

AVTCore
Internet-Draft
Intended status: Standards Track
Expires: May 29, 2016

W. Kim
J. Lee
J. Park
D. Kwon
NSRI

November 26, 2015

The Addition of SRTP crypto suites based on the ARIA algorithms to the
SDP Security Descriptions
draft-ietf-avtcore-aria-sdes-01

Abstract

This document defines SRTP crypto suites based on the ARIA block cipher algorithm for use with the Session Description Protocol (SDP) security descriptions.

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 May 29, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

Internet-Draft The Addition of ARIA crypto suites to SDP November 2015

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	ARIA	2
1.2.	SRTP Crypto Suites	2
1.3.	Terminology	3
2.	Parameters	3
3.	IANA Considerations	7
4.	References	7
4.1.	Normative References	7
4.2.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

This document defines the SDP Security Descriptions attributes [[RFC4568](#)] corresponding to the ARIA transforms which are defined in [[I-D.ietf-avtcore-aria-srtp](#)].

[1.1.](#) ARIA

ARIA is a general-purpose block cipher algorithm developed by Korean cryptographers in 2003. It is an iterated block cipher with 128-, 192-, and 256-bit keys and encrypts 128-bit blocks in 12, 14, and 16 rounds, depending on the key size. It is secure and suitable for most software and hardware implementations on 32-bit and 8-bit processors. It was established as a Korean standard block cipher algorithm in 2004 [[ARIAKS](#)] and has been widely used in Korea, especially for government-to-public services. It was included in PKCS #11 in 2007 [[ARIAPKCS](#)]. The algorithm specification and object identifiers are described in [[RFC5794](#)].

[1.2.](#) SRTP Crypto Suites

The transforms based on ARIA and the corresponding SRTP protection profiles for DTLS-SRTP are defined in [[I-D.ietf-avtcore-aria-srtp](#)]. The SDP Security Descriptions [[RFC4568](#)] crypto suites corresponding to ARIA transforms [[I-D.ietf-avtcore-aria-srtp](#)] are sets as shown in Table 1.

Internet-Draft The Addition of ARIA crypto suites to SDP November 2015

Name	Enc. Key Length	Auth. Tag Length
ARIA_128_CTR_HMAC_SHA1_80	16 octets	10 octets
ARIA_128_CTR_HMAC_SHA1_32	16 octets	4 octets
ARIA_192_CTR_HMAC_SHA1_80	24 octets	10 octets
ARIA_192_CTR_HMAC_SHA1_32	24 octets	4 octets
ARIA_256_CTR_HMAC_SHA1_80	32 octets	10 octets
ARIA_256_CTR_HMAC_SHA1_32	32 octets	4 octets
AEAD_ARIA_128_GCM	16 octets	16 octets
AEAD_ARIA_256_GCM	32 octets	16 octets

Table 1: ARIA Crypto Suites for SRTP

1.3. 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. Parameters

The parameters in each crypto suite listed in Table 1 are described for use with the SDP Security Descriptions attributes [[RFC4568](#)].

Parameter	Value
Master key length	128 bits
Master salt length	112 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime (SRTP)	2 ⁴⁸ packets
Default key lifetime (SRTCP)	2 ³¹ packets
Cipher (for SRTP and SRTCP)	ARIA_128_CTR
SRTP authentication function	HMAC-SHA1

SRTP authentication key length	160 bits	
SRTP authentication tag length	80 bits	
SRTCP authentication function	HMAC-SHA1	
SRTCP authentication key length	160 bits	
SRTCP authentication tag length	80 bits	

Table 2: The ARIA_128_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value	
Master key length	128 bits	
Master salt length	112 bits	
Key Derivation Function	ARIA_128_CTR_PRF	
Default key lifetime (SRTP)	2 ⁴⁸ packets	
Default key lifetime (SRTCP)	2 ³¹ packets	
Cipher (for SRTP and SRTCP)	ARIA_128_CTR	
SRTP authentication function	HMAC-SHA1	
SRTP authentication key length	160 bits	
SRTP authentication tag length	32 bits	
SRTCP authentication function	HMAC-SHA1	
SRTCP authentication key length	160 bits	
SRTCP authentication tag length	80 bits	

Table 3: The ARIA_128_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value	
Master key length	192 bits	
Master salt length	112 bits	
Key Derivation Function	ARIA_192_CTR_PRF	
Default key lifetime (SRTP)	2 ⁴⁸ packets	
Default key lifetime (SRTCP)	2 ³¹ packets	
Cipher (for SRTP and SRTCP)	ARIA_192_CTR	
SRTP authentication function	HMAC-SHA1	

SRTCP authentication key length	160 bits	
SRTCP authentication tag length	80 bits	
SRTCP authentication function	HMAC-SHA1	
SRTCP authentication key length	160 bits	
SRTCP authentication tag length	80 bits	

Table 4: The ARIA_192_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value	
Master key length	192 bits	
Master salt length	112 bits	
Key Derivation Function	ARIA_192_CTR_PRF	
Default key lifetime (SRTCP)	2 ⁴⁸ packets	
Default key lifetime (SRTCP)	2 ³¹ packets	
Cipher (for SRTCP and SRTCP)	ARIA_192_CTR	
SRTCP authentication function	HMAC-SHA1	
SRTCP authentication key length	160 bits	
SRTCP authentication tag length	32 bits	
SRTCP authentication function	HMAC-SHA1	
SRTCP authentication key length	160 bits	
SRTCP authentication tag length	80 bits	

Table 5: The ARIA_192_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value	
-----------	-------	--

Master key length	256 bits
Master salt length	112 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime (SRTP)	2 ⁴⁸ packets
Default key lifetime (SRTCP)	2 ³¹ packets
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	80 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 6: The ARIA_256_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value
Master key length	256 bits
Master salt length	112 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime (SRTP)	2 ⁴⁸ packets
Default key lifetime (SRTCP)	2 ³¹ packets
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	32 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 7: The ARIA_256_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value
Master key length	128 bits
Master salt length	96 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime (SRTP)	2 ⁴⁸ packets
Default key lifetime (SRTCP)	2 ³¹ packets
Cipher (for SRTP and SRTCP)	AEAD_ARIA_128_GCM
AEAD authentication tag length	128 bits

Table 8: The AEAD_ARIA_128_GCM Crypto Suite

Parameter	Value
Master key length	256 bits
Master salt length	96 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime (SRTP)	2 ⁴⁸ packets
Default key lifetime (SRTCP)	2 ³¹ packets
Cipher (for SRTP and SRTCP)	AEAD_ARIA_256_GCM
AEAD authentication tag length	128 bits

Table 9: The AEAD_ARIA_256_GCM Crypto Suite

3. IANA Considerations

SDP Security Descriptions [RFC4568] defines SRTP "crypto suites". In order to allow SDP to signal the use of the algorithms defined in this document, IANA is requested to add the below crypto suites to the "SRTP Crypto Suite Registrations" created by [RFC4568], at time of writing located on the following IANA page:

<http://www.iana.org/assignments/sdp-security-descriptions/> .

```
srtp-crypto-suite-ext = "ARIA_128_CTR_HMAC_SHA1_80"/
                        "ARIA_128_CTR_HMAC_SHA1_32"/
                        "ARIA_192_CTR_HMAC_SHA1_80"/
                        "ARIA_192_CTR_HMAC_SHA1_32"/
                        "ARIA_256_CTR_HMAC_SHA1_80"/
                        "ARIA_256_CTR_HMAC_SHA1_32"/
                        "AEAD_ARIA_128_GCM"      /
                        "AEAD_ARIA_256_GCM"      /
                        srtp-crypto-suite-ext
```

[4. References](#)

[4.1. Normative References](#)

[I-D.ietf-avtcore-aria-srtp]

Kim, W., Lee, J., Park, J., and D. Kwon, "The ARIA Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP)", [draft-ietf-avtcore-aria-srtp-08](#) (work in progress), May 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", [RFC 4568](#), DOI 10.17487/RFC4568, July 2006, <<http://www.rfc-editor.org/info/rfc4568>>.

[4.2. Informative References](#)

[ARIAKS] Korean Agency for Technology and Standards, "128 bit block encryption algorithm ARIA - Part 1: General (in Korean)", KS X 1213-1:2009, December 2009.

[ARIAPKCS]

RSA Laboratories, "Additional PKCS #11 Mechanisms", PKCS #11 v2.20 Amendment 3 Revision 1, January 2007.

Description of the ARIA Encryption Algorithm", [RFC 5794](#),
DOI 10.17487/RFC5794, March 2010,
<<http://www.rfc-editor.org/info/rfc5794>>.

Authors' Addresses

Woo-Hwan Kim
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

E-Mail: whkim5@ensec.re.kr

Jungkeun Lee
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

E-Mail: jkleee@ensec.re.kr

Je-Hong Park
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

E-Mail: jhpark@ensec.re.kr

Daesung Kwon
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

E-Mail: ds_kwon@ensec.re.kr