INTERNET-DRAFT
TLS Working Group
Expires February 6 2003

S. Moriai
Nippon Telegraph and Telephone Corporation

August 6 2002

Addition of Camellia Ciphersuites to Transport Layer Security (TLS)

<draft-ietf-tls-camellia-02.txt>

Status of this Memo

Abstract

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) protocol to support the Camellia encryption algorithm as a bulk cipher algorithm.

1. Introduction

This document proposes the addition of new cipher suites to the TLS protocol [TLS] to support the Camellia encryption algorithm as a bulk cipher algorithm. This proposal provides a new option for fast, efficient, and royalty-free bulk cipher algorithms.

Camellia is a 128-bit block cipher with 128-, 192-, and 256-bit key sizes, i.e. it supports the same block and key sizes as the Advanced Encryption Standard (AES). A description of the Camellia cipher algorithm is in [CamelliaSpec][CamelliaTech].

Efficiency on both software and hardware platforms is a remarkable characteristic of Camellia. In particular, Camellia's small hardware design is suitable for mobile, portable and low power applications. Furthermore, Camellia has withstood extensive cryptanalytic efforts in several open, worldwide cryptographic evaluation projects.

2. Proposed Cipher Suites

The new ciphersuites proposed here have the following definitions:

```
CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA      = { 0x00,0x41 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x42 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x43 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x44 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x45 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x46 };

CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA      = { 0x00,0x47 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x48 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x49 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4A };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4B };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4C };
```

Note: The above numeric definitions for Cipher Suites have not yet been registered.

3. CipherSuite Definitions

3.1 Cipher

All the ciphersuites described here use Camellia in cipher block chaining (CBC) mode as a bulk cipher algorithm. Camellia is a 128-bit block cipher with 128-, 192-, and 256-bit key sizes, i.e. it supports the same block and key sizes as the Advanced Encryption Standard (AES). However, this document only defines ciphersuites for 128- and 256-bit keys as well as AES ciphersuites for TLS [AES]. They are enough for use in efficient and practical cases as well as high-security applications.

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
CAMELLIA_128_CBC	Block	16	16	128	16	16
CAMELLIA_256_CBC	Block	32	32	256	16	16

3.2 Hash

All the ciphersuites described here use SHA-1 in an HMAC construction as described in section 5 of [TLS], a modified SHA-1

version of the algorithm.

3.3 Key exchange

The ciphersuites defined here differ in the type of certificate and key exchange method. They use the following options:

CipherSuite	Key Exchange Algorithm
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	DH_anon
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	DH_anon

For the meanings of the terms RSA, DH_DSS, DH_RSA, DHE_DSS, DHE_RSA and DH_anon, please refer to sections 7.4.2 and 7.4.3 of [TLS].

4. Security Considerations

It is not believed that the new ciphersuites are ever less secure than the corresponding older ones. Camellia is believed to be secure, and it has withstood extensive cryptanalytic efforts in several open, worldwide cryptographic evaluation projects.

For other security considerations, please refer to the security considerations of the corresponding older ciphersuites described in [TLS] and [AES].

5. Intellectual Property

Mitsubishi Electric Corporation (Mitsubishi Electric) and Nippon Telegraph and Telephone Corporation (NTT) have pending applications or filed patents which are essential to Camellia. License policy for these essential patents declared formally by NTT and Mitsubishi Electric is available on the IETF page of Intellectual Property Rights Notices.

References

[CamelliaSpec] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Specification of Camellia - a 128-bit Block Cipher''. http://info.isl.ntt.co.jp/camellia/

[CamelliaTech] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis -'', In Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, August 2000, Proceedings, Lecture Notes in Computer Science 2012, pp.39--56, Springer-Verlag, 2001.

[AES] P. Chown, ``Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)'', RFC 3268, June 2002.

[TLS] T. Dierks, and C. Allen, ``The TLS Protocol Version 1.0'', RFC 2246, January 1999.

Author's Address

Shiho Moriai
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka, 239-0847, Japan
Phone: +81-468-59-2007
FAX: +81-468-59-3858
Email: shiho@isl.ntt.co.jp