NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

NEWS RELEASE

November 8, 2006

The Open Source Community OpenSSL Project Adopts the Next Generation International Standard Cipher "Camellia" Developed in Japan

- Free integration and distribution of Camellia as an open source library provides impetus towards global spread -

The OpenSSL Project, an international open source community, adopted "Camellia," a 128-bit block cipher[*1] algorithm jointly developed in 2000 by Nippon Telegraph and Telephone Corporation (hereafter NTT) and Mitsubishi Electric Corporation (hereafter Mitsubishi), into its OpenSSL toolkit for use in the development of SSL/TLS[*2] protocol.

To support a secure advanced information society, and with the goal of disseminating Camellia, which was selected as a major international standard and recommended cipher, NTT released Camellia source codes as open source on April 13, 2006 so that Camellia can be freely used as an international basic technology. NTT has also provided its source codes to open source communities.

As a result, in September of this year Camellia was incorporated into OpenSSL version 0.9.8c.
The adoption of Camellia into the OpenSSL toolkit means that Camellia provides security and performance equivalent to the US government standard cipher AES[*3] and is the world's only alternative to AES. From now on, since the OpenSSL toolkit equipped with Camellia will be installed into WWW servers worldwide and used as a world leading open cryptographic toolkit, we anticipate that Camellia will be spread even further through its use and commercialization on a global scale.

Camellia Website: http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
Information related to open source:
http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html
OpenSSL Project Website: http://www.openssl.org/

[Background and Significance of Adoption into OpenSSL]

Camellia, the next generation encryption algorithm that provides the world's highest security and performance, is an international standard and recommended cipher. Camellia was selected into the first ISO/IEC international standard cipher[*4], EU (NESSIE) recommended cipher[*5], and Japanese e-government recommended cipher[*6], and is internationally recognized as the de facto representative of Japanese encryption algorithm. Furthermore, Camellia was adopted as the IETF standard track RFC[*7] encryption algorithm in mainstream Internet encryption communications protocols such as SSL/TLS, IPsec, S/MIME, and XML.

NTT released free of charge the source codes (C language and Java) as open source and is providing an environment in which any Camellia users can use the Camellia essential patents at no charge without concluding the royalty-free licensing agreement so that more people can benefit from the merits of Camellia, which are highly evaluated worldwide. Furthermore, NTT is providing the Camellia source codes to open source communities and undertaking continuous activities for adoption.

The OpenSSL toolkit has three types of functionality: SSL/TLS de facto stack, encryption engine, and PKI application development toolkit.
Many current standard ciphers, such as Triple DES and RC4, are available in it as engines for symmetric key encryption, but only AES has been supported as the next generation encryption algorithm in OpenSSL version 0.9.7 and later. This time since Camellia will be equipped in OpenSSL version 0.9.8c and later, an environment*note) is available in which multiple ciphers can be used as next generation encryption algorithms, and we believe that this will contribute to the actualization of more secure advanced information society.

Table. Ciphers Equipped in OpenSSL Toolkit

Block ciphers		Stream cipher (current standard)
64-bit block ciphers (current standard)	**128-bit block ciphers (next generation)**	
DES, Triple DES, DESX, Blowfish, RC2, RC5, CAST5(CAST-128), IDEA	**AES, Camellia**	RC4

*note In the current OpenSSL version 0.9.8x, Camellia is not automatically installed with the standard compile option. In the next major revision, Camellia is scheduled to become a part of the standard installation.

Currently, more than 60% of the WWW servers worldwide have the OpenSSL toolkit installed, and in the future Camellia will be sequentially installed into these servers. Since the OpenSSL toolkit is used in various commercial developments and the selection of Camellia can be made easily, we anticipate that the use and commercial development of Camellia will accelerate.

[Significance of Disclosing Specifications and Releasing Camellia as Open Source]
From the beginning, the specification for Camellia was publicly disclosed, and cryptographic researchers worldwide have already evaluated the security and performance of the algorithm a great many times. The evaluation results were published in reports and presented at international cryptographic conferences, etc. These form the technical basis for the reputation of Camellia as one of the world's most excellent encryption algorithm and provide the rationale behind its selection as the internationally standardized and recommended specifications.

In the future, since the open source code of Camellia incorporated in the OpenSSL toolkit will be distributed worldwide, engineers around the world will evaluate, improve, and implement Camellia codes as part of implementation process. We anticipate that it will become easier to use Camellia.
Although, for practical products, vulnerability in the implementation could be a threat to the reliability and security, engineers worldwide will inspect the implementation by disclosing the encryption engine as open source in the same way as the algorithm is disclosed. Therefore we anticipate that the security based on that implementation will

improve as a result.

[Merits and History of Camellia]

Camellia is a 128-bit block cipher (with allowable key lengths of 128, 192, and 256 bits) that was jointly developed by NTT and Mitsubishi in 2000. Camellia not only maintains the world's highest security, but also can be built into high-speed software implementation independent of the platform such as PCs or IC cards and the world's smallest hardware implementation with the highest efficiency among 128-bit block ciphers. That is, Camellia is simultaneously equipped with excellent security and performance.

According to third party evaluations and verifications performed by many cryptographers worldwide over the last few years concerning these features, compared to the current mainstream 64-bit block cipher Triple DES, the security of Camellia is extraordinarily high and the processing speed is four to five times faster. Based on these results, Camellia is internationally recognized as Japan's representative cipher with security and performance equivalent to those of AES, and the world's only 128-bit block cipher alternative to AES.

Camellia, with NTT's fundamental objective of sound development of the advanced information society as a criterion to open source, has followed the sequence of events provided below to arrive at its current state.

March 2000	Camellia encryption algorithm is released by NTT and Mitsubishi
April 2001	Camellia royalty-free licenses are granted
February 2003	Camellia is selected as the Japanese e-government recommended cipher by CRYPTREC
February 2003	Camellia is selected as the European Union recommended cipher by NESSIE
February 2003	Camellia is adopted as the DRM encryption by TV-Anytime Forum
January 2004	Camellia is accepted as the IETF standard cipher for S/MIME [RFC3657]
April 2005	Camellia is accepted as the IETF standard cipher for XML security URIs [RFC4051]
May 2005	Camellia is adopted as the ISO/IEC standard cipher [ISO/IEC18033-3]
July 2005	Camellia is accepted as the IETF standard cipher for SSL/TLS Cipher suites [RFC4132]
December 2005	Camellia is accepted as the IETF standard cipher for IPsec [RFC4312]
April 2006	Open source codes of Camellia are released
September 2006	Camellia is adopted into OpenSSL (adopted from OpenSSL version 0.9.8c)

[Future Plan]

In order to widen further the use of Camellia, NTT did not stop working with the adoption of Camellia into the OpenSSL toolkit. It is continuing with activities toward the adoption into other open source communities such as Linux and FreeBSD. Furthermore, in addition to NTT's positively influencing development of products and services equipped with Camellia, we plan to cooperate with hopeful corporations and enterprises for their development, industrialization, and introduction of Camellia-equipped products.

[Glossary]

*1 128-bit block cipher

The 128-bit block cipher is a symmetric key encryption that encrypts data in 128-bit long (the size of the data bundle) blocks. Symmetric key encryption is an encryption scheme that uses the same secret key to encrypt and decrypt data. Since it achieves high-speed processing, it is used widely in various applications such as communication sessions that deal with large-volume data, file encryption, and mobile terminal authentication.

64-bit block ciphers (64-bit long blocks) such as Triple DES and MISTY1 were constructed by the mid 1990's. And 128-bit block ciphers such as Camellia and AES were produced in and after the second half of the 1990's.

*2 SSL/TLS (Secure Socket Layer /Transport Layer Security)

The Netscape Communications Corporation developed the SSL protocol, which provides a secure communications mechanism by encrypting transmitted data for Internet communications. The next version of SSL3.0 was renamed as TLS and was standardized by the IETF.

Since SSL/TLS is normally equipped in current browsers such as IE and Firefox, when accessing sites such as EC sites and services such as internet banking, it is common that SSL/TLS is used when transmitting passwords, credit card numbers, and personal information. Recently, in many sites where encrypted communications is required, SSL/TLS is automatically used without the user's awakening.

*3 AES (Advanced Encryption Standard)

In 2001, the National Institute of Standards and Technology (NIST) established the US Government standard 128-bit block cipher called the Advanced Encryption Standard. The AES project ran from 1997 to 2000, and AES was based on the "Rijndael" algorithm, proposed by J. Daemen and V. Rijmen, whose security and performance were considered to be the highest among the proposed algorithms.

*4 ISO/IEC international standard ciphers

These are the first international standard cipher algorithms selected by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). After changing the focus from ISO/IEC9979 (encryption algorithm registration system), ISO/IEC18033 was standardized as the first international standard cipher, based on third party (NESSIE, CRYPTREC, etc.) security and performance evaluation reports. The 128-bit block ciphers, AES, Camellia, and SEED, are the only ciphers adopted as the next generation standard.

*5 EU recommended ciphers

These are recommended encryption primitives selected based on high-level security and performance by the New European Schemes for Signature, Integrity, and Encryption (NESSIE) project conducted from 2000 to 2003 by the European Union (EU). Out of the total 44, including the 39 proposed encryption algorithms, 17 encryption algorithms were selected. The Japanese ciphers Camellia (128-bit block cipher by NTT/Mitsubishi), MISTY1 (64-bit block cipher by Mitsubishi), and PSEC-KEM (Public key encryption by NTT) were selected.

*6 Japanese e-government recommended ciphers

These are recommended cryptographic techniques suitable for the Japanese electronic government selected by the Cryptography Research and Evaluation Committees

(CRYPTREC) organized to investigate and evaluate them from the viewpoints of various objective specialists in terms of security. Out of the total 66, including the 52 proposed encryption techniques, 31 encryption techniques were selected.

*7 Standard Track RFC (Standard Track Requests For Comments)
This is an official draft document opened to the public as a specification for an Internet Standard.
The RFC number is given to all documents that the IETF issues. They are classified into Standard Track RFC for which the IETF holds a standard discussion, approves, and manages as Internet standards, and Non-standard Track RFC which is opened to the public with the aim of dissemination.

[Contact information]
Chizuka, Sano, Nakamura
Public Relations Section
Planning Department
NTT Information Sharing Laboratory Group
Nippon Telegraph and Telephone Corporation
Phone: 0422-59-3663
E-mail: islg-pr@lab.ntt.co.jp