| | | |
|---|---|---|
| Network Working Group | S. Kanno | |
| Internet-Draft | NTT Software Corporation | |
| Intended status: Standards Track | M. Kanda | |
| Expires: September 27, 2010 | NTT | |
| | March 26, 2010 | |

**The Camellia Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP)**
**draft-avt-kanno-srtp-camellia-02**


**Abstract**

This document describes the use of the Camellia block cipher algorithm in the Secure Real-time Transport Protocol (SRTP) for providing confidentiality for the Real-time Transport Protocol (RTP) traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).


**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 27, 2010.

must include Simplified BSD License text as 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 describes the use of the Camellia [RFC3713] (Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm," April 2004.) block cipher algorithm in the Secure Real-time Transport Protocol (SRTP) [RFC3711] (Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," March 2004.) for providing confidentiality for the Real-time Transport Protocol (RTP) [RFC3550] (Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.) traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP) [RFC3550] (Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.).

---

### 1.1. Camellia

Camellia is a symmetric cipher with a Feistel structure. Camellia was developed jointly by NTT and Mitsubishi Electric Corporation in 2000. It was designed to withstand all known cryptanalytic attacks, and it has been scrutinized by worldwide cryptographic experts. Camellia is suitable for implementation in software and hardware, offering encryption speed in software and hardware implementations that is comparable to Advanced Encryption Standard (AES) [FIPS.197.2001] (National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," November 2001.).
Camellia supports 128-bit block size and 128-, 192-, and 256-bit key lengths, i.e., the same interface specifications as the AES. Therefore, it is easy to implement Camellia based algorithms by replacing the AES block of AES based algorithms with a Camellia block.
Camellia already has been adopted by the IETF and other international standardization organizations; in particular, the IETF has published specifications for the use of Camellia with IPsec [RFC4312] (Kato, A., Moriai, S., and M. Kanda, "The Camellia Cipher Algorithm and Its Use With IPsec," December 2005.), TLS [RFC4132] (Moriai, S., Kato, A., and M. Kanda, "Addition of Camellia Cipher Suites to Transport Layer Security (TLS)," July 2005.), S/MIME [RFC3657] (Moriai, S. and A. Kato, "Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)," January 2004.) and XML Security [RFC4051] (Eastlake, D., "Additional XML Security Uniform Resource Identifiers (URIs)," April 2005.). Camellia is one of the three ISO/IEC international standard [ISO/IEC 18033-3] (International Organization for

Standardization, “Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers,” July 2005.) 128-bit block ciphers (Camellia, AES, and SEED). Camellia was selected as a recommended cryptographic primitive by the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [NESSIE] (, “The NESSIE project (New European Schemes for Signatures, Integrity and Encryption),” .) and was included in the list of cryptographic techniques for Japanese e-Government systems that was selected by the Japanese CRYPTREC (Cryptography Research and Evaluation Committees) [CRYPTREC] (Information-technology Promotion Agency (IPA), “Cryptography Research and Evaluation Committees,” .).
Since optimized source code is provided under several open source licenses [open source license] (, “Camellia open source software,” .), Camellia is also adopted by several open source projects (OpenSSL, GnuTLS, FreeBSD, and Linux). Camellia is also adopted by Mozilla and Camellia is ready for use with Firefox 3.0 released in June 2008.
The algorithm specification and object identifiers are described in [RFC3713] (Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” April 2004.).
The Camellia web site [Camellia web site] (, “Camellia web site,” .) contains a wealth of information about Camellia, including detailed specification, security analysis, performance figures, reference implementation, optimized implementation, test vectors(TV), and intellectual property information.

---

### 1.2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" that appear 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. Camellia Algorithm Suites for SRTP

All symmetric block cipher algorithms share common characteristics and valuables, including mode, key size, weak keys, and block size. Camellia algorithm is specified as well as AES, those relations are following:

- Camellia-CTR complies with [RFC3711]

---

## 3. Default and mandatory-to-implement Transforms

The default transforms also are mandatory-to-implement transforms in SRTP. Of course, "mandatory-to-implement" does not imply "mandatory- to-use". Table 1 summarizes the pre-defined transforms. The default values below are valid for the pre-defined transforms.

| | man.-to-impl. | default |
|---|---|---|
| encryption | Camellia-CTR | Camellia-CTR |
| message integrity | HMAC-SHA1 | HMAC-SHA1 |
| key derivation (PRF) | Camellia-CTR | Camellia-CTR |

Table 1: Mandatory-to-implement and default transforms in SRTP and SRTCP.

---

## 4. 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] (, “The NESSIE project (New European Schemes for Signatures, Integrity and Encryption),” .), [CRYPTREC] (Information-technology Promotion Agency (IPA), “Cryptography Research and Evaluation Committees,” .), and [LNCS] (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 [RFC3711] (Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” March 2004.) apply to this document as well.

---

## 5. IANA Considerations

RFC 4568 [RFC4568] (Andreasen, F., Baugher, M., and D. Wing, “Session Description Protocol (SDP) Security Descriptions for Media Streams,” July 2006.) defines SRTP "crypto suites"; In order to allow SDP to signal the use of the algorithms defined in this document, IANA will register the following crypto suites into the subregistry for SRTP crypto suites under the SRTP transport of the SDP Security Descriptions:

```
srtp-crypto-suite-ext = "CAMELLIA_CTR_128_HMAC_SHA1_80" /
                        "CAMELLIA_CTR_128_HMAC_SHA1_32" /
                        srtp-crypto-suite-ext
```

---

## 6. Test Vectors

---

### 6.1. Camellia-CTR Test Vectors

```
Keystream segment length: 1044512 octets (65282 Camellia blocks)
Session Key:      2B7E151628AED2A6ABF7158809CF4F3C
Rollover Counter: 00000000
Sequence Number:  0000
SSRC:             00000000
Session Salt:     F0F1F2F3F4F5F6F7F8F9FAFBFCFD0000 (already shifted)
Offset:           F0F1F2F3F4F5F6F7F8F9FAFBFCFD0000

Counter                            Keystream

F0F1F2F3F4F5F6F7F8F9FAFBFCFD0000   B2D8ED5E9E74E2B22F24D190290304F1
F0F1F2F3F4F5F6F7F8F9FAFBFCFD0001   917D4D59E7A62AAA3EC3037481304FAC
F0F1F2F3F4F5F6F7F8F9FAFBFCFD0002   876DDA20079D808ABE045C84FFA50E6B
...                                ...
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF   D3C8AAEA599D89569F4577158BAEFA3B
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFF00   156C6C1985F2DA529B6377C760295A98
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFF01   7920339AFE329CBA9DE8A2FC0D8BAE74
```

---

### 6.2. Key Derivation Test Vectors using Camellia-128 in Counter Mode

```
  master key:  E1F97A0D3E018BE0D64FA32C06DE4139
  master salt: 0EC675AD498AFEEBB6960B3AABE6

(1) session key

    index DIV kdr: 000000000000
    label:         00
    master salt:   0EC675AD498AFEEBB6960B3AABE6
    ----------------------------------------------
    xor:        0EC675AD498AFEEBB6960B3AABE6     (x, PRF input)

    x*2^16:     0EC675AD498AFEEBB6960B3AABE60000 (Camellia-CTR input)

    cipher key: 259EA7329BD8BCFC0E42D6336F7EC339 (Camellia-CTR output)


(2) session salt

    index DIV kdr: 000000000000
    label:         02
    master salt:   0EC675AD498AFEEBB6960B3AABE6

    ----------------------------------------------
    xor:        0EC675AD498AFEE9B6960B3AABE6     (x, PRF input)

    x*2^16:     0EC675AD498AFEE9B6960B3AABE60000 (Camellia-CTR input)

                69AF5169A7C7D257D0A19C38D81DF16A (Camellia-CTR ouptut)

    cipher salt:   69AF5169A7C7D257D0A19C38D81D

(3) auth key

    index DIV kdr:   000000000000
    label:           01
    master salt:     0EC675AD498AFEEBB6960B3AABE6
    ----------------------------------------------
    xor:        0EC675AD498AFEEAB6960B3AABE6     (x, PRF input)

    x*2^16:     0EC675AD498AFEEAB6960B3AABE60000 (Camellia-CTR input)

  akey                              Camellia input blocks
  CA06DDE96B5B0C71F02F878B8D376FCC  0EC675AD498AFEEAB6960B3AABE60000
  83750D2E61365F8BE33E6DD24519C5A8  0EC675AD498AFEEAB6960B3AABE60001
  17CE96CF61AB9C4F4EEB0689148A7A32  0EC675AD498AFEEAB6960B3AABE60002
  0FD78D243DDE852CA7C266D50E077CA7  0EC675AD498AFEEAB6960B3AABE60003
  BBCBF3EF45BCE67141ABA950063CF86E  0EC675AD498AFEEAB6960B3AABE60004
  73513A989FC1CBC3E8E11FF0DD20      0EC675AD498AFEEAB6960B3AABE60005
```

## 7. References

### 7.1. Normative References


| | |
|---|---|
| [RFC2119] | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML). |
| [RFC3550] | Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," STD 64, RFC 3550, July 2003 (TXT, PS, PDF). |
| [RFC3711] | Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," RFC 3711, March 2004 (TXT). |
| [RFC3713] | Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm," RFC 3713, April 2004 (TXT). |
| [RFC4568] | Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," RFC 4568, July 2006 (TXT). |


### 7.2. Informative References


| | |
|---|---|
| [CRYPTREC] | Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees" (HTML). |
| [Camellia web site] | "Camellia web site." |
| [FIPS. 197.2001] | National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS PUB 197, November 2001. |
| [ISO/IEC 18033-3] | International Organization for Standardization, "Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers," ISO/IEC 18033-3, July 2005. |
| [LNCS] | Mala, H., Shakiba, M., and M. Dakhil-alian, "New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128," November 2009. |
| [NESSIE] | "The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)." |
| [RFC3657] | |

| | |
|---|---|
| | Moriai, S. and A. Kato, “Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS),” RFC 3657, January 2004 (TXT). |
| [RFC4051] | Eastlake, D., “Additional XML Security Uniform Resource Identifiers (URIs),” RFC 4051, April 2005 (TXT). |
| [RFC4132] | Moriai, S., Kato, A., and M. Kanda, “Addition of Camellia Cipher Suites to Transport Layer Security (TLS),” RFC 4132, July 2005 (TXT). |
| [RFC4312] | Kato, A., Moriai, S., and M. Kanda, “The Camellia Cipher Algorithm and Its Use With IPsec,” RFC 4312, December 2005 (TXT). |
| [open source license] | “Camellia open source software.” |


---

**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 |