NEWS RELEASE

NTT

April 17, 2001
Nippon Telegraph and Telephone Corporation

Announcement of Royalty-free Licenses for Essential Patents of NTT Encryption and Digital Signature Algorithms

Nippon Telegraph and Telephone Corporation (NTT) is pleased to announce that it is directing the following statement towards national/international organizations/projects related to standardization activities.
NTT intends to grant royalty-free licenses for the essential patents of the below-listed world-leading encryption and digital signature algorithms, developed by NTT Information Sharing Platform Laboratories, with the provision that said algorithms are to be used as is.

- Symmetric-key encryption algorithm (*1) "Camellia" (developed in cooperation with Mitsubishi Electric Corporation (Mitsubishi))
- Public-key encryption algorithms (*2) "EPOC" and "PSEC"
- Digital signature algorithm (*3) "ESIGN"

Caution: This statement is valid only for implementing Camellia, EPOC, PSEC, and ESIGN, respectively, as is, and does not permit modification of said algorithms.

As electronic commerce on the Internet is now a hot topic, secure communication networks are in strong demand to protect company and personal information. The Japanese government has also issued plans for the E-Government, e.g., "Action Plan for Building Foundations of Information Systems Protection from Hackers, and Other Cyber-threats" (January 2000), and "MITI Action Plan for a Secure E-Government " (April 2000).

Encryption and digital signature algorithms are the critical technologies for achieving the secure advanced telecommunication society. Furthermore, worldwide interoperability of encryption and digital signature systems is also important as economic globalization advances. Accordingly, na-tional/international organizations/projects toward standardization are now evaluating and standardizing encryption and digital signature algorithms. To this end, NTT has proposed Camellia (in cooperation with Mitsubishi), EPOC, PSEC, and ESIGN to some organizations/projects.
Because NTT is playing an important role in the realization of the secure advanced telecommunication society, NTT has decided to grant royalty-free licenses for the essential patents of the above-mentioned encryption and digital signature algorithms. NTT believes that this decision will promote the utilization of encryption and digital

signature algorithms. One goal is the creation of secure information providing services, electronic commerce, and security applications at low cost.
Hereafter, NTT desires to promote utilization of its encryption and digital signature algorithms for security applications and secure network services by distributing reference codes and contributing to standardization activities. Furthermore, NTT will continue to develop security application systems with the algorithms, e.g., electronic certification systems, electronic money systems, and electronic commerce systems.

Please pay close attention to the limits of this statement. The statement describes the granting of royalty-free licenses only for the essential patents of the above-mentioned encryption and digital signature algorithms as long as Camellia, EPOC, PSEC, and/or ESIGN are implemented without alteration. NTT continues to reserve all implementation techniques and related patents of Camellia, EPOC, PSEC, and ESIGN. Mitsubishi also continues to reserve those of Camellia.
The essential patents of Camellia are the common properties of NTT and Mitsubishi, and Mitsubishi has agreed with NTT's this decision.

<< The Features of the Encryption and Digital Signature Algorithms Covered by This Announcement >>

□ Camellia

Camellia is a block cipher with 128-bit block size (*4). It was developed by NTT and Mitsubishi using i) NTT's cipher design technologies geared to high-speed software implementation, ii) Mitsubishi's cipher design technologies for compact and high-speed hardware implementation, and iii) state-of-the-art security evaluation technologies of both companies. Camellia has a higher security margin than Rijndael, which was selected as the proposed Advanced Encryption Standard (*5). Furthermore, it can be implemented efficiently in software, including the 8-bit processors used in low-end smart cards, the 32-bit processors widely used in PCs, and the 64-bit processors used in some servers. Moreover, Camellia encryption hardware offers the smallest area and best efficiency in the world among existing 128-bit block ciphers.
Camellia home page: http://info.isl.ntt.co.jp/camellia/
Camellia press release: http://www.ntt.co.jp/news/news00e/0003/000310.html

□ EPOC

EPOC is a practical public-key encryption algorithm. It has been mathematically proven that EPOC cannot be broken under the assumptions that hash function (*6) outputs are random, and that factoring problems (*7) are difficult. On the other hand, the security of the RSA primitive has not been mathematically proven.
EPOC home page: http://info.isl.ntt.co.jp/epoc/
EPOC press release: http://www.ntt.co.jp/news/news98e/980416.html

□ PSEC (Provably Secure Elliptic Curve encryption)

PSEC is a public-key encryption algorithm, and it is mathematically proven that PSEC cannot be broken under the assumptions that hash function outputs are random, and that elliptic curve discrete logarithm problems (*7) are difficult. Compared to the RSA encryption algorithm, it yields higher implementation speed in software since high security is realized even with shorter length keys. Furthermore, the speed can be improved by adding the speed-up implementation techniques developed by NTT.
PSEC home page: http://info.isl.ntt.co.jp/psec/

PSEC press release: http://www.ntt.co.jp/news/news99/9905/990524b.html (in Japanese)

□ ESIGN (Efficient digital SIGNature scheme)
ESIGN is one of the digital signature algorithms authorized under the guideline based on "Law Concerning Electronic Signatures and Certification Services" (enforced from April 1, 2001). Compared with previous digital signature algorithms, its processing speed is much faster, and ESIGN can be implemented on smart cards without special coprocessors.
ESIGN home page: http://info.isl.ntt.co.jp/esign/

<< Related Standardization Activities >>
Recent evaluation/standardization activities are described below.

□ ISO (ISO/IEC JTC1 SC27)
ISO/IEC JTC1 SC27 is the special committee for standardization of information security technologies under the International organization for standardization, ISO. Before April 2000, it focused only on authentication schemes including digital signature algorithms. ESIGN was accepted in 1998. ISO is now focusing on encryption algorithms as well as authentication schemes. ISO/IEC JTC1 SC27 is now considering Camellia (proposed in cooperation with Mitsubishi), EPOC, and PSEC.

□ IEEE (IEEE P1363)
The Institute of Electrical and Electronics Engineers, Inc. (IEEE), which is the biggest society related to electronics in the world, has been standardizing public-key encryption and authentication algorithms since 1996. The standard specification is P1363. IEEE has written EPOC and ESIGN into P1363a, which will be published in 2001.

□ CRYPTREC (Cryptography Research and Evaluation Committee, Secretariat: Information technology Promotion Agency (IPA), sponsored by the Ministry of Economy, Trade and Industry (previous name: the Ministry of International Trade and Industry))
CREPTREC was organized for investigating and evaluating cryptographic techniques suitable for the Japanese electronic government in terms of security, implementation, and other characteristics from the viewpoints of various objective specialists. This project is an essential part of the MITI Action Plan for a Secure E-Government - announced by the Ministry of Economy, Trade and Industry (previous name: the Ministry of International Trade and Industry, MITI) in April 2000. NTT has proposed FEAL, Camellia (in cooperation with Mitsubishi), EPOC, PSEC, and ESIGN to CRYPTREC.

□ NESSIE (New European Schemes for Signatures, Integrity, and Encryption)
NESSIE is a three-year project for making a portfolio of strong cryptographic primitives starting in 2000 within the Information Societies Technology (IST) Programme of the European Commission. NTT has proposed Camellia (in cooperation with Mitsubishi), EPOC, PSEC, and ESIGN to NESSIE.

□ IETF (Internet Engineering Task Force)
IETF is a large, open international community concerned with the evolution of the Internet architecture. IETF has been standardizing cryptographic algorithms for Transport Layer Security (TLS). NTT has proposed Camellia (in cooperation with Mitsubishi) to IETF.

<< Glossary >>

***1 Symmetric-key encryption**
An encryption algorithm that uses the same key for both encryption and decryption. Since its encryption speed is fast, it is widely used to quickly encrypt large quantities of data in messages or files, and authenticate mobile terminals. NTT developed the 64-bit block cipher FEAL (Fast data Encipherment ALgorithm, 1987) and the 128-bit block cipher Camellia (in cooperation with Mitsubishi, 2000).

***2 Public-key encryption**
An encryption algorithm that uses different keys in the case of encryption and decryption. It is suitable for secure communication on open networks, since public keys can be open. It is also used as key distribution scheme to share the secret keys used for symmetric-key encryption. NTT developed EPOC in 1998 and PSEC in 1999.

***3 Digital signature**
An authentication scheme in which only a decryption key holder can create signatures in public-key encryption. NTT developed ESIGN in 1991 and the elliptic curve Okamoto-Schnorr signature scheme in 1999.

***4 Block size**
This is the size of the bundle used in block cipher processing. DES, the old-fashioned U.S. standard encryption algorithm, uses a block size of 64 bits. NIST has mandated a block size of 128 bits for the Advanced Encryption Standard to improve security.

***5 AES (Advanced Encryption Standard)**
This is the next U.S. standard encryption algorithm. Five finalists were selected from among the candidates proposed from around the world: MARS (U.S.), RC6 (U.S.), Rijndael (Belgium), Serpent (UK, Israel, Norway), and Twofish (U.S.). Finally, on October 2000, NIST selected Rijndael as the AES winner. NIST is proceeding to establish the FIPS (Federal Information Processing Standards) for the AES.

***6 Hash function**
This is a function that compresses messages of arbitrary lengths to fixed length messages.

***7 Factoring problem, (Elliptic curve) discrete logarithm problem**
These are open problems in the mathematical field. It is believed that, if the order of a

problem (equivalent meaning to "key length" in cryptology) is large, solving the problem is very difficult even if super computers are used.

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

NTT NEWS RELEASE