FLEXIBLE LICENSE TRANSFER SYSTEM USING MOBILE TERMINAL

Masaki Inamura, Toshiaki Tanaka
KDDI R&D Laboratories Inc., 2-1-15 Ohara, Fujimino-shi, Saitama, Japan

Toshiyuki Fujisawa, Kazuto Ogawa, Takeshi Kimura
Science & Technical Research Laboratories, Japan Broadcasting Corporation, 1-10-11 Kinuta, Setagaya-ku, Tokyo, Japan

Keywords: Prepaid Ticket, License Transfer, Anonymity, Blind Signature.

Abstract: Content delivery is one of the promising services for both digital broadcasting and the Internet. The provision of home gateway for connecting the internet provider or set top box for broadcasting causes a variety of content services and convenient functions. However, if a user wants to enjoy digital content not only in his home but also outside of it, it is difficult to use, because a license for digital content is usually bound to the set top box or home gateway. For the purpose to utilize the digital content in the open space, we propose a new system where a user can purchase a license and securely delegate the license stored in the set top box to the mobile terminal. Therefore he can enjoy content by showing the license stored in the mobile terminal as a prepaid ticket. Moreover, to protect user's privacy, our proposed mechanism supports anonymity when using the ticket.

1 INTRODUCTION

Recently we can easily obtain many kinds of service and digital content through the Internet or the digital broadcasting. For the purpose to realize sophisticated services, the provision of home terminals (HT), gateway and set top box (STB) is necessary, which have a tamper resistant module and securely manage user's license in the module instead of making users remember his password. However in this system, we cannot extract the license from HT and cannot use it separately, so we must obtain services through the HT anytime. Therefore we cannot use services under the license in the open or in public space, such as internet CAFÉ, unless we bring the HT itself. On the other hand, there is a broadcasting system using license card. Conditional Access System (CAS) is one of the above examples, where broadcasting station manages licensed users by means of the license cards. The card contains integrated circuit (IC) and is used for authentication and authorization of the licensed user. In the case, users can separate the license card from STB, so users may use services in the open by means of bringing the card. However users cannot use services at home while other member bringing the card. Furthermore, we must consider some risks that the card may be stolen or the user information may be leaked out when the user get services at the public places.

On the other hand, a mobile terminal, especially mobile phone, is owned by each person, and the terminal has high-level functions. Accordingly mobile terminal is expected to be a personal gateway of information world. Recent mobile terminal has also security functions, i.e. encryption/decryption and digital signature, so we have realized productions of secure system over mobile network, i.e. e-commerce, e-banking, mobile contents distribution with DRM and so on. Moreover, mobile terminals may have temper resistant module, called UIM. Taking into account of the above background, mobile terminal would be a good candidate for a special tool of carrying his license. Even though a smart card has the same security functions as the mobile terminal, it does not have communication function and user interface. On the contrary, mobile terminal has them. Therefore we think that mobile terminal is more suitable to inquire a service or

Inamura M., Tanaka T., Fujisawa T., Ogawa K. and Kimura T. (2006).
FLEXIBLE LICENSE TRANSFER SYSTEM USING MOBILE TERMINAL.
In *Proceedings of the International Conference on Security and Cryptography*, pages 397-404
DOI: 10.5220/0002102303970404

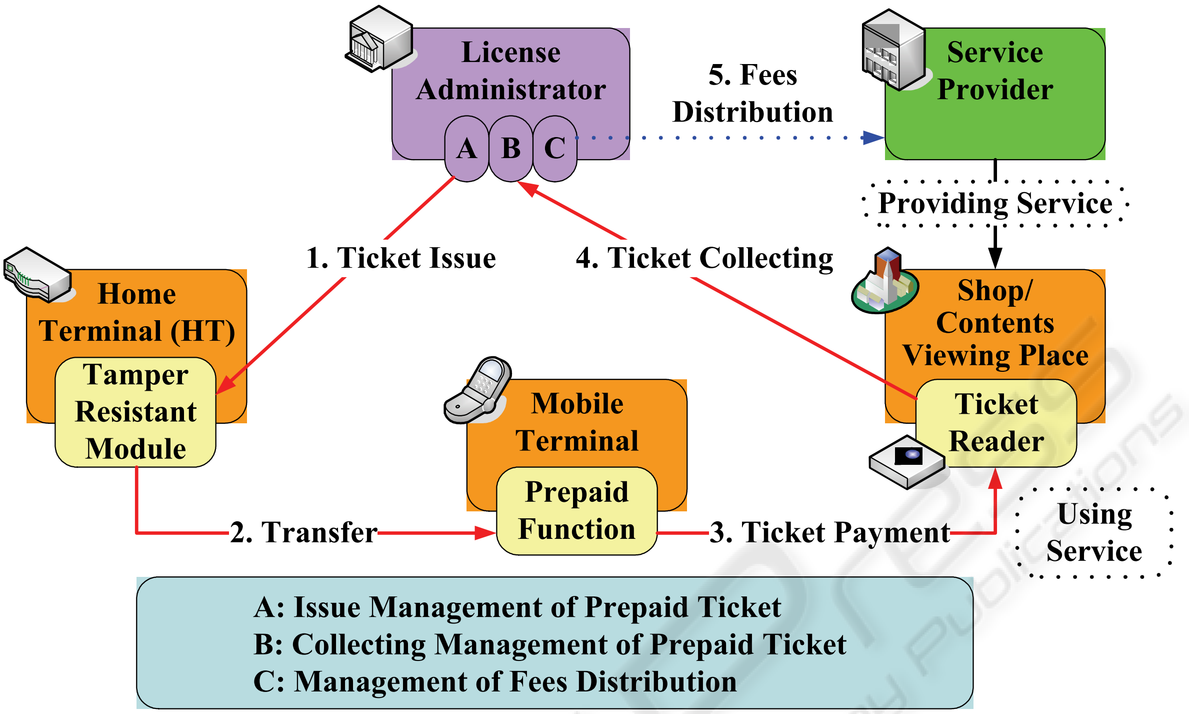

Figure 1: Service Model.

check in the memory at any time. You may also think that if the license in the HT is delegated to the mobile terminal temporally and securely, users can use services in the open. In the case, mobile operator may know all users' private information, for example the date when the user uses the terminal, the location where the user stays and the content that the user uses.

In this paper, we propose a license transfer system from HT to mobile terminals with privacy preservation. To transfer the license with preserving users' privacy, we employ a prepaid scheme. In the system, the user purchases prepaid tickets before he gets services, and he can get service by paying the tickets. Naturally, the value of ticket is limited and is not determined until purchasing content. Thus, the damage from the lost of ticket can be minimized. Moreover, there is no information about the user on the ticket. Therefore, users' privacy can be preserved. We assume that both the HT and the mobile terminal have security functions, so we can realize a prepaid system on the mobile terminal using encryption and digital signature. Moreover, because we use existing infrastructure, a HT for administrating license and a mobile terminal for handling prepaid ticket, this system does not need other hardware or infrastructure. Therefore we can immediately and easily construct a new prepaid system at low cost.

2 SERVECE MODEL AND SECURITY REQUIREMENT

2.1 Service Model

In our proposed system, when carrying license and prepaid ticket, a user uses a mobile terminal which has secure recording area. This premise is realistic because the number of mobile terminals with security function increase, i.e. SIM card for mobile phone with PKI function, and we can easily set up the secure recording area to mobile terminals by means of this function.

Figure 1 shows service model. First a user request prepaid ticket issuance to his HT. If the license administrator succeeds authentication of the license, the administrator makes prepaid ticket and sends it to the user. Simultaneously, the fees of the ticket are paid by direct debit from the user bank account. The user transfers the ticket to his mobile terminal which has already been resisted to the user's HT.

When the user obtains some services by paying the prepaid ticket, the user pays the ticket to the administrator through a ticket reader in shop /contents viewing place. The adminstrator distributes the collected fees to service provider according to the service. After receiving fees, the service provider provides items/contents to shop/contents viewing place, and the user gets them at the place.

2.2 Security Requirement

In the model of section 2.1, the prepaid ticket is used to show that the user has already paid the fees prior to obtaining services, and the administrator distributes the fees to the service provider by the ticket. Therefore the system must be secure against malicious person's attack to the ticket or protocols. We show security requirements of the prepaid ticket as follows:

- **Sound Charge:** fees of prepaid ticket are certainly paid by direct debit from user bank account.
- **Unforgeability:** users or third parties cannot generate prepaid ticket and modify information of a amount of fees on the ticket without license administrator's help.
- **Terminal Legitimacy:** users or third parties cannot use illegal HT/mobile terminal.
- **Wiretapping Impossibility:** the prepaid ticket, that is obtained through wiretapping, cannot be used.
- **Double-spending Impossibility:** users cannot use the same ticket twice or cannot use copied ticket.
- **Anonymity:** license administrator and third parties cannot get any user's information from their paid history.
- **Dividability:** a user can divide the ticket into small value tickets as long as he pays by prepaid ticket legally.

3 PREPAID TICKET TIED TO HOME TERMINAL

In a secure payment system, it is important to protect license administrator from a malicious person's attacks who uses this system illegally and to preserve users' privacy from the administrator and third parties. Blind signature is one of efficient countermeasures to realize such security. In the system, a user first sets serial number for digital money and blind it. The user sends blinded serial number to a bank. The bank signs blinded serial number by digital signature and issues digital money with the blind signature to the user. The user unblinds the serial number and indicates the number at payment. The bank cannot know the serial number until digital money is paid. We show this sequence in the following:

payer: Serial >> Blind(Serial)
>bank: Sign(Blind(Serial))
>payer: Sign(Serial)

NOTICE: ">>" means "changing blind data", and ">" means "send to."

In this scheme, the bank can protect payment by administrating serial number of used ticket against illegal behaviour. On the other hand, the payer is not tied to the payer's account or information on digital money issuance, so anyone cannot know what, when and where the payer does on digital money payment.

This scheme is used efficiently, when the ticket value is unique and the ticket value is a unit of digital money. It means it is impossible to divide a ticket into small value tickets or any value of ticket which a user wants. Considering realization of prepaid system with mobile terminal, it is recommended that the prepaid ticket is dividable without any increase of computational cost and memory size.

Now we assume that a license administrator, such as banks, trusts tamper resistant module within HT, and users and third parties cannot forge the data recorded in the module, i.e. license information, encryption/decryption/signature key and value of prepaid ticket. Under the assumption, we propose a new prepaid system. In the system, when a user demands some value of prepaid ticket, the value can be known by the administrator. The administrator then adds blind signature to the serial number and returns it with the ticket. We show the sequence as follows:

HT: Serial, Sum >> Blind(Serial, Sum)
>administrator: Sign(Blind(Serial, Sum))
>HT: Sign(Serial, Sum), Keyed-hash(Sum)

NOTICE: Sum denotes the value of tickets and it is presented to the license administrator.

Since the value is included in a ticket, the administrator can issue arbitrary value of ticket the user wants. Furthermore when the user pays by this ticket, the balance of ticket is calculated and the same value of ticket is generated and issued. It is thus possible to divide into small value of tickets.

When the administrator signs to the combined data of the serial number and the value of ticket, we have to take into account such risks that the user tells a false value and that he forces the administrator to issue higher value of ticket. We propose a countermeasure against such fraud. It adds keyed hash to the combined data of Sum and serial number using shared key between HT and the administrator. It makes such fraud impossible. Thus we realize a prepaid system with sound payment, anonymity and dividability of tickets.

4 PROTOCOL

In section 3, we explained the prepaid ticket issued to license holders. In this section, we propose a charge protocol using prepaid tickets. The protocol consists of three parts; mobile terminal registration, prepaid ticket issue and prepaid ticket payment.

We define requirements, assumptions and notations of this protocol as follows:

REQUIREMENTS:

- Mobile terminal can compute asymmetric encryption and digital signature, and has encryption/signing keys.
- License administrator can compute asymmetric encryption and digital signature, and has encryption/signing keys.
- HT can compute asymmetric encryption and verification of digital signature, but does not have asymmetric encryption/signing keys.
- There is a master key which is shared among license administrator, all ticket reader and all HT. This master key is used for the HT and ticket reader authentication by the administrator.

ASSUMPTIONS:

- License administrator is honest and trustful.
- License administrator provides HT machine in which user license information is installed.
- HT has tamper resistant module.
- HT does not send any information to license administrator without user operation.

NOTATIONS:

- ||: Concatenation.
- S_n, X_n: Serial number (S_n) and a value (X_n) of prepaid ticket.
- r_n: Random value.
- PUB_a, PUB_{at}: Public key of mobile terminal used in asymmetric encryption scheme (a: authenticated key issued by CA, at: temporal key generated by mobile terminal.)
- ID_a: Identity of a mobile terminal.
- H-ID: Identity of a HT.
- PENC(m,k): Encrypted data of message (m) with key (k). Encryption method is asymmetric encryption.
- K_w, K_{wt}: Shared Work key (w: a key for communication between HT of user and mobile terminal at home, wt: a temporal key for communication between ticket reader and mobile terminal in the open.)
- K_m: Master key shared among license administrator, all ticket reader and all HT.
- SENC(m,k): Encrypted data of message (m) with key (k). Encryption method is symmetric encryption.
- MAC(m,k): Message authentication code of message (m) with key (k) (if m=ALL, all concatenated message is target.)
- SIGadm(m): Digital signature of message (m) generated by license administrator.
- BL(m): Blinded data of message (m) generated by user using blind signature.

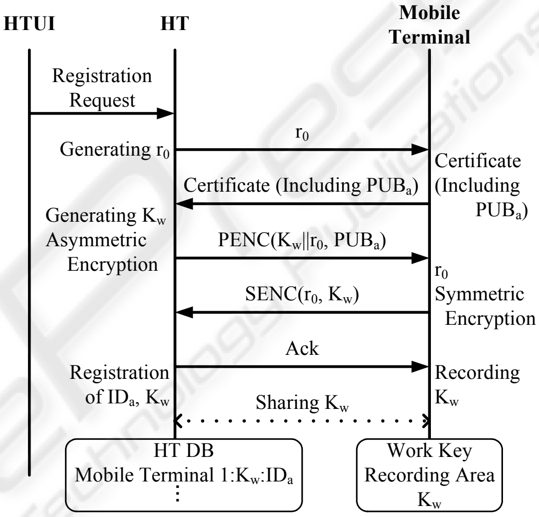
HTUI
HT
Mobile Terminal
Registration Request
Generating r_0
r_0
Certificate (Including PUB_a)
Certificate (Including PUB_a)
Generating K_w Asymmetric Encryption
PENC(K_w||r_0, PUB_a)
r_0 Symmetric Encryption
SENC(r_0, K_w)
Ack
Registration of ID_a, K_w
Recording K_w
Sharing K_w
HT DB
Mobile Terminal 1:K_w:ID_a
⋮
Work Key Recording Area
K_w

Figure 2: Mobile Terminal Registration.

4.1 Mobile Terminal Registration

We show the mobile terminal registration protocol in figure 2.

1. When a user requests his mobile terminal registration through user interface of his HT (HTUI), a HT generates random value r_0 and sends it to a mobile terminal.
2. The mobile terminal sends public key, PUB_a, and its certificate.
3. The HT generates work key, K_w. Then the HT sends encrypted data, PENC(K_w||r_0, PUB_a), to mobile terminal.
4. The mobile terminal computes encryption data, SENC(r_0, K_w), and sends it to the HT.
5. The HT verifies r_0. If verification is succeeded, the HT sends acknowledge signal to the mobile terminal. At the same time, the HT registers K_w and ID_a on database in the HT.
6. The mobile terminal records K_w.

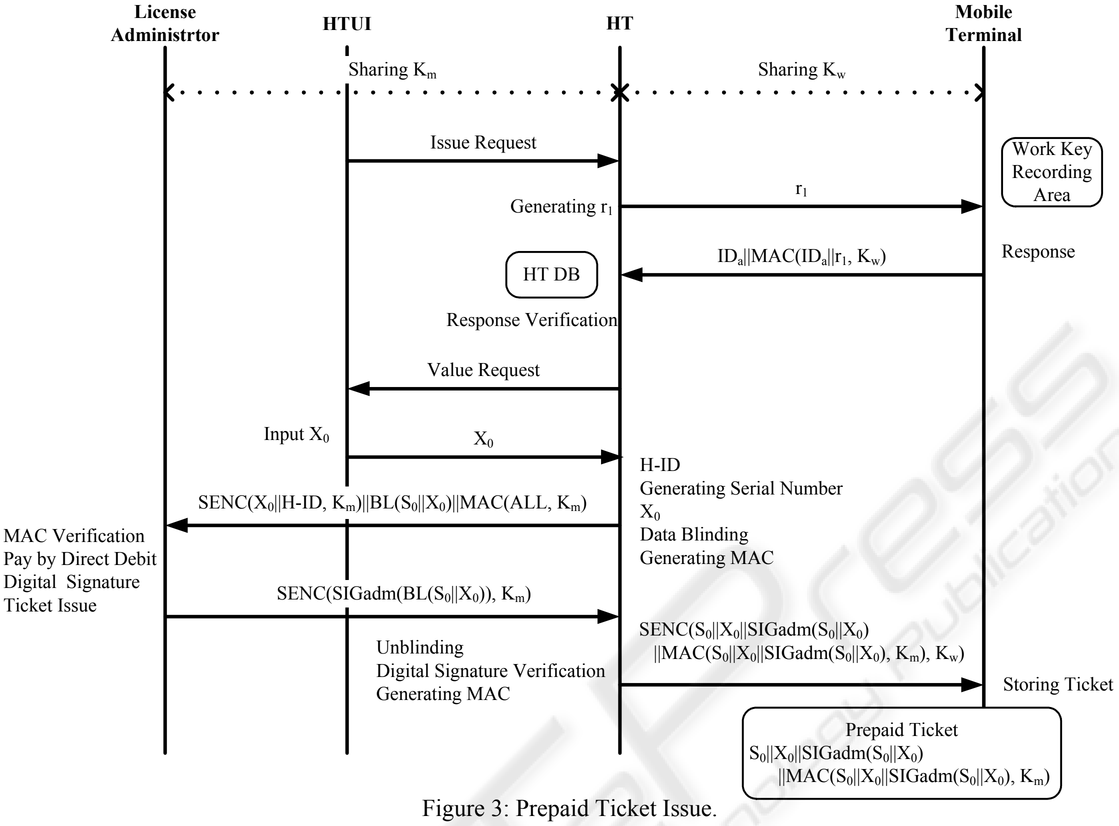

Figure 3: Prepaid Ticket Issue.

4.2 Prepaid Ticket Issue

We show the prepaid ticket issuance protocol in figure 3.

1. When a user requests prepaid ticket issuance through HTUI, his HT generates random value r_1 and sends it to his mobile terminal.
2. The mobile terminal generates response data, $ID_a||MAC(ID_a||r_1, K_w)$, using recorded K_w and sends it to the HT.
3. If verification of response data is succeeded, the user inputs a value of money for prepaid ticket, X_0, from HTUI.
4. The HT generates a serial number for the prepaid ticket, S_0, and blinds the combined data of S_0 and X_0. Furthermore the HT generates issuance request, $SENC(X_0||H\text{-}ID, K_m)||BL(S_0||X_0)||MAC(All, K_m)$, and sends it to the license administrator.
5. If verification of MAC sent by theHT is succeeded, fees of prepaid ticket are paid by direct debit from the user's bank account. The fees depend on H-ID. Furthermore the license administrator signs blinded data, generates a part of prepaid ticket data, $SENC(SIGadm(BL(S_0||X_0)), Km)$, and sends them to theHT.
6. The HT unblinds the data sent by the license administrator and verifies it. If the verification is succeeded, the HT encrypts full prepaid ticket data, $SENC(S_0||X_0||SIGadm(S_0||X_0)||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m), K_w)$ and sends it to the mobile terminal.
7. The mobile terminal decrypts prepaid ticket data, $S_0||X_0||SIGadm(S_0||X_0)||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m)$, and stores it.

4.3 Prepaid Ticket Payment

We show the prepaid ticket payment protocol in figure 4.

1. The mobile terminal generates temporal public key, PUB_{at}, and sends it to a ticket reader. The ticket reader generates temporal work key, K_{wt}, and encrypts it with PUB_{at}, $PENC(K_{wt}, PUB_{at})$, and sends it to the mobile terminal.
2. The ticket reader displays a price of obtaining services or buying items (Y) through user interface of the ticket reader (TRUI.) If the user agrees with paying, he sends acknowledgement to the ticket reader through TRUI.
3. The ticket reader generates payment request data using Y and K_{wt},

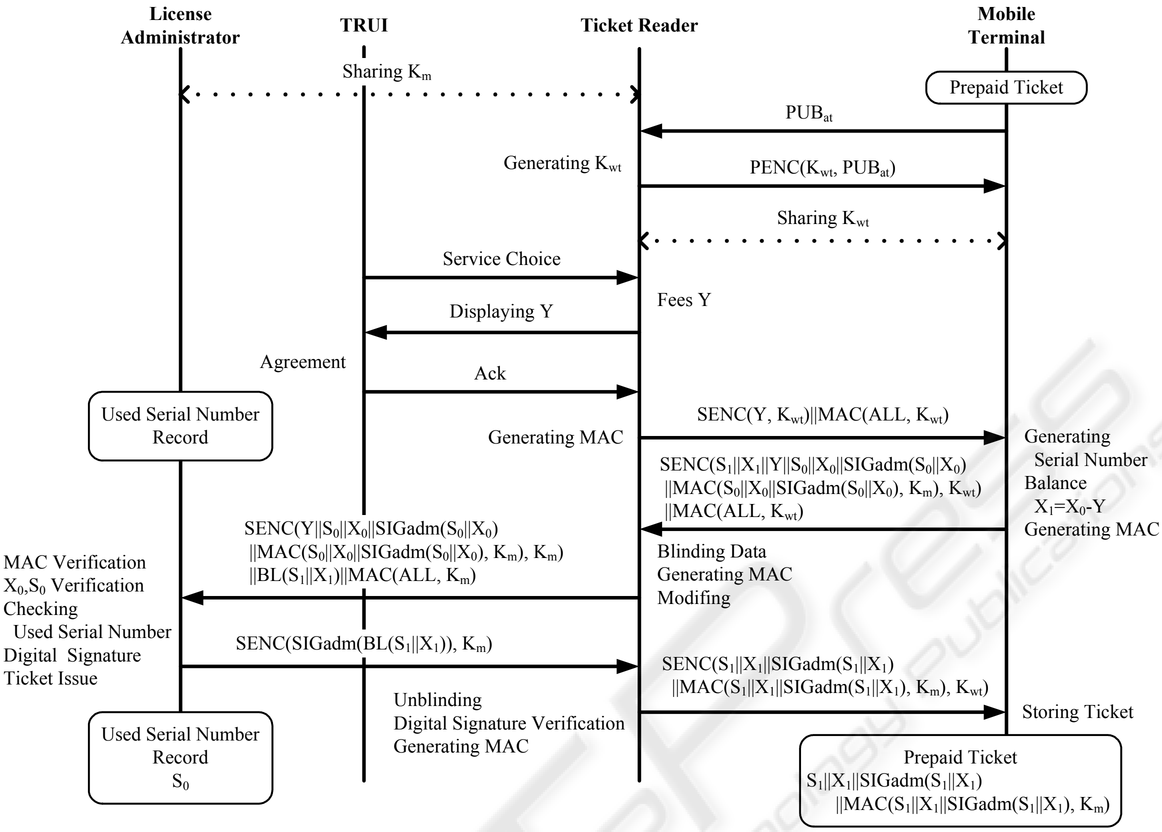
License Administrator
TRUI
Ticket Reader
Mobile Terminal
Sharing K_m
Prepaid Ticket
PUB_{at}
Generating K_{wt}
$PENC(K_{wt}, PUB_{at})$
Sharing K_{wt}
Service Choice
Fees Y
Displaying Y
Agreement
Ack
Used Serial Number Record
Generating MAC
$SENC(Y, K_{wt})||MAC(ALL, K_{wt})$
Generating Serial Number
Balance
$X_1=X_0-Y$
Generating MAC
$SENC(S_1||X_1||Y||S_0||X_0||SIGadm(S_0||X_0)$
$||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m), K_{wt})$
$||MAC(ALL, K_{wt})$
$SENC(Y||S_0||X_0||SIGadm(S_0||X_0)$
$||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m), K_m)$
$||BL(S_1||X_1)||MAC(ALL, K_m)$
Blinding Data
Generating MAC
Modifing
MAC Verification
X_0,S_0 Verification
Checking
Used Serial Number
Digital Signature
Ticket Issue
$SENC(SIGadm(BL(S_1||X_1)), K_m)$
$SENC(S_1||X_1||SIGadm(S_1||X_1)$
$||MAC(S_1||X_1||SIGadm(S_1||X_1), K_m), K_{wt})$
Unblinding
Digital Signature Verification
Generating MAC
Storing Ticket
Used Serial Number Record S_0
Prepaid Ticket
$S_1||X_1||SIGadm(S_1||X_1)$
$||MAC(S_1||X_1||SIGadm(S_1||X_1), K_m)$

Figure 4: Prepaid Ticket Payment.

$SENC(Y, K_{wt})||MAC(ALL, K_{wt})$, and sends it to the mobile terminal. The mobile terminal calculates the balance of payment, $X_1=X_0-Y$, and new serial number, S_1. Furthermore the mobile terminal generates payment data, $SENC(S_1||X_1||Y||S_0||X_0||SIGadm(S_0||X_0) ||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m), K_{wt}) ||MAC(ALL, K_{wt})$, and sends it to the ticket reader.

4. The ticket reader concatenates X_1 and S_1, blinds it, and sends modified payment data with blinded data, $SENC(Y||S_0||X_0||SIGadm(S_0||X_0) ||MAC(S_0||X_0||SIGadm(S_0||X_0), K_m), K_m) ||BL(S_1||X_1)||MAC(ALL, K_m)$, to the license administrator. If the administrator succeeds verification of payment data and confirms no existence of S_0 in used serial number record, this administrator signs blinded data, generates a part of prepaid ticket data, $SENC(SIGadm(BL(S_1||X_1)), K_m)$, and sends it to the ticket reader. At the same time, this administrator stores S_0 in used serial number database.
5. Through the same procedure of No. 6 and 7 in section 4.2, the mobile terminal stores new prepaid ticket, $S_1||X_1||SIGadm(S_1||X_1) ||MAC(S_1||X_1||SIGadm(S_1||X_1)), K_m)$.

5 DISCUSSION

5.1 Security

We discuss security, defined in section 2.2, of the proposed system in this section.

- **Sound Charge:** Through the procedures of section 4.1 and 4.2, fees of prepaid ticket are undoubtedly paid by direct debit from user's bank account according to H-ID.
- **Unforgeability:** MAC generated with Km is added to prepaid tickets, and then malicious users cannot create illegal prepaid ticket nor forge different value of the tickets, and the balance of the tickets.
- **Terminal Legitimacy:** Master key is installed in tamper resistant module of legal HT. Therefore license administrator can distinguish legal HTs from illegal ones by verifying MAC generated with K_m. Legal mobile terminals have public key certificate, so users or third parties cannot use

illegal mobile terminal without verification of the public key certificate.

- **Wiretapping Impossibility:** Serial number is introduced and it is used for verification of the correctness of the prepaid tickets. Malicious users cannot get this number because this number over network is blinded or encrypted.
- **Double-spending Impossibility:** The serial number which has been used already is recorded in used serial number database at a license administrator, and it is checked at every use of tickets, so the user or malicious person cannot use the same ticket twice.
- **Anonymity:** The license administrator cannot know any serial numbers at prepaid ticket issuance, and this administrator cannot identify a user with the serial number written on the prepaid tickets.
- **Dividability:** When the user pays by the prepaid tickets, the balance is calculated and the same value of prepaid ticket is issued, and thus the user can pay the arbitrary value of prepaid ticket.

Furthermore, if any illegality should happen, license administrator can suspend prepaid function on mobile terminal through mobile communication line. Therefore it is possible to keep the damage to a minimum.

In proposed system, when a prepaid ticket /balance is issued, the license administrator cannot know whether the requested value (X_0, X_1) is the same as the blinded value or not. If the administrator wants to verify X_n without trust in HT, it is necessary for HT to show true value of the blinded data to the administrator. For example, partial blind signature is a useful primitive for this purpose.

When user pays by a prepaid ticket, the user needs to show a serial number of the balance prepaid ticket to ticket reader. In this case, for secure communication a temporal key instead of the user's master key is used, and hence it is impossible to know the temporal key's owner. Consequently, anonymity is realized. However, the mobile terminal must generate the temporal key. If asymmetric encryption scheme in this system is RSA, the mobile terminal needs to select two very large primes and to calculate public key and private key. The computational cost of these operations may be high for mobile terminal. In this case, if HT generates one or more sets of key pairs instead of mobile terminal and sends them simultaneously with prepaid ticket issue, the cost can be reduced. On the other hand, if user rarely cuts off the power of mobile phone, there is a method that mobile phone generates the keys when idling, i.e. there is no other active processes.

It is necessary to hide the serial number to any other terminals except for the user's HT. In this case, the mobile terminal has to have function to blind/unblind the serial number, because malicious users' attacks, such as illegal copy, double use and so on, must be taken into account. Then for protection against such attacks, the license administrator has to record the serial numbers related to X_n and Y in used serial number database.

5.2 Specification

We consider a specification of proposed system in virtual conditions.

If one server of license administrator can process prepaid ticket payment in 30ms, the server can process 30 ticket payments per 1sec (used serial number search time is not included). If a permissible viewing duration without any payment is 1min, it is possible to process 1800 ticket payments during the period. This result shows that the administrator has to have 56 servers to process 100,000 tickets payments on peak time. It is realistic, so we think that this proposed system is enough practical.

In proposed system, the amount of used serial number record data increases in proportion to time, and it results in the waste of search time of the license administrator. To solve such a problem, the proposed system sets valid period of a prepaid ticket. The user adds ticket issuance time to the serial number which should be blinded. Thus the license administrator can prohibit prepaid ticket use beyond the valid duration, and the administrator can scrap old serial number. In this case, the valid period is used to reduce the amount of used serial number recorded in the database. However, we must consider CPU costs of valid duration's confirmation and the usability of the tickets with valid duration.

We will study a new protocol which can reduce search time and increase the usability in future.

6 CONCLUSION

We propose a new prepaid system based on PKI. The prepaid ticket is issued to only license administrators and the payment is performed with the help of prepaid ticket issuer. In addition, blind signature is used to protect the system from illegal use, and it is used to realize sound charge/payment and anonymity. Moreover, since the balance of the ticket is calculated and the same value of the ticket is issued, user can pay the arbitrary value of ticket.

Furthermore, we considered the system specification on virtual conditions, and we confirm that the proposed system is practical.

In future, we will develop securer and more practical system, which solves problems shown in section 5.

REFERENCES

ARIB STD-B25, 2003. Conditional Access System Specifications for Digital Broadcasting. In *Association of Radio Industries and Businesses,* ARIB Standards.

Chaum, D., 1983. Blind signatures for Untraceable Payments. In *CRYPTO'82,* Plenum Press.

Song, R., Korba, L., 2003. Pay-TV System with Strong Privacy and Non-Repudiation Protection. In *IEEE Transactions on Consumer Electronics.* IEEE.

Shigetomi, R., Otsuka, A., Ogawa, T., Imai, H., 2003. Refreshable Tokens and its application to Anonymous Loan. In *SCIS2003,* IEICE.

Chaum, D., 1990. Online cash checks. In *EUROCRYPT'89,* Springer-Verlag.

Nakanishi, T., Haruna, N., Sugiyama, Y., 1999. Electronic Coupon Ticket Protocol with Unlinkable Transcripts of Payments. In *SCIS'99,* IEICE.

Abe, M., Okamoto, T., 2000. Provably Secure Partially Blind Signatures. In *CRYPTO2000,* Springer-Verlag.

Abe, M., Camenisch, J., 1997. Partially Blind Signature Schemes. In *SCIS'97,* IEICE.

Abe, M., Fujisaki, E., 1996. How to Date Blind Signatures. In *ASIACRYPT'96,* Springer-Verlag.