Network Working Group	S. Kanno
Internet-Draft	NTT Software Corporation
Intended status: Informational	K. Raeburn
Expires: August 30, 2010	Massachusetts Institute of
	Technology
	M. Kanda
	NTT
	T. Hardjono
	Massachusetts Institute of
	Technology
	February 26, 2010

Camellia Encryption for Kerberos 5
draft-krb-wg-kanno-camellia-01

Abstract

This document is a specification for the addition of Camellia cipher to the Kerberos 5 cryptosystem suite. The Camellia cipher was developed by NTT and Mitsubishi Electric Corporation in 2000, which is comparable to Advanced Encryption Standard (AES).

Status of this Memo

Copyright Notice

---

1. Introduction

This document defines encryption key and checksum types for Kerberos 5 using the Camellia algorithm developed by NTT and Mitsubishi Electric Corporation in 2000. These new types support 128-bit block encryption and key sizes of 128 or 256 bits. It is same that interface speficiations as the AES.
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.).
Using the "simplified profile" of [RFC3961] (Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” February 2005.), we can define a pair of encryption and checksum schemes. Camellia is used with ciphertext stealing (CTS) to avoid message expansion, and SHA-1 is the associated checksum function.

---

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.).

---

3. Protocol Key Representation

The profile in [RFC3961] (Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” February 2005.) treats keys and random octet strings as conceptually different. But since the AES key space is dense, we can use any bit string of appropriate length as a key. We use the byte representation for the key described in [RFC3713] (Matsui, M., Nakajima, J., and S. Moriai, “A Description of the Camellia Encryption Algorithm,” April 2004.), where the first bit of the bit string is the high bit of the first byte of the byte string (octet string) representation.

---

4. Key Generation from Pass Phrases or Random Data

Given the above format for keys, we can generate keys from the appropriate amounts of random data (128 or 256 bits) by simply copying the input string.
To generate an encryption key from a pass phrase and salt string, the Camellia uses the PBKDF2 function from PKCS #5 v2.0 [RFC2898] (Kaliski, B., “PKCS #5: Password-Based Cryptography Specification Version 2.0,” September 2000.). This function of Camellia can define as same specification of AES [RFC3962] (Raeburn, K., “Advanced Encryption Standard (AES) Encryption for Kerberos 5,” February 2005.)
The pseudorandom function used by PBKDF2 will be a SHA-1 HMAC of the passphrase and salt. The case of AES described in Appendix B of [RFC3962] (Raeburn, K., “Advanced Encryption Standard (AES) Encryption for Kerberos 5,” February 2005.). For pseudorandom function, Camellia can use like an AES.

---

5. CipherText Stealing mode

The specification of CipherText Stealing (CTS) mode for Camellia complies with AES-CTS in [RFC3962] (Raeburn, K., “Advanced Encryption Standard (AES) Encryption for Kerberos 5,” February 2005.).
A test vector of Camellia-CTS is given in Section 10 (Test Vector).

---

6. Kerberos Algorithm Profile Parameters

This is a summary of the parameters to be used with the simplified algorithm profile described in [RFC3961] (Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” February 2005.):

protocol key format	128- or 256-bit string
string-to-key function	PBKDF2+DK with variable iteration count
default string-to-key parameters	00 00 10 00
key-generation seed length	key size
random-to-key function	identity function
hash function, H	SHA-1
HMAC output size, h	12 octets (96 bits)
message block size, m	1 octet
encryption/decryption functions, E and D	Camellia in CBC-CTS mode (cipher block size 16 octets), with next-to-last block (last block if only one) as CBC-style ivec

Using this profile with each key size gives us two each of encryption and checksum algorithm definitions.

---

7. Assigned Numbers

The following encryption type numbers are assigned:

encryption types		
type name	etype value	key size
camellia128-cts-hmac-sha1-96	<TBD1>	128
camellia256-cts-hmac-sha1-96	<TBD2>	256

The following checksum type numbers are assigned:

checksum types		
type name	sumtype value	length
hmac-sha1-96-camellia128	<TBD3>	96
hmac-sha1-96-camellia256	<TBD4>	96

These checksum types will be used with the corresponding encryption types defined above.

8. 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.)).
For security considerations of CTS mode, this document refers to Section 8 of [RFC3962] (Raeburn, K., “Advanced Encryption Standard (AES) Encryption for Kerberos 5,” February 2005.).

9. IANA Considerations

Kerberos encryption and checksum type values used in section 7 were previously reserved in [RFC3961] (Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” February 2005.) for the mechanisms defined in this document. The registries have been updated to list this document as the reference.

10. Test Vector

Some test vectors for CTS mode, using an initial vector of all-zero.

```
Camellia 128-bit key:
  0000:  63 68 69 63 6b 65 6e 20 74 65 72 69 79 61 6b 69

IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20
Output:
  0000:  <TBD>
  0010:
Next IV:
  0000:  <TBD>

IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20 47 65 6e 65 72 61 6c 20 47 61 75 27 73 20
Output:
  0000:  <TBD>
  0010:
Next IV:
  0000:  <TBD>

IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20 47 65 6e 65 72 61 6c 20 47 61 75 27 73 20 43
Output:
  0000:
  0010:  <TBD>
Next IV:
  0000:  <TBD>

IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20 47 65 6e 65 72 61 6c 20 47 61 75 27 73 20 43
  0020:  68 69 63 6b 65 6e 2c 20 70 6c 65 61 73 65 2c
Output:
  0000:  <TBD>
  0010:
  0020:
Next IV:
  0000:  <TBD>
```

```
IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20 47 65 6e 65 72 61 6c 20 47 61 75 27 73 20 43
  0020:  68 69 63 6b 65 6e 2c 20 70 6c 65 61 73 65 2c 20
Output:
  0000:  <TBD>
  0010:
  0020:
Next IV:
  0000:  <TBD>

IV:
  0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Input:
  0000:  49 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 68 65
  0010:  20 47 65 6e 65 72 61 6c 20 47 61 75 27 73 20 43
  0020:  68 69 63 6b 65 6e 2c 20 70 6c 65 61 73 65 2c 20
  0030:  61 6e 64 20 77 6f 6e 74 6f 6e 20 73 6f 75 70 2e
Output:
  0000:  <TBD>
  0010:
  0020:
  0030:
Next IV:
  0000:  <TBD>
```

11. References

11.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2898]	Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0," RFC 2898, September 2000 (TXT).
[RFC3713]	Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm," RFC 3713, April 2004 (TXT).
[RFC3961]	

	Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5," RFC 3961, February 2005 (TXT).
[RFC3962]	Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5," RFC 3962, February 2005 (TXT).

11.2. Informative References

[CRYPTREC]	Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees" (HTML).
[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)."

Authors' Addresses

	Satoru Kanno
	NTT Software Corporation
Phone:	+81-45-212-9803
Fax:	+81-45-212-9800
Email:	kanno.satoru@po.ntts.co.jp
	Kenneth Raeburn
	Massachusetts Institute of Technology
Email:	raeburn@mit.edu
	Masayuki Kanda
	NTT
Phone:	+81-422-59-3456
Fax:	+81-422-59-4015
Email:	kanda.masayuki@lab.ntt.co.jp
	Thomas Hardjono
	Massachusetts Institute of Technology
Email:	hardjono@mit.edu