NTT Communications Corporation
Nippon Telegraph and Telephone Corporation

February 2, 2001

FOR IMMEDIATE RELEASE

NTT Com, NTT Realize World's First High-Speed Processing of Public-Key Encryption Using Combined Contact/Contactless IC Cards

Enables electronic payments in 0.4 seconds using high-security contactless IC cards

NTT Communications Corporation (NTT Com) and Nippon Telegraph and Telephone Corporation (NTT) announced today that they have developed a high-processing and high-security e-money system using public-key digital signature. The new e-money allows users to make store payments in less than 0.4 seconds. The system is based on technology developed by NTT Information Sharing Platform Laboratories and it uses commercially available combined contact/contactless IC cards. The two companies are the first in the world to make practical use of highly-functioning applications, such as e-money, over an contactless IC card, which also provides a high degree of security and uses public-key encryption.

Previously, it has been difficult for contactless IC cards to conduct high-speed processing with complicated calculations, such as public-key encryption, due to the lack of electric supply to the cards. Instead of using RSA encryption*1, NTT used elliptic-curve encryption*2 with less processing. NTT also refined*3 the calculation of the elliptic-curve encryption to realize high-speed processing.

Such processing technology enables even contactless IC cards to realize high-speed processing, along with a high degree of security. The need to use public-key encryption with contactless IC cards is crucial. Such cards would include financial cards (e.g. credit, debit), electronic tickets, and personal forms of identification, such as official-seal and residential registration cards. The new system, therefore, is expected to spur the future proliferation of contactless IC cards*4.

The system uses a commercially marketed contact/contactless IC card, whose interface complies with the ISO7816 (contact) and ISO14443 (contactless) standards*5. The system uses such cards with consideration given to interchangeability of virtual (contact) and real (contactless) IC card applications. For example, it will be possible to buy an electronic train ticket on a home PC (via a contact interface) and use the ticket to access a train station wicket (contactless interface).

NTT Com has begun talks with financial, transportation, distribution and content industry representatives regarding the IC-card service applications. The company plans to start related services within this year. Functions to add new applications to already issued IC cards will be developed in the future to ensure long-term use of the cards.

Notes:

*1 RSA encryption:

A typical public-key encryption that uses different keys for data encryption and decryption. It is widely used for authentication and digital signatures. The security of RSA depends on the difficulty of factoring large integers.

*2 Elliptic-curve encryption:
A type of public-key encryption that is difficult to decipher, even though its key lengths are shorter compared with the RSA. As for key lengths, which are related to security, 160 bits of elliptic-curve encryption is said to equal 1,000 bits of RSA. The name of the encryption is derived from the use of elliptic-curb discrete logarithms for encryption and decryption processes.

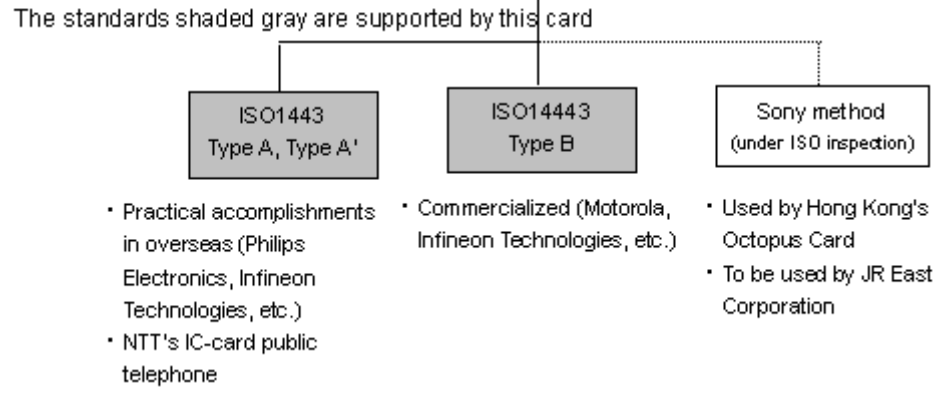
*3: NTT decreased the time needed to create digital signature for public-key encryption by one-third, meaning that the signature can be created in approximately 0.2 seconds. This was possible by processing a part of the public-key encryption before the real processing, and by using that result for the real processing.

*4: Contact IC cards, for its high security, have been mainly used to date in the financial industry. With today's announcement, however, contactless IC cards can be applied more widely.

*5: Complies with both Type A and B of ISO14443 standard (see figure below). To enable use of multiple terminals, the laboratories are now researching ways to support both Type A and B.

Types of Contactless IC Cards

	Close-coupled	Proximity	Vicinity
ISO	ISO10536	ISO14443	ISO15693
Communication distance	up to 2 mm	up to 10 cm	up to 70 cm
Data speed	more than 9.6 kb/s	more than 106 kb/s	up to 26 kb/s
Carrier frequency (Performance clock)	(4.91 MHz)	(13.56 MHz)	(13.56 MHz)



# # #

For further information, please contact:

Ms. Megumi Inaji or Mr. Fuyuki Natsumeda
Public Relations Office
NTT Communications Corporation
Telephone: +81 (3) 6700-4010

NTT NEWS RELEASE