NEWS RELEASE

NTT

(Press Release)

November 29, 2001

Digital cash that can be used to purchase services and goods with complete safety and at high speed is here now.

-Its usage is virtually unlimited, from simple store purchases to bus fare payments to regular cash register transactions.
- Digital cash can be downloaded through many public telephones.

Nippon Telegraph and Telephone Co. (hereafter NTT, Headquarters: Chiyodaku Tokyo Prefecture, President and Senior Director: Junichirou Miyazu) has developed a public key digital cash system, based on contactless smart cards, that can be used in a variety of eminently practical settlement scenarios. It is suitable for any application that demands high-speed payment processing such as transportation fare collection.

The digital signature processing time is only 1msec, the shortest yet reported, because an advanced public key cryptosystem processing scheme is used (*1). Digital cash payments take no more than 250msec.

The high level of security offered by public key cryptography with the world's fastest processing scheme is married the benefits of contactless smart cards. The cards show the true advantages of contactless operation in situations of transportation fare collections like buses. Moreover, the functionality of the contactless smart cards permits them to be recharged (monetary value is added to the card) at smart card public telephones.

The use of smart cards raises the expectations of electronic commerce and encourages the move to electronic government. Existing settlement processing systems such as those of financial institutions are mainly using contact-type smart cards or terminals. In addtion to contact-type smart cards, the contactless smart cards are introduced to use in some areas.

In February of this year, NTT Information Sharing Platform Laboratory was the first to complete the development of a highly secure digital cash platform that also offers high-speed processing and excellent convenience (see http://www.ntt.co.jp/news/news01e/0102/010202.html). Its security and speed are due to its use of an advanced public key cryptographic scheme based on elliptic curve digital signature scheme(*2). Its convenience comes from its use of contactless smart cards.

This time, the performance of the digital cash system was much improved to the practical usage level. The current level of performance is sufficient to support real-world applications, in all operations from fare adjustments in transportations to cash register payments.

The key benefit of this system is its high-speed payment processing. This is achieved with the use of elliptic curve digital signature scheme and the pre-calculation technique that prepares and stores the needed calculation results prior to any actual transaction. The digital signature processing time can be dramatically reduced to only 1msec, and the whole payment processing can be done within 250msec.

Furthermore, technology was developed that allows digital cash transactions to performed through the smart card public phone. NTT East Japan Corp. and NTT West Japan Corp. has established 42,200 smart card public telephones (As of the end of September, 2001). This technology enables that digital cash can be easily transferred from the user's account via the smart card public telephones in addition to the issuer-specific terminals, such as those of financial institutions (ATM etc.). This charging flexibility was achieved by using the contactless smart card technology and the smart card public telephone technology, both of which were developed by the research laboratories of NTT.

This digital cash system was implemented referring to the specification for off-line debit specifications (*4) and the EMV specification (*3), which is the smart card credit card terminal standard for financial institutions etc. It is also suitable for making purchases at shops across the nation including convenience stores and department stores. This installation was done in cooperation with NTT Communications Ltd.

NTT Information Sharing Platform Laboratory plans to convert this cutting-edge research into applications that use mobile payments via cellular phones so as to "replace the purse".

< System features >

1)Speedy payment processing is possible.
Payment processing is possible within 250msec, a world record, through the combination of the contactless smart card and the public key cryptography. Therefore, when applying this system to a smart card bus fare payment system, far speedier payment processing becomes possible compared to the use of magnetic.

2) The smart card bus fare payment system permits off-line charging.
The off-line charging system increases the monetary value to the digital cash (charging) by way of the driver in the smart card bus payment system. To prevent illicit acts against the digital cash, an original security technique is employed that is also very practical.

3)Using smart card public telephones as transaction terminals.
Since the many smart card public telephones installed throughout the country can be used as a transaction platform, you can increase the monetary value held in your digital cash card anytime and anywhere. No additional software need be installed in the smart card IC public telephones to offer this functionality.

4) It supports various usages.
Because it was implemented referring to the EMV specification and the off-line debit specification of the Federation of Bankers Association of Japan, it can promote in use at a variety of shop terminals including convenience stores and department stores.

< key technology points >

(The world's highest processing speed is achieved through the use of public-key cryptography)
Several of the code processing algorithms needed to realize signature processing can be "preprocessed" (i.e. performed before being needed). This shortens the signature processing time by 90% to 1msec or less, a new world record.
Moreover, the payment processing time was cut to no more than 250msec by optimizing the elliptic curve signature generation operation, the protocol, and the reading/writing devices.

< glossary >

***1 Public key Cryptography**
This is a security approach that uses a public key to encrypt data while requiring a secret key to achieve decryption. This can also be used for electronic signature and common key exchange because the public key can be used by anyone to confirm transaction accuracy. The arithmetic processes needed for encryption and decryption are complex, so processing speed is a problem. Fortunately, various innovative methods have been developed to achieve high-speed processing.

***2 Elliptic curve digital signature scheme**
This scheme is far superior (efficient) to the RSA(*5) method.
A 160-bit key offers the same level of security as an RSA scheme with a 1,000-bit key.
Its name comes from its use of operations on elliptic curves to realize cryptographic functions.

***3 EMV (Europay/Mastercard/Visa)**
This smart card type credit card and terminal specification is the result of the joint efforts of three European credit card companies. It is a de facto world standard.

***4 Off-line debit**
The monetary values in the digital cash card are assumed to originate directly from banks or other financial institutions. Sums can be disbursed in an off-line fashion without connecting to the center (host).
(In usual debit schemes, connection must be made to a central host in general, and monetary values are disbursed online)
The monetary value is then immediately adjusted.

***5 RSA encryption method**
This is a commonly used method for encrypting and decrypting data Different keys are used to realize data encryption and decryption.
It is widely used to realize functions such as attestation systems and digital signatures.
Its security is assured by the difficulty of factorizing large prime numbers. The acronym is derived from the names (R. Rivest, A. Shamir, L. Adleman) of its developers.

- Appendix: Various Scene of NTT Digital Cash

[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