NEWS RELEASE

NTT

November 13, 2007

Major Open Source Software Communities Have Successively Adopted Next Generation International Standard Cipher "Camellia" Developed in Japan

- Use of Camellia by Major Vendor Products Has Also Rapidly Progressed -

An international standard 128-bit block cipher[*1] "Camellia," jointly developed in 2000 by Nippon Telegraph and Telephone Corporation (hereafter NTT) and Mitsubishi Electric Corporation (hereafter Mitsubishi), has been successively adopted into many major international open source software such as Linux and Firefox, following the adoption of OpenSSL in last year. Herewith, Camellia can be practically applied in various environments, and has gained international trust in name and reality as a next generation cipher in international infrastructure technology to support secure advanced information society.
Furthermore, by the commercialization and development of Camellia equipped products by major enterprises such as the QuickSec toolkit by Nihon SafeNet K.K., the use of Camellia in security products and services has rapidly progressed.

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

Background and Significance of Promoting Camellia

Based on the fundamental plans on disseminating Camellia, selected to major international standards and recommendations, as an international infrastructure technology to support secure advanced information society, NTT released Camellia source codes as open source software on April 13, 2006 in order to provide an environment in which Camellia can be freely used. Also, NTT has contributed to major open source software communities by providing extension patches for Camellia source code.
Fortunately, following the adoption of OpenSSL 0.9.8c encryption toolkit released in September 2006, Camellia has been widely adopted into many major international open source software; e.g., OS kernels such as Linux and FreeBSD, and Web browsers such as Firefox (next version) (see Table 1). This is not only the first brilliant achievement in Japan, but also is evidence that Camellia has gained international trust in name and reality as a next generation cipher.
According to Mozilla, the addition of new encryption technologies to Firefox, a widely used web browser, is rather special. This is because ciphers that have been reviewed, deployed, and attacked repeatedly (and survived!) are best. Actually, Camellia is the only symmetric cipher added to Firefox for the last 5 years, that is, after the adoption of the US Government standard cipher AES[*2] in 2002. In the next version of Firefox or its development version (Gran Paradiso alpha 7 or later), it can be confirmed that

Web encrypted communication (SSL/TLS communication[*3]) is actually established using Camellia by accessing Camellia supported Web server (such as the address below) (see Figure).

Camellia Website for https: https://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
Notes: After connecting, right click and select "View Page Info."

Figure SSL/TLS encrypted communications established using Camellia

The situation that the use of Camellia is now expected to disseminate especially in the Japanese market promotes rapidly the commercialization and development of Camellia equipped products by major enterprises other than the NTT and Mitsubishi groups; e.g., the QuickSec toolkit (Nihon SafeNet K.K.), the Netcocoon Analyzer (Matsushita Electric Works, Ltd.), SH7781 group (Renesas Technology Corp.), and netHSM/nShield (nCipher Corporation Ltd.). Furthermore, the adoption of Camellia in information systems of major corporations such as mixi, Inc. also progresses (For details, please view the press releases or website from each company, or the product information on the Camellia home page).

In this way, since Camellia can be practically applied in various environments, products and services employing encryption can select from two of next generation encryption algorithms, AES and Camellia. That is, Camellia is greatly expected to contribute significantly toward more secure advanced information society, not dependent on only one encryption technology.

TABLE 1. Camellia Equipped Products Offered by Open Source Software Communities

Open Source Software	Version Equipped	Notes
OpenSSL toolkit	0.9.8c or later	Encryption toolkit
Crypto++ library	5.4 or later	Encryption toolkit
NSS (Network Security Services)	3.12 or later (planned)	Encryption toolkit
The Legion of the Bouncy Castle	1.30 or later	Java encryption toolkit
libgcrypt (GnuPG)	2 or later	GNU encryption toolkit
Linux kernel	2.6.21 or later	OS kernel
Fedora	7 or later	OS kernel (Linux distribution)
FreeBSD	7.0 or later (6.x prepared)	OS kernel
Firefox	3.0 (planned)*	Web browser
IPsec-tools	0.7 or later	IPsec supported application

* Firefox 3.0 is scheduled for release in late 2007. Currently, Camellia can be used in the development version of Firefox 3.0 (Gran Paradiso alpha 7 or later).

Features 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.

Since the specification of Camellia is public, many third party evaluations and verifications concerning these features have been performed by many worldwide first-class cryptographers. According to the results published in official reports, papers, and cryptographic conferences, Camellia has received high reputations for a world top-class encryption algorithm featuring technically security and performance equivalent to AES.

Actually, this is why Camellia is internationally recognized not only as Japan's representative cipher but also as the world's only 128-bit block cipher alternative to AES, and adopted to many international standards and recommendations (see Table 2).

TABLE 2. Standards and Recommendations for Camellia

Standardization Body	Standardization Summary
ISO/IEC	ISO/IEC international standard cipher (ISO/IEC18033-3)
NESSIE	European Union recommended cipher
CRYPTREC	E-government recommended cipher in Japan
IETF	SSL/TLS standard cipher (RFC4132)
	IPsec standard cipher (RFC4312)
	S/MIME standard cipher (RFC3657)
	XML standard cipher (RFC4051)
	OpenPGP cipher (in deliberation)
	Description of Camellia (RFC3713)
RSA Laboratories	Encryption token standard interface (RSA PKCS#11)
ITU-T	Cipher for next generation network (NGN) (in deliberation)
TV-Anytime Forum/ ETSI	Copyright protection and information protection (DRM) for broadcast contents in the next generation information sharing system

Future Plans

In addition to continued appeal activities regarding the adoption and use of Camellia to open source software communities and software engineers, NTT promotes the research and development of application services incorporating Camellia equipped open source software and products, and extensively contributes to the construction of secure advanced information society.

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 1990s, and 128-bit block ciphers such as Camellia and AES were produced in and after the second half of the 1990s.

*2 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.

*3 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 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 being aware.

- Figure SSL/TLS encrypted communications established using Camellia

For more information, contact:
NTT Information Sharing Laboratory Group
Planning Dept. Public Relations Contact Person
Chizuka, and Yamagata
E-mail: islg-pr@lab.ntt.co.jp