Korea Communications Standard

방송통신표준

KCS.KO-12.2001 제정일: 2013년 12월 31일

TLS·SRTP·MIKEY에서 블록 암호 ARIA 활용 방법

The Use of the Block Cipher ARIA in TLS·SRTP·MIKEY

미래창조과학부

국립전파연구원

방송통신표준

KCS.KO-12.2001 제정일: 2013년 12월 31일

TLS·SRTP·MIKEY에서 블록 암호 ARIA 활용 방법

The Use of the Block Cipher ARIA in TLS·SRTP·MIKEY

미래창조과학부
국립전파연구원

서 문

1. 표준의 목적

본 표준은 웹 서비스 또는 인터넷 전화 서비스 제공 시 도청과 같은 사이버 침해 사고 예방을 목적으로 사용하는 보안 프로토콜인 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)에 국가 표준 블록 암호 ARIA의 적용 방법을 제시한다.

2. 주요 내용 요약

본 표준은 서버와 클라이언트 간의 암호 통신을 위한 프로토콜인 TLS(Transport Layer Security)와 멀티미디어 데이터 전송 규격 RTP(Real-time Transport Protocol)를 위한 보안 프로토콜인 SRTP(Secure Real-time Transport Protocol)에서 블록 암호 ARIA를 사용하기 위한 Cipher Suite를 기술한다. TLS(Transport Layer Security)의 경우, 데이터 암호화에 사용할 대칭 키 암호 알고리즘으로 ARIA를 적용하는 Cipher Suite를 제시하고, 프로토콜 참여자 간의 키 교환과 Cipher Suite 협상 과정인 TLS Handshake Layer에서 각각의 Cipher Suite를 식별하는 데 필요한 참조값을 규정한다. SRTP(Secure Real-time Transport Protocol)의 경우, RTP(Real-time Transport Protocol)와 RTCP(RTP Control Protocol) 트래픽 암호화와 키 유도에 사용할 대칭 키 암호 알고리즘으로 ARIA를 적용하는 Cipher Suite를 제시한다. 그리고 각각의 Cipher Suite를 SRTP(Secure Real-time Transport Protocol)의 키 관리 프로토콜인 MIKEY(Multimedia Internet KEYing)와 SDES(Session Description Protocol Security Description)를 통해 협상하는데 필요한 참조값과 파라미터를 명시한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)는 국내 웹 서비스와 인터넷 전화 서비스의 보안 기능 제공을 위해 일반적으로 사용되는 프로토콜이다. 본 표준은 기반 블록 암호로 ARIA를 적용하는 TLS(Transport Layer Security) 또는 SRTP(Secure Real-time Transport Protocol)의 운용이 필요한 다양한 정보보호 시스템 및 암호 제품에 활용될 수 있다. 이를 통해 국내 정보통신망의 안정성과 신뢰성을 제고하는 데 기여할 수 있다.

4. 참조 표준(권고)

4.1. 국외 표준(권고)

해당 사항 없음.

4.2. 국내 표준

- TTAK.KO-12.0201, 'MIKEY에서 ARIA알고리즘 사용을 위한 파라미터 정의', 2012.12.
- TTAK.KO-12.0115/R1, 'SRTP에서의 ARIA 암호 알고리즘 운영 방법', 2011.12.
- TTAK.KO-12.0114/R1, 'TLS에서의 ARIA 암호 알고리즘 운영 방법', 2011.12.

5. 참조 표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

본 표준은 국내 웹 보안 또는 인터넷 전화 보안 서비스 제공을 위해 적용하는 주요 프로토콜인 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)를 대상으로 ARIA 적용 방법을 제시한 'TTAK.KO-12.0114/R1'과 'TTAK.KO-12.0115/R1', 그리고 'TTAK.KO-12.0201'을 병합하여 작성하였다.

5.2. 참조한 표준(권고)과 본 표준의 비교표

KCS.KO-12.2001	참조 표준			비고
	TTAK.KO-12.0114/R1	TTAK.KO-12.0115/R1	TTAK.KO-12.0201	
1. 개요	1. 개요	1. 개요	1. 개요	병합
2. 표준의 구성 및 범위	2. 표준의 구성 및 범위	2. 표준의 구성 및 범위	2. 표준의 구성 및 범위	병합
-	-	-	3. 참조 표준(권고)	서문에 포함
3. 용어 정의 및 약어	3. 용어 정의	3. 용어 정의	4. 용어 정의	병합
4. TLS에서의 ARIA 사용 방법	4. Cipher Suites	-	-	동일
-	5. 필수 Cipher Suite	-	-	4 절에 포함
5. SRTP에서의 ARIA 사용 방법	-	4. 암호 알고리즘	-	동일

-	-	5. 키유도 함수	-	5 절에 포함
-	-	6. 필수 Cipher Suite	-	5 절에 포함
6. SRTP의 키 관리 프로토콜에서 ARIA Cipher Suite 파라미터 설정	-	-	5. SRTP 정책	6 절에 포함
7. 안전성 관련 고려 사항	6. 안전성 관련 고려 사항	7. 안전성 관련 고려 사항	-	병합
부록 I. 관련 문헌	-	-	-	추가

6. 지식 재산권 관련 사항

본 표준의 '지적 재산권 취급 확약서' 제출 현황은 국립전파연구원 웹사이트에서 확인할 수 있다.

※ 이 표준을 이용하는 자는 이용함에 있어 지식 재산권이 포함되어 있을 수 있으므로, 확인 후 이용한다.

※ 본 표준과 관련하여 접수된 확약서 이외에도 지식 재산권이 존재할 수 있다.

7. 시험 인증 관련 사항

7.1. 시험 인증 대상 여부

해당 사항 없음.

7.2. 시험 표준 제정 현황

해당 사항 없음.

8. 표준의 이력 정보

8.1. 표준의 이력

판 수	제정·개정일	제정·개정 내역
제 1 판	2013.12.31.	제정 KCS.KO-12.2001

8.2. 주요 개정 사항

해당 사항 없음.

Preface

1. Purpose of Standard

This standard provides a method to use the national standard block cipher ARIA in main security protocols TLS(Transport Layer Security) and SRTP(Secure Real-time Transport Protocol), applied for preventing cyber attacks such as eavesdropping against Web or VoIP(Voice over IP) services.

2. Summary of Contents

This standard describes how ARIA can be used as a base block cipher in TLS(Transport Layer Security) and SRTP(Secure Real-time Transport Protocol). TLS(Transport Layer Security) is a cryptographic protocol that provides communication security over the Internet and allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. SRTP(Secure Real-time Transport Protocol) is a cryptographic protocol that provides several security services on a standardized packet format for delivering multimedia data over IP network. For TLS(Transport Layer Security), this standard provides new Cipher Suites that use ARIA as symmetric key cipher for data encryption. To negotiate a master secret key and a proper ARIA Cipher Suite in TLS Handshake Layer, additionally, this standard defines values assigned to each Cipher Suite. For SRTP(Secure Real-time Transport Protocol), this standard provides new Cipher Suites that use ARIA as symmetric key cipher for RTP(Real-time Transport Protocol) and RTCP(RTP Control Protocol) payload encryption and key derivation. This standard also defines identifiers and parameters to be used in key management protocols MIKEY(Multimedia Internet KEYing) and SDES(Session Description Protocol Security Description) for negotiating Cipher Suites for SRTP(Secure Real-time Transport Protocol).

3. Applicable Fields of Industry and its Effect

TLS(Transport Layer Security) and SRTP(Secure Real-time Transport Protocol) are commonly applied as main cryptographic protocols for providing security services on Web or VoIP(Voice over IP) networks in Korea. This standard may be applied to various information security systems and cryptographic equipments, requiring operations of TLS(Transport Layer Security) or SRTP(Secure Real-time Transport Protocol) which use ARIA as a base block cipher. This can make to improve stability and reliability of national information communication networks.

4. Reference Standards(Recommendations)

4.1. International Standards(Recommendations)

None

4.2. Domestic Standards

- TTAK.KO-12.0201, “Parameters for the ARIA Algorithm Support in the Multimedia Internet KEYing (MIKEY)”, 2012.12.
- TTAK.KO-12.0115/R1, “The Use of ARIA Algorithm in SRTP”, 2011.12.
- TTAK.KO-12.0114/R1, “The Use of ARIA Algorithm in TLS”, 2011.12.

5. Comparison between Reference Standards(Recommendations) and this Standard

5.1. Relevance of this standard with Reference Standards(Recommendations)

This standard focuses on the main security protocols TLS(Transport Layer Security) and SRTP(Secure Real-time Transport Protocol) for Web services and VoIP services in Korea, and refers three standards “TTAK.KO-12.0114/R1”, “TTAK.KO-12.0115/R1”, and “TTAK.KO-12.0201” which describe how ARIA can be used in such protocols.

5.2. A Comparative Table of Reference Standard(Recommendation) and this Standard

KCS.KO-12.2001	Reference Standard			Remarks
	TTAK.KO-12.0114/R1	TTAK.KO-12.0115/R1	TTAK.KO-12.0201	
1. Introduction	1. Introduction	1. Introduction	1. Introduction	Merged
2. Constitution and Scope	2. Constitution and Scope	2. Constitution and Scope	2. Constitution and Scope	Merged
-	-	-	3. Reference Standards	Condensed in Preface
3. Terms Definitions and Abbreviations	3. Terms and Definitions	3. Terms and Definitions	4. Terms and Definitions	Merged
4. The Use of ARIA in TLS	4. Cipher Suites	-	-	Equivalent
-	5. Mandatory Cipher Suite	-	-	Condensed in Sec.4
5. The Use of ARIA in SRTP	-	4. Cryptographic Transforms	-	Equivalent
-	-	5. Key Derivation Function	-	Condensed in Sec.5
-	-	6. Mandatory Cipher Suite	-	Condensed in Sec.5
6. ARIA Cipher Suite Parameter Setting for Key Management Protocols of SRTP	-	-	5. SRTP Policy	Condensed in Sec.6
7. Security Considerations	6. Security Considerations	7. Security Considerations	-	Merged
Appendix I. Related Documents	-	-	-	Added

6. Statement of Intellectual Property Rights

“Written Confirmation of Intellectual Property Rights” for this standard can be referenced to the website of the National Radio Research Agency.

Those using this standard must confirm that whether intellectual property rights are included in this standard.

Other intellectual property rights may exist in relation to written confirmation received for this standard.

7. Statement of Testing and Certification

7.1. Object of Testing and Certification

None

7.2. Standards of Testing and Certification

None

8. Detailed History of Standard

8.1. History of Standard

Edition	Issued date	History
The 1st edition	2013.12.31.	Established KCS.KO-12.2001

8.2. Revisions Related Details

None

목 차

Contents

TLS·SRTP·MIKEY에서의 블록 암호 ARIA 활용 방법
(The Use of Block Cipher ARIA in TLS·SRTP·MIKEY)

1. 개요

TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)는 국내 웹 서비스와 인터넷 전화 서비스의 보안 기능 제공을 위해 일반적으로 사용되는 프로토콜이다. 따라서 부록 I의 [13]에 기술된 국가 표준 블록 암호 ARIA를 적용한 웹 서비스 또는 인터넷 전화 서비스의 보안 시스템 구축을 위해서는 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)에 ARIA 사용 방식을 설정하는 별도의 Cipher Suite가 필요하다. 본 표준에서는 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol) 각각에 대한 ARIA 기반의 Cipher Suite를 제시한다. 그리고 프로토콜 참여자의 Cipher Suite 설정 공유에 필요한 키 관리 프로토콜을 별도로 운용해야 하는 SRTP(Secure Real-time Transport Protocol)를 위해, MIKEY(Multimedia Internet KEYing)와 SDES(SDP Security Description)를 키 관리 프로토콜로 사용할 경우 SRTP(Secure Real-time Transport Protocol)의 ARIA Cipher Suite 식별에 필요한 파라미터와 참조값을 제시한다.

2. 표준의 구성 및 범위

본 표준은 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)에서 ARIA를 사용하기 위한 규격과 SRTP(Secure Real-time Transport Protocol)의 키 관리 프로토콜인 MIKEY(Multimedia Internet KEYing)와 SDES(SDP Security Description)에서 ARIA Cipher Suite를 식별하기 위한 참조값을 제시한다. 4 절은 TLS(Transport Layer Security)에서 ARIA를 사용하기 위한 규격을 제시하고, 5 절에서는 SRTP(Secure Real-time Transport Protocol)에서 ARIA를 사용하기 위한 규격을 제시한다. 이어서 6 절에서는 SRTP(Secure Real-time Transport Protocol)의 키 관리 프로토콜로 MIKEY(Multimedia Internet KEYing)와 SDES(SDP Security Description)를 사용할 경우 ARIA Cipher Suite를 식별하기 위해 필요한 파라미터와 참조값을 제시한다. 7 절에서는 ARIA를 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)에서 사용하는 것과 관련된 안전성 고려 사항을 기술한다.

3. 용어 정의 및 약어

3.1. 용어 정의

인증 암호화 운영 모드 (AEAD, Authenticated Encryption with Associated Data)	블록 암호 운영 모드 중에서 기밀성과 메시지 인증을 동시에 제공하는 운영 모드를 지칭하며 대표적인 예로 CCM, GCM이 있음.
AES (Advanced Encryption Standard)	국제 공모 사업을 통해 개발된 미국 연방정부 표준 블록 암호로, 블록 길이는 128 비트이고 키 길이는 128, 192, 256 비트를 지원함. 키 길이에 따라 규격의 차이가 있기 때문에 이를 구분할 경우 AES-128, AES-192, AES-256으로 표기.
ARIA	국내 전자정부 안전성 강화를 목적으로 개발된 블록 암호로, AES와 인터페이스가 동일하며, 키 길이에 따라 각각 ARIA-128, ARIA-192, ARIA-256으로 표기.
CCM (Counter with CBC-MAC)	블록 암호 운영 모드 중의 하나로 카운터 모드와 블록 암호 기반 메시지 인증 코드 CBC-MAC을 조합한 방식.
GCM (Galois/Counter Mode)	블록 암호 운영 모드 중의 하나로 카운터 모드와 유한체 곱셈으로 정의된 특화된 해시 함수를 조합한 방식.
HMAC (Keyed-Hash Message Authentication Code)	해시 함수 기반 MAC 알고리즘.
IPsec (Internet Protocol Security)	IP 계층의 패킷 단위 암호화 및 메시지 인증을 통해 정보보호 서비스를 제공하는 프로토콜.
SHA (Secure Hash Algorithm)	미국 연방정부 표준 해시 함수로 현재 7 개의 알고리즘으로 구성됨. 알고리즘은 출력값의 길이에 따라 각각 SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256로 구분하며, 내부함수 구조나 초기값 등의 차별 요소가 존재.

S/MIME (Secure/Multipurpose Internet Mail Extension)	전자 우편을 통해 다양한 종류의 데이터를 전송하기 위해 만들어진 규약인 MIME에 기밀성과 인증, 그리고 부인 방지 등의 정보보호 서비스를 제공하는 프로토콜.
멀티미디어 인터넷 키 관리 방식(MIKEY, Multimedia Internet KEYing)	SRTP와 같은 멀티미디어 보안 프로토콜을 지원하는 일-대-다(One-to-Many) 또는 소규모 상호 작용형 그룹에 적합한 키 관리 프로토콜.
사전 공유 키 (PSK, Pre-Shared Key)	보안 프로토콜 시작 전에 프로토콜 참여자가 별도의 방식을 통해 공유하고 있는 암호 키.
실시간 전송 프로토콜 (RTP, Real-time Transport Protocol)	인터넷상의 오디오와 비디오 같은 멀티미디어 데이터를 실시간으로 전송하기 위해 설계된 표준 패킷 구조와 운영 방식.
세션 기술 프로토콜 (SDP, Session Description Protocol)	멀티미디어 통신에 있어 세션 개시, 초대, 시작 등 세션 전반에 대한 규격을 명시한 프로토콜.
안전한 실시간 전송 프로토콜 (SRTP, Secure RTP)	RTP의 암호화, 메시지 인증, 재전송 공격 방어 등의 정보 보호 서비스를 제공하기 위한 프로토콜.
인터넷 할당 번호 관리 기관 (IANA, Internet Assigned Numbers Authority)	IETF의 RFC 규격으로 발간되는 각종 인터넷 프로토콜의 고유 매개변수들과 프로토콜 파라미터를 관리하는 기관.
전송 계층 보안 (TLS, Transport Layer Security)	TCP/IP 계층의 서버-클라이언트 통신에 대한 정보보호 서비스를 제공하는 프로토콜로, Cipher Suite와 키 교환 및 사용자 인증을 수행하는 Handshake Layer, 데이터 암호화 및 메시지 인증을 수행하는 Record Layer로 기능 구분.
카운터 모드 (CTR, Counter mode)	블록 암호 운영 모드 중의 하나로, 블록 단위로 증가하는 카운터(counter)를 블록 암호 입력값으로 하여 얻어진 연속된 출력값을 평문과 XOR하는 방식으로 암호화를 수행.
충돌쌍 공격 (Collision Attack)	주어진 해시 함수의 출력 비트 길이를 n이라 할 때, 같은 출력값을 가지는 서로 다른 2 개의 입력 데이터를 $2^{n/2}$보다 적은 계산량으로 찾는 공격.

해시 함수	임의 길이의 메시지를 일정 길이의 출력값으로 압축하는 알고리즘.

3.2. 약어

AES-CBC	AES in Cipher Block Chaining Mode
AES-CCM	AES in Counter with CBC-MAC Mode
AES-CM	AES in Counter Mode
AES-GCM	AES in Galois/Counter Mode
anon	anonymous
ARIA-CBC	ARIA in Cipher Block Chaining Mode
ARIA-CTR	ARIA in Counter Mode
ARIA-CCM	ARIA in Counter with CBC-MAC Mode
ARIA-GCM	ARIA in Galois/Counter Mode
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining-Message Authentication Code
DH	Diffie-Hellman
DSS	Digital Signature Standard
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
IETF	Internet Engineering Task Force
IP	Internet Protocol
IV	Initialization Vector
MAC	Message Authentication Code
PRF	Pseudo Random Function
RTCP	RTP Control Protocol
SDES	SDP Security Descriptions
SRTCP	Secure RTP Control Protocol
TCP	Transmission Control Protocol

VoIP	Voice over IP

4. TLS에서의 ARIA 사용 방법

ARIA와 AES는 키와 블록 길이, 그리고 운영 모드 사용 방법이 동일하며, ARIA 사용에 대한 특이한 제약 사항이 존재하지 않는다. 따라서 TLS에서의 ARIA 적용 방법은 부록 Ⅰ의 [4], [5], [7], [8]에서 제시한 AES의 적용 방법을 준용한다. 본 절에서는 ARIA를 TLS에 적용하기 위한 방법을 설정하는 Cipher Suite와, Handshake Layer를 통해 프로토콜 참여자가 ARIA Cipher Suite를 협상하는 과정에서 필요한 참조값을 제시한다. ARIA Cipher Suite와 참조값은 부록 Ⅰ의 [10]에 제시된 Cipher Suite와 IANA 참조값을 그대로 수용한다.

4.1. Cipher Suite 목록

4.1.1. HMAC 기반 Cipher Suite

ARIA-CBC와 HMAC을 사용하는 Cipher Suite 20 개는 표 4.1과 같다.

표 4.1 HMAC 기반 Cipher Suite

번호	Cipher Suite	참조값(value)
1	TLS_RSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x3C
2	TLS_RSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x3D
3	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256	0xC0, 0x3E
4	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384	0xC0, 0x3F
5	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x40
6	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x41
7	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256	0xC0, 0x42
8	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384	0xC0, 0x43
9	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x44
10	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x45
11	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256	0xC0, 0x46
12	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384	0xC0, 0x47
13	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x48
14	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x49
15	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x4A

번호	Cipher Suite	참조값(value)
16	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x4B
17	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x4C
18	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x4D
19	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256	0xC0, 0x4E
20	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384	0xC0, 0x4F

4.1.2. GCM 기반 Cipher Suite

인증 암호화 운영 모드를 사용하여 데이터 암호화를 수행하는 대칭 키 암호로 ARIA-GCM을 사용하는 Cipher Suite 20 개는 표 4.2와 같다. 이들 Cipher Suite는 부록 Ⅰ의 [7]에 기술된 TLS 1.2 또는 TLS 1.2의 상위 버전에서만 사용 가능하다.

표 4.2 GCM 기반 Cipher Suite

번호	Cipher Suite	참조값(value)
1	TLS_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x50
2	TLS_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x51
3	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x52
4	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x53
5	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x54
6	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x55
7	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256	0xC0, 0x56
8	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384	0xC0, 0x57
9	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256	0xC0, 0x58
10	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384	0xC0, 0x59
11	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256	0xC0, 0x5A
12	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384	0xC0, 0x5B
13	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x5C
14	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x5D
15	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x5E
16	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x5F
17	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x60
18	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x61
19	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x62
20	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x63

4.1.3. PSK 기반 Cipher Suite

송수신자 사이에 PSK가 있을 경우 사용할 수 있는 Cipher Suite 14 개는 표 4.3과 같다. 이들 중 8 개(1 ~ 6 번, 13 ~ 14 번)는 별도의 MAC 알고리즘으로 HMAC을 사용하는 Cipher Suite이고 나머지 6 개(7 ~ 12 번)는 대칭 키 암호로 ARIA-GCM을 사용하는 Cipher Suite이다.

표 4.3 PSK 기반 Cipher Suite

번호	Cipher Suite	참조값(value)
1	TLS_PSK_WITH_ARIA_128_CBC_SHA256	0xC0, 0x64
2	TLS_PSK_WITH_ARIA_256_CBC_SHA384	0xC0, 0x65
3	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256	0xC0, 0x66
4	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384	0xC0, 0x67
5	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256	0xC0, 0x68
6	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384	0xC0, 0x69
7	TLS_PSK_WITH_ARIA_128_GCM_SHA256	0xC0, 0x6A
8	TLS_PSK_WITH_ARIA_256_GCM_SHA384	0xC0, 0x6B
9	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256	0xC0, 0x6C
10	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384	0xC0, 0x6D
11	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256	0xC0, 0x6E
12	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384	0xC0, 0x6F
13	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256	0xC0, 0x70
14	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384	0xC0, 0x71

4.2. Cipher Suite 구성

4.2.1. 대칭 키 암호

ARIA 사용을 위해 본 절에서 제시하는 모든 Cipher Suite는 ARIA-CBC 또는 ARIA-GCM을 이용한다. Cipher Suite 표기에서 'ARIA_(키 길이)_CBC'와 'ARIA_(키 길이)_GCM'은 각각 데이터 암호화를 위한 대칭 키 암호로 해당 키 길이의 ARIA-CBC와 ARIA-GCM을 사용하는 것을 의미한다. ARIA를 기반 블록 암호로 하는 운영 모드의 구체적인 동작 방법은 부록Ⅰ의 [14]에 명시되어 있다.

ARIA의 블록 길이는 키 길이에 관계없이 128 비트이며, ARIA의 키, 블록, 그리고 운영 모드에서 사용하는 초기 벡터(IV)의 길이는 AES의 경우와 동일하다. 따라서 ARIA-CBC와 ARIA-GCM은 각각 AES-CBC, AES-GCM과 동일한 방식으로 동작하며, TLS에 적용하는 방법 또한 부록 Ⅰ의 [7], [8]에서 규정한 AES의 적용 방법을 준용한다.

4.2.2. 해시 함수와 MAC

4.1 절에서 제시한 모든 Cipher Suite는 HMAC의 기반 해시 함수로 SHA-256또는 SHA-384를 사용한다. Cipher Suite 표기에서 'SHA256'은 SHA-256, 'SHA384'는 SHA-384 해시 함수를 의미한다. TLS에서 HMAC은 Record Layer에서 데이터 무결성을 제공하는 용도와 Handshake Layer의 PRF를 구성하는 용도로 사용된다. PRF의 경우 TLS 1.2에서는 Cipher Suite에 표기된 해시 함수를 기반으로 하는 HMAC으로 구성하는 반면, TLS 1.1 이하 버전에서는 SHA-1 기반 HMAC과 MD5 기반 HMAC을 결합하는 방식으로 구성한다. 따라서 TLS 1.2를 기준으로 하위 버전과 호환이 필요할 경우 하위 버전의 PRF를 사용한다. 그리고 TLS 1.2에서 ARIA-GCM을 사용하는 Cipher Suite의 경우 해시 함수는 PRF에만 적용한다.

4.2.3. 키 설정 방식

본 절에서 제시하는 Cipher Suite 각각에 대응하는 키 설정 방식은 표 4.4와 같이 구분할 수 있다.

표 4.4 Cipher Suite와 키 설정 방식

Cipher Suite	키 설정 방식
TLS_RSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	RSA
TLS_DH_DSS_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DH_DSS
TLS_DH_RSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DH_RSA
TLS_DHE_DSS_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DHE_DSS
TLS_DHE_RSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DHE_RSA
TLS_DH_anon_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DH_anon
TLS_ECDH_ECDSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	ECDH_ECDSA
TLS_ECDH_RSA_WITH_ARIA_ARIA_128(256)_CBC/GCM_SHA256(384)	ECDH_RSA
TLS_ECDHE_ECDSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	ECDHE_ECDSA
TLS_ECDHE_RSA_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	ECDHE_RSA
TLS_ECDH_anon_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	ECDH_anon
TLS_PSK_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	PSK
TLS_DHE_PSK_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	DHE_PSK
TLS_RSA_PSK_WITH_ARIA_128(256)_CBC/GCM_SHA256(384)	RSA_PSK

키 설정 방식 'ECDH(E)_ECDSA', 'ECDH(E)_RSA', 'ECDH_anon'에 대한 상세 규격은 부록 Ⅰ의 [5]를 참조한다. 그리고 키 설정 방식 'PSK', 'DHE_PSK', 'RSA_PSK', 'ECDHE_PSK'에 대한 상세 규격은 부록 Ⅰ의 [4]를 참조한다.

4.3. 필수 Cipher Suite

TLS는 필수(mandatory) Cipher Suite로 'TLS_RSA_WITH_AES_128_CBC_SHA'를 지정하여, TLS를 통해 호환이 필요한 애플리케이션에서 반드시 구현하도록 권고하고 있다. 그러나 국내의 경우 국가 표준 블록 암호인 ARIA의 우선 적용이 필요한 환경이 있음을 고려하여, 이러한 환경에서 암호 제품 간의 기본적인 호환성을 보장할 수 있도록 별도의 필수 Cipher Suite를 다음과 같이 규정한다.

TLS_RSA_WITH_ARIA_128_CBC_SHA256

5. SRTP에서의 ARIA 사용 방법

ARIA와 AES는 키와 블록 길이, 그리고 운영 모드 사용 방법이 동일하며, ARIA 사용에 대한 특이한 제약 사항이 존재하지 않는다. 따라서 ARIA는 AES와 동일한 방법으로 SRTP에 적용할 수 있기 때문에, 부록 Ⅰ의 [2], [9], [11]에서 제시한 AES의 적용 방법을 준용한다. 본 절에서는 ARIA를 SRTP에서 사용하기 위한 방법을 설정하는 Cipher Suite를 제시한다.

5.1. Cipher Suite 목록

5.1.1. HMAC 기반 Cipher Suite

ARIA-CTR과 HMAC을 사용하는 Cipher Suite는 표 5.1과 같다.

표 5.1 HMAC 기반 Cipher Suite

번호	Cipher Suite	키 길이 (단위 : octet)		인증 태그 길이 (단위 : octet)
		블록 암호	HMAC	
1	ARIA_128_CTR_HMAC_SHA1_80	16	20	10
2	ARIA_128_CTR_HMAC_SHA1_32	16	20	4
3	ARIA_192_CTR_HMAC_SHA1_80	24	20	10
4	ARIA_192_CTR_HMAC_SHA1_32	24	20	4
5	ARIA_256_CTR_HMAC_SHA1_80	32	20	10
6	ARIA_256_CTR_HMAC_SHA1_32	32	20	4

5.1.2. AEAD 기반 Cipher Suite

인증 암호화 운영 모드를 사용하여 데이터 암호화를 수행하는 대칭 키 암호로 ARIA-CCM과 ARIA-GCM을 사용하는 Cipher Suite는 각각 표 5.2, 표 5.3과 같다.

표 5.2 ARIA-GCM 기반 Cipher Suite

번호	Cipher Suite	블록암호 키 길이 (단위 : octet)	인증 태그 길이 (단위 : octet)
1	AEAD_ARIA_128_GCM	16	16
2	AEAD_ARIA_256_GCM	32	16
3	AEAD_ARIA_128_GCM_8	16	8
4	AEAD_ARIA_256_GCM_8	32	8
5	AEAD_ARIA_128_GCM_12	16	12
6	AEAD_ARIA_256_GCM_12	32	12

표 5.3 ARIA-CCM 기반 Cipher Suite

번호	Cipher Suite	블록암호 키 길이 (단위 : octet)	인증 태그 길이 (단위 : octet)
1	AEAD_ARIA_128_CCM	16	16
2	AEAD_ARIA_256_CCM	32	16
3	AEAD_ARIA_128_CCM_8	16	8
4	AEAD_ARIA_256_CCM_8	32	8
5	AEAD_ARIA_128_CCM_12	16	12
6	AEAD_ARIA_256_CCM_12	32	12

5.2. Cipher Suite 구성

5.2.1. 대칭 키 암호

ARIA 사용을 위해 본 절에서 제시하는 모든 Cipher Suite는 ARIA-CTR 또는 ARIA-CCM, ARIA-GCM을 이용한다. Cipher Suite 표기에서 'ARIA_(키 길이)_CTR'은 데이터 암호화를 위한 대칭 키 암호로 해당 키 길이의 ARIA-CTR을 사용하는 것을 의미하며, 'AEAD_ARIA_(키 길이)_(운영 모드)'는 해당 키 길이의 ARIA-CCM 또는 ARIA-GCM을 대칭 키 암호로 사용하는 것을 의미한다. ARIA를 기반 블록 암호로 하는 운영 모드의 구체적인 동작 방법은 부록 I 의 [14]에 명시되어 있다.

ARIA의 블록 길이는 키 길이에 관계없이 128 비트이며, ARIA의 키, 블록, 그리고 운영

모드에서 사용하는 초기 벡터(IV)의 길이는 AES의 경우와 동일하다. 따라서 ARIA-CTR, ARIA-CCM, ARIA-GCM은 각각 AES-CM, AES-CCM, AES-GCM과 동일한 방식으로 동작하며, SRTP에 적용하는 방법 또한 부록 I 의 [2], [9], [11]에서 규정한 AES의 적용 방법을 준용한다.

5.2.2. 해시 함수와 MAC

5.1.1 절에서 제시한 Cipher Suite는 기밀성 운영 모드인 CTR을 사용하므로 데이터 무결성 제공을 위한 별도의 MAC 알고리즘을 함께 사용해야 한다. ARIA-CTR의 cipher suite는 SHA-1에 기반한 MAC 알고리즘 HMAC-SHA-1을 사용한다. Cipher Suite 표기에서 'HMAC-SHA1_(인증 태그 길이)'는 기반 해시 함수로 SHA-1을 사용하며 해당 길이의 인증 태그를 출력하는 HMAC을 MAC 알고리즘으로 사용하는 것을 의미한다. HMAC의 인증 태그 길이는 32 또는 80 비트로 한정한다.

반면 5.1.2 절에서 제시한 Cipher Suite는 인증 암호화 운영 모드를 사용하므로 별도의 MAC 알고리즘을 사용하지 않는다. SRTP에서 인증 암호화 운영 모드를 사용할 경우 인증 태그의 길이는 64, 92, 또는 128 비트로 한정한다.

5.2.3. 키 유도 함수

부록 I 의 [2]의 '4.3.3' 절에서는 CTR로 동작하는 AES-128을 키 유도 함수로 제시하고 이를 "AES-CM PRF"로 표기하였다. 부록 I 의 [9]에서는 CTR로 동작하는 AES-192와 AES-256을 키 유도 함수로 제시하고 이들을 각각 'AES_192_CM_PRF'와 'AES_256_CM_PRF'로 표기하였다. ARIA를 사용하는 키 유도 함수는 AES의 경우와 동일하게 구성하며, 키 길이에 따라 각각 ARIA_128_CTR_PRF, ARIA_192_CTR_PRF, 그리고 ARIA_256_CTR_PRF로 표기한다. ARIA Cipher Suite에서 사용하는 키 유도 함수는 표 5.4에서와 같이 대칭 키 암호와 동일한 키 길이를 가지는 ARIA-CTR PRF로 규정한다.

표 5.4 ARIA 기반 Cipher Suite와 키 유도 함수

번호	Cipher Suite	키 유도 함수
1	ARIA_128_CTR_HMAC_SHA1_80	ARIA_128_CTR_PRF
2	ARIA_128_CTR_HMAC_SHA1_32	ARIA_128_CTR_PRF
3	ARIA_192_CTR_HMAC_SHA1_80	ARIA_192_CTR_PRF
4	ARIA_192_CTR_HMAC_SHA1_32	ARIA_192_CTR_PRF
5	ARIA_256_CTR_HMAC_SHA1_80	ARIA_256_CTR_PRF
6	ARIA_256_CTR_HMAC_SHA1_32	ARIA_256_CTR_PRF
7	AEAD_ARIA_128_GCM	ARIA_128_CTR_PRF
8	AEAD_ARIA_256_GCM	ARIA_256_CTR_PRF

번호	Cipher Suite	키 유도 함수
9	AEAD_ARIA_128_GCM_8	ARIA_128_CTR_PRF
10	AEAD_ARIA_256_GCM_8	ARIA_256_CTR_PRF
11	AEAD_ARIA_128_GCM_12	ARIA_128_CTR_PRF
12	AEAD_ARIA_256_GCM_12	ARIA_256_CTR_PRF
13	AEAD_ARIA_128_CCM	ARIA_128_CTR_PRF
14	AEAD_ARIA_256_CCM	ARIA_256_CTR_PRF
15	AEAD_ARIA_128_CCM_8	ARIA_128_CTR_PRF
16	AEAD_ARIA_256_CCM_8	ARIA_256_CTR_PRF
17	AEAD_ARIA_128_CCM_12	ARIA_128_CTR_PRF
18	AEAD_ARIA_256_CCM_12	ARIA_256_CTR_PRF

5.3. 필수 Cipher Suite

SRTP에서는 필수 Cipher Suite로 'AES_CM_128_HMAC_SHA1_80'을 지정하여, 호환이 필요한 애플리케이션에서 반드시 구현하도록 권고하고 있다. 그러나 국내의 경우 국가 표준 블록 암호인 ARIA의 우선 적용이 필요한 환경이 있음을 고려하여, 이러한 환경에서 암호 제품 간의 기본적인 호환성을 보장할 수 있도록 별도의 필수 Cipher Suite를 다음과 같이 규정한다.

ARIA_128_CTR_HMAC_SHA1_80

6. SRTP의 키 관리 프로토콜에서 ARIA Cipher Suite 파라미터 설정

6.1. MIKEY

부록 Ⅰ의 [3]의 '6.1' 절에는 MIKEY를 키 관리 프로토콜로 사용하여 프로토콜 참여자가 SRTP의 Cipher Suite 설정을 공유하기 위해 필요한 파라미터를 규정하고 있다. 각 파라미터는 형(Type)과 값(Value) 항목으로 구성되며, 일부 파라미터 형(Type)에 대한 값(Value)의 사전 지정이 필요한 경우는 IANA에서 참조값으로 할당한다.

표 6.1에서는 암호화 알고리즘 파라미터(Type 0)에 추가할 ARIA 운영 모드와 그에 대한 참조값 및 기본 키 길이를 명시한다. 기본 키 길이는 세션 암호화 키 길이 파라미터(Type 1)에 값이 명기되지 않았을 경우에 사용하는 값이다.

표 6.1 MIKEY의 SRTP 암호화 알고리즘 파라미터

SRTP 암호화 알고리즘	참조값	기본 키 길이 (단위 : octet)
ARIA-CTR	-	16
ARIA-CCM	-	16
ARIA-GCM	-	16

참고 1) 표 6.1에서 제시한 각각의 SRTP 암호화 알고리즘에 대한 참조값은 부록 Ⅰ의 [12]가 IETF RFC로 출판되는 시점에 IANA에 의해 할당될 예정이다. 본 표준에서는 추후 IANA에 의해 할당되는 참조값을 준용한다.

SRTP 암호화 알고리즘으로 ARIA-CTR을 선택할 경우, 인증 알고리즘 파라미터(Type 2)에서 'HMAC-SHA-1'(Value 1)을 선택하고 인증 태그 길이 파라미터(Type 11)에서 설정하는 값을 HMAC-SHA-1 계산값의 길이로 사용한다. 해당 Cipher Suite에 대한 관련 MIKEY 파라미터 값을 정리하면 표 6.2와 같다.

표 6.2 ARIA-CTR Cipher Suite에 대한 MIKEY 파라미터

Cipher Suite	SRTP 암호화 알고리즘	키 길이 (단위 : octet)	인증 태그 길이 (단위 : octet)
ARIA_128_CTR_HMAC_SHA1_80	ARIA-CTR	16	10
ARIA_128_CTR_HMAC_SHA1_32	ARIA-CTR	16	4
ARIA_192_CTR_HMAC_SHA1_80	ARIA-CTR	24	10
ARIA_192_CTR_HMAC_SHA1_32	ARIA-CTR	24	4
ARIA_256_CTR_HMAC_SHA1_80	ARIA-CTR	32	10
ARIA_256_CTR_HMAC_SHA1_32	ARIA-CTR	32	4

반면 ARIA-CCM이나 ARIA-GCM을 선택할 경우 인증 알고리즘 파라미터(Type 2)는 'NULL'(Value 0)을 선택하며, 인증 태그의 길이는 AEAD 인증 태그 길이 파라미터(Type 미정)에서 설정한 값을 사용한다. 해당 Cipher Suite에 대한 관련 MIKEY 파라미터 값을 정리하면 표 6.3과 같다.

표 6.3 AEAD_ARIA Cipher Suite에 대한 MIKEY 파라미터

Cipher Suite	SRTP 암호화 알고리즘	키 길이 (단위 : octet)	AEAD 인증 태그 길이 (단위 : octet)
AEAD_ARIA_128_GCM	ARIA-GCM	16	16
AEAD_ARIA_256_GCM	ARIA-GCM	32	16

Cipher Suite	SRTP 암호화 알고리즘	키 길이 (단위 : octet)	AEAD 인증 태그 길이 (단위 : octet)
AEAD_ARIA_128_GCM_8	ARIA-GCM	16	8
AEAD_ARIA_256_GCM_8	ARIA-GCM	32	8
AEAD_ARIA_128_GCM_12	ARIA-GCM	16	12
AEAD_ARIA_256_GCM_12	ARIA-GCM	32	12
AEAD_ARIA_128_CCM	ARIA-CCM	16	16
AEAD_ARIA_256_CCM	ARIA-CCM	32	16
AEAD_ARIA_128_CCM_8	ARIA-CCM	16	8
AEAD_ARIA_256_CCM_8	ARIA-CCM	32	8
AEAD_ARIA_128_CCM_12	ARIA-CCM	16	12
AEAD_ARIA_256_CCM_12	ARIA-CCM	32	12

참고 2) AEAD 인증 태그 길이 파라미터의 Type은 부록 Ⅰ의 [11]에서 신규 제안하여 표준화가 진행 중이며, 완료 후 IANA에서 할당하는 Type을 본 표준에서도 준용한다.

SRTP의 키 유도 함수를 MIKEY를 통해 공유하기 위해서는 키 유도 함수 파라미터(Type 5)에 지정되는 참조값을 사용해야 한다. 이때 키 유도 함수에 사용되는 키의 길이는 세션 암호화 키 길이 파라미터(Type 1)에 설정한 값을 사용한다.

표 6.4 MIKEY의 SRTP 키 유도 함수 파라미터

SRTP 키 유도 함수	참조값
ARIA-CTR	–주1)

주 1) 표 6.4에서 제시한 SRTP 키 유도 함수의 참조값은 표 6.1의 경우와 같이 부록 Ⅰ의 [12]가 IETF RFC로 출판되는 시점에 IANA에 의해 할당될 예정이다. 본 표준에서는 추후 IANA에 의해 할당되는 참조값을 준용한다.

6.2. SDES

SDES를 SRTP의 키 관리 프로토콜로 사용할 때 프로토콜 참여자가 5 절에서 제시한 Cipher Suite를 협상하기 위해서는, 부록 Ⅰ의 [6]에서 제시한 'SRTP Crypto Suite Registrations'에 해당 Cipher Suite를 다음과 같이 추가시켜야 한다.


```
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" /
                         "AEAD_ARIA_128_GCM_8" /
                         "AEAD_ARIA_256_GCM_8" /
                         "AEAD_ARIA_128_GCM_12" /
                         "AEAD_ARIA_256_GCM_12" /
                         "AEAD_ARIA_128_CCM" /
                         "AEAD_ARIA_256_CCM" /
                         "AEAD_ARIA_128_CCM_8" /
                         "AEAD_ARIA_256_CCM_8" /
                         "AEAD_ARIA_128_CCM_12" /
                         "AEAD_ARIA_256_CCM_12" /
                         srtp-crypto-suite-ext
```

7. 안전성 관련 고려 사항

블록 암호 ARIA는 현재까지 안전성과 관련하여 어떠한 취약점도 발견되지 않았으며, 현재까지 ARIA에 대한 최선의 공격은 키 전수 조사 방법이다. ARIA-GCM의 안전성과 관련하여 주의해야 할 부분은 초기 벡터(IV)의 사용이다. AES-GCM을 TLS 1.2에서 사용하기 위한 확장규격인 부록 Ⅰ의 [8]에서 초기 벡터(IV) 적용 방법에 대해 구체적으로 기술하고 있으며, ARIA-GCM도 이를 준용한다.

해시 함수 충돌쌍 공격에 의해 SHA-1의 안전성이 저하되었지만 아직 SHA-256과 SHA-384는 충분한 내성을 가지고 있다. SHA-1을 기반 해시 함수로 사용하는 HMAC은 아직 취약점이 발견되지 않았지만, 현재 SHA-1의 사용이 점차 배제되고 있는 점을 감안하여 본 표준에서 제시하는 TLS Cipher Suite는 SHA-256 또는 SHA-384를 사용한다. 반면 멀티미디어 데이터를 다루는 SRTP의 특성을 고려하여 SRTP Cipher Suite는 SHA-1의 사용을 유지한다.

SRTP의 키 관리 프로토콜로 SDES를 사용할 경우, SDES 자체에 암호 속성 보호를 위한 방법이 없기 때문에 TLS, IPsec, S/MIME 등 별도의 보안 프로토콜을 함께 사용해야 한다.

부 록 I
관련 문헌

다음 문서들은 본 표준의 이해를 돕기 위한 문서로서 특정 문서(발행일 및 판 번호 또는 개정 번호를 명시한 것)와 일반 문서로 구별된다.

- 특정 문서인 경우 해당 판본 이후의 개정판은 적용되지 않는다.
- 일반 문서인 경우 최신 판본이 적용된다.

[1] IETF RFC 3550, 'RTP: A Transport Protocol for Real-time Applications', 2003.

[2] IETF RFC 3711, 'The Secure Real-time Transport Protocol (SRTP)', 2004.

[3] IETF RFC 3830, 'MIKEY: Multimedia Internet KEYing', 2004.

[4] IETF RFC 4279, 'Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)', 2006.

[5] IETF RFC 4492, 'Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)', 2006.

[6] IETF RFC 4568, 'Session Description Protocol (SDP) Security Descriptions for Media Streams', 2006.

[7] IETF RFC 5246, 'The TLS protocol v1.2', 2008.

[8] IETF RFC 5288, 'AES Galois Counter Mode (GCM) Cipher Suites for TLS', 2008.

[9] IETF RFC 6188, 'The Use of AES-192 and AES-256 in Secure RTP', 2011.

[10] IETF RFC 6209, 'Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)', 2011.

[11] I-D.ieft-avtcore-srtp-aes-gcm, 'AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)', 2013.

[12] I-D.ietf-avtcore-aria-srtp, 'The ARIA Algorithm and Its Use with Secure Real-time Transport Protocol (SRTP)', 2013.

[13] KS X 1213-1, '128비트 블록 암호 알고리즘 ARIA - 제1부: 일반', 2009.

[14] KS X 1213-2, '128비트 블록 암호 알고리즘 ARIA - 제2부: 운용 모드', 2009.

방송통신표준

TLS·SRTP·MIKEY에서 블록 암호 ARIA 활용 방법
(The Use of the Block Cipher ARIA in TLS·SRTP·MIKEY)

발행인 : 미래창조과학부 장관
발행처 : 미래창조과학부 국립전파연구원
140-848, 서울 용산구 원효로41길 29
발행일 : 2013.12.
국립전파연구원 고시 제 2013-20호