Korea Communications Standard

방송통신표준

KCS.KO-12.2000 제정일: 2013년 12월 31일

TLS·SRTP·MIKEY에서 블록 암호 SEED 활용 방법

The Use of SEED Algorithm in TLS·SRTP·MIKEY

미래창조과학부

국립전파연구원

방송통신표준

KCS.KO-12.2000 제정일: 2013년 12월 31일

TLS·SRTP·MIKEY에서 블록 암호 SEED 활용 방법

The Use of SEED Algorithm in TLS·SRTP·MIKEY

미래창조과학부

국립전파연구원

서 문

1. 표준의 목적

본 표준은 웹 서비스 또는 인터넷 전화 서비스 제공 시 도청 등 사이버 침해 사고 예방을 목적으로 적용하는 보안 프로토콜인 TLS(Transport Layer Security), SRTP(Secure Real-time Transport Protocol) 및 SRTP를 위한 키 관리 알고리즘인 MIKEY(Multimedia Internet KEYing)와 SDES(Session Description Protocol Security Descriptions for Media Streams)에서의 국산 암호 알고리즘인 SEED를 활용할 수 있도록 하는 데 그 목적이 있다.

2. 주요 내용 요약

본 표준은 서버와 클라이언트 간의 암호 통신을 위한 프로토콜인 TLS와 멀티미디어 데이터 전송 규격 RTP(Real-time Transport Protocol)를 위한 보안 프로토콜인 SRTP 및 SRTP를 위한 키 관리 프로토콜인 MIKEY와 SDES에서 블록 암호 SEED를 사용하기 위한 Cipher Suite를 기술한다. 구체적으로 살펴보면, TLS의 경우 데이터 암호화에 사용할 대칭 키 암호 알고리즘으로 SEED를 운용하는 규격을 기술한다. 또한 SRTP의 경우 RTP와 RTCP(Real-time Transport Control Protocol) 트래픽 암호화와 키 유도에 사용할 대칭 키 암호 알고리즘으로 SEED를 사용하는 Cipher Suite를 기술한다. 그리고 SRTP에서 정의한 SEED 규격을 SRTP의 키 관리 프로토콜인 MIKEY와 SDES에서 활용하기 위한 참조 값과 파라미터를 명시한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

TLS와 SRTP는 국내 웹 서비스와 인터넷 전화 서비스의 보안 기능 제공을 위해 일반적으로 적용되는 프로토콜이다. 본 표준은 SEED 암호 알고리즘을 사용하는 TLS 또는 SRTP의 직접 적용 또는 호환이 필요한 정보보호 시스템 및 암호 제품에 다양하게 활용되어 국내 정보통신망의 안정성과 신뢰성을 제고할 수 있다.

4. 참조 표준(권고)

4.1. 국외 표준(권고)

해당 사항 없음.

4.2. 국내 표준

- TTAS.IF-RFC4162, ‘TLS를 위한 SEED 암호알고리즘’, 2006.12.
- TTAE.IF-RFC5669, ‘SRTP에서의 SEED알고리즘 운영방법’, 2011.12.
- TTAE.IF-RFC5748, ‘MIKEY에서 SEED알고리즘 사용을 위한 파라미터 정의’, 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 TLS와 SRTP를 대상으로 SEED를 적용하는 방법을 제시한 ‘TTAS.IF-RFC4162’와 ‘TTAE-IF-RFC5669’, 그리고 ‘TTAE-IF-RFC5748’을 병합하여 작성하였다.

5.2. 참조한 표준(권고)과 본 표준의 비교표

KCS.KO-12.2000	참조 표준			비고
	TTAS.IF-RFC4162	TTAE.IF-RFC5669	TTAE.IF-RFC5748	
1. 개요	1. 개요	1. 개요	1. 개요	병합
2. 표준의 구성 및 범위	1. 개요	1. 개요	1. 개요	병합
3. 용어 정의 및 약어	1. 개요	1. 개요	1. 개요	병합
4. TLS에서의 SEED 암호 사용 방법	2. Cipher Suite	-	-	동일
5. SRTP에서의 SEED 암호 사용 방법	-	2. 암호 알고리즘	-	1, 2 절에 포함
-	-	3. Nonce 형태	-	1, 2 절에 포함
-	-	4. 키 유도 함수		3 절에 포함
-	-	5. 필수 구현 규격	-	4 절에 포함
6. SRTP를 위한 키 관리 프로토콜에서 SEED 암호 사용 방법		6. IANA 고려 사항	4. IANA 고려 사항	병합

6. 지식 재산권 관련 사항

본 표준의 ‘지적 재산권 확약서’ 제출 현황은 국립전파연구원 웹사이트에서 확인할 수 있다.

※본 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 여부(해당 시험 표준 번호)

해당 사항 없음.

8. 표준의 이력 정보

8.1. 표준의 이력

판 수	제정·개정일	제정·개정 내역
제1판	2013.12.31.	제정 KCS.KO-12.2000

8.2. 주요 개정 사항

해당 사항 없음.

Preface

1. Purpose of Standard

To facilitate the interoperability of SEED algorithm when used in security protocols for preventing eavesdropping and tampering against Web or VoIP services, this standard describes Cipher Suite for the use of SEED algorithm in TLS(Transport Layer Security) protocol, SRTP(Secure Real-time Transport Protocol), MIKEY(Multimedia Internet KEYING) and SDES(Session Description Protocol(SDP) Security Descriptions for Media Streams).

2. Summary of Contents

This standard describes how SEED can be used for providing security services in TLS and SRTP. TLS 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 is a cryptographic protocol that provides several security services on a standardized packet format for delivering audio and video over IP network.

First, this standard defines Cipher Suite for the TLS protocol that use the SEED algorithm as symmetric key cipher for data encryption. To negotiate proper SEED based Cipher Suite in TLS handshake layer, additionally, this standard defines values assigned to each Cipher Suite.

Next, this standard defines new Cipher Suite for SRTP that use the SEED algorithm as symmetric key cipher for RTP and RTCP payload encryption and key derivation function. This standard also defines identifiers and parameters to be used in key management protocols MIKEY and SDES for negotiating Cipher Suite for SRTP.

3. Applicable Fields of Industry and its Effect

TLS and SRTP are commonly applied as main cryptographic protocols for providing security services on Web or Voice over IP networks in Korea. This standard may be applied to various information security systems and cryptographic equipments, requiring operations of TLS or SRTP which use SEED 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

- TTAS.IF-RFC4162, “The SEED Cipher Algorithm for Transport Layer Security (TLS)”, 2006.12
- TTAE.IF-RFC5669, “The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)”, 2011.12.
- TTAE.IF-RFC5748, “IANA Registry Update for the SEED Cipher Algorithm Support in the Multimedia Internet KEYing (MIKEY)”, 2011.12.

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

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

This standard describes cipher sutes to use TLS, SRTP, MIKEY and SDES based on the IETF RFC 4162, IETF RFC 5669, IETF RFC 5748.

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

KCS.KO-12.2000	Reference Standards			Remarks
	TTAS.IF-RFC4162	TTAE.IF-RFC5669	TTAE.IF-RFC5748	
1. Introduction	1. Introduction	1. Introduction	1. Introduction	Merged
2. Constitution and Scope	1. Introduction	1. Introduction	1. Introduction	Merged
3. Terms Definition and Abbreviations	1. Introduction	1. Introduction	1. Introduction	Merged
4. The Use of SEED in TLS	2. Proposed Cipher Suites	-	-	Equivalent
5. The Use of SEED in SRTP	-	2. Cryptographic Transforms	-	Condensed in Sec.1 and 4
-	-	3. Nonce Format	-	Condensed in Sec.1 and 4

-	-	4. Key Derivation Function		Condensed in Sec.3
-	-	5. Mandatory -to-Implement Transforms	-	Condensed in Sec.4
6. The Use of SEED in SRTP Key Management Protocol		6. IANA Considerations	4. IANA Considerations	Merged

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. History of Standard

8.1. Change History

Edition	Issued date	History
The 1st edition	2013.12.31.	Established KCS.KO-12.2000

8.2. Revisions Related Details

None

목 차

Contents

TLS·SRTP·MIKEY에서의 블록 암호 SEED 활용 방법 (The Use of SEED Algorithm 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 적용되는 프로토콜이다. 따라서 국산 암호 알고리즘인 SEED를 해당 프로토콜에서 사용하기 위해서는 각 프로토콜에 맞게 Cipher Suite를 정의할 필요가 있다. 본 표준에서는 TLS, SRTP 및 SRTP를 위한 키 관리 프로토콜인 MIKEY(Multimedia Internet KEYing) 및 SDES (Session Description Protocol Security Descriptions for Media Streams)에서 SEED를 적용하기 위한 관련 규격을 기술한다.

2. 표준의 구성 및 범위

본 표준은 TLS(Transport Layer Security)와 SRTP(Secure Real-time Transport Protocol)에서 SEED를 사용하기 위한 규격과 SRTP의 키 관리 프로토콜인 MIKEY 및 SDES에서 이를 식별하기 위한 참조값을 제시한다. 4절은 TLS에서 SEED를 사용하기 위한 규격을 기술하고, 5절에서는 SRTP에서 SEED를 사용하기 위한 규격을 기술한다. 마지막 6절에서는 SRTP의 키 관리 프로토콜로 MIKEY(Multimedia Internet KEYing) 및 SDES(Session Description Protocol Security Descriptions for Media Streams)를 사용할 경우 SEED 규격을 식별하기 위해 필요한 파라미터와 참조값을 명시한다.

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 인증을 동시에 제공하는 운영 모드를 지칭하며 대표적인 예로 CCM, GCM이 있음

AES (Advanced Encryption Standard)	국제 공모 사업을 통해 개발된 미국 연방정부 표준 블록 암호 알고리즘으로 블록 길이는 128 비트이고 키 크기는 128, 192, 256 비트를 지원함. 키 크기에 따라 규격의 차이가 있기 때문에 이를 구분할 경우 AES-128, AES-192, AES-256으로 표기
CCM (Counter with CBC-MAC)	블록 암호 운영 모드 중의 하나로 카운터 모드와 블록 암호 기반 메시지 인증 코드 CBC-MAC을 조합하여 암호문과 인증 태그를 계산함으로써 기밀성과 인증을 동시에 제공할 수 있도록 설계됨
GCM (Galois/Counter Mode)	블록 암호 운영 모드 중의 하나로 카운터 모드와 유한체 곱셈으로 정의된 특화된 인증값 계산 함수를 조합하여 암호문과 인증 태그를 계산함으로써 기밀성과 인증을 동시에 제공할 수 있도록 설계됨
HMAC (Keyed-Hash Message Authentication Code)	해시 함수 기반 메시지 인증 코드
SEED	민간 부분인 인터넷, 전자 상거래, 무선 통신 등에서 공개 시에 민감한 영향을 미칠 수 있는 정보와 개인 프라이버시 등을 보호하기 위하여 개발된, 블록 단위로 메시지를 처리하는 대칭키 블록 암호 알고리즘
SHA (Secure Hash Algorithm)	미국 연방정부 표준 해시 함수로 현재 7 개의 알고리즘으로 구성. 알고리즘은 출력값의 크기에 따라 각각 SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-224/512, SHA-256/512로 구분하며, 내부함수 구조나 초기값 등의 차별 요소가 존재
MIKEY (Multimedia Internet KEYing)	SRTP와 같은 실시간 멀티미디어 보안 프로토콜을 지원하는 일대다(One-to-Many) 또는 소규모 상호 작용형 그룹에 적합한 키 관리 프로토콜
RTP (Real-time Transport Protocol)	인터넷상의 오디오와 비디오 같은 멀티미디어 데이터를 실시간으로 전송하기 위해 설계된 표준 패킷 구조

SDES (Session Description Protocol Security Descriptions for Media Streams)	SRTP에서 사용되는 암호 키를 교환하기 위한 프로토콜
SRTP (Secure RTP)	RTP의 암호화, 메시지 인증, 재전송 공격 방어 등의 정보 보호 서비스를 제공하기 위한 프로토콜
카운터 모드 (CTR, Counter mode)	블록 암호 운영 모드 중의 하나로, 블록 단위로 증가하는 카운터(counter)를 블록암호 입력값으로 하여 얻어진 연속된 출력값을 평문과 XOR하여 암호화를 수행
해시 함수	임의의 크기의 메시지를 일정 크기의 출력값으로 압축하는 알고리즘

3.2. 약어

AAD	Additional Authentication Data
AES-CM	AES in Counter Mode
CBC	Cipher Block Chaining
DH	Diffie-Hellman
DHE	Ephemeral Diffie-Helman
DSS	Digital Signature Standard
IETF	Internet Engineering Task Force
MAC	Message Authentication Code
PRF	Pseudo Random Function
RTCP	RTP Control Protocol
SRTCP	Secure RTP Control Protocol
SSRC	Synchronization Source
TLS	Transport Layer Security
VoIP	Voice over IP

4. TLS에서의 SEED 암호 사용 방법

본 절에서는 SEED 알고리즘을 TLS에서 사용하기 위한 규격을 기술한다. TLS에서 SEED의 사용은 AES와 동일하며, 특별한 제약 사항이 존재하지 않는다.

4.1. Cipher Suite 정의

```
CipherSuite TLS_RSA_WITH_SEED_CBC_SHA        = { 0x00, 0x96};
CipherSuite TLS_DH_DSS_WITH_SEED_CBC_SHA     = { 0x00, 0x97};
CipherSuite TLS_DH_RSA_WITH_SEED_CBC_SHA     = { 0x00, 0x98};
CipherSuite TLS_DHE_DSS_WITH_SEED_CBC_SHA    = { 0x00, 0x99};
CipherSuite TLS_DHE_RSA_WITH_SEED_CBC_SHA    = { 0x00, 0x9A};
CipherSuite TLS_DH_anon_WITH_SEED_CBC_SHA    = { 0x00, 0x9B};
```

4.2. Cipher Suite 구성

4.2.1. 암호 알고리즘

SEED 알고리즘 사용을 위해 정의하는 운영 모드는 CBC이며 키 크기는 128 비트이다.

4.2.2. 해시 함수

4.1 절에서 제시한 Cipher Suite는 HMAC에 사용할 기반 해시 함수로 SHA-1을 사용하며, 구성은 부록 Ⅰ.[4]의 5절에 기술되어 있다.

4.2.3. 키 교환

Cipher Suite는 인증서와 키 교환 방법에 의해 달라진다. 본 절에서 제시한 방법은 부록 Ⅰ.[4]의 7.4.2 절과 7.4.3 절을 참고한다.

Cipher Suite	키 교환 알고리즘
TLS_RSA_WITH_SEED_CBC_SHA	RSA
TLS_DH_DSS_WITH_SEED_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_SEED_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE_RSA
TLS-DH-anon-WITH SEED_CBC_SHA	DH_anon

5. SRTP에서의 SEED 암호 사용 방법

본 절에서는 SEED 알고리즘을 SRTP에서 사용하기 위한 Cipher Suite를 기술한다. SEED 알고리즘은 블록 암호의 운용 모드 사용에 제한이 없으며, AES와 동일한 방법으로 SRTP에 적용할 수 있기 때문에, AES의 적용 방법을 준용한다. 본 절에서 제시하는 SRTP의 Cipher Suite는 운영 모드에 따라 세 가지로 분류할 수 있다.

5.1. SEED-CTR

AES-128을 카운터 모드(CTR)로 동작시켜 RTP/RTCP 패킷을 암호화하는 방법은 SRTP 표준에 기술되어 있으며, SEED-CTR은 AES-CM과 동일한 방식으로 SRTP에 적용할 수 있다. CTR은 기밀성 운영 모드이기 때문에 SEED-CTR을 사용할 경우, 데이터 무결성 제공을 위한 별도의 MAC 알고리즘을 같이 사용해야 한다. SEED-CTR의 Cipher Suite는 SHA-1에 기반한 MAC 알고리즘 HMAC-SHA1을 사용한다. SEED-CTR의 Cipher Suite는 다음과 같다.

SEED_128_CTR_HMAC_SHA1_80

5.2. SEED-CCM과 SEED-GCM

AES를 인증 암호화 운영 모드인 GCM 또는 CCM으로 동작시켜 RTP/RTCP 패킷을 암호화하는 방법은 부록 Ⅰ-[7]에 기술되어 있다. SEED 알고리즘을 GCM이나 CCM과 결합(SEED-CCM/SEED-GCM)하여 SRTP에서 사용하는 방법은 각각 AES의 경우와 동일하며, Cipher Suite는 다음과 같다.

SEED_128_CCM_80
SEED_128_GCM_96

5.2.1. 관련 파라미터

본 절에서는 SRTP를 위한 운영 모드 중 하나인 CCM 모드를 기술한다. CCM 모드는 다음 2 가지 파라미터를 사용한다.

- M : 인증 태그의 사이즈로서, SRTP에서 인증 태그의 길이는 80 bits(10 octets)이므로, SEED-CCM에서 M의 크기는 10이다.
- L : 길이 필드의 사이즈로서, Nonce의 크기는 15-L로 계산됨. SEED-CCM에서 Nonce 크기는 12 octets이므로 L의 크기는 3이다.

또한 4 개의 파라미터를 입력값으로 사용한다.

o Key : 인증 태그 계산 및 페이로드 암호화에 사용되는 키로서, SEED는 128 bits의 키 길이를 이용한다.
o Nonce : 난수로서 SEED-CCM에서 난수의 길이는 96 bits(12 octets)이다.
o Plaintext : SRTP에서는 RTP 패킷의 페이로드 및 패팅, RTP pad count 필드가 해당된다. SRTCP에서는 Encryption flag가 1로 세팅되어 있는 경우에 부록 Ⅰ-[7]의 'Figure 2: AEAD inputs from an SRTP packet'에서 기술하고 있는 부분이 평문이며, encryption flag가 0으로 세팅되어 있는 경우에는 사용되지 않는다.
o AAD(Additional Authentication Data) : 인증 태그 계산에 사용될 추가 데이터로서, SRTP에서는 RTP 패킷의 헤더를 나타낸다. SRTCP에서는 encryption flag가 0으로 세팅되어 있는 경우에 부록 Ⅰ-[7]의 'Figure 2: AEAD inputs from an SRTP packet'에서 기술하고 있는 부분이 AAD이며, 1로 세팅되어 있는 경우에는 첫 번째 8 octets과 encryption flag, SRTCP index가 AAD이다.

GCM 모드에서 입력값으로 사용되는 4 개의 파라미터는 CCM 모드에서 기술된 값을 그대로 사용한다. 단, GCM 모드의 인증 태그의 길이는 표준에서 기술한 바와 같이 96 bits를 이용한다.

5.2.2. Nonce 형태

o SRTP를 위한 난수 형태

Nonce = (16 bits of zeroes || SSRC || ROC || SEQ) XOR Salt

SSRC와 SEQ는 RTP 헤더에 포함되어 있으며, Salt 값은 SRTP 키 유도 함수(Key Derivation Function)로부터 얻는다.

o SRTCP를 위한 난수 형태

Nonce = (16 bits of zeroes || SSRC || 16 bits of zeroes ||
SRTCP index) XOR Salt

SSRC와 SEQ는 RTP 헤더에 포함되어 있다. SRTCP index는 각각의 패킷으로부터 얻으며, Salt 값은 SRTP 키 유도 함수(Key Derivation Function)로부터 얻는다.

5.3. 키 유도 함수

부록 Ⅰ-[1]의 4.3.3 절에서는 AES-128을 CTR로 동작하는 의사 난수 함수를 기술하고 이를 AES-CM PRF로 표기하였다. SEED-CTR에서 사용되는 의사 난수 함수는 AES에서 사용하고 있는 의사 난수 함수와 동일한 형태를 가진다.

5.4. 필수 Cipher Suite

SRTP를 위한 SEED 운영 모드 중 반드시 구현해야 할 모드로서, 데이터 암호는 SEED-CTR이며, 데이터 무결성을 위한 인증 메커니즘은 HMAC-SHA1이다.

구분	필수	선택	기본
암호화	SEED-CTR	SEED-CCM, SEED-GCM	SEED-CTR
메시지 무결성	HMAC-SHA1	SEED-CCM, SEED-GCM	HMAC-SHA1
의사 난수 함수	SEED-CTR	-	SEED-CTR

6. SRTP를 위한 키 관리 프로토콜에서 SEED 암호 사용 방법

6.1. MIKEY

본 절에서는 SRTP 암호화에 사용되는 암호 알고리즘 및 운영 모드에 대한 값을 기술한다. SEED 암호 알고리즘을 사용하기 위해서는 기술된 값은 아래와 같다.

SRTP 암호 알고리즘	값
NULL	0
AES-CM	1
AES-F8	2
SEED-CTR	3
SEED-CCM	4
SEED-GCM	5

또한 SRTP 암호화에 사용되는 세션 키, 인증 키, Salt 키를 생성하는 키 유도 함수에 대한 값을 기술한다. MIKEY에서 SEED-CTR을 사용하기 위해서는 기술된 값은 아래와 같다.

SRTP 키 유도 함수	값
AES-CM	1
SEED-CTR	2

6.2. SDES

SDES에서 SEED 알고리즘을 사용하기 위한 관련 파라미터는 다음과 같다.

srtp-crypto-suite-ext = “SEED_CTR_128_HMAC_SHA1_80”/
“SEED_128_CCM_80”/
“SEED_128_GCM_96”/
srtp-crypto-suite-ext

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 3711, 'The Secure Real-time Transport Protocol (SRTP)', 2004.
[2] IETF RFC 4162, 'Addition of SEED Cipher Suites to Transport Layer Security (TLS)', 2005.
[3] IETF RFC 4269, 'The SEED Encryption Algorithm', 2005.
[4] IETF RFC 5246, 'The TLS protocol v1.2', 2008.
[5] IETF RFC 5669, 'The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)', 2010.
[6] IETF RFC 5748, 'IANA Registry Update for Support of the SEED Cipher Algorithm in Multimedia Internet KEYing (MIKEY)', 2010.
[7] I-D.ieft-avtcore-srtp-aes-gcm, 'AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)', 2013.
[8] TTAS.KO-12.0004/R1, '128비트 블록암호알고리즘 SEED', 2005.12.

방송통신표준

TLS·SRTP·MIKEY에서 블록 암호 SEED 활용 방법
(The Use of SEED Algorithm in TLS·SRTP·MIKEY)

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