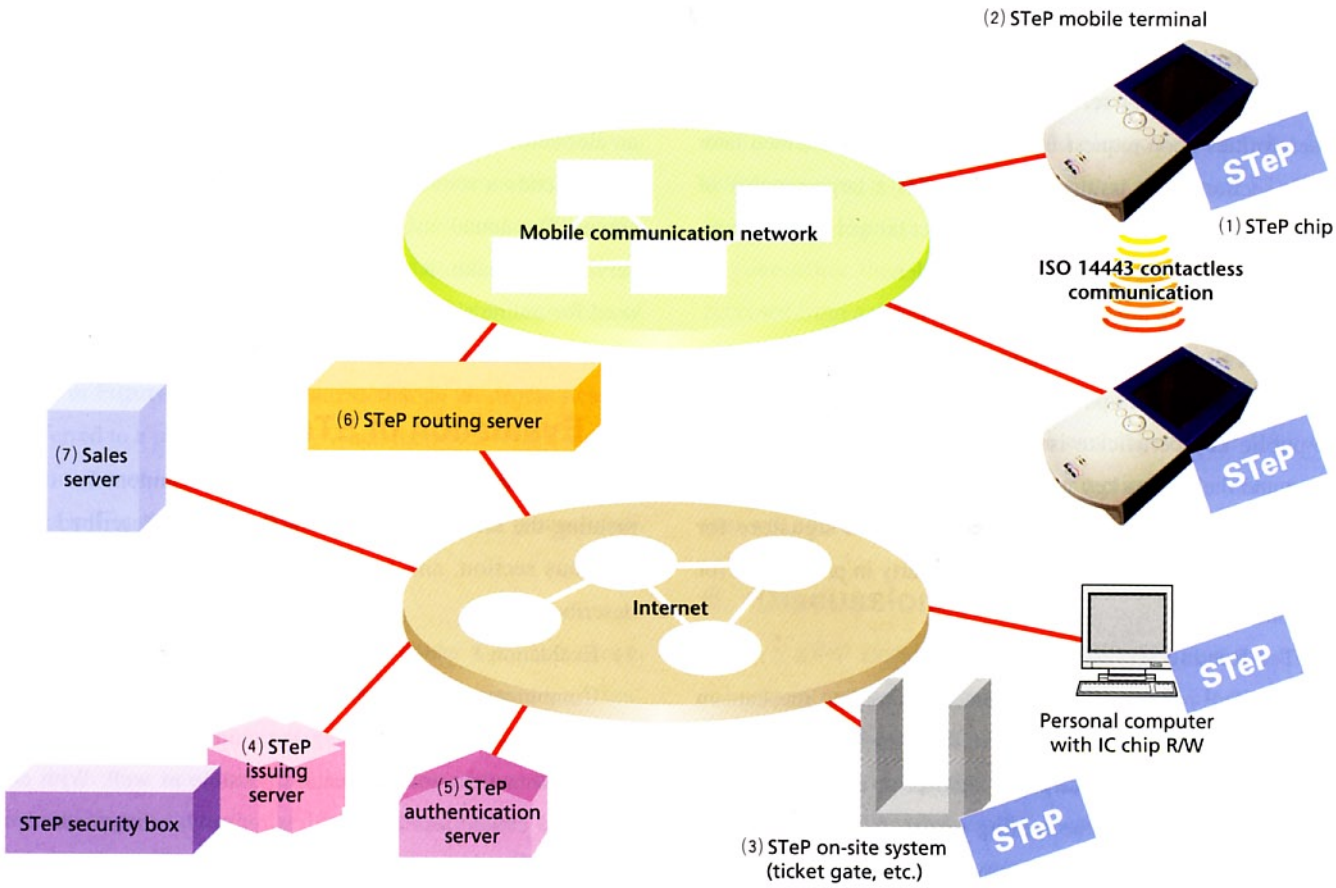

Figure 4 STeP configuration

Photo 1 The STeP chip

Photo 2 The STeP mobile terminal

mobile communication card, such as a Personal Handy-phone System (PHS) card or Freedom Of Mobile multimedia Access (FOMA) card, is inserted into the PC card slot of the STeP mobile terminal. It enables the user to purchase electronic tickets from a server and connect to the Internet.

iii) Contactless Communication Interface

The STeP mobile terminal has an Institute of Electrical and Electronics Engineers (IEEE) 14443 contactless IC card interface on the back side. That allows the exchange of entities between STeP mobile phones that are brought close together. It can also be used for passing through ticket gates.

3) STeP On-Site System

The STeP on-site system is installed at ticket gates, store registers and other locations where the electronic entities are used. The on-site system is one kind of eTRON service client. It communicates with the STeP mobile terminal to recover or

issue entities.

4) STeP Issuing Server

The STeP issuing server is an eTRON service client that issues entities upon request from a sales server (described later in this section). The issuing server handles a large number of entities, and so is equipped with a compact tamper-proof security box to serve as the eTRON content holder.

5) STeP Authentication Server

The STeP authentication server verifies the validity of each eTRON ID and issues public key certificates. The eTRON ID, the public key certificate issued by the STeP authentication server and the private key are stored within the STeP chip. The STeP chip uses the public key certificate and signature for mutual authentication to verify the other party in preparation for communication.

6) STeP Routing Server

The STeP routing server implements a routing mechanism based on the eTRON ID. When the STeP chip is connected to a network, the IP address, telephone number or other such information is registered in the routing server. When STeP chips connect to each other via the network, the routing server is queried for the eTRON ID of the other party, and communication is conducted with the obtained IP address or telephone number.

7) Sales Server

The sales server has more or less the same functions as an ordinary Web server. When a STeP mobile terminal purchases an electronic ticket or other entity from a sales server, the sales server sends a request for entity issuing to the STeP issuing server. The actual issuing of the entity is done by the issuing server. This makes it possible for general Web servers that are used for online shopping to issue electronic entities with minimum modification.

4. Evaluation of STeP

We constructed an experimental environment for implementing the services assumed for the system described in the previous section, and to evaluate the feasibility of STeP as described below.

1) Evaluation 1

Combining a STeP chip serving as a contact interface with a mobile terminal, incorporating the chip into mobile terminal makes contactless communication possible as well. With conventional contactless communication only, other methods of communication are possible only via a contactless card reader/writer (**Figure 5**), but the method described here allows direct use of the mobile communication network and the Internet, etc. via the mobile terminal in addition to contactless

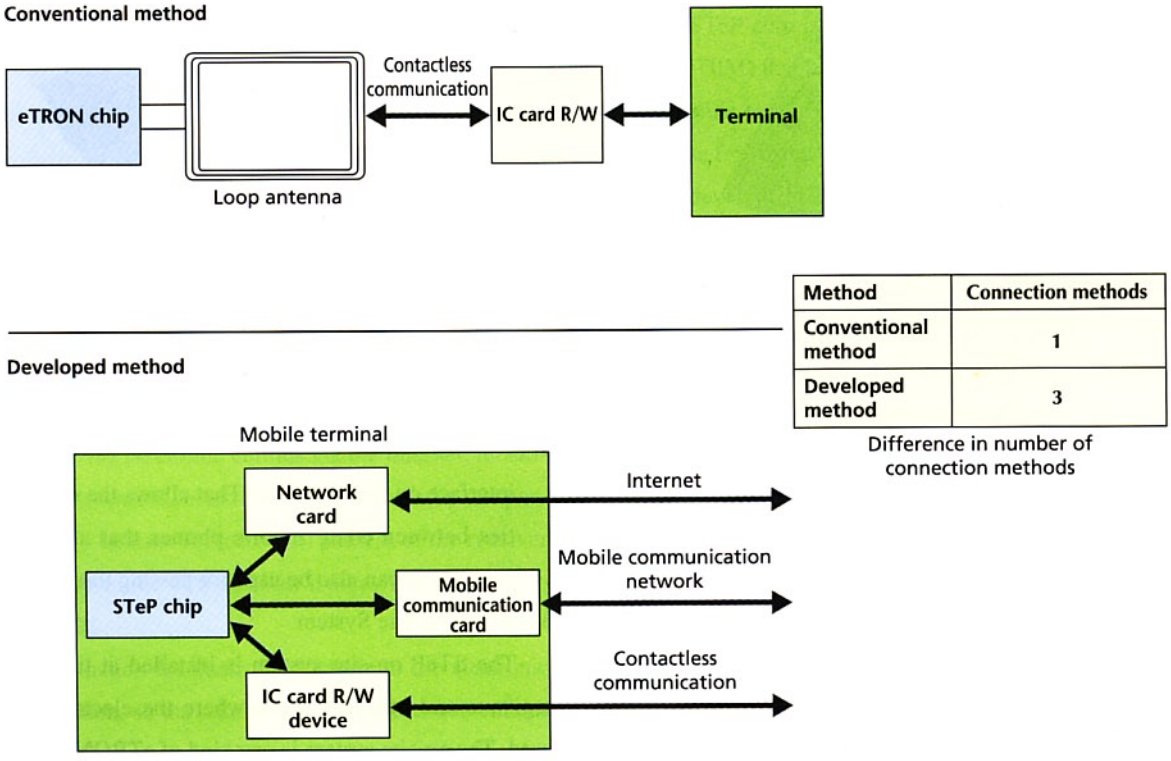

Figure 5 Expansion of available communication method

communication.

2) Evaluation 2

With eTP communication via the Internet by means of ARS, too, connections can be made by seaching the IP address from the eTRON ID. The conventional method does not allow search for the other party from the eTRON ID, so connection to the other eTRON chip is not possible. Querying the ARS, however, makes it possible to connect to another STeP chip regardless of the type of network. The screen displays for this process are shown in **Figure 6**. Fig. 6(a) shows that an electronic ticket is transferred to a mobile terminal. When there is no ARS, the destination cannot be found and a communication error occurs, as shown in Fig. 6(b). With the ARS, however, the process ends normally as shown in Fig. 6(c).

3) Evaluation 3

Setting up an ACL allows the card holder to control access by others to the card holder's own electronic entities. Conventionally, there is no access control on the IC card side. The application must monitor all of the entities one by one for protection against unauthorized access to the entities or permissions, so inconsistencies may arise due to card replacement or the adding and reduction of entity value. The ACL of STeP chip in this system, however, allows flexible access control for each individual entity without inconsistencies (**Figure 7**). We have confirmed that an e-book card and electronic ticket that have different access rights can reside together in a single STeP chip as shown in Fig. 7(a). The e-book card cannot be accessed by anyone other than the owner; the electronic ticket can be accessed from a ticket gate as well as by the owner.

Furthermore, users can exchange electronic entities with other users in a mobile terminal environment using the eTRON functions. We confirmed that such exchange can be done without copying or altering and that interruption of the communication will not result in duplication or destruction of the entity.

5. Discussion

1) In a STeP system, STeP chips directly perform mutual authentication and encrypted communication with each other. However, the Central Processing Unit (CPU) of an IC card has low processing capability, from 1/10 to 1/100 that of a personal computer CPU, so the authentication and cryptographic computation takes time. The mutual authentica-

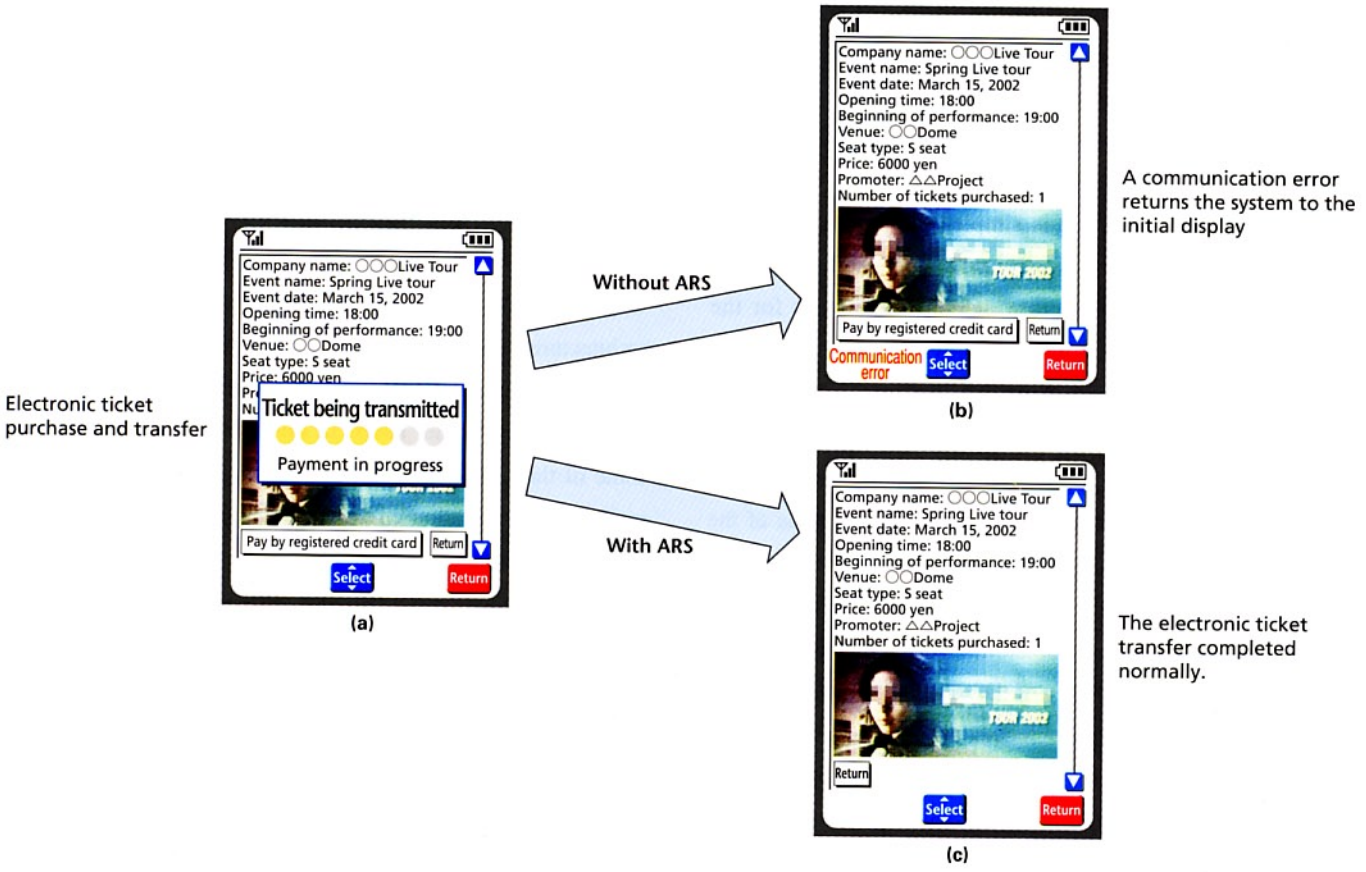

Figure 6 Destination search using ARS

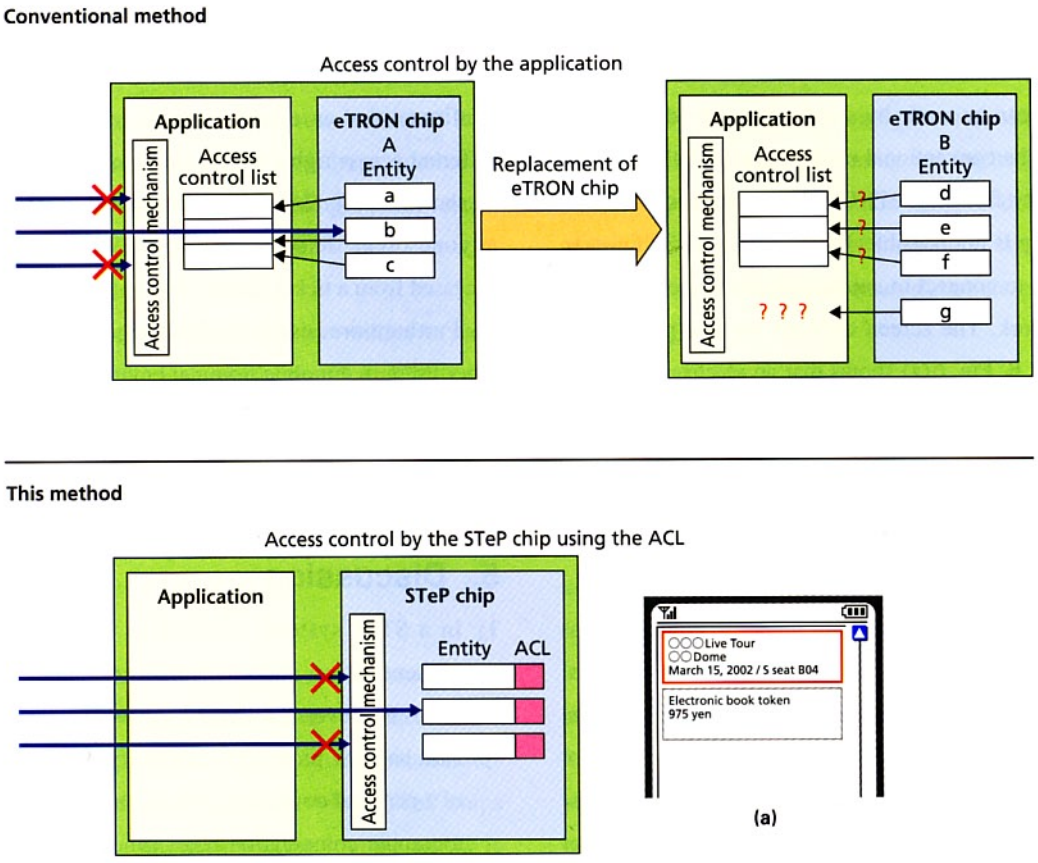

Figure 7 Access rights

tion requires about 1,200 ms, which is about six times longer that authentication by current mainstream shared key IC cards. In future work, we intend to improve the processing speed by using a fast encryption algorithm.

2) The eTRON architecture is simple and has the minimum necessary functions for possible wide applicability as a distributed security architecture, which is the basis for the STeP chip. Therefore, it does not provide a function for listing the electronic entities that are in the chip, a function for simply changing the access rights or other such functions that are required for application in a mobile environment. However, other methods take a long time, and some of the functions that were originally to be available may not be usable. In future work, the functions must be extended to include those required for the mobile environment while preserving the applicability of the eTRON architecture.

3) Although the STeP chip achieves the transfer of electronic entities from one terminal to another, transactions nearly all involve the exchange of entity for entity in the real world. When electronic entities are exchanged, however, the simple execution of a transfer two times may result in only half of the transaction being completed when an interruption in communication occurs. Therefore, we will implement a safe and fair means of accomplishing entity exchange in the STeP chip.

6. Conclusion

We have described STeP, a platform that adopts the eTRON architecture for electronic entity transfer in a mobile communication environment. STeP allows users to securely transfer electronic entities to other users. In this research, we have solved some of the problems associated with applying eTRON to the mobile communication environment, designed and constructed a system that enables flexible electronic entity transfer based on mobile terminals, and evaluated that system though specific application examples by demonstrating its feasibility. Furthermore, new problems were revealed, as mentioned in the Discussion section. We intend to solve those problems in future work and to achieve an environment in which mobile terminals can easily use STeP as a platform for safe and convenient mobile e-commerce services.

REFERENCES

[1] K. Sakamura and N. Koshizuka: "The eTRON Wide-Area Distributed-System Architecture for E-Commerce," IEEE MICRO, pp. 7–12, Vol. 21, No. 6, Dec. 2001.

[2] N. Koshizuka, K. Sakamura, et al.: "eTRON: Entity and Economy TRON," IEICE, 19th CSEC Conference.

[3] Aono, et al.: "Securely Transferable entity Platform for a Mobile Environment," IEICE, 19th CSEC Conference.

ABBREVIATIONS

ACL: Access Control List
ARS: Address Resolution Server
CPU: Central Processing Unit
eTP: entity Transfer Protocol
eTRON: entity and economy TRON
FOMA: Freedom Of Mobile multimedia Access
IEEE: Institute of Electrical and Electronics Engineers
IP: Internet Protocol
PHS: Personal Handy-phone System
SteP: Securely Transferable entity Platform for eTRON
UIM: User Identity Module