# Japan's First 128-bit Block Cipher 'Camellia' Approved as a New Standard Encryption Algorithm in the Internet

July 20 2005

Nippon Telegraph and Telephone Corporation (NTT) and Mitsubishi Electric Corporation (Mitsubishi) jointly developed in 2000 the 128-bit block cipher algorithm "Camellia." On this occasion, as the first Japanese encryption algorithm, Camellia was adopted as a new standard encryption algorithm (Standard Track RFC) in three major Internet secure protocols, SSL/TLS, S/MIME, and XML. Furthermore, the deliberations by the IETF have approved addition of Camellia into IPsec protocol, and Camellia will be adopted this fall.

As an encryption scheme with the world's highest level of excellent security and performance, Camellia was adopted as International standardization specification and recommended specification, the EU recommended cipher, E-government recommended cipher, ISO/IEC international standard cipher, etc., and it was acknowledged as the standard that should be implemented in the Internet for the next generation encryption scheme.

## Background and Significance of Standardization

Camellia is internationally recognized as the representative of Japanese ciphers and as the unique 128-bit block cipher that possesses the security level and processing capability equivalent to AES. Indeed, Camellia was selected as the EU recommended cipher and E-government recommended cipher in 2003 and was also adopted as the ISO/IEC

international standard cipher recently.

Still, when using Web services such as online shopping and Internet banking, people generally take advantage of the SSL/TLS with which web browsers used on the Internet are standard-equipped. This also applies to the Web services in the E-government system.

The ciphers that are standard-equipped with the Web browsers are limited to those adopted by IETF as the SSL/TLS standard. This means that if Camellia were not adopted by the SSL/TLS standard, Camellia would not be able to be used with the Web services even in the E-government system, despite the fact that Camellia was already selected as the E-government recommended cipher.
In short, only in technical superiority of the algorithm and the adoption as de jure standard etc., it was insufficient as the environment that can be widely used for products and services.

In regard with the major encrypted communication protocols such as SSL/TLS and S/MIME, IETF adopted as standard Internet ciphers Triple DES, IDEA, RC2 and RC4 which were created prior to 1995 and hence available at the time of standardizing the protocols. Among these, Triple DES and RC4 are still currently used as standards. However, along with the recent progress in cipher research, anxiety has arisen regarding the security of these standard ciphers. To address this, the IETF has conducted additional investigations on the next generation encryption schemes, especially the 128-bit block ciphers that are recommended internationally as next generation ciphers and are secure than 64-bit block cipher Triple DES and RC4 to which weakness is pointed out.

Camellia was evaluated to have the world's highest level of excellent security and performance. It was also adopted into various standard/recommended specifications. As a result, Camellia was approved for adoption as a next generation Internet standard encryption

specification for SSL/TLS and represents the first Japanese cipher algorithm to achieve this status. The IETF has also adopted or slated for adoption Camellia as IPsec, S/MIME, XML.

In regard to this, up until now aside from Camellia's adoption as the EU recommended cipher and E-government recommended cipher, in May of this year it was adopted as the ISO/IEC next generation international standard cipher. In light of this, Camellia should also be implemented as an Internet standard next generation encryption scheme. Accordingly, in the future, based on various systems such as the E-government system, Internet banking, and online shopping that use very convenient Internet communication methods, the Japanese encryption algorithm can be used for the first time as an Internet standard cipher.

The IETF has adopted or slated for adoption of only Camellia, AES, and SEED, as the next generation Internet standard ciphers. These are corresponding to 128 bit block ciphers adopted for the ISO/IEC international standard cipher as the next generation standard.

## Future Expansion

This time, in addition to adoption by the three main encryption evaluation/standardization projects supported by Japan (E-government cipher recommendation), the EU (EU cipher recommendation), and internationally (ISO/IEC international standard cipher), through the adoption of Camellia, we anticipate that Japanese encryption technology will be further broadly utilized as an international specification.

In order for Camellia to be more widely used, NTT continues on installing it into security products employing SSL/TLS. In addition to actively promoting the development of Camellia-equipped product and services, in order to contribute to achieving a truly secure information society, NTT will continue to actively pursue research and development

in the future.

From the viewpoint of the early proliferation of Camellia as a world de facto standard, we will enrich the Camellia-equipped product line, and encourage other companies interested in Camellia to expand Camellia-equipped products through the royalty-free licensing of the essential patents.

RFC Numbers of Camellia
- RFC 3657 [Standard Track - Proposed Standard]:
Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)
- RFC 3713 [Non-standard Track - Informational]:
A Description of the Camellia Encryption Algorithm
- RFC 4051 [Standard Track - Proposed Standard]:
Additional XML Security Uniform Resource Identifiers (URIs)
- RFC 4132 [Standard Track - Proposed Standard]:
Addition of Camellia Cipher Suites to Transport Layer Security (TLS)
- RFC Ed Queue [Standard Track - Proposed Standard]:
The Camellia Cipher Algorithm and Its Use With IPsec

## Features of Camellia

Camellia is a 128-bit block cipher (key lengths of 128, 192, and 256 bits) with the world's highest level of excellent security and performance. High-speed software implementation independent of the platform such as PC or IC cards, and the world's smallest hardware implementation that provides the highest level of processing efficiency can be achieved. In particular, Camellia differs from AES in terms of implementation. Since encryption processing and decryption processing are achieved using the same structure in Camellia, it exhibits superior performance particularly in IC cards that have a low capacity memory or compact hardware.

Furthermore, over several years, cryptographers around the world have conducted thorough evaluation of Camellia. The security of Camellia is very high, and the processing speed is several times or more as high-speed as that of 64 bit block cipher of the main current now, Triple DES etc.

Camellia is the only world's 128-bit block cipher which has the equivalent security and processing efficiency as AES. As Japan's representative, this cipher has gained international recognition. Actually, because Camellia has a different cipher structure compared to AES and since a sufficiently large security margin is adopted, from a security viewpoint, AES and Camellia are selected for many standardization/recommended specifications.

In order to fulfill a leadership role in establishing a secure high-level information society at a low cost through the spread and promotion of Camellia, the offering of non-exclusively royalty-free licenses of the essential patents for Camellia under reciprocal principles has been put into practice since 2001 to mainly enterprises and corporations that are willing to develop and commercialize products equipped with Camellia based on the disclosed specifications.

Camellia Homepage: info.isl.ntt.co.jp/crypt/camellia/index.html