Camellia Cipher Suites for TLS
draft-kato-tls-rfc4132bis-05

Abstract

This document specifies a set of cipher suites for the Transport Security Layer (TLS) protocol to support the Camellia encryption algorithm as a block cipher. It amends the cipher suites originally specified in RFC 4132 by counterparts using the newer cryptographic hash algorithms from the SHA-2 family. This document obsoletes RFC 4132.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 24, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) [RFC5246] protocol to support the Camellia [RFC3713] encryption algorithm as a block cipher algorithm, adding variants using the SHA-2 family of cryptographic hash algorithms [FIPS180-3] to the TLS cipher suite portfolio originally specified in RFC 4132 [RFC4132]. This document obsoletes RFC 4132.

The Camellia algorithm and its properties are described in [RFC3713].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Proposed Cipher Suites

The cipher suites defined here have the following identifiers:
### Cipher Suite Definitions

#### 3.1. Key Exchange

The RSA, DHE_RSA, DH_RSA, DHE_DSS, DH_DSS, and DH_anon key exchanges are performed as defined in [RFC5246].

#### 3.2. Cipher

The CAMELLIA_128_CBC cipher suites use Camellia [RFC3713] in CBC mode with a 128-bit key and 128-bit IV; the CAMELLIA_256_CBC cipher suites use a 256-bit key and 128-bit IV.

#### 3.3. Hash and Pseudorandom Function

##### 3.3.1. Hash and Pseudorandom Function for TLS 1.1

The cipher suites ending with _SHA use HMAC-SHA1 as the MAC algorithm.
When used with TLS versions prior to 1.2, the PRF is calculated as specified in the appropriate version of the TLS specification.

### 3.3.2. Hash and Pseudorandom Function for TLS 1.2

The cipher suites ending with _SHA256 use HMAC-SHA-256 as the MAC algorithm. The PRF is the TLS PRF [RFC5246] with SHA-256 as the hash function. These cipher suites MUST NOT be negotiated by TLS 1.1 or earlier versions. Clients MUST NOT offer these cipher suites if they do not offer TLS 1.2 or later. Servers which select an earlier version of TLS MUST NOT select one of these cipher suites.

### 4. IANA Considerations

IANA has already allocated the following numbers for RFC 4132, and is requested to update them to reference this document:

- **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** = { 0x00,0x84 }
- **CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA** = { 0x00,0x85 }
- **CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA** = { 0x00,0x86 }
- **CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA** = { 0x00,0x87 }
- **CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA** = { 0x00,0x88 }
- **CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA** = { 0x00,0x89 }

IANA is requested to allocate (has allocated) the following numbers in the TLS Cipher Suite Registry:

- **CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256** = { TBD,TBD }

- **CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
- **CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256** = { TBD,TBD }
5. Security Considerations

At the time of writing this document there are no known weak keys for Camellia. And no security problem has been found on Camellia (see [NESSIE], [CRYPTREC], and [LNCS]).

Also, Security issues are discussed throughout RFC 5246 [RFC5246], especially in Appendices D, E, and F of [RFC5246].

6. References

6.1. Normative References


6.2. Informative References


[NESSIE] "The NESSIE project (New European Schemes for Signatures,
Integrity and Encryption",


Authors’ Addresses

Akihiro Kato
NTT Software Corporation
Phone: +81-45-212-9803
Fax: +81-45-212-9800
Email: kato.akihiro@po.ntts.co.jp

Masayuki Kanda
NTT
Phone: +81-422-59-3456
Fax: +81-422-59-4015
Email: kanda.masayuki@lab.ntt.co.jp

Satoru Kanno
NTT Software Corporation
Phone: +81-45-212-9803
Fax: +81-45-212-9800
Email: kanno.satoru@po.ntts.co.jp