Network Working Group	S. Kanno
Internet-Draft	NTT Software Corporation
Intended status: Informational	M. Kanda
Expires: July 31, 2010	NTT
	January 27, 2010

Addition of Camellia Elliptic Curve Cipher Suites with SHA-1 and SHA-2
draft-kanno-tls-camellia-ecc-sha-01

Abstract

This document specifies a set of elliptic curve cipher suites for the Transport Security Layer (TLS) protocol to support the Camellia encryption algorithm as a block cipher. This document describes sixteen new cipher suites for TLS that specify HMAC-SHA1 and HMAC-SHA2.

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 July 31, 2010.

described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

---

1. Introduction

This document specifies a set of elliptic curve cipher suites for the Transport Security Layer (TLS) protocol to support the Camellia encryption algorithm as a block cipher. This document describes sixteen new cipher suites for TLS that specify HMAC-SHA1 and HMAC-SHA2.
The Camellia algorithm and its properties are described in [RFC3713] (Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” April 2004.).

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Cipher Suites

This document defines sixteen new cipher suites to be added to TLS. All use Elliptic Curve Cryptography for key exchange and digital signature, as defined in [RFC4492] (Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS),” May 2006.).
The sixteen cipher suites use Camellia [RFC3713] (Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” April 2004.) in Cipher Block Chaining (CBC) mode with HMAC-based MAC.
The cipher suites defined here have the following identifiers:

```
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA    = {TBD,TBD}
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA    = {TBD,TBD}
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA   = {TBD,TBD}
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA   = {TBD,TBD}
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA      = {TBD,TBD}
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA      = {TBD,TBD}
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA     = {TBD,TBD}
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA     = {TBD,TBD}

CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256  = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256   = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256     = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384     = {TBD,TBD};
```

---

3. IANA Considerations

IANA is requested to allocate the following numbers in the TLS Cipher Suite Registry:

```
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA    = {TBD,TBD}
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA    = {TBD,TBD}
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA   = {TBD,TBD}
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA   = {TBD,TBD}
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA      = {TBD,TBD}
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA      = {TBD,TBD}
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA     = {TBD,TBD}
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA     = {TBD,TBD}

CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256  = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256   = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256     = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384     = {TBD,TBD};
```

---

4. Security Considerations

At the time of writing of this document there are no known weak keys for Camellia and no security problems have been found with Camellia (see [NESSIE] (, "The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)," .), [CRYPTREC] (Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees," .), and [Research] (Mala, H., Shakiba, M., and M. Dakhil-alian, "New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128," November 2009.)).
The security considerations in RFC 5289 [RFC5289] (Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)," August 2008.) apply to this document as well.

---

5. References

5.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3713]	Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm," RFC 3713, April 2004 (TXT).
[RFC4492]	Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)," RFC 4492, May 2006 (TXT).
[RFC5289]	Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)," RFC 5289, August 2008 (TXT).

5.2. Informative

[CRYPTREC]	Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees" (HTML).
[NESSIE]	"The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)."
[Research]	Mala, H., Shakiba, M., and M. Dakhil-alian, "New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128," November 2009.

Authors' Addresses

	Satoru Kanno
	NTT Software Corporation
Phone:	+81-45-212-9803
Fax:	+81-45-212-9800
Email:	kanno.satoru@po.ntts.co.jp
	Masayuki Kanda
	NTT
Phone:	+81-422-59-3456
Fax:	+81-422-59-4015
Email:	kanda.masayuki@lab.ntt.co.jp