Electronic Entity Transfer Platform for eTRON-equipped Mobile Terminals

Kazuhiko Ishii†, *Masayuki Terada, Kensaku Mori, and Sadayuki Hongo*

Abstract

Although 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 describes a mobile e-commerce environment that can meet these requirements. It also describes the design and implementation of a new electronic entity transfer system that uses the eTRON chip (a tamper-proof IC chip that is equipped with functions for mutual authentication and encrypted communication) and 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 services that provide information and ring melodies in the cyberworld towards ones that can be used in the real world, such as electronic money and tickets. Mobile terminals that are equipped with FeliCa[*1], an electronic money service system, are also being implemented, allowing mobile terminals to be used to make payments with electronic money or by credit card and to purchase train tickets by holding up a 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. However, unlike conventional paper tickets and currency, the electronic tickets and money used by these mobile e-commerce services cannot be freely passed around among users.

If we consider FeliCa as an example, we can see that one major reason that there is no exchange of entities among users is the difficulty of 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. To enable the exchange electronic entities freely like conventional paper tickets and currency, we need some means of exchanging them safely while preventing their duplication or alteration.

For this purpose, we developed a securely transferable entity platform (STeP) [1] using the eTRON [2] chip, a tamper-proof IC (integrated circuit) chip based on eTRON (the entity and economy TRON), which provides functions for mutual authentication and encrypted communication (TRON: the realtime operating nucleus). Here, we briefly explain the eTRON architecture and describe the design policy for STeP that uses it in a mobile communication environment and the construction of a specific system. We also present an evaluation of the feasibility of this approach.

† NTT DoCoMo Inc.
Yokosuka-shi, 239-8536 Japan
E-mail: ishiikaz@nttdocomo.co.jp

*1 FeliCa: a registered trademark of Sony Corporation.

2. eTRON

Previous 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 using shared key encryption. A problem with shared key encryption, however, is the trade-off between the great damage that would affect the entire system if the key were compromised and the huge cost of key management if each user were assigned a unique key. In contrast to that approach, the eTRON architecture [3] uses an IC chip 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 that can be caused by a compromised key while keeping the key management cost extremely low.

An overview of the eTRON architecture is shown in **Fig. 1**. The eTRON architecture consists of the content holder provided by a tamper-proof IC chip, and a service client for operating it. The content holder has a unique ID referred to as the eTRON ID. It can store electronic entities securely. Content holders use the eTRON ID for mutual authentication and encrypted communication, a kind of secure communication that 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

Using the eTRON architecture, we developed STeP, a platform that allows the transfer of electronic entities. This section explains the services assumed for this platform. It also describes the requirements of a system for implementing the platform and the design of a system that satisfies them.

3.1 Assumed services

We consider two types of electronic entity transfer services: services for transferring and consuming i) electronic entities in their existing forms and ii) subdivided electronic entities. As examples of these two types, we consider an electronic ticket sales service and an e-book delivery charging service, respectively.

3.1.1 Electronic ticket sales

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

The overall system flow is shown in **Fig. 2**. (1) The user uses the STeP mobile terminal to select and purchase the desired electronic ticket from the Web site of a sales server. (2) The sales server sends a request to the STeP issuing server to issue the electronic entity. (3) 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 in the STeP mobile terminal. After successful mutual authentication 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. (4) The user can transfer an electronic ticket to another person's terminal. Here too, 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 the transfer. (5) A user with an electronic ticket

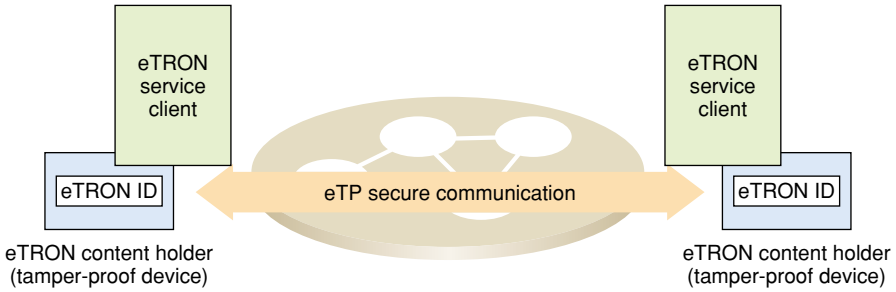

Fig. 1. Overview of the eTRON architecture.

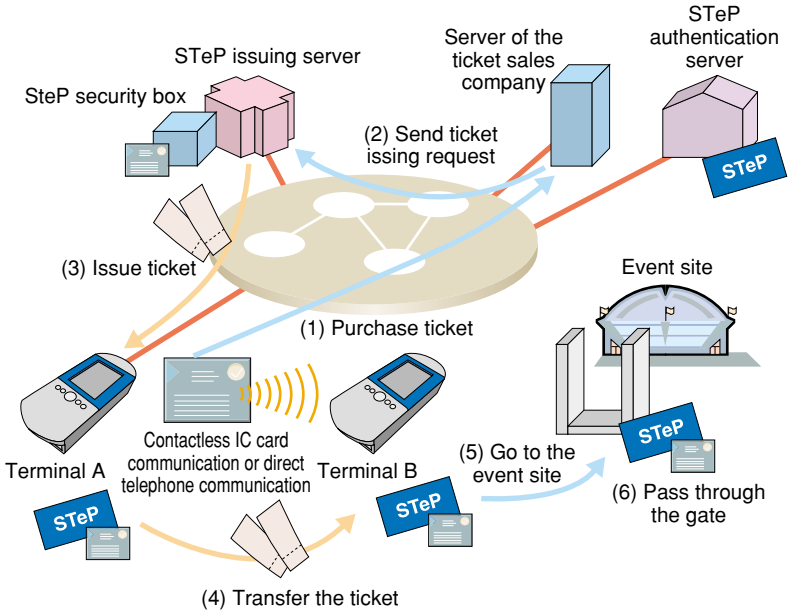

Fig. 2. Actions involved in electronic ticket sales.

takes his or her STeP mobile terminal to the site of the event. (6) At the ticket 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.

3.1.2 An e-book charging system

In this e-book system, the contents of the e-books are widely distributed free of charge in encrypted form. Then, an e-book charging system handles payment for using the contents by selling e-book cards as separate entities. The e-book card contains information about how many usage units the user has purchased, which can be shown by the credit balance like a pre-paid train card or the number of the usage units like a telephone card. It also contains a key and program for decrypting one particular e-book. Unused usage units can be transferred to another card. This approach makes it possible to decrypt and read e-books and charge the user page by page.

The overall system is shown in **Fig. 3**. The e-book server holds e-books in encrypted form. (1) When the user wants to buy an e-book card, the e-book server requests the issuing of an e-book card by sending the key for decrypting the encrypted e-book and the information on the number of usage units purchased by the user to the issuing server. (2) The issuing server issues the e-book card, which contains the permitted-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 encrypted communication, the key is transmitted securely even if there is eavesdropping on the STeP mobile terminal or network. (3) The user can freely download encrypted e-books at any time, but cannot read them without a properly purchased key. The possessor of the e-book card (whether the buyer or a thief) is prevented from reading the decryption key contained in the e-book card in the STeP chip because an access control list (ACL) has been set. (4) When the user wants to read the e-book, he/she uses the e-book reader application on 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. (5) The decryption program in the STeP chip first decrements the remaining-usage number (which may be expressed as the number of pages of a given book that may be read or as a monetary credit balance) stored in the e-book card and then decrypts the e-book data. (6) The remaining-usage number can be reduced in various units, such as by the page or even by a single character. (7) Next, the decryption program uses the key stored in the e-book card to decrypt and output the e-book data. Since the whole process from decrementing the remaining-usage number to decryption is performed within the STeP chip, users cannot perform unauthorized decryption of the data without decreasing the remaining-usage number. (8) Finally, the decrypted page is displayed on the terminal.

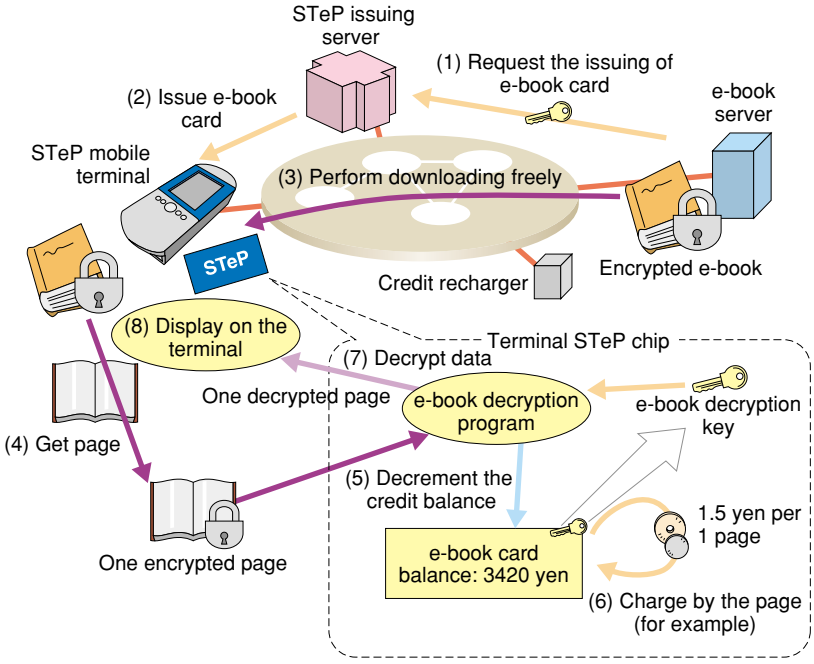

Fig. 3. An e-book charging system.

3.2 System requirements

The conventional eTRON chip has the single function of exchanging electronic entities with other eTRON chips by contactless, short-distance communication. Therefore, for flexible electronic entity transfer with the chip mounted in a mobile terminal, the system should meet the following requirements.

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

3.3 Design policy

To satisfy the system requirements, the system was designed according to the following policy.

1) The STeP chip was given a contact-type IC card interface to allow direct communication with the mobile terminal. The mobile terminal was given a contactless IC card reader/writer for communication when a contactless card is used.
2) Address resolution servers (ARSs) were set up on the Internet to provide IP addresses when eTP sessions are established over the Internet. Furthermore, a cache for eTRON ID and IP address correspondence information (a routing cache) was installed 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) An ACL area was added to the electronic entity data specifications to allow flexible control of access by IC card holders to their own electronic entity information.

3.4 System design

Based on the design policy, we designed an electronic entity transfer system using eTRON for mobile communication environment (**Fig. 4**). The system configuration is discussed below.

1) STeP chip

The STeP chip is a card with a contact interface. It is the same size as a user identity module (UIM). When inserted into a STeP mobile terminal, as described later, it allows the free exchange of electronic entities between users. A photograph of the developed STeP chip is shown in **Fig. 5**.

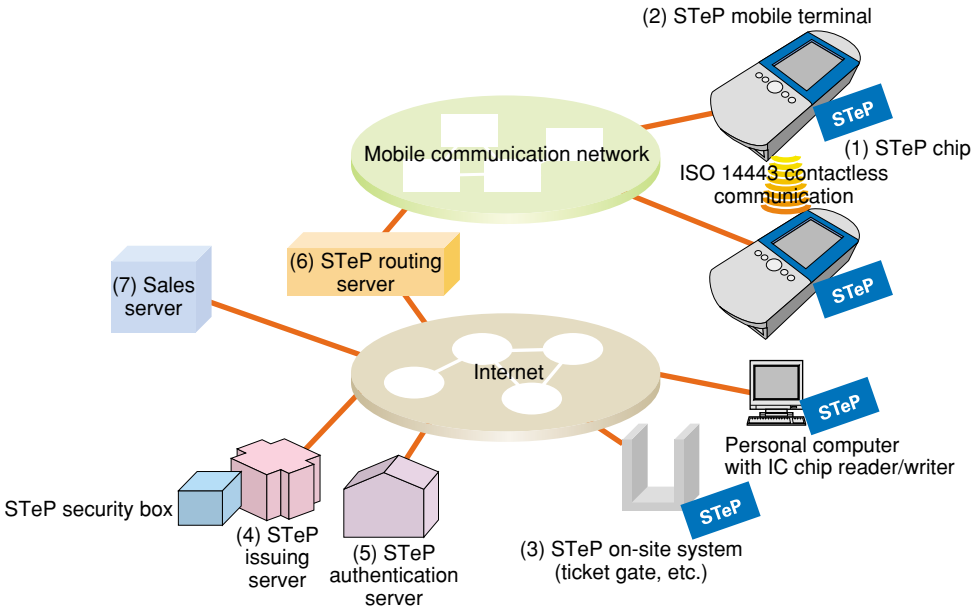

Fig. 4. STeP configuration.

Fig. 5. STeP chip.

Fig. 6. STeP mobile terminal.

2) STeP mobile terminal

The STeP mobile terminal is based on the T-Engine [4] and has a large liquid crystal display (LCD) with a touch panel and buttons. A photograph of it is shown in **Fig. 6**. It has three functions.

i) The electronic entity handling 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) The mobile communication function is used for data communication when a mobile communication card, such as a PHS (personal handy-phone system) card or FOMA (freedom of mobile multimedia access) card is inserted into the terminal's PC card slot. It enables the user to purchase electronic tickets from a server and connect to the Internet.

iii) The contactless communication interface on the rear of the terminal allows the exchange of entities between STeP mobile phones that are brought into close proximity. It can also be used for contactless communication with ticket gates.

3) STeP on-site system

The STeP on-site system is installed at ticket gates, shop registers, and other locations where the elec-

tronic 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 (see (7)). The issuing server handles a large number of entities, so it has 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 an entity issuing request to the STeP issuing server. The actual issuing of the entity is done by the issuing server, which makes it possible for ordinary Web servers used for online shopping to issue electronic entities with minimum modification.

4. Evaluation of STeP

We constructed an experimental environment for implementing our assumed services and evaluated the feasibility of STeP.

1) Evaluation 1

If a STeP chip serving as a contact interface is incorporated in a mobile terminal, then contactless communication is made possible as well. With conventional contactless communication, other methods of communication are possible only via a contactless card reader/writer (**Fig. 7**), 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 communication.

2) Evaluation 2

When eTP communication via the Internet is per-

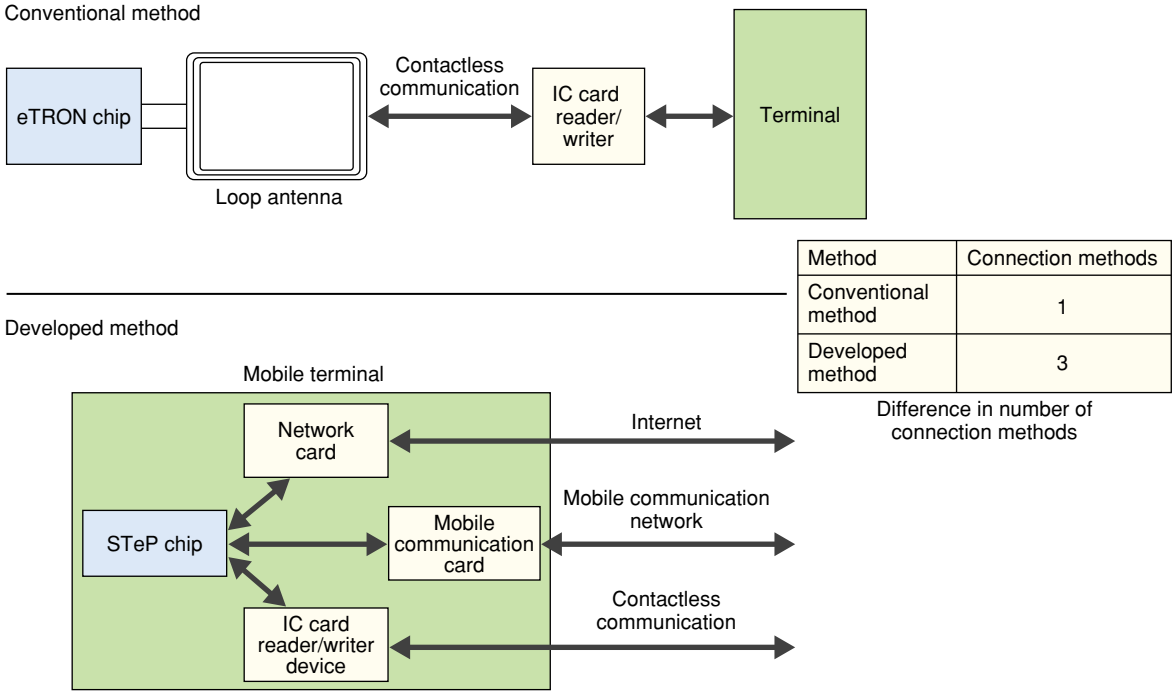

Fig. 7. Expansion of available communication method.

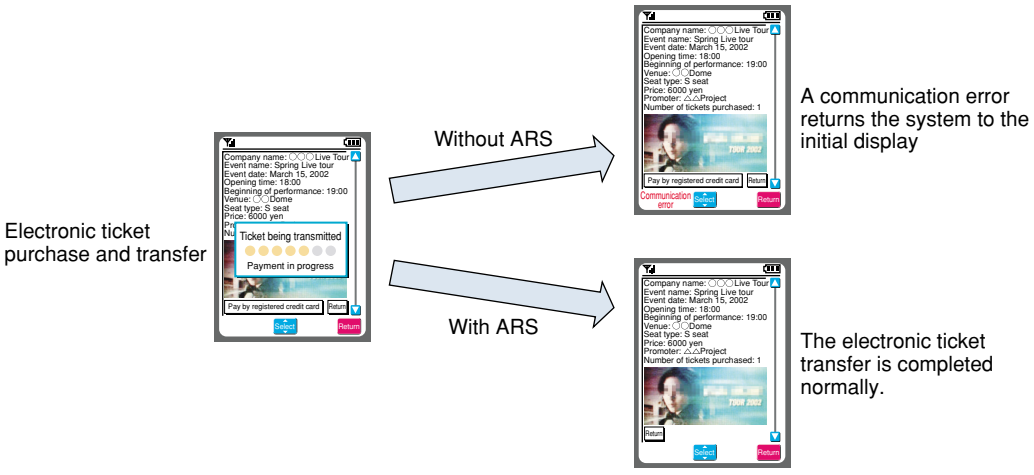

Fig. 8. Destination search using ARS.

formed by means of ARS, connections can be made by searching for the IP address using the eTRON ID. The conventional method does not let you search for the other party based on the eTRON ID, so connection to the other eTRON chip is not possible. By querying the ARS, however, it is possible to connect to another STeP chip regardless of the type of network. Screen displays for this process when an electronic ticket is transferred to a mobile terminal are shown in **Fig. 8**. Without ARS, the destination cannot be found and a communication error occurs. With ARS, however, the process ends normally.

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 to prevent unauthorized access to the entities or permissions, so inconsistencies may arise due to card replacement or the addition/reduction of entity values. The ACL in the STeP chip in this system allows flexible access control for each individual entity without inconsistencies (**Fig. 9**). We have confirmed that e-book cards and electronic tickets that have different access rights can reside together in a single STeP chip. The e-book card can be accessed only by the owner, while the electronic ticket can be accessed by a ticket gate as well as by the owner. Furthermore, the eTRON functions allow users to exchange electronic entities with other users in a mobile terminal environment. We confirmed that such exchanges could be done without any copying or altering of entities and that an interruption of the communication did not result in duplication or destruction of the entity.

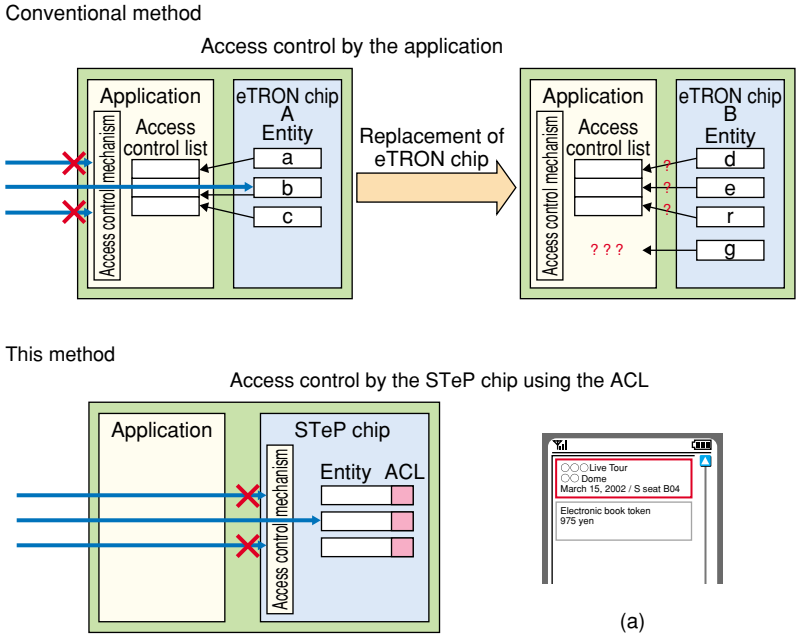

Fig. 9. Access rights.

5. Discussion

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's CPU, so the authentication and cryptographic computation take time. The mutual authentication requires about 1200 ms, which is about six times longer than the authentication by current mainstream shared key IC cards. We intend to improve the processing speed by using a fast encryption algorithm. The eTRON architecture is simple and has the minimum necessary functions for possible wide applicability as a distributed security architecture based on the STeP chip. Therefore, it does not provide functions for listing the electronic entities that are in the chip, for simply changing the access rights, or performing other actions required for application to a mobile environment. However, other methods take a long time and some of the functions that were originally intended to be available may not be feasible. We are trying to extend the functions of the eTRON architecture to include those required for the mobile environment while preserving its applicability.

Although the STeP chip achieves the transfer of electronic entities from one terminal to another, transactions in the real world nearly all involve the exchange of one entity for another. When electronic entities are exchanged, however, the execution of a pair of transfers might lead to only half of the transaction being completed if an interruption in communication occurs. Therefore, we intend to implement a safe and fair means of accomplishing entity exchange in the STeP chip.

6. Conclusion

We have described STeP, a platform that uses the eTRON architecture for electronic entity transfer in a mobile communication environment. STeP allows users to securely transfer electronic entities to other users. We 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 demonstrated its feasibility by evaluating the trial system for specific application examples. This revealed new problems, which we intend to solve in future work. Our goal is to create an environment in which mobile terminals can easily use STeP as a platform for safe and convenient mobile e-commerce services.

References

[1] H. Aono, K. Ishii, K. Mori, S. Hongo, N. Koshizuka, K. Sakamura, "Securely Transferable entity Platform for a Mobile Environment," IEICE, 19th CSEC Conference (in Japanese).
[2] 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.
[3] N. Koshizuka and K. Sakamura, "eTRON: Entity and Economy TRON," IEICE, 19th CSEC Conference (in Japanese).
[4] T-Engine: http://www.t-engine.org/

Kazuhiko Ishii
Manager, Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. degree in computer science from the university of Electro-Communication, Tokyo in 1990. He joined NTT DoCoMo in 2002 and engaged in R&D of software development networks and network multimedia technology. He is currently engaged in R&D of mobile e-commerce security. He is a member of the Information Processing Society of Japan (IPSJ).

Masayuki Terada
Assistant Manager, Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. and M.E. degrees in engineering from Kobe University, Hyogo in 1993 and 1995, respectively. He joined NTT DoCoMo in 1995. He is currently engaged in research on consistency guarantee in wide-area distributed environments, digital-rights distribution protocol/architecture, and fairness guarantee in electronic transactions. He is a member of IPSJ.

Kensaku Mori
Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. degree in electrical engineering and the M.E. degree in information science and electrical engineering from Kyushu University, Fukuoka in 1998 and 2000, respectively. He joined NTT DoCoMo in 2000 and engaged in R&D of location-based services. He is currently engaged in R&D of mobile e-commerce security. He is a member of IPSJ.

Sadayuki Hongo
Director, Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. and M.E. degrees in electronic engineering from Iwate University. Iwate in 1982 and 1984, respectively. He joined NTT in 1984. He is engaged in research on intelligent telephone terminals, telephone-terminal operation behavior, icon recognition, computational theory of visual information processing, multimedia education, and information security. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan and IPSJ.