Network Working Group	S. Kanno	
Internet-Draft	NTT Software Corporation	
Intended status: Informational	M. Kanda	
Expires: August 1, 2011	NTT	
	January 28, 2011	

TOC

Camellia cipher for the Secure Shell Transport Layer Protocol
draft-kanno-secsh-camellia-02

Abstract

Secure shell (SSH) is a secure remote-login protocol. SSH provides for algorithms that provide authentication, key agreement, confidentiality, and data-integrity services. The purpose of this document is to specify the Camellia cipher as symmetric encryption algorithm for the SSH Transport Layer Protocol.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on August 1, 2011.

Copyright Notice

Table of Contents

1. Introduction

TOC

The SSH protocol [3] (Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Transport Layer Protocol,” January 2006.) can support many different symmetric ciphers as encryption methods.
This document describes the necessary information to use the Camellia [1] (Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” April 2004.) symmetric cipher in the SSH protocol.
This document specifies three modes (Cipher Block Chaining (CBC) mode, Counter (CTR) mode, and Galois Counter Mode (GCM)) as encryption method.

2. Encryption

TOC

This document describes the Camellia cipher for use with the SSH Transport Protocol. For the Camellia modes, these specifications comply with AES:

Modes	Specifications
Camellia in CBC mode	RFC4253
Camellia in CTR mode	RFC4344
Camellia in GCM mode	RFC5647

This document describes the following new methods:

camellia256-cbc	OPTIONAL	Camellia in CBC mode, with a 256-bit key
camellia192-cbc	OPTIONAL	Camellia with a 192-bit key
camellia128-cbc	OPTIONAL	Camellia with a 128-bit key
camellia256-ctr	OPTIONAL	Camellia in CTR mode, with 256-bit key
camellia192-ctr	OPTIONAL	Camellia with a 192-bit key
camellia128-ctr	OPTIONAL	Camellia with a 128-bit key
AEAD_CAMELLIA_256_GCM	OPTIONAL	Camellia in GCM mode, with a 256-bit key
AEAD_CAMELLIA_128_GCM	OPTIONAL	Camellia with a 128-bit key

The "camellia256-cbc" cipher is Camellia in CBC mode. This version uses a 256-bit key. The "camellia192-cbc" cipher is the same as above, but with a 192-bit key. The "camellia128-cbc" cipher is the same as above, but with a 128-bit key.
The "camellia256-ctr" cipher is Camellia in CTR mode. This version uses a 256-bit key. The "camellia192-ctr" cipher is the same as above, but with a 192-bit key. The "camellia256-ctr" cipher is the same as above, but with a 256-bit key.
The "AEAD_CAMELLIA_256_GCM" is Camellia in GCM mode. This version uses a 256-bit key. The "AEAD_CAMELLIA_128_GCM" is the same as above, but with a 128-bit key.

---

3. MAC

TOC

This document describes the Camellia-GCM for use with the SSH Transport Protocol as a MAC. For the MAC of Camellia-GCM, the specification comply with AES for GCM mode:

Modes	Specification
Camellia in GCM mode	RFC5647

This document describes the addition of the following two entities to the SSH MAC algorithm names registry described in [2] (Lehtinen, S. and C. Lonvick, “The Secure Shell (SSH) Protocol Assigned Numbers,” January 2006.):

AEAD_CAMELLIA_256_GCM	OPTIONAL	Camellia in GCM mode, with a 256-bit key
AEAD_CAMELLIA_128_GCM	OPTIONAL	Camellia with a 128-bit key

The "AEAD_CAMELLIA_256_GCM" is Camellia in GCM mode. This version uses a 256-bit key. The "AEAD_CAMELLIA_128_GCM" is the same as above, but with a 128-bit key.

4. Key Exchange

TOC

The Camellia cipher uses these key exchange protocols as well as AES. These key exchange protocols are described in Section 7 of [3] (Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," January 2006.), Section 5.1 of [6] (Igoe, K. and J. Solinas, "AES Galois Counter Mode for the Secure Shell Transport Layer Protocol," August 2009.), and Section 4 and 5 of [5] (Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer," December 2009.).

5. Security Considerations

TOC

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 [7] (Mala, H., Shakiba, M., and M. Dakhil-alian, "New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128," November 2009.), [8] (, "The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)," .), and [9] (Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees," .)).
For the SSH security considerations, this document refers to Section 14 of [3] (Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," January 2006.), Section 6 of [4] (Bellare, M., Kohno, T., and C. Namprempre, "The Secure Shell (SSH) Transport Layer Encryption Modes," January 2006.), Section 8 of [6] (Igoe, K. and J. Solinas, "AES Galois Counter Mode for the Secure Shell Transport Layer Protocol," August 2009.), and Section 9 of [5] (Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer," December 2009.).

6. IANA Considerations

TOC

The eight encryption algorithm names are defined in Section 2, and the two MAC algorithm names are defined in Section 3. These names request to add to the Secure Shell Encryption Algorithm Name registry.

TOC

7. References

7.1. Normative

TOC

[1]	Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” RFC 3713, April 2004 (TXT).
[2]	Lehtinen, S. and C. Lonvick, “The Secure Shell (SSH) Protocol Assigned Numbers,” RFC 4250, January 2006 (TXT).
[3]	Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Transport Layer Protocol,” RFC 4253, January 2006 (TXT).
[4]	Bellare, M., Kohno, T., and C. Namprempre, “The Secure Shell (SSH) Transport Layer Encryption Modes,” RFC 4344, January 2006 (TXT).
[5]	Stebila, D. and J. Green, “Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer,” RFC 5656, December 2009 (TXT).
[6]	Igoe, K. and J. Solinas, “AES Galois Counter Mode for the Secure Shell Transport Layer Protocol,” RFC 5647, August 2009 (TXT).
[7]	Mala, H., Shakiba, M., and M. Dakhil-alian, “New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128,” November 2009.

7.2. Informative

TOC

[8]	“The NESSIE project (New European Schemes for Signatures, Integrity and Encryption).”
[9]	Information-technology Promotion Agency (IPA), “Cryptography Research and Evaluation Committees” (HTML).

Authors' Addresses

TOC

	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