FBMF Standard

미래방송미디어표준포럼표준 (국문표준)

FBMF-STD-003 제정일: 2017 년 06 월 15 일

IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Transport Layer Security 규격

Transport Layer Security

Specifications for

IP-based Multi-CA/DRM Content Protection

FBMF

미래방송미디어표준포럼

Future Broadcast and Media Standards Forum

표준초안 검토 위원회	**방송콘텐츠보호기술WG**				
표준안 심의 위원회	**미래방송미디어표준포럼 운영위원회**				
	성명	**소 속**	**직위**	**위원회 및 직위**	**표준번호**
표준(과제) 제안	구한승	ETRI	책임연구원	방송콘텐츠보호기술WG 의장	FBMF-STD-003
표준 초안 작성자	구한승	ETRI	책임연구원	방송콘텐츠보호기술WG 의장	
	이주한	한양대	-	-	
사무국 담당	김제우	KETI	수석연구원	미래방송미디어표준포럼 운영위원회 간사	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 FBMF 웹사이트에서 확인할 수 있습니다.

본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 미래방송미디어표준포럼 의장

발행처 : 미래방송미디어표준포럼

135-703, 서울시 강남구 테헤란로 7길 22 본관 610호 (역삼동 한국과학기술회관)

Tel : 02-568-3556, Fax : 02-568-3557

발행일 : 2017.5.15.

서 문

1 표준의 목적

본 표준은 다운로드 방식 기반 멀티 CA/DRM (Conditional Access/Digital Rights Management) 솔루션 기술과 관련해 국제 표준인 ITU-T J. 1010및 ITU-T J.1011과 유럽 표준인 ETSI ISG ECI를 기반으로 하여 한국 상황에 맞는 IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Transport Layer Security 규격 정의를 목적으로 한다.

2 주요 내용 요약

본 표준은 CPE(Customer Premises Equipment)가 신뢰 환경에서 CA/DRM 클라이언트를 다운로드 하기 위한 교환 가능한 IMCP (IP-based Multi-CA/DRM Content Protection) 시스템의 TLS (Transport Layer Security) 규격을 명시한다. IMCP 시스템에서 콘텐츠는 지상파방송(over-the-air)뿐만 아니라 IP기반의 광대역 채널을 통해서도 전송된다. TLS은 IMCP 클라이언트와 IMCP 서버 간의 또는 IMCP 클라이언트와 IMCP 클라이언트간의 양방향 채널을 통한 보안 연결을 보장한다. IMCP 시스템은 TLS을 통해 통신하는 두 피어(peer)간의 인증 및 암호화 통신을 제공한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

본(이) 표준은 참조 표준 문서들을 기반으로 하여 한국 지상파 방송 현황에 맞춰서 IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Transport Layer Security 규격을 정의하였다.

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Architecture, Definitions and Overview”, 2016.
- ETSI GS ECI 001-1, “ETSI GS ECI 001-1: Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview”,

2014.

- ETSI GS ECI 001-2, “ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements”, 2014.

- TG3-S31-087r13, “System Requirements for ATSC 3.0”, 2016.

- TG3-S36-086r10, “ATSC Candidate Standard: ATSC 3.0 Security and Service Protection”, 2017.

- IETF: “TLS 1.3, The Transport Layer Security (TLS) Protocol Version 1.3,” draft-ietf-tls-tls13-14, Internet Engineering Task Force, Fremont, CA

- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016

- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

3.2 인용 표준과 본 표준의 비교표

FBMF-STD-003	참조 표준	비고
5. IMCP 시스템 Transport Layer Security 규격	ATSC 3.0, TG3-S36-086r10	준용

Preface

1 Purpose

The purpose of this standard is to define the specifications of Transport Layer Security for the multi-device content protection system eligible for IP-based broadcasting environment in Korea (Rep. of) by referencing the international standards ITU-T J.1010, ITU-T J.1011 and the European standards ETSI ISG ECI.

2 Summary

This standard specifies the specifications of Transport Layer Security for exchangeable, embedded CA/DRM solutions, enabling CPE to download CA/DRM clients under a trusted environment. In the IMCP system, content is transmitted over broadband channels as well as over-the-air broadcasting. Transport Layer Security ensures a secure connection between the IMCP client and the IMCP server or between the IMCP client and the IMCP client through the interaction channels. The IMCP system Transport Layer Security provides authentication and encrypted communications between two peers communicating.

3 Relationship to Reference Standards

3.1 Relationship of Reference Standards

This standard specifies the specifications of Transport Layer Security for broadcasting service of Republic of Korea based on the reference standards.

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Architecture, Definitions and Overview”, 2016.
- ETSI GS ECI 001-1, “ETSI GS ECI 001-1: Embedded Common Interface for

exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview", 2014.

- ETSI GS ECI 001-2, "ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements", 2014.

- TG3-S31-087r13, "System Requirements for ATSC 3.0", 2016.

- TG3-S36-086r10, "ATSC Candidate Standard: ATSC 3.0 Security and Service Protection", 2017.

- ISO/IEC 23001-7, "MPEG systems technologies - Part 7: Common encryption in ISO base media file format files", 2016.

- NGBF-STD-017, "IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항", 2016

- FBMF-STD-002, "IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처", 2017

3.2 Differences between Reference Standards and this Standard

FBMF-STD-003	Reference Standard	Remarks
5. Transport Layer Security Specification for IMCP system	ATSC 3.0, TG3-S36-086r10	modified

목 차

IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠보호 시스템을 위한 Transport Layer Security 규격

Transport Layer Security Specifications for IP-based Multi-CA/DRM Content Protection

1 적용 범위

본 표준은 CPE(Customer Premises Equipment)가 신뢰 환경에서 CA/DRM 클라이언트를 다운로드 하기 위한 교환 가능한 IMCP (IP-based Multi-CA/DRM Content Protection) 시스템의 TLS (Transport Layer Security) 규격을 명시한다. IMCP 시스템에서 콘텐츠는 지상파방송(over-the-air)뿐만 아니라 IP기반의 광대역 채널을 통해서도 전송된다. TLS은 IMCP 클라이언트와 IMCP 서버 간의 또는 IMCP 클라이언트와 IMCP 클라이언트간의 양방향 채널을 통한 보안 연결을 보장한다. IMCP 시스템은 TLS을 통해 통신하는 두 상대 간의 인증 및 암호화 통신을 제공한다.

본 표준은 IMCP 시스템상에서 콘텐츠 보호를 위해 다음의 일련의 방법을 정의한다.

1) IMCP 애플리케이션 인증
2) IMCP 애플리케이션과 웹 컨텐츠 서버 간의 인터넷 연결을 통해 교환되는 양방향 데이터
3) IMCP 주 장치와 주변(companion) 장치간의 데이터 처리 흐름

본 표준에서는 IETF에서 정립된 보안 규격을 위한 다수의 프로파일을 정의한다. 이러한 프로파일을 정의함에 있어, 본 표준에서는 서로 다른 컨텐츠와 데이터 처리 흐름 전반에 걸쳐 일관된 암호 알고리즘을 사용하고자 한다. 이 프로파일은 특정 처리 흐름에서 사용되는 암호화 알고리즘의 선택에 있어 어느 정도의 유연성을 제공하면서 명시된 표준 기술의 쉬운 구현이 가능하도록 설계되었다.

2 참조 표준

다음 문서들이 본 표준의 참고 문서로 사용되었다.

2.1 국외 표준

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Architecture, Definitions and Overview”, 2016.
- ETSI GS ECI 001-1, “ETSI GS ECI 001-1: Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview”, 2014.
- ETSI GS ECI 001-2, “ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements”, 2014.
- TG3-S31-087r13, “System Requirements for ATSC 3.0”, 2016.
- TG3-S36-086r10, “ATSC Candidate Standard: ATSC 3.0 Security and Service Protection”, 2017.
- IETF: “TLS 1.3, The Transport Layer Security (TLS) Protocol Version 1.3,” draft-ietf-tls-tls13-14, Internet Engineering Task Force, Fremont, CA

2.1 국내 표준

- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016
- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

3 용어 정의

3.1 IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 (IMCP, IP-based Multi-CA/DRM Content Protection)

CPE 내 소프트웨어 기반 변경 가능한 IMCP 클라이언트의 구현과 개발을 허용하고, IMCP를 준수하는 다른 CPE 장치와의 상호 호환성을 제공하는 아키텍쳐와 시스템.

3.2 IMCP서버 (IMCP Server)

IMCP 클라이언트에 컨텐츠 또는 기타 서비스를 제공하고 본 표준의 규범적 요구사항을 준수하는 모든 IP 연결 장치

3.3 IMCP 클라이언트 (IMCP Client)

IMCP와 호환되는 CA/DRM 클라이언트의 구현. 이것은 CPE에 있는 소프트웨어 모듈이고 콘텐츠 제공자나 운영자로부터 분배되는 콘텐츠에 대한 소비자 자격과 권리를 보호 받기 위한 모든 수단을 제공한다. 또한, IMCP 클라이언트는 소비자가 사용하는 권리나 자격 같은 조건을 받고 다양한 암호화된 메시지와 콘텐츠를 해석하기 위한 키를 받는다.

4 약어 및 규약

4.1 약어

본 표준은 다음 약어들을 사용한다.

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CD	Companion Device
CEA	Consumer Electronics Association
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DRM	Digital Rights Management
DTCP	Digital Transmission Content Protection
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral key exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galios Counter Method
IKM	Input Keying Material
IMCP	IP-based Multi-CA/DRM Content Protection
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
PD	Primary Device
RFC	Request for Comments
RSA	Rivest, Shamir, and Adelman

RTT	Round Trip Time
SECP	Standard for Efficient Cryptography Elliptic Curve Domain Parameters
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
UUID	Universally Unique Identifier

4.2 규약

본 표준은 다음의 규약을 따른다:

- “**반드시 ~ 해야한다.**” 또는 “**반드시 ~ 할 수 있어야 한다.**” 또는 “**절대 ~ 해서는 안된다.**”: 어떠한 경우에도 예외 없이 필수적인 항목 (영어의 SHALL에 해당)
- “**~ 해야한다.**” 또는 “**~할 수 있어야 한다.**”: 아주 명백한 사유가 있지 않는 한 “반드시 ~ 해야한다.”인 항목 (영어의 SHOULD에 해당)
- “**~ 할 수도 있다.**”: 추가적으로 허용될 수 있는 항목 (영어의 MAY에 해당)

5 IMCP 시스템 Transport Layer Security 규격

5.1 시스템 개요

IPTV와 테블릿, 스마트폰 등과 같은 장치들은 일반적으로 소프트웨어 내에서 더 많은 기능들을 구현하고 양방향 IP 통신을 제공한다. 이는 새로운 타입의 향상된 보안 메커니즘을 가능하게 한다. 이러한 장치들에 사용되는 칩셋들이 다양한 보안 처리 기능을 갖는 하드웨어를 포함하기 때문에, IMCP는 호환을 위해 전용 하드웨어 지원 보안과 강건성 기능들이 필요하다.

IMCP는 CA/DRM 제공자가 각 소비자 도메인 내에 CA를 위한 솔루션뿐만 아니라 DRM을 위한 솔루션도 구현할 수 있게 한다. 그림 1은 IMCP의 완전한 구현으로 인해 완전히 지원되는 레퍼런스 환경설정을 보여준다.
각 소비자의 도메인 안에서 다중 화면 환경을 지원하기 위해, 도메인 안에 있는 IMCP 클라이언트들은 서로 통신할 수 있어야 하며, 제공자와 양방향 네트워크를 이용할 수 있어야 한다.

IMCP 클라이언트는 게이트웨이 또는 IMCP 비 호환 클라이언트로 동작하는 방식으로 구현될 수 있다.

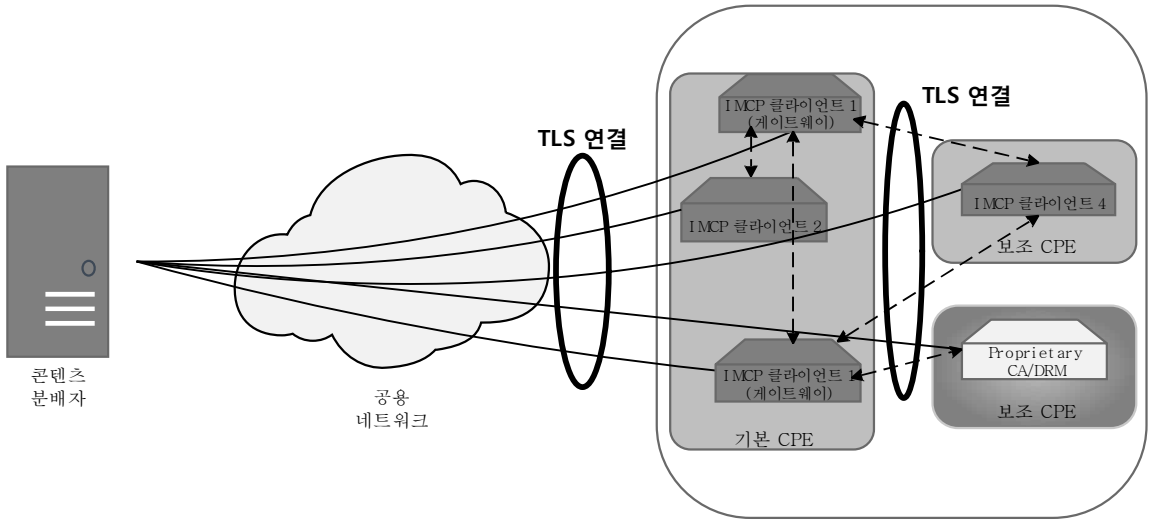

그림 1 단일 시청자 도메인 상의 IMCP 클라이언트 TLS 연결 예시

5.2 전송 계층 보호

전송 계층 보호는 데이터의 전송 과정에서 데이터가 스푸핑(spoofing)되거나 가로채는 것에 대한 보호 기능을 제공한다. 전송 계층 보호에는 별도로 암호화되지 않은 콘텐츠의 보호가 포함될 수도 있다. 전송 중 콘텐츠의 암호화는 본 절에서 설명한다.

5.2.1 인터넷 스트리밍 전송 보호

5.2.1.1 TLS (Transport Layer Security)

IMCP 클라이언트는 양방향 채널을 통한 보안 연결을 위해 TLS 1.3과 TLS 1.2 모두를 구현해야 한다. TLS 1.3은 이전 버전에 비해 처리 속도와 보안 측면에서 개선이 되었다. 처리 속도측면에서의 개선점은 TLS 1.3의 응답/확인(handshake)과 세션 재개 과정의 RTT (Round Trip Time)가 한 단계씩 줄어든 것이다. TLS 1.2의 응답/확인(handshake) 과정의 RTT는 2단계인데 반해, TLS 1.3은 1단계의 RTT이다. 또한 세션 재개 과정의 경우 TLS 1.2는 RTT 1단계인데 반해, TLS 1.3은 0단계의 RTT이다. 보안 측면에서의 개선은 TLS 1.2 대비 지금까지 노출된 대표적인 공격 (high-profile attacks)에 대한 보완적인 측면과 오래되어 지금은 더 이상 사용되지 않는 알고리즘들 (예, MD5, SHA-224, 등)에 대한 제거측면에서 이루어졌다.

IMCP 클라이언트는 TLS 1.3 (ProtocolVersion {0x03, 0x04})을 사용하여 연결을 요청하는 것이 정상이지만, TLS 1.3 부록 C에 명시된 것처럼 TLS 1.2 (ProtocolVersion {0x03, 0x03})로 버전을 낮추라는 서버의 요청이 있을 경우에도 이에 대한 해석 및 처리를 할 수 있어야 한다.

IMCP 서버는 IMCP 양방향 채널 프로토콜을 사용하여 보안 연결을 협상 프로토콜(negotiation protocol)을 통해 수행 시 TLS 1.3을 준수해야한다.

TLS 1.3을 지원하지 않는 IMCP 서버는 TLS 1.2 를 나타내는 ProtocolVersion {0x03, 0x03}을 포함하는 "Server Hello" 메시지로 반드시 응답해야한다.

서버는 {0x03, 0x03} 버전과 같거나 높은 ProtocolVersion을 지원하지 않는 클라이언트와의 보안 연결 협상 프로토콜 (negotiation protocol) 과정을 반드시 거부해야 한다.
그리고 서버는 TLS 1.3 부록 C (TLS 1.2 부록 E)에 명시된 대로 protocol_version 경고 메시지를 반드시 보내야 한다.

5.2.1.2 TLS 1.3 서버 연결 협상 프로토콜

TLS 1.3을 지원하는 IMCP 서버는 5.2.1.2.1절과 5.2.1.2.2절과 5.2.1.2.3절에 명시된 Cipher Suite와 Elliptic Curve 그룹과 서명 알고리즘 중 반드시 하나 이상의 조합을 사용하여 보안 연결을 위한 협상 프로토콜을 운영 해야 한다.

TLS 1.3을 지원하는 IMCP 서버는 이러한 서명 알고리즘과 Cipher Suite와 Elliptic Curve 그룹 중 적어도 하나의 조합을 요청하지 않는 연결은 반드시 거부해야 한다.

TLS 1.3을 지원하는 IMCP 클라이언트는 본 절에서 명시된 서명 알고리즘과 Elliptic Curve 그룹과 Cipher Suite들만 사용해야 된다.

5.2.1.2.1 Cipher Suites

```
TLS_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA384
TLS_CHACHA20_POLY1305_GCM_SHA256
```

5.2.1.2.2 Elliptic Curve 그룹

```
secp256r1
secp384r1
secp512r1
```

각 elliptic curve 그룹은 반드시 비압축 포인트 포맷과 함께 사용되어야 한다.

5.2.1.2.3 서명 알고리즘

```
rsa_pkcs1_sha256
rsa_pkcs1_sha384
rsa_pkcs1_sha512
ecdsa_secp256r1_sha256
ecdsa_secp384r1_sha384
ecdsa_secp512r1_sha512
rsa_pss_sha256
rsa_pss_sha384
rsa_pss_sha512
```

5.2.1.3 TLS 1.2 서버 연결 협상 프로토콜

TLS 1.2 만 지원하는 IMCP 서버는 반드시 다음의 Cipher Suite (RFC 5289에 명시되어 있는) 중 하나 이상을 사용하여 보안 연결을 위한 협상 프로토콜을 운영 해야한다:

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

또는 TLS 1.2 만 지원하는 IMCP 서버는 클라이언트에 의해 요청되는 다음의 Cipher Suite (RFC 7539에 명시되어 있는) 중 하나 이상을 반드시 사용하여 보안 연결을 위한 협상 프로토콜을 운영해야 한다:

```
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

또는 TLS 1.2 만 지원하는 IMCP 서버는 클라이언트가 제공한 순서에 관계없이 다음의 Cipher Suite (RFC 5246에 명시되어 있는)를 클라이언트 Cipher Suite 중 최우선으로 반드시 선택해야만 한다:

```
TLS_RSA_WITH_AES_128_CBC_SHA
```

5.2.1.3.1 Elliptic Curve 그룹

IMCP 서버는 다음 elliptic curve 그룹 (secp256r1와 secp384r1 및 secp521r1)을 반드

시 지원해야 한다.

IMCP 서버는 비압축 포인트 포맷을 반드시 지원해야 한다.

IMCP 서버는 이러한 curve 그룹 또는 포인트 포맷 중 하나 이상을 요청하지 않는 연결은 반드시 거부해야 한다.

5.2.1.3.2 서명 알고리즘

IMCP 서버는 sha256 또는 sha384 또는 sha512 해시 알고리즘 중 하나를 사용하여 rsa 또는 ecdsa 서명 알고리즘을 지원해야 한다.

TLS 1.2 연결을 협상 (또는 재협상)하는 IMCP 클라이언트는 이러한 서명 알고리즘과 해시 알고리즘 조합 중 하나를 요청하거나, 서명 알고리즘 확장을 생략할 수도 있다.

클라이언트가 서명 알고리즘 확장을 포함하지 않는 경우에 IMCP 서버는 insufficient_security 에러로 연결 요청을 반드시 거부해야 한다.

5.2.1.4 서버 인증서 선택

IMCP 서버는 클라이언트(클라이언트가 다른 알고리즘으로 협상을시도하는 경우도 포함)에 의해 협상된 서명 및 해시 알고리즘의 조합 중 하나를 이용하는 서명을 반영한 인증서만을 반드시 제공 해야 한다.

그리고 IMCP 서버는 다른 알고리즘을 사용하는 인증서를 포함한 보안 연결은 절대 구축하면 안된다.

IMCP 서버는 TLS 응답/확인(handshake)에서 클라이언트에게 반환할 적합한 서버 인증서의 선택을 지원하기 위해 반드시 클라이언트에 의해 제공되는 Server Name Indication을 사용해야 한다.

IMCP 서버는 TLS 응답/확인(handshake)에서 클라이언트에게 반환할 적합한 인증서 체인의 선택을 지원하기 위해 신뢰할 수 있는 CA 표시 반드시 확장(extension)을 사용해야 한다.

IMCP 서버가 Server Name Indication 확장(extension)이나 신뢰할 수 있는 CA Indication 확장(extension)으로 클라이언트 기준에 적합한 인증서 체인을 선택할 수 없는 경우에, IMCP 서버는 반드시 연결을 하지 않아야 한다.

5.2.1.5 TLS 인증서 상태 요청과 응답

클라이언트는 RFC 6066 8장에 명시된 대로 인증서 상태 요청 확장(extension)을 포함해야 한다. 인증서 상태 요청 확장에는 RFC 6960에서 정의된 신뢰할 수 있는 OCSP 응답자 공개 키의 SHA-1 해시로 각각 인코딩된 OCSP 응답자 식별자 목록이 포함된다.

IMCP 서버는 클라이언트가 신뢰할 수 있고 클라이언트가 지원하는 서명 알고리즘을 사용하여 서명한 응답자 공용 키의 OCSP 응답자로부터 받은 OCSP 응답만을 반드시 클라이언트에게 제공해야 한다.

IMCP 서버가 신뢰할 수 있는 응답자로 식별한 OCSP 응답자가 제공하는 인증서에 대한 OCSP 응답을 얻을 수 없는 경우, IMCP 서버는 접속 연결을 절대 하면 안 된다.

IMCP 서버는 IMCP 클라이언트와의 접속 연결에 사용하는 인증서에 대한 가장 최신의 OCSP 응답을 반드시 전송해야 한다.

OCSP 응답의 포맷은 RFC 5019에 정의된 필수 요소로 제한되어야 하고, 옵션 요소는 응답에 포함되지 않아야 한다.

TLS 1.2을 통해 서버가 연결을 시도할 때, 서버는 RFC 6960에 정의된 대로 OCSP 인증서 응답/확인(handshake) 메시지 수신 직후에 OCSP 응답의 인증서 상태 응답/확인(handshake) 메시지에 OCSP 응답을 반드시 포함해야 한다.

TLS 1.3을 통해 서버가 연결을 시도할 때, 서버는 Server Hello 응답/확인(handshake) 메시지의 암호화된 확장에 OCSP 응답을 반드시 포함해야 한다.

IMCP 클라이언트는 RFC 6066 8장에 명시된 대로 서버가 제공한 인증서 상태 메시지를 검증해야한다. 클라이언트는 수신한 OCSP 응답 데이터를 사용하여 서버 연결을 인증하는 인증서가 유효한지 확인한다.

5.2.1.6 TLS 세션 재개

새로 설정된 TLS 1.3 연결을 가진 IMCP 서버는 클라이언트의 응답/확인(handshake) 완료 메시지를 수신하면 새 세션 티켓 메시지를 제공할 수 있다.

새 세션 티켓 메시지는 ticket_early_data_info extension 을 절대 포함하면 안된다.

클라이언트는 TLS 세션을 재개하기 위해 후속 클라이언트 Hello 메시지의 **pre_shared_key** 확장에서 이 세션 티켓의 정보를 제공할 수 있다.

세션 재개 클라이언트 Hello 메시지 수신 시, IMCP 서버는 세션 티켓이 여전히 유효하고 클라이언트가 원래 연결에 사용된 것과 동일한 elliptic curve 그룹과 cipher suite를 선택했는지 반드시 확인해야 한다.

또한 IMCP 서버는 클라이언트 Hello 메시지에 제공된 Server Name Indication 확장(extension)이 원래 연결에 제공된 것과 동일한지 반드시 확인해야 한다.

서버는 `psk_dhe_ek` 로 설정된 Pre-Shared Key Exchange Mode를 포함하는 세션 재개 요청 만을 반드시 협상(negotiation) 한다.

IMCP 서버는 early_data를 포함하는 Client Hello 메시지에 절대 응답하면 안되므로 클라이언트는 초기 데이터 없이 세션 재개 Client Hello 메시지를 발행해야 한다.

TLS 1.2 연결 세션을 설정한 IMCP 서버는 나중에 해당 세션을 다시 시작할 수 있도록 세션 티켓 확장 (RFC 5077)을 지원할 수 있다.

만약 IMCP 서버가 이 확장을 지원하지 않으면 세션 티켓 정보를 요청한 클라이언트에 빈 세션 티켓 확장을 절대 보내면 안된다.

5.2.1.6.1 TLS 연결 재협상

TLS 1.2 응답/확인(handshake)을 처리하는 IMCP 클라이언트는 재협상 표시 확장(extension) (RFC 5746)을 지원할 것이지만, 이 확장(extension)에 있는 모든 데이터가 포함된 클라이언트 Hello 응답/확인(handshake) 메시지를 보낸다는 것을 의미하지는 않는다.

TLS 1.2 응답/확인(handshake)을 처리하고 있는 IMCP 서버는 RFC 5746에서 요구하는 바와 같이 서버 Hello 메시지에 재협상(renegotiation)을 지원하지 않는다는 것을 나타내는 빈 재협상(renegotiation) 표시 확장을 반드시 포함해야한다.

TLS 1.2 응답/확인(handshake)를 처리하는 IMCP 서버는 연결 파라미터의 재협상(renegotiation)을 유도하기 위한 Hello 요청 메시지를 클라이언트에 절대 보내면 안된다.

5.2.1.7 DNSSEC (Domain Name System Security Extension)

IMCP 서버는 반드시 RFC 6840과 RFC 4033에 설명된 DNSSEC 서명 구역의 구성원이어야 한다.

5.3. IMCP 애플리케이션 코드 서명 (IMCP Application Code Signing)

실행 가능하거나 해석 가능한 코드는 멀티 파트 MIME 패키지로 패키징되어야하며 암호로 서명되어야 한다.

서명된 애플리케이션들은 반드시 다음과 같이 S/MIME 버전 3.2 (RFC 5751에 명시되어 있는) 포맷으로 되어야 한다:

(1) 작성자 서명은 단독 서명을 생성하기 위해 S/MIME 3.4.3 절에 명시된 방식으로 먼저 추가되어야 한다. 새로 생성 된 Content Type application/pkcs7-signature의 **name** 속성은 반드시 **author.p7s** 로 설정되어야 하고, 해당 Content Disposition 의 **filename** 속성은 반드시 **author.p7s** 로 설정되어야 한다. 작성자 서명은 반드시 최종 MIME 패키지의 첫번째 단독 서명으로만 나타나야 한다

(2) 배포자 서명은 단독 서명을 생성하기 위해 S/MIME 3.4.3 절에 명시된 방식으로 추가되어야 한다. 새로 생성된 Content Type application/pkcs7-signature의 name 속성은 반드시 distrib.p7s 로 설정되어야 하고, 해당 Content Disposition 의 filename 속성은 반드시 distrib.p7s 로 설정되어야 한다. 만약 작성자 서명이 없으면 배포자 서명은 최종 MIME 패키지의 첫번째 단독 서명으로 표시되어야 한다. 그렇지 않으면 배포자 서명은 최종 MIME 패키지의 두번째 단독 서명으로 표시되어야 한다.

(3) 모든 서명은 멀티 파트 MIME 패키지에 포함된 후에 적용되어야 한다.

S/MIME 프로세싱을 사용하여 생성된 서명은 RFC 5753에 정의된 대로 elliptic curve 서명 처리를 위한 확장이 있는 암호화 메시지 문법(syntax) (RFC 5652)에 따라 인코딩되어야 한다.

S/MIME 디지털 서명을 만드는 데는 다음의 프로필이 사용되어야 한다:

(1) 서명 및 메시지 다이제스트 알고리즘은 다음 쌍 중 하나이어야 한다:

- rsa- pkcs1 with sha-256
- ecdsa curve secp256r1 with sha-256
- ecdsa curve secp384r1 with sha-384
- ecdsa curve secp512r1 with sha-512

(2) SignerInfo 타입은 S/MIME 2.5 절에 명시된 대로 서명이 생성된 시간을 포함하는 SigningTime 속성을 반드시 포함해야 한다. 이 속성은 반드시 서명된 속성으로

인코딩되어야 한다.

5.4 인증서 및 인증서 관리

본 표준에서는 인터넷 X.509 공개 키 기반(infrastructure) 프로파일 (RFC 5280)을 IMCP TLS 서버와 IMCP 애플리케이션 서명 기관 인증에 사용되는 인증서의 기본 프로필로 사용한다.

다음 타입의 인증서들이 IMCP 장치에서 인증 프로세스 중에 사용된다:

- 하나 또는 그 이상의 루트 인증서: 이 인증서는 신뢰된 인증 기관이 신뢰 루트로 발급한 신뢰할 수 있는 자체 서명된 인증서이다. 신뢰할 수 있는 루트 인증서에 도달하면 각 인증서 경로 유효성 검사 프로세스가 완료된다. TLS 에서는 이러한 인증서에 포함된 서명을 검사할 필요가 없다.
- 인증기관 인증서: 이 인증서는 신뢰할 수 있는 루트 인증 기관이나 신뢰할 수 있는 루트 인증 기관에 대해 인증서 경로를 확인할 수 있는 인증 기관에서 발급한다.
- TLS 서버 인증서: 이 인증서는 신뢰할 수 있는 인증 기관에서 발급하며 서버 인증에 사용된다.
- IMCP 애플리케이션 서명자 인증서: 이 인증서는 신뢰할 수 있는 인증 기관에서 발급하며 코드 서명에 사용된다.
- OCSP 응답자 인증서: 이 인증서는 신뢰할 수 있는 인증 기관에서 발급하며 OCSP 응답자 인증에 사용된다.

5.4.1 인증서 프로파일

5.4.1.1 일반적 사양

모든 IMCP 인증서는 반드시 X.509 버전 3 인증서이어야 한다.

IMCP 인증서에 포함된 모든 키는 반드시 RFC 3279에 명시된 방법으로 인코딩된 최소 사이즈 (2048bit) RSA 키나 RFC 5480에서 정의된 포인트 포맷과 elliptic curve 그룹을 사용하는 ECDSA 키 이어야 한다.

IMCP 인증서에 포함된 모든 RSA 서명은 반드시 RFC 3279와 RFC 4055에 명시된 RSA 서명 알고리즘을 따라 인코딩 되어야 한다.

IMCP 인증서에 포함된 모든 ECDSA 서명은 반드시 RFC 5758에 명시된 ECDSAS 서명 알고리즘을 따라 인코딩 되어야 하고 ECDSA 서명 알고리즘을 같이 사용하기 위해 위에서 명시된 (5.2.1.1.과 5.2.1.3.) 해시 알고리즘 중 하나를 반드시 사용해야 한다.

모든 IMCP 인증서는 최소 digitalSignature 값을 포함하고 RFC 3279와 RFC 4055에 명시된 값을 포함하는 Key Usage extension을 반드시 포함해야 한다.

5.4.1.2 루트 인증서 프로파일

모든 최상위 인증서를 위한 RSA 키 크기는 반드시 최소 2048bit이고 4096bit이어야 한다.

모든 최상위 인증서를 위한 ECDSA 키 크기는 반드시 최소 384bit이어야 한다.

5.4.1.3 인증 기관 인증서 프로파일

모든 인증기관 인증서를 위한 RSA 키 크기는 반드시 최소 2048bit이어야 한다.

모든 인증기관 인증서를 위한 ECDSA 키 크기는 반드시 최소 256bit이어야 한다.

5.4.1.4 서버 인증 인증서 프로파일

서버 인증을 위한 인증서의 RSA 키 크기는 반드시 최소 2048bit이어야 한다.

모든 서버 인증을 위한 인증서의 ECDSA 키 크기는 반드시 최소 256bit이어야 한다.

Subject Alternative Name 확장(extension)은 인증될 서버의 DNS Name 또는 IP Address를 반드시 나타내고 포함해야 한다.

Extended Key Usage 확장(extension)은 인증서가 TLS 서버 인증에 사용된다는 것을 나타내기 위해 id-kp-serverAuth 값을 반드시 나타내고 설정해야 한다.

5.4.1.5 IMCP 애플리케이션 서명자 인증서 프로파일

모든 애플리케이션 서명자 인증서를 위한 RSA 키 크기는 반드시 최소 2048bit이어야 한다.

Key Usage extension은 필수 사항으로 표시되어야 하고 반드시 digitalSignature 값만을 포함해야 한다.

Extended Key Usage extension은 인증서가 다운로드 및 실행 가능한 코드를 서명하는데 사용된다는 것을 나타내기 위해 id-kp-codeSigning 값을 반드시 나타내고 필수 사항으

로 표시하고 설정해야 한다.

5.4.1.6 OCSP 응답자 인증서 프로파일

모든 OCSP 응답자 인증서를 위한 RSA 키 크기는 반드시 최소 2048bit이어야 한다.

모든 OCSP 응답자 인증서를 위한 ECDSA 키 크기는 반드시 최소 256bit이어야 한다.

Extended Key Usage extension은 인증서가 OCSP 응답을 서명하는데 사용된다는 것을 나타내기 위해 id-kp-OCSPSigning 값을 반드시 나타내고 설정해야 한다.

5.5 IMCP 클라이언트 인증서 저장소

본 표준에서 사용된 인증서의 안전한 저장소와 클라이언트 장치가 사용하는 인증서를 수정하기 위한 메커니즘에 대한 설명은 CEA 2053을 따르고 있다.

클라이언트는 다음 인증서 세트에 보안 저장소를 제공한다:

- 신뢰할 수 있는 루트 인증서 세트
- 신뢰할 수 있는 서명 인증서 기관 인증서 세트
- 신뢰할 수 있는 OCSP 응답자 인증서 세트

인증서는 클라이언트 장치 코드 다운로드 또는 다른 방법으로 시간이 지남에 따라 변경된다.

5.6 인증서 폐기 및 상태 정보

인증서 상태 관리는 정의된 인증 관행 및 정책에 따라 작동하는 발급 기관의 통제하에 있다. IMCP 서버 또는 IMCP 애플리케이션 프로그램 서명 기관에서 사용하는 인증서를 발급하는 각 인증 기관은 OCSP 응답자에게 인증서 상태 정보를 적시에 제공할 책임이 있다.

5.6.1 TLS 서버 인증서를 위한 인증서 폐기와 상태 정보

IMCP 서버는 TLS 접속을 연결할 때 서버를 식별할 수 있게 각각의 서버 인증서에 대한 상태 정보를 OCSP 응답자에게 최소 1분에 한번씩 반드시 요청해야 한다.

이 요청은 반드시 RFC 6960에 명시된 포맷이어야 하고, 반드시 서명되지 않아야 하며 요청에 포함된 extension만이 반드시 Preferred Signature Algorithm extension이어야 한다.

주) 다른 서명 알고리즘을 지원하는 클라이언트를 만족시키기 위해 서버는 Preferred Signature Algorithm extension에서 다른 값을 사용하여 동일한 OCSP 응답자로부터 인증서 상태 정보를 요청해야 한다.

5.6.2 IMCP 애플리케이션 서명 인증서를 위한 인증서 폐기와 상태 정보

IMCP 애플리케이션 서명 관리자는 반드시 인증서 상태 정보를 OCSP 응답자에게 요청해야 하며, 이는 서명 동작에 사용되는 서명키를 인증하는 관리 인증서에 서명하기 위함이다.

OCSP 요청은 OCSP 응답자가 사용하는 선호 서명 알고리즘이 SHA-256를 포함하는 RSA이라는 것을 반드시 나타내야 한다.

IMCP 애플리케이션 서명에 관련된 SigningTime과 서명 관리 인증서의 상태를 나타내는 해당 OCSP 응답의 producedAt time은 반드시 달라야 하며 그 차이는 1분 이하이어야 한다.

IMCP 애플리케이션 서명 관리자는 OCSP 응답을 반드시 서명된 애플리케이션에 포함해야 하고, OCSP 응답에 서명 관리 인증서의 상태가 “good”이 아니라면(RFC 6960에 명시된 것처럼) 서명된 애플리케이션을 발행하지 말아야 한다.

애플리케이션 서명 기관은 서명된 멀티 파트 MIME 컨텐츠에 포함된 각 Cryptographic Message Syntax (RFC 5652) 포맷의 디지털 서명의 otherRevInfoFormat 필드에 OCSPResponse를 포함해야 한다.

OCSPResponse는 RFC 5940에 명시되어 있는 포맷을 따라야한다.

클라이언트는 수신한 OCSP 응답 데이터를 사용하여 애플리케이션 프로그램 서명 기관을 인증하는 인증서가 애플리케이션 프로그램 서명 시점에 유효한지 확인한다.

5.7 사전 공유 키 암호화 연결

본 절에서는 클라이언트 장치와 서버 장치로 알려진 두 장치가 사전 공유 키 (pre-shared key)를 파생시키고 해당 키를 사용하여 암호화된 연결을 설정하는 일반적인 방법을 설명한다. 이 방법은 두 장치간의 UUID (Universally Unique Identifiers) 교환과 각 장치에서 동일한 IKM (Input Keying Material)의 교환을 기반으로 한다. 생성된 사전 공유 키는 5.7.2. 절에 명시된 TLS 1.3 사전 공유 키 파라미터를 사용하여 장치간의 TLS 1.3 연결에 사용된다.

사전 공유 키를 사용하여 A/338에 따라 주 장치 (PD, Primary Device)와 컴패니언 장치 (CD, Companion Device) 애플리케이션간의 암호화된 연결을 설정하면, CD는 클라이언트 역할을 하고 PD는 서버의 역할을 하게 된다.

5.7.1 사전 공유 키 등록

5.7.1.1 사전 공유 키 식별자

클라이언트에 설치된 각 사전 공유키는 키를 공유하는 해당 서버의 UUID에 의해 반드시 참조 되어야 한다.

서버에 설치된 각 사전 공유키는 키를 공유하는 해당 클라이언트의 UUID에 의해 반드시 참조되어야 한다.

예를 들면, UUID는 A/338에 명시된 장치 검출(discovery) 프로토콜에 제공된다.

5.7.1.2 사전 공유 키 해시 알고리즘

사전 공유 키는 TLS 1.3에서 사용하기 위한 시크릿을 도출할 때, TLS 1.3 키 스케쥴 프로세스에서 sha 256 해시 알고리즘과 함께 사용되어야 한다.

5.7.1.3 사전 공유 키 생성

사전 공유 키는 다음과 같이 RFC 8018에 명시된 PBKDF2 알고리즘을 사용하여 IKM에서 도출되어야 한다:

1) 서버의 128 비트 UUID 와 클라이언트의 128 비트 UUID 를 순서대로 연결하여 256 비트 바이너리 값의 솔트를 생성
2) HMAC-sha256 을 기본 의사 난수 함수로 사용하여 사전 공유 키를 PBKDF2 (IKM, salt, 50000, 32)로 설정한다 (RFC 8018 참조).

5.7.1.4 키 생성 테스트 벡터

아래의 예제 파라미터를 사용하여 위의 사전 공유 키 생성을 올바르게 구현하면 아래의 출력 파라미터가 생성된다.

Input:
Server UUID = 0x123e4567e89b12d3a456426655440000
Client UUID = 0x98734716276497582763764874687252
IKM = ‘UserPassword' (0x5573657250617373776f7264)

Intermediate results:

Salt = 0x123e4567e89b12d3a4564266554400009873471627649758276376487468725 2

Output:

PSK = 0xf7a28206cfad1076eba1fce76245e012f357f5f70bcbe407f03d53ca8265de32

5.7.1.5 통신 시작

사전 공유 키가 파생되면 클라이언트와 서버 모두 32 자 이하의 ASCII 문자로 구성된 IKM과 함께 제공되어야 한다.

IKM은 클라이언트 또는 서버의 영구 메모리에 절대 저장되어서는 안되며, 클라이언트와 서버는 IKM을 절대 재사용해서도 안된다.

5.7.1.6 사전 공유 키 저장소

클라이언트와 서버는 TLS 연결을 설정하는 알고리즘과 애플리케이션으로 용도 제한되는 신뢰할 수 있는 키 저장소에 각각의 사전 공유 키를 저장한다.

신뢰할 수 있는 키 저장소에 새로운 사전 공유 키를 입력하거나 신뢰할 수 있는 키 스토어에서 사전 공유 키를 삭제하는 기능은 클라이언트와 서버의 Privileged Application 으로 제한되어야 한다.

보안 하드웨어 기반의 신뢰할 수 있는 키 저장소가 클라이언트 또는 서버 장치에서 사용 가능한 경우, 여기에 사전 공유 키를 저장해야 한다.

5.7.2 TLS 1.3 사전 공유 키 교환 파라미터

TLS 클라이언트 역할을 하는 클라이언트 장치와 TLS 서버 역할을 하는 서버 장치는 5.7.1절에 따라 파생된 사전 공유 키를 사용하여 TLS 1.3 연결을 설정할 수 있다.

이 연결을 설정하기 위해 5.2.1.2 절에서 정의된 TLS 1.3 서버 연결 협상(negotiation) 파라미터가 사전 공유 키와 함께 사용된다.

TLS 클라이언트 응답/확인(handshake) 요청은 TLS 1.3 프로토콜의 사용을 나타내며, TLS 서버는 이전 버전의 TLS로의 다운그레이드(downgragde)를 협상(negotiation)해서는 안된다.

TLS 클라이언트는 일시적인 ECDHE 키를 설정할 수 있게 Pre-Shared Key Exchange Mode를 psk_dhe_ek로 설정하여야 한다.

사전 공유 키를 사용하여 TLS 1.3 연결을 설정한 서버 장치는 해당 연결에 대한 TLS 세션 재개 (5.2.1.6 참조)를 지원해야 한다.

5.7.2.1 사전 공유 키 해시 알고리즘

사전 공유 키는 TLS 1.3에서 사용하기 위한 시크릿을 도출할 때, TLS 1.3 키 스케쥴 프로세스에서 sha 256 해시 알고리즘과 함께 사용되어야 한다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

‘해당 사항 없음’

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

‘해당 사항 없음’

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 관련 국내 표준

본 표준의 연계(family) 표준은 다음과 같다:

- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016
- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

상기 표준은 본 표준에서 다루고 있는 IMCP 시스템의 유스케이스 및 요구사항과 시스템 아키텍처를 정의하고 있다.

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] IEEE: “Use of the International Systems of Units (SI): The Modern Metric System,” Doc. SI10, Institute of Electrical and Electronics Engineers, New York, N.Y.

[2] ATSC: “ATSC Mobile DTV Standard, Part 6 – Service Protection,” A/153 Part 6:2011, Advanced Television Systems Committee, Washington, D.C., 23 May 2011.

[3] IETF: “RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” L. Bassham, W. Polk, R. Housley, Internet Engineering Task Force, Fremont, CA, April 2002.

[4] IETF: “RFC 4033, DNS Security Introduction and Requirements,” Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, Internet Engineering Task Force, Fremont, CA, March 2005.

[5] IETF: “RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” J. Schaad, B. Kaliski, R. Housley, Internet Engineering Task Force, Fremont, CA, June 2005.

[6] IETF: “RFC 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments,” A. Deacon, R. Hurst, Internet Engineering Task Force, Fremont, CA, September 2007.

[7] IETF: “RFC 5077, Transport Layer Security (TLS) Session Resumption without Server-Side State,” J. Salowey, H. Zhou, P. Eronen, H. Tschofenig, Internet Engineering Task Force, Fremont, CA, January 2008.

[8] IETF: “RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2,” T. Dierks, E. Rescorla, Internet Engineering Task Force, Fremont, CA, August 2008.

[9] IETF: “RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet Engineering Task Force, Fremont, CA, May 2008.

[10] IETF: “RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM),” E. Rescorla, Internet Engineering Task Force, Fremont, CA, August 2008.

[11] IETF: “RFC 5480, Elliptic Curve Cryptography Subject Public Key

Information," S. Turner, D. Brown, K. Yiu, R. Housley, T. Polk, Internet Engineering Task Force, Fremont, CA, March 2009.
[12] IETF: "RFC 5652, Cryptographic Message Syntax (CMS)," R. Housley, Internet Engineering Task Force, Fremont, CA, September 2009.
[13] IETF: "RFC 5746, Transport Layer Security (TLS) Renegotiation Indication Extension," E. Rescorla, M. Ray, S. Dispensa, N. Oskov, Internet Engineering Task Force, Fremont, CA, February 2010.
[14] IETF "RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3. Message Specification," B. Ramsdell, S. Turner, Internet Engineering Task Force, Fremont, CA, January 2010.
[15] IETF: "RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)," S. Turner, D. Brown, Internet Engineering Task Force, Fremont, CA, January 2010.
[16] IETF: "RFC 5758, Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA," Q. Dang, S. Santesson, K. Moriarty, D. Brown, T. Polk, Internet Engineering Task Force, Fremont, CA, January 2010.
[17] IETF: "RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," H. Krawczyk, P. Eronen, Internet Engineering Task Force, Fremont, CA, May 2010.
[18] IETF: "RFC 5940: Additional Cryptographic Message Syntax (CMS) Revocation
Information Choices," S. Turner, R. Housley, Internet Engineering Task Force, Fremont, CA, August 2010.
[19] IETF: "RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions," D. Eastlake 3rd, Internet Engineering Task Force, Fremont, CA, January 2011.
[20] IETF: "RFC 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC)", S. Weiler, and D. Blacka, Internet Engineering Task Force, Fremont, CA, February 2013.
[21] IETF: "RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, Internet Engineering Task Force, Fremont, CA, June 2013.
[22] IETF: "RFC 8018, PKCS #5: Password-Based Cryptography Specification, Version 2.1," K. Moriarty, B. Kaliski, A. Rusch, Internet Engineering Task Force, Fremont, CA, January 2017.
[23] IETF: "TLS 1.3, The Transport Layer Security (TLS) Protocol Version 1.3," draft-ietf-tlstls13-18, Internet Engineering Task Force, Fremont, CA,
[24] IETF: "RFC 7539, ChaCha20 and Poly1305 for IETF Protocols," Y. Nir, A.

Langley, Internet Engineering Task Force, Fremont, CA, May 2015.
[25] ITU-T: “Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components”, Rec. X.667, International Telecommunication Union, September 2004.

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

‘해당 사항 없음’

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2017.06.15	제정 FBMF-STD-003	-	UHDTV분과위원회
오류정정				
오류정정				
제2판				