NEWS RELEASE

NTT

December 21, 2001

A new digital ticket system that allows a single smart card to be used for a wide-range of services including travel and entertainment

FlexTicket -- provides description flexibility, high security level, and high speed

Nippon Telegraph and Telephone Corporation (hereafter NTT, Headquarters: Chiyodaku Tokyo Prefecture, President and Senior Director: Junichirou Miyazu) has developed a digital ticket system "FlexTicket" that can be used to circulate various types of "Values" such as admission tickets and meal coupons ("Ticket" in the following text) in the form of digitalized tickets over the network.

FlexTicket makes it possible for users to acquire various types of tickets like concert tickets and hotel vouchers over the Internet, to store them in single smartcard, and to transfer tickets between themselves. FlexTicket is the first digital ticket system to adopt public key cryptography(*1), thereby offering an extremely high level of security; Furthermore, FlexTicket uses an elliptic curve encryption scheme (*2) and so achieves high-speed processing.

Based on the FlexTicket technology, NTT Communications Corporation and PIA Corporation are currently planning to develop digital ticketing services.

Electronic commerce is rapidly advancing in all fields. One such field is ticketing. Digitalizing ticket information and issuing tickets over the Internet yields many advantages as they can be obtained more timely and more cheaply than paper tickets. Currently, there are several digital ticket systems that offer such services, but most of them were designed for specific applications and so they can't provide the new comprehensive electronic commerce infrastructure needed.

NTT Information Sharing Platform Laboratory has, over the last few years, developed a digital ticket system that can be used as a new digital medium for the circulation of diverse types of "ticket". Key design goals were to realize user comfort (in terms of security) and convenience. Its efforts have culminated in the business-ready system called FlexTicket.

FlexTicket prevents counterfeiting, double spending, and intrusion into the user's privacy through its original and high-level security technique. It supports the issue, circulation, and the redemption (confirmation of tickets) of various digital tickets. In addition, XML (*3) language is adopted to offer adequate flexibility in describing the contents of tickets. This makes it possible for all ticket issuers, regardless of their field, to use the same program for circulating digital tickets easily and securely. Moreover, transfers between users (individuals) are possible, and it is also easy to store tickets from different issuers in one smartcard. Therefore, users can store various tickets, such as concert passes acquired over the Internet, in one smartcard.

NTT Information Sharing Platform Laboratory is planning to implement FlexTicket on top of cellular phones to realize ubiquitous commerce (*4).

< Main features >

1) Applicable to any field: Since it offers a flexible ticket definition language, it is not restricted to any one specific digital ticket issue system; its description capability supports ticket issuers in any field . Anticipated applications include:

- Airline tickets, mileage cards, and commutation tickets (transportation)
- Gift certificates, meal coupons, and hotel vouchers (shopping)
- Concert tickets, baseball tickets, and advance movie bookings (entertainment)

2) Any ticket can be issued easily: It is much more practical than dedicated digital ticket systems, which need different software and hardware for each application, since any issuer can create tickets simply by defining the operating condition in XML.

This yields great flexibility in issuing tickets which greatly reduces development cost and the difficulty of coping with changes in issuance conditions. For example, new kinds of tickets can be supported without requiring the program in the smartcards, which have already been distributed to the users, to be updated.

3) High security level: The security technique of NTT digital cash (see http://www.ntt.co.jp/news/news01e/0111/011129.html) is followed. Special attention was paid to data protection to prevent counterfeiting, double spending, and privacy attacks by adopting a public key cryptosystem. rs will, therefore, feel comfortable in using the tickets.

4) High-speed, off-line confirmation of ticket processing: This system offers the benefits of high-speed encryption technology and the convenience of contactless operation. Since this system does not employ a central server to process the tickets, high-speed processing is possible which is essential in many applications such as popular music venues, sports games etc. All operations are performed locally between the gate terminal and the smartcard.

< System Overview > Figure

1) A special dual interface smartcard (contact and contactless) is prepared.
2) The user can access the server of a digital ticket issuer (or an agent) through the Internet, and buy various "Tickets".
3) The purchased "Tickets" are stored in the dual interface smartcard using a KIOSK terminal/personal PC equipped with smartcard reader/writer. (Contact interface used)
4) The "Ticket" is deleted when it is presented to the collection party, when presented at a movie theater entrance for example. (Contactless interface used to achieve high-speed gating)
5) By installing FlexTicket in personal PCs, transfers between individuals become possible. "Tickets" can be sent either directly to users (synchronous transfer), or to a "ticket account" server (asynchronous transfer).

< Key points to the technology >

1) Ticket definition language
Details of rights represented by the ticket (expiration date and seat number, etc.), and the circulation conditions (issuer and the restrictions placed on the ticket collector etc.) are described using a newly developed digital ticket rights information definition language based on XML. Therefore, new applications can be supported in a very flexible manner without requiring special applications to be newly created. Flexibility in the face of changes in the operating conditions is also offered.

2) Genuineness transfer technology
To store a "Ticket" in a smartcard, a digest ("Token") of the complete "Ticket" information description, written in the Ticket definition language, is created and loaded into the card. Our advanced circulation protocol ensures that this "Token" is not copied or altered illegally. Since each "Token" is small, various digital tickets of different kinds can be stored in a low cost smartcard and thus carried at the same time. Holding a "Token" represents ownership of an original "Ticket". The right to use a "Ticket" disappears if its "Token" is consumed.

3) First use of public key cryptosystem in a digital ticket system (elliptic curve coding)
This digital ticket system is the first in the world to employ a truly effective public key cryptosystem. As a result, it offers an unprecedented level of security. Moreover, to achieve high-speed processing, elliptic curve encryption (*2) is used as the basis of the public key cryptosystem. As a result, high-speed, off-line ticket processing is offered with the convenience of the contactless smartcard interface.

< Glossary >

***1 Public key cryptography**
Cryptography in which encryption is performed using a public key while decryption requires the corresponding secret key. Since the public key can be disclosed, key management can be simplified in this cryptosystem. Also, the cryptography can be applied to generate electronic signatures and to perform common key exchange.

The arithmetic processes needed to realize encryption and decryption are complex so processing speed may seem to be a problem. However, various methods to achieve high-speed processing have been developed recently.

***2 Elliptic curve encryption scheme**
A public key encryption scheme that can provide stronger security with shorter key length compared to the RSA scheme. This system with a 160 bit key offers the same level of security as the RSA scheme with a 1,000bit key. Its name is derived from the elliptic curve used for encryption and decryption.

***3 XML**
The Extensible Markup Language (XML) is the universal format for structured documents on the Web. It is recommended by W3C (World Wide Web Consortium) as a standard of the Internet.

***4 Ubiquitous Commerce:**
A form of commerce in which devices embedded in all terminals and goods are interworked. Mobile commerce based on the use of personal cellular phones is considered to be the first phase of ubiquitous commerce.

- Figure : System Overview of FlexTicket

For inquiries related to this matter
NTT Information Sharing Laboratory Group
Planning Department, Public Relations:
Iizuka, Sano, and Ikeda
TEL: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE