E-TICKET ISSUING SYSTEM WITH 3-D PATTERN RECOGNITION FOR MOBILE TERMINALS

Ryuya Uda, Masahito Ito, Kohei Awaya, Hiroshi Shigeno and Yutaka Matsushita

*Matsushita Laboratory, Faculty of Science & Technology, Keio University
3-14-1, Hiyoshi, Kouhoku Ward, Yokohama, Japan*

Abstract The electronic ticket issuing system for cellular phones is described in this paper. The system has strong security for commercial use and has flexibility to support any cellular phone and PDA. A cellular phone needs no adding hardware module. A user can deal with everything related with a ticket such as issue, payment and showing with his cellular phone. A user accesses to the ticket issuing server to get a ticket and shows that ticket holding his cellular phone to the ticket reader at an entrance gate. 3-D pattern is used in order to show a ticket, and its recognition is free from tilt, rotation and moving of a cellular phone during reading. This electronic ticket issuing system can be used for concert ticket, train ticket, etc. This system allows reentrance, and still more, this ticket can be used as a coupon ticket that is used any number of times.

Keywords: E-commerce, Mobile Telephony, Privacy, 3-D code.

1. INTRODUCTION

Normally, someone who wants a ticket for a concert, for train and so on will go to a ticket shop to get a ticket. Recently, a ticket can be ordered by telephone, FAX or PC, and be sent later by physical mail. However, these steps mentioned above take high cost and bothersome. An electronic ticket

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35586-3_46](https://doi.org/10.1007/978-0-387-35586-3_46)

issuing system using display of a mobile terminal is proposed in this paper. This system provides integrative electronic ticket environment for a user. A user can deal with issuing, paying and showing of a ticket with his cellular phone.

In terms of security, public-key infrastructure must be needed. In this e-ticket system, using 3-D patterns for recognition of tickets can save the space for public-key signature of more than 1024bits. It is impossible in using 2-D barcode. Preventing from cracking ticket data, first, a tentative ticket called PreTicket is issued, and then, FinalTicket that has 3-D patterns are issued from PreTicket just before using. FinalTicket has short life span. Malicious users have no enough time to crack those ticket data, though 3-D patterns are obviously visible. In terms of privacy protection, user's IDs and onetime user's IDs are managed on different servers. A trustable communication carrier manages user's IDs that are related with personal information, and event providers manages onetime user's IDs issued by that communication carrier. In terms of convenience, reentrance is available in this e-ticket system. OnetimeUserID is locked and unlocked every time a user goes through a gate. This e-ticket issuing system guarantees security and privacy protection and provides convenience.

2. ELECTRONIC TICKETS FOR CELL PHONES

The overview of electronic ticket systems for cellular phones is described in this section.

2.1 Security Problems in Existing Systems

There are some studies and experiments for electronic ticket with cellular phones.

Some of them use 2-D code[7][8][9], that is, 2-dimensional bar code[4][5]. 2-D code has problem of security. The code displaying on LCD of a cellular phone is easily copied, and not so many data can be displayed on one frame of the LCD screen. 2-D code electronic ticket issuing system developed by HITACHI uses "QR code(Quick Response Code)"[6]. QR code is developed by DENSO CORPORATION. "CyberCode"[11] developed by SONY is 2-D code too. In the system with 2-D code, ticket data embedded in one frame have error correcting code(ECC)[3] bits in order to recover unread data. To

recover 30 percent of unread data, effective ticket data size in one frame becomes smaller.

Another electronic ticket issuing system using a public-key[1][2] hardware module is developed by OMRON. A cellular phone used for the system is an exclusive one. When a ticket is used, that phone communicates to a gate with IrDA. Therefore, a public-key hardware module and an infrared device are needed for a cellular phone for the service.

2.2 E-Ticket System with 1024bits PKI Security

The e-ticket issuing system in this paper uses 3-D pattern communication. 3-D pattern has no limited space to store the data of a ticket. 1024 bits RSA electronic signature[10] is used for authentication of this e-ticket in order to keep the security, but no hardware module is added to a cellular phone. There are still more devices in this system to protect user's privacy and to prevent falsification of a ticket. This e-ticket system works on any cellular phone, PDA and Handheld PC without remodeling.

Figure.1: The relationship with each server and each terminal

Figure.1 shows the relationship with each server and each terminal. A User of this system uses a mobile terminal like a cellular phone to get and show a ticket. The ticket issuing server and the event server are connected with a mobile terminal via Internet with packet communication, and connected with

an entrance terminal at an event hall via dedicated line. Ticket issuing server directly manages users and issues PreTickets. While, event server deals with OnetimeUserIDs and issues FinalTickets. The entrance terminal at the event hall receives ticket data from user's mobile terminal by 3-D pattern recognition. It compares a signature of ticket data with data from event server, and allows or denies user's entrance.

3. ISSUING TICKET

Issuing ticket process is divided into three steps i.e. user registration, issuing PreTicket, issuing FinalTicket.

3.1 User Registration

A user must be registered to this e-ticket system before requiring a ticket in order to get his UserID and his Password. A user accesses to the ticket issuing server from his cellular phone, and registers himself with his name, address, phone number, credit card number, etc. It is desirable that serial number of the cellular phone or any other information that identifies the cellular phone is logged, if possible. UserID and Password are generated and sent to the user after that registration, and they are managed only in the ticket issuing server.

3.2 Issuing PreTicket

Figure.2 shows the procedure for issuing PreTicket.

Figure.2: The procedure for issuing PreTicket.

A user who wants a ticket accesses to the ticket issuing server from his

cellular phone via HTTP with SSL. He selects a ticket and sends a request for buying it, inputting his UserID and his password. The ticket issuing server receives the request, it generates OnetimeUserID for that user, and it sends a PreTicketData page in which a URL link to FinalTicketData is embedded.

An example of an embedded URL link is as follows.

https://www.***.co.jp/ticket?ID=ABC12345&ticket=ZX1qdyd3ikV8WDaT

The user caches that PreTicketData page, if possible, or bookmarks that URL. PreTicket is a temporary ticket, but a sales contract is concluded in it. If the user cancels the contract, a cancellation fee may be required.

After issuing PreTicket, the user accesses to an event server instead of the ticket issuing server. That event server knows relationship between OnetimeUserID and FinalTicketData, but does not know who has this OnetimeUserID.

3.3 Issuing FinalTicket

Figure.3 shows the procedure for issuing FinalTicket.

Figure.3: The procedure for issuing FinalTicket.

A user accesses to an event server from a URL link to get FinalTicketData. An example of a URL link is as follows.

https://www.***.co.jp/ticket?ID=ABC12345&ticket=ZX1qdyd3ikV8WDaT

OnetimeUserID and PreTicketData are sent to an event server, and AccessData that includes TimeStamp is generated at the same time. Event

server verifies OnetimeUserID and PreTicketData and sends SigFinalTicket to user's terminal.

TimeStamp is needed in order to reissue the ticket. If a user requests reissuing the same ticket, an event server reissues SigFinalTicket generated from new AccessData. SigFinalTicket generated from AccessData having old TimeStamp is not valid after this reissuing. SigFinalTicket has the period of validity. It should be set between 5 to 30 minutes. Reissuing is needed after that period of validity in order to prevent illegal access.

SigFinalTicket is PKI signature on OnetimeUserID, on AccessData and on FinalTicketData. Sequence or XOR of OnetimeUserID, AccessData and FinalTicketData is hashed to hash value, and the hash value is encrypted into SigFinalTicket with RSA private key of this event.

SigFinalTicket =

```
RSAPri{
  hash{
    Sequence(OnetimeUserID, AccessData, FinalTicketData) ||
    XOR(OnetimeUserID, AccessData, FinalTicketData)
  }
}
```

The form of SigFinalTicket is dependent on a user's terminal. It is written by Java for i-mode or au, by sequence of PNG graphics for J-SKY, or by animation-GIF graphics etc.

4. ENTRANCE AND REENTRANCE

4.1 Entrance

Figure.4 shows the procedure for entrance. Entrance terminal receives user's information data from event server via dedicated line when a user receives SigFinalTicket. That information data includes OnetimeUserID, AccessData, FinalTicketData and RSA public-key of this event, and those data are updated every time FinalTicket is reissued to the user.

When a user enters through the gate, he holds it to e-ticket reader. Entrance terminal receives OnetimeUserID and SigFinalTicket via 3D pattern recognition, and decrypts SigFinalTicket with the public key of this event.

When decrypted data of SigFinalTicket is equal to hash value of OnetimeUserID, AccessData and FinalTicketData, entrance terminal allows the user who has that OnetimeUserID to enter. This is described with the expression as follows.

$$\text{RSAPubEvent(this)\{SigFinalTicket\}} = \text{hash}(\text{OnetimeUserID}, \text{AccessData}, \text{FinalTicketData})$$

Figure.4: The procedure for entrance

4.2 Reentrance

When a user enters through a gate of an event hall, entrance terminal locks that user's OnetimeUserID. When he exits from that hall while the event is holding on, exit terminal unlocks his OnetimeUserID. It assumes temporal exit. An exit terminal can be the same as an entrance terminal. The function of exit and that of entrance are switched according to the direction of a passing user. When he reenters into that hall, entrance terminal relocks his OnetimeUserID.

5. 3-D PATTERN COMMUNICATION

3-D pattern is different from barcode. 3-D pattern is a communication method and not a printed identification mark. 3-D pattern communication using time-domain is free from resolution of LCD, so that data capacity is unlimited by using it.

5.1 2-D Barcode

2-D barcode is a cell pattern shown in Figure.5.

Each cell which is painted black or white shows "0" or "1", that is, it shows 1 bit, and the cells are placed along the x-axis and y-axis. 2-D barcode shown in Figure.5 is a QR code pattern developed by DENSO Corporation. Three big cells placed in each corner are positioning markers. They are used in order to decide the position of this barcode. White area on the outside of those positioning markers is quiet zone which is always kept white to help the scanner read positioning markers easily.

Figure.5: 2-D barcode

5.2 3-D Pattern

3-D pattern described in this paper stores data along the x-axis, y-axis and time axis. As shown in Figure.6, 3-D pattern has 4 positioning markers surrounded by quiet cells, 1 synchronizing marker and quiet zone.

Synchronizing marker is used in order to synchronize between LCD and the reader. Each cellular phone refreshes its screen as fast as possible at the maximum speed within the limit of the performance of that cellular phone.

While, the reader can read the LCD of a cellular phone at the speed of 30 frames per second since normal DV camera is used for e-ticket reader in this implementation. Changing the color into black or white alternately, synchronizing marker tells the timing of refreshed frames on LCD to the reader. Moreover, synchronizing marker tells the reader which is the top of the screen.

Figure.6: 3-D pattern

Only 4 positioning markers are needed in 3-D pattern recognition. They are smaller than those of QR code, because LCD is neither folded nor bent unlike a sheet of paper. The ticket reader can read 3-D pattern even if a cellular phone tilts to one side or rotates horizontally during reading. Tilt, rotation and moving of a cellular phone during reading are detected by positioning markers.

6. COMMUNICATION SPEED

6.1 Minimum Communication Speed

In this implementation, 1 cell is consisted of 7 times 7 pixels square in order to disregard bad pixels, owing to the restriction of performance of the reader. It takes 2 seconds to read the data now, because the camera of the reader is an

ordinary DV camera and a note PC with low CPU power is used for analyzing each frame. The note PC used for this implementation deals with only 80,000 pixels per frame. Using an appropriate camera and a more powerful PC, 3-D pattern is read within 0.5 second.

Any cellular phone used for this implementation has display resolution 120 pixels in width and 130 pixels in height. As shown in Figure.6, there are 15 x 16 cells in one frame except quiet zone. To express the data, positioning markers and quiet cells and synchronizing marker cannot be used.

$$15 \times 16 - 17 = 223 \text{ cells}$$

So there are 223 effective cells in one frame. Therefore, 223 bits data per frame can be sent to the reader. Using the time-axis, bits of data can be increased unlimitedly with increasing of frames.

6.2 Maximum Communication Speed

If the e-ticket reader is idealistic, maximum communication speed may be calculated as follows. Normal i-mode terminal resolution is 120 pixels in width and 130 pixels in height. If 1 cell is consisted of 1 time 1 pixel square, each frame can send 15.6 kbits.

$$120 \times 130 = 15.6 \text{ kbits / frame}$$

If response speed of LCD is 50ms, the data transfer speed is 312 kbits per second.

$$15.6 \text{ kbits} \times (1/0.05) = 312 \text{ kbits / sec}$$

Moreover, monochrome terminal that can display 8 bits grayscale is able to send 124.8 kbits / frame.

$$120 \times 130 \times 8 = 124.8 \text{ kbits / frame}$$

Color terminal that can display 16 bits color is able to send 249.6 kbits / frame.

$$120 \times 130 \times 16 = 249.6 \text{ kbits / frame}$$

But at high speed-communication mentioned above, some error correcting code methods, for example, Read-Solomon may be needed.

7. ADVANTAGES

7.1 Advantages of System

This e-ticket system has the advantages of security, flexibility and convenience. Using 3-D pattern recognition, bits of embedded data can be increased unlimitedly with increasing of frames. The bits are long enough to use public-key cipher with secure bit length.

Using OnetimeUserID, this system protects user's privacy from a malicious ticket dealer. UserID related with user's privacy is managed only at ticket issuing server under the control of common carrier. Event servers under the control of ticket dealers know relationship between OnetimeUserID and FinalTicketData, but do not know who has this OnetimeUserID.

FinalTicket is not revealed until the time some hours or minutes before the event hall opens. The system gives no enough time to any user to analyze the FinalTicket.

Electronic Signature is added to a ticket at the servers. A user does not need to encrypt or decrypt his data with PKI at his cellular phone. Need for calculation hardware module for PKI hinders the electronic ticket services from spreading to cellular phones.

This system can implement on any cellular phone e.g. i-mode, J-SKY, au, and PDA, Handheld PC and so on. This system works on some i-mode terminals and some J-SKY terminals.

This system allows reentrance, and still more, this e-ticket can be used as a coupon ticket that is used any number of times.

7.2 Advantages of Reading

The ticket reader of this system can read 3D pattern even if a cellular phone tilts to one side or rotates horizontally during reading. Tilt, rotation and moving of a cellular phone during reading are detected by positioning markers.

8. SUMMARY

E-ticket will rapidly spread to various services instead of a paper ticket. Magnetic card has become the main current and many kinds of cards are used

for many services. Almost all cards are prepaid and management system for payment is not unified. There are many users who don't want to have a lot of cards in the wallet. The system of this paper allows e-ticket issuing to have the plural organizations for management and payment. While, one event ticket managed by one organization can be provided by plural communication carriers. Furthermore, a population having a cellular phone is increasing. The system is desirable for electronic ticket issuing in a new generation.

9. REFERENCES

1. Douglas R. STINSON, "CRYPTOGRAPHY: Theory and Practice", CRC Press, Inc, 1995.
2. Shigeo Tsujii, "Cryptography and Information Security", SHOKODO CO.,LTD., 1990.
3. Vera Pless, "INTRODUCTION TO THE THEORY OF ERROR-CORRECTING CODES", Wiley Japan, Inc., 1984.
4. Toshifumi Ogata, Hideo Makino, Ikuo Ishii, Makoto Nakashizuka, "Location Guidance System for the Visually Impaired Using an Invisible Bar Code", IEICE Journal, Vol.J80-D-II No.11, pp.3101-3107, 1997.
5. Hideo Makino, Fumihito Morishita, Yoshio Abe, Shirou Yamamiya, Masaru Hasegawa, Ikuo Ishii, Makoto Nakashizuka, "3-D Object Guidance Method for the Visually Impaired Using an Invisible Bar Code", IEICE Journal, Vol.J80-D-II No.11, pp.3094-3100, 1997.
6. Takayuki Nagaya, Tomohiko Yamazaki, Masahiro Hara, Tadao Nojiri, "Two Dimensional Code for High-Speed Reading", Proceedings of the 52nd National Convention IPSJ, Vol.2, pp.253-254, 1996.
7. Ryoko Seki, Hideo Makino, Shinji Watanabe, Ikuo Ishii, Makoto Nakasizuka, "Image Processing and Verbal Guidance using an Invisible 2-D Code -Application for Portrait Data Encoding and Book Guidance-", TECHNICAL REPORT OF IEICE, MBE96-73, pp.85-92, 1996.
8. Hideo Nakamura, Hideo Makino, Shiro Yamamiya, Yoshinobu Maeda, Mikihiro Hirono, "Consideration on Recognition of Block-type 2-D Bar Code", TECHNICAL REPORT OF IEICE, HCS98-39, pp.1-8, 1999.
9. Tetsuya Sugahara, Hideo Makino, Ikuo Ishii, Makoto Nakashizuka, "Object Guidance System for the Visually Impaired using a 2-D Bar Code", TECHNICAL REPORT OF IEICE, MBE94-148, pp.79-84, 1995.
10. Rivest, R.L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.
11. Jun Rekimoto, Yuji Ayatsuka, "CyberCode: Designing Augmented Reality Environments with Visual Tags", Designing Augmented Reality Environments (DARE 2000), 2000.