INTERNET-DRAFT
TLS Working Group
Expires September 2001

H. Ohta
H. Tsuji
Mitsubishi Electric Corporation
March 2001

Addition of MISTY1 to TLS

<draft-ietf-tls-misty1-01.txt>

Status of this Memo

Abstract

This document proposes the addition of new cipher suites to the TLS protocol version 1.0 to support the MISTY1 encryption algorithm as a bulk cipher algorithm. Major change from the previous version is the addition of intellectual property section.

1. Introduction

This document proposes the addition of new cipher suites to the TLS protocol version 1.0[2] to support MISTY1 encryption algorithm[1] as a bulk cipher algorithm. MISTY1 is a block cipher with a 128-bit key and a 64-bit block. It is designed on the basis of the theory of provable security against differential and linear cryptanalysis, and moreover it realizes high-speed encryption on hardware platforms as well as on software environments.

This document defines the additional cipher specification to the TLS protocol version 1.0.

2. The Cipher Suites

The following values define the CipherSuite codes for the cipher suites that use the MISTY1 CBC mode as a bulk cipher algorithm.

```
CipherSuite TLS_RSA_WITH_MISTY1_CBC_SHA           = { 0x00,0x3B };
CipherSuite TLS_DH_DSS_WITH_MISTY1_CBC_SHA        = { 0x00,0x3C };
CipherSuite TLS_DH_RSA_WITH_MISTY1_CBC_SHA        = { 0x00,0x3D };
CipherSuite TLS_DHE_DSS_WITH_MISTY1_CBC_SHA       = { 0x00,0x3E };
CipherSuite TLS_DHE_RSA_WITH_MISTY1_CBC_SHA       = { 0x00,0x3F };
CipherSuite TLS_DH_anon_WITH_MISTY1_CBC_SHA       = { 0x00,0x40 };
```

Note: Above CipherSuite numbers are tentative, they should be assigned by the authority.

3. CipherSuite Definitions

CipherSuite	Is Exportable	Key Exchange	Cipher	Hash
TLS_RSA_WITH_MISTY1_CBC_SHA		RSA	MISTY1_CBC	SHA
TLS_DH_DSS_WITH_MISTY1_CBC_SHA		DH_DSS	MISTY1_CBC	SHA
TLS_DH_RSA_WITH_MISTY1_CBC_SHA		DH_RSA	MISTY1_CBC	SHA
TLS_DHE_DSS_WITH_MISTY1_CBC_SHA		DHE_DSS	MISTY1_CBC	SHA
TLS_DHE_RSA_WITH_MISTY1_CBC_SHA		DHE_RSA	MISTY1_CBC	SHA
TLS_DH_anon_WITH_MISTY1_CBC_SHA		DH_anon	MISTY1_CBC	SHA

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
MISTY1_CBC	Block	16	16	128	8	8

Note: Key Exchange Algorithms and Hash Functions are defined in TLS.

4. Security Considerations

MISTY1 cipher suites are subject to the same security consideration as TLS. In addition, MISTY1 is designed in consideratin of the theory of provable security against differential and liner cryptanalysis.

5. Intellectual Property

MISTY1[1] algorithm is applied for a patent. However, the patent holder (Mitsubishi Electric Corporation) is prepared to grant, on the

basis of reciprocity and non-discriminatory, a royalty-free license in accordance with Section 10 of RFC 2026. For more information, please contact to "misty@isl.melco.co.jp". A detail license policy will be submitted soon.

6. References

[1] H. Ohta and M. Matsui, "A Description of the MISTY1 Encryption Algorithm", RFC 2994, November 2000

[2] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999

7. Author's Addresses

Hidenori Ohta
Mitsubishi Electric Corporation, Information Technology R&D Center
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
Phone: +81-467-41-2183
FAX: +81-467-41-2185
EMail: hidenori@iss.isl.melco.co.jp

Hirosato Tsuji
Mitsubishi Electric Corporation, Information Technology R&D Center
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
Phone: +81-467-41-2183
FAX: +81-467-41-2185
EMail: hirosato@iss.isl.melco.co.jp