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.

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 algorithm specification and object identifiers 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. 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].

The sixteen cipher suites use Camellia [RFC3713] in Cipher Block Chaining (CBC) mode with HMAC-based MAC.

The cipher suites defined here have the following identifiers:
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 this document, there are no known weak keys for Camellia.
The security considerations in RFC 5289 [RFC5289] apply to this document as well.

5. Normative References


Authors’ Addresses

Satoru Kanno
NTT Software Corporation

Phone: +81-45-212-7577
Fax: +81-45-212-9800
Email: kanno-s@po.ntts.co.jp

Masayuki Kanda
Nippon Telegraph and Telephone Corporation

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