NGB Standard

차세대방송표준포럼표준 (국문표준)

NGBF-STD-017 제정일: 2016 년 08 월 26 일

IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠보호 시스템 유스케이스 및 요구사항

Use cases and Requirements of Multi- CA/DRM Content Protection System in IP-based Broadcasting Enviroment

ngB 차세대방송표준포럼

Next-Generation Broadcast Standards Forum

차세대방송표준포럼표준 (국문표준)
NGBF-STD-017
제정일: 2016 년 08 월 26 일

IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠보호 시스템 유스케이스 및 요구사항

Use cases and Requirements of Multi-CA/DRM Content Protection System in IP-based Broadcasting Enviroment

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. 1010 및 ITU-T J. 1011 과 유럽 표준인 ETSI ISG ECI 와 북미 차세대 지상파방송 표준인 ATSC3.0 요구사항을 기반으로 한국 상황에 맞는 IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호를 위한 시스템 유스케이스 및 요구사항 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 유스케이스 및 요구사항을 명시한다. 비록 CPE 가 콘텐츠 관련된 CA/DRM 클라이언트를 갖지 않더라도, 다운로드 가능한 멀티 CA/DRM 서비스를 활용함으로써 시청 자격을 가진 시청자들이 CA/DRM 이 관리하는 방송과 광대역 콘텐츠를 시청할 수 있다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

현재 구현된 embedded 또는 분리 가능한 하드웨어 CA/DRM 솔루션들은 시장에서 “Lock-in” 효과를 초래한다. 이 솔루션들은 디지털 멀티미디어 콘텐츠 시장에서 많은 회사들의 자유를 심각하게 제한한다. 기술적인 개선 덕분에, 혁신적이고 소프트웨어 기반의 CA/DRM 솔루션들이 실현 가능하게 되었다. 높은 수준의 보안을 유지하면서 모듈의 상호 호환성을 최대화하는 것이 폭넓은 소비자의 선택과 새로운 사업이 허락되는 미래의 시장 요구를 충족시킨다.

소비자 맞춤, 환경에 민감한 CA/DRM 시스템들의 교환성을 보장해줌으로써 더 많은 CPE 시장의 분열을 막을 수 있고 회사 간의 경쟁이 독려될 것이다.

4. 참조 표준(권고)

4.1. 국외 표준(권고)

- 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.

4.2. 국내 표준

- 해당 사항 없음

5. 참조 표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

본(이) 표준은 참조 표준 문서들을 기반으로 하여 한국 지상파방송 현황에 맞춰서 콘텐츠보호 시스템을 정의함

5.2. 참조한 표준(권고)과 본 표준의 비교표

NGBF-STD-017	참조 표준	비고
6. IMCP 시스템 유스케이스	ITU-T J.1010, ETSI ISG ECI Part 2	준용
7. IMCP 시스템 요구사항	ITU-T J.1010, ETSI ISG ECI Part 2	준용

6. 지적재산권 관련사항

본 표준의 '지적재산권 확약서‘ 제출 현황은 NGB 웹사이트에서 확인할 수 있다.

※본 표준을 이용하는 자는 이용함에 있어 지적재산권이 포함되어 있을 수 있으므로, 확인 후 이용한다.

※본 표준과 관련하여 접수된 확약서 이외에도 지적재산권이 존재할 수 있다.

7. 시험인증 관련사항

7.1. 시험인증 대상 여부

해당사항 없음

7.2. 시험표준 제정 현황

해당사항 없음

8. 표준의 이력 정보

8.1. 표준의 이력

판수	제정. 개정일	제정. 개정내역
제 1 판	2016.08.26.	제정 NGBF-STD-017

8.2. 주요 개정 사항

해당사항 없음

Preface

1. Purpose of Standard

The purpose of this standard is to define use cases and requirements for the multi-device content protecioin system for the Republic of Korea IP-based broadcasting environment, which is based on the international standards ITU-T J.1010, ITU-T J.1011 and the European standards ETSI ISG ECI and the North America next generation terrestrial broadcasting standards ATSC 3.0.

2. Summary of Contents

This standard specifies use cases and requirements for exchangeable, embedded CA/DRM solutions, enabling CPE to download CA/DRM clients under a trusted environment. By utilizing downloadable multi-CA/DRM service, entitled consumers can consume broadcast and broadband content, which is controlled by DRM and/or CAS, even though a CPE does not have a required content-related CA/DRM client available by downloading it from a trusted source.

3. Applicable fields of industry and its effect

Currently implemented solutions, whether embedded or as detachable hardware, result in "Lock-in" effects. This seriously restricts the freedom of many players in digital multimedia content markets. Due to technological advances, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, they promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice.

4. Reference Standards (Recommendations)

4.1. International Standards (Recommendations)

- 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.

4.2. Domestic Standards

- None

5. Relationship to Reference Standards (Recommendations)

5.1. Relationship of Reference Standards

This standard specifies the usecases and requirements for broadcasting service of Republic of Korea based on the reference standards.

5.2. Differences between Reference Standard(recommendation) and this Standard

NGBx.xx.xxxx	Reference Standard	Remarks
6. Use Cases of IMCP system	ITU-T J.1010, ETSI ISG ECI Part 2	modified
7. Requirements for IMCP system	ITU-T J.1010, ETSI ISG ECI Part 2	modified

6. Statement of Intellectual Property Rights

IPRs related to the present document may have been declared to NGB. The information pertaining to these IPRs, if any, is available on the NGB Website.
No guarantee can be given as to the existence of other IPRs not referenced on the NGB website.

And, please make sure to check before applying the 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	Outline
The 1st edition	2016.08.26.	Established NGBF-STD-017

8.2. Revisions

None

목 차

Contents

IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠보호 시스템

유스케이스 및 요구사항

Use cases and Requirements of Multi-CA/DRM Content

Protection System in IP-based Broadcast Environment

1. 개요

CA (Conditional Access)와 DRM (Digital Rights Management)에 구현된 서비스 및 콘텐츠 보호는 콘텐츠, 서비스, 네트워크와 CPE (Customer Premises Equipment)를 포함하는 디지털 방송과 광대역 영역이 빠르게 발전하는데 필수적이고, 그 목적은 콘텐츠 소유자, 네트워크 및 PayTV 운영자의 사업 모델들을 보호하기 위함이다. 개념적으로 CA 는 네트워크를 통해 서비스 제공자로부터 분배되는 보호 콘텐츠에 접근하는 메커니즘에 초점을 두고 있는 반면, DRM 은 구독자의 계약에 따른 사용권리의 종류 및 정도를 기술한다.

기존의 디지털 방송, IPTV 나 새로운 OTT (Over-The-Top) 서비스들에 사용되는 대부분의 CA 와 DRM 시스템들은 적절한 고유 보안 관련 요소를 바인딩하여 CPE 를 식별한다. 그 결과, 네트워크 A 또는 플랫폼 A 환경에 맞춰 설정된 CPE 는 네트워크 B 또는 플랫폼 B 에 사용할 수 없다. 그 반대의 경우도 마찬가지이다. 그러므로, 디지털 TV 소비자 시장은 표준이 지역뿐만 아니라 플랫폼마다 다른 특징 때문에 아직도 분열되어 있다. 분리 가능한 CA/DRM 모듈들은 완전한 솔루션을 제공하지 않는다: 가격이 저렴하지 않으며, 주로 케이블이나 위성 TV 에 사용되고, 물리적인 인터페이스가 없는 테블렛과 같은 최신형 장비에 사용될 수 없다.

현재 구현된 embedded 또는 분리 가능한 하드웨어 CA/DRM 솔루션들은 시장에서 “Lock-in” 효과를 초래한다. 이 솔루션들은 디지털 멀티미디어 콘텐츠 시장에서 많은 회사들의 자유를 심각하게 제한한다. 기술적인 개선 덕분에, 혁신적이고 소프트웨어 기반의 CA/DRM 솔루션들이 실현 가능하게 되었다. 높은 수준의 보안을 유지하면서 모듈의 상호 호환성을 최대화하는 것이 폭넓은 소비자의 선택과 새로운 사업이 허락되는 미래의 시장 요구를 충족시킨다.

소비자들은 그들이 구매했던 CPE 들을 계속 사용할 수 있을지에 관심이 있다. 예를 들면, 이사 또는 네트워크 사업자의 변경 후에 장비를 다른 상업 비디오 포탈의 서비스에 이용할 수 있는지를 궁금해 한다. 이는 적절한 보안 아키텍쳐를 기반으로 한 CA 와 DRM 관련 CPE 들의 상호 호환성이 보장되어야만 가능하다. 소비자 친화형, 상황 정보에 민감한 교환 가능 CA/ DRM 시스템을 보장해줌으로써 CPE 시장의 분열을 막을 수 있고 더 많은 회사 간의 경쟁이 독려될 것이다.

2. 표준의 구성 및 범위

본 표준은 IP 기반 방송환경에서 다운로드 방식을 사용해 멀티 CA/DRM 솔루션을 제공할 수 있는 단말 터미널에 대한 표준 인터페이스 규격을 정의한다. 다운로드 과정은 신뢰적인 환경에서 작동하고 종단 사용자가 취득한 콘텐츠에 대한 권리로 입증된 다양한 종류의 단말장치로 방송과/또는 광대역 연결을 통해 전달된 보호 콘텐츠의 시청을 가능하게 한다. 본 표준 기반 방송 콘텐츠 보호 솔루션은 본 솔루션이 적용되는 방송시스템의 전송 방식과 독립적으로 설치 및 운영될 수 있다.

3. 참조 표준(권고)

다음 문서들이 본 표준의 참고 문서로 사용되었다.

- 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.

4. 용어정의

4.1. 본 표준에서 정의한 용어

4.1.1. IP 기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 (IMCP, IP-based Multi-CA/DRM Content Protection)

CPE 내 소프트웨어 기반 변경 가능한 IMCP 클라이언트의 구현과 개발을 허용해, IMCP 에 관련된 CPE 장치의 상호 호환성을 제공한다.

4.1.2. IMCP 클라이언트 (IMCP Client)

IMCP 와 호환이 되는 CA/DRM 클라이언트의 구현. 이 것은 CPE 에 있는 소프트웨어 모듈이고 콘텐츠 분배자나 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.

4.1.3. IMCP 호스트 (IMCP host)

IMCP 와 관련된 기능들을 갖고 IMCP 클라이언트와의 인터페이스를 갖는 CPE 의 하드웨어 및 소프트웨어 시스템. IMCP 호스트는 CPE 펌웨어의 한 부분이다.

4.1.4. 보호 콘텐츠 (protected content)

실시간 혹은 비실시간 전달 수단을 통해 소비자 응용프로그램에 전달되는 모든 종류의 보호 미디어.

4.1.5. IMCP 컨테이너 (IMCP container)

CA/DRM 호스트로부터 CA/DRM 클라이언트를 완전히 분리하는 호스트 및 클라이언트와의 소프트웨어 인터페이스들의 묶음. 인터페이스의 권한 설정을 통해 CA/DRM 클라이언트의 상호 호환성을 보장한다. IMCP 컨테이너는 소프트웨어 또는 하드웨어 형태로 구성될 수 있다. 예를 들어 소프트웨어 형태의 IMCP 컨테이너는 VM 이며, 하드웨어 컨테이너는 TEE 가 될 수 있다.

4.2. 약어

본 표준은 다음 약어들을 사용한다:

AES Advanced Encryption Standard
CA Conditional Access
CA/DRM Conditional Access/Digital Rights Management
CE Consumer Electronics
CENC Common Encryption
CPE Customer Premises Equipment
CSA Common Scrambling Algorithm
DECE Digital Entertainment Content Ecosystem
DRM Digital Rights Management
ECI Embedded Common Interface
IMCP IP-based Multi-CA/DRM Content Protection
IP Internet Protocol
IPTV TV using the Internet Protocol (IP)
ISOBMFF ISO Base Media File Format

OTT Over-The-Top (over the open Internet)

PVR Personal Video Recorder
TEE Trusted Execution Environmnet
URI Usage Rights Information
VM Virtual Machine

4.3 규약

본 표준에서는 다음과 같이 규약을 정의한다:
- “의무”: 어떠한 경우에도 예외 없이 필수적인 항목 (영어의 SHALL 에 해당)
- “권고”: 아주 명백한 사유가 있지 않는 한 “의무”인 항목 (영어의 SHOULD 에 해당)
- “선택”: 추가적으로 허용될 수 있는 항목 (영어의 MAY 에 해당)

5. IMCP 시스템 소개

본 표준에서 다루는 IMCP 시스템의 주요 이점은 다음과 같다.

- 소프트웨어 기반 구현으로 인한 유연성과 확장성
- 미래 솔루션을 발전시키고 혁신을 가능하게 하는 교체성
- OTT를 포함한 광대역 인터넷 및 방송을 통해 분배되는 콘텐츠에 대한 적용 가능성
- 멀티스크린 환경의 지원
- “Lock-in” 현상을 막음으로써 플랫폼 운영자, 네트워크/서비스 사업자 및 소비자를 위한 시장 활성화 자극
- 시장 발전 조성을 위한 오픈 에코 시스템 사양

IMCP 시스템은 CPE 내 CA/DRM 시스템들에 관련된 모든 수준과 측면을 보장해주는 교체 가능성에 목표를 두고 있으며, 소비자를 위해 가능한 저비용을 목표로 하고 디지털 콘텐츠 시장에서 회사의 목표 상품 개발에 필요한 CA /DRM 에 대한 규제 완화를 목표로 한다. 그러므로, IMCP 는 다음 기능들을 갖는다:

- 각 CA, DRM 커널에 대한 IMCP 클라이언트 (CA/DRM 클라이언트)는 CPE 관련 모든 기능에 대한 표준 인터페이스가 있으며, IMCP 클라이언트를 CPE 펌웨어와 소프트웨어적 또는 하드웨어적으로 격리 운영할 수 있는 VM 또는 TEE와 같은 격리 모듈 상에서 동작된다.
- 하나의 CPE에는 복수 개의 개별 IMCP 컨테이너가 포함된다. 각 컨테이너는 VM 또는 TEE와 같은 격리 모듈의 인스턴스를 소유하며 그 인스턴스에서 실행된다.
- 안전한 표준 로더 개념 하에 다른 CPE 소프트웨어와 독립적으로 IMCP 클라이언트가 설치된다.
- 콘텐츠 보호를 지원하고 권한이 없는 콘텐츠에 대한 접근을 막을 수 있는 고급 보안 능력 (Chip Set Security로도 알려짐).
- 사용자가 IMCP 클라이언트 다운로드 권리를 획득할 수 있는 방법

- IMCP 클라이언트 및 CPE의 기능 폐지 방법 (일부도 가능).
- 기존 디지털 방송, IPTV 또는 현대의 OTT 기반 시스템에도 적합함.

IMCP 가 기존 관련 분야 솔루션에 비해 다음의 차이점들이 존재한다.

- CA/DRM 클라이언트들은 공통 하드웨어뿐만 아니라 소프트웨어에 포함되어 운용 될 수 있다.
- 복수 개의 IMCP 클라이언트는 하나의 같은 CPE에서 특별한 소프트웨어 및 하드웨어의 추가 없이 구현될 수 있다.
- 이 클라이언트들은 하나의 장치에서 동시에 동작 될 수 있다.

결론적으로, CA/DRM 구성요소는 훨씬 쉽게 교체될 수 있고, 비싼 모듈로의 교체 없이도 종단 사용자의 CPE 가 지원하는 다양한 운영자로부터 폭넓은 서비스를 받을 수 있다.

6. IMCP 시스템 유스케이스

6.1. 유스케이스 1

디지털 TV 사업 환경에서 CPE 장비의 CA/DRM 시스템을 교체해야하는 다음과 같은 다양한 이유가 있을 수 있다.

- 디지털 미디어 콘텐츠 제공자는 다음과 같은 이유로 고객을 위해 CPE의 CA/DRM 시스템 교체를 결정할 수 있다.
  - 향상된 CA/DRM 기능, 높은 신뢰성 레벨, 높은 시스템 성능 혹은 현재 시스템의 많은 변화에 대한 요구사항과 같은 다양한 기술 및 상업적인 이유.
  - 경쟁사의 액세스 서비스 네트워크를 사용하는 새로운 고객 가입.
- 플랫폼 운영자는 다음과 같은 이유로 자사의 플랫폼 CPE의 CA/DRM 시스템 교환을 결정할 수 있다.
  - 향상된 CA/DRM 기능, 높은 신뢰성 레벨, 높은 시스템 성능 혹은 현재 시스템의 많은 변화의 요구사항과 같은 다양한 기술 및 상업적인 이유.
  - 추후 구매할 네트워크 기술과의 호환성.
- CA/DRM 사업자가 다른 CA/DRM 사업자를 인수 또는 다른 사업자의 CA 시스템이 운영되었던 방송 사업자를 새로운 고객으로 받게 되는 상황 발생 시 보안 시스템간 상호 연동을 바랄 수 있다.
- 종단 사용자는 어떠한 상점에서 CPE를 사서 이를 액세스 네트워크 제공자 A에 연결할 수 있다. 다수의 서비스 제공자들은 이 네트워크 A 를 통해 서비스를 제공할 수 있다. 종단 사용자는 인증 및 허가 과정을 통해 해당 서비스 제공자에 등록 되면, 자신이 선택한 서비스에 맞는 CA/DRM 시스템을 다운로드 할 수 있다.
- 시간이 흘러, 이 종단 사용자는 액세스 네트워크 제공자 B에 연결하기로 결정한다. 그 사용자는 CPE를 네트워크 B에 연결한다. 만약 그 사용자의 CPE가 요구하는 수신 기술을 지원한다면, 다수의 서비스 제공자는 그들의 서비스를 네트워크 B로 제

공한다. 종단 사용자는 인증 및 허가 과정을 통해 해당 서비스 제공자에 등록되면, 선택한 서비스에 맞는 CA/DRM 시스템을 다운로드할 수 있다.

- CE 제조사는 CPE를 FreeTV와 PayTV 모두 지원하는 소매 시장에 팔길 원한다. 하지만 CPE들은 종단 사용자의 동의 하에 소프트웨어 업그레이드를 통해 특정 PayTV 서비스의 사용만이 가능하다.

6.2. 유스케이스 2

CA 플랫폼상의 기본 사양이 설치된 CPE 의 CA 시스템 변경이 필요한 경우, 현재 CA 사업자, 플랫폼 운영자나 디지털 미디어 콘텐츠 제공자, CPE 제조업체, 새로운 CA 사업자가 필요하다.

현재 CA 사업자는 새로운 CA 사업자에게 기본 사양이 설치된 CPE 로 접근하기 위한 기술적인 정보뿐만 아니라 CPE 에 구현된 소프트웨어, 프로토콜 및 특정 하드웨어 부품을 사용하기 위한 라이센스도 같이 제공해야 한다. 어떠한 경우에도 새로운 CA 사업자는 자사의 CA 시스템을 현재 필드에서 사용되는 CPE 에 기능, 하드웨어/소프트웨어의 제약 및 프로토콜을 적용시킬 수 있어야 한다. CPE 제조사들은 새로운 CA 시스템을 다른 소프트웨어가 설치된 기존 CPE 의 소프트웨어에 통합시켜야 한다. CA/DRM 시스템의 교체는 최악의 경우 기술적/상업적 옵션으로도 실행되지 않을 수 있다. 이 경우는 더 나은 호환성 보장을 위해 바뀌어야 한다.

고유 보안 모듈들은 CA 시스템의 중요한 부분이므로, CPE 는 보통 특정 CA 시스템 전용으로 제조된다. 그러므로 CA 시스템이 교체가 되는 경우 필드에서 사용되고 있는 CPE 의 보안 수준을 제한할 수 있다. 이 경우는 어떤 고급 보안이라도 완전히 호환될 수 있는 방식으로 바뀌어야 한다.

6.3. 유스케이스 3

IMCP 시스템은 어플리케이션에 대한 소비뿐만 아니라 세컨더리 장치로의 보호 콘텐츠 전송도 지원해야 한다. 다음 두 개의 유스케이스들은 세컨더리 장치 어플리케이션 지원에 관한 것이다.

- 중앙 어플리케이션: 게이트웨이 타입으로, IMCP를 준수하는 CPE는 URI와 암호화된 콘텐츠를 세컨더리 장비에 전달한다.
- 분산 어플리케이션: 게이트웨이 타입으로, IMCP를 준수하는 CPE는 URI만 세컨더리 장비에 전달하고 세컨더리 장비는 네트워크로부터 암호화된 콘텐츠를 얻는다. IMCP 시스템은 세컨더리 장비에서 DRM 클라이언트의 구현과 관련된 어떠한 요구사항을 포함하지 않는다. 보호 콘텐츠를 게이트웨이에서 세컨더리 장비로 전송하기 위해 필요한 것은 두 개의 DRM 클라이언트들간의 안전한 통신과 콘텐츠 소유자의 DRM 시스템 구현이다.

6.4. 유스케이스 4

현재 어떠한 요구되는 유일 ID 나 증명서라도 CA/DRM 시스템의 제공자에 의해 정의된 고유한 방법으로 CPE 에 내장되어야 한다. 사업자는 유일 ID 나 증명서로 접근하는 메커니즘을 공개하려 하지 않기 때문에, 상호 호환성에 관해서 이는 적절하지 않은 솔루션이다. 예를 들어, CI 플러스 컨소시엄은 “Trusted Third Party” 에게 안전하게 증명서를 전송하는 것이 실현 가능하다는 것을 증명했다. 이와 비슷한 솔루션들은 호환가능한 CA/DRM 이 필요하다.

7. IMCP 시스템 요구사항

7.1. 일반 요구사항

[R 01] IMCP 는 어떠한 종류의 방송, 광대역 인터넷 그리고 하이브리드(방송과 광대역 인터넷을 같이 쓴다는 의미) 서비스에 적용 가능해야 하며, 어떠한 종류의 적절한 액세스 네트워크를 통해 어떠한 종류의 적용가능한 디바이스에 보호 콘텐츠를 전달할 수 있어야 한다 **(의무)**.

[R 02] IMCP 는 IMCP 커널 소프트웨어에 대한 IMCP 컨테이너를 정의해야 하며, 이 IMCP 컨테이너는 CA/DRM 소프트웨어 기능과 분명하게 관련되어야 할 뿐만 아니라 다른 소프트웨어 요소들과 분명하게 구분되어야 한다 **(의무)**.

[R 03] IMCP 는 현재 운영중인 CA/DRM 시스템에서 사용하고 있는 보안 기능과 견줄 수 있는 개선된 보안 기능들을 제공해야 한다 **(의무)**.

7.2. 확장 기능 관련 요구사항

[R 04] IMCP 는 최소 두 개의 서로 다른 보호 콘텐츠 이벤트에 대해 동시에 처리 가능한 해결책을 제공할 수 있는 한 개 이상의 CA/DRM client 를 단일 CPE 에 구현할 수 있어야 한다 **(의무)**.

[R 05] IMCP 는 CPE 에 존재하는 서로 다른 IMCP 클라이언트를 서로 인식할 수 있도록 해야 하며, 상호 간 신뢰성 여부를 확인할 수 있어야 할 뿐만 아니라 콘텐츠 및 콘텐츠 관련 URI 를 한쪽에서 다른 한쪽으로 전달할 수 있어야 한다 **(의무)**.

[R 06] IMCP 는 IMCP 클라이언트들이 연결되어 있는 IMCP 호스트와 신뢰성 관계를 구축할 수 있어야 하며 안전하게 URI 를 IMCP 호스트로 전달할 수 있어야 한다 **(의무)**.

[R 07] 국가적 기준과 법령이 정하는 요구사항을 따라야 한다 **(의무)**.
예) 데이터 프라이버시 보호와 미성년자 보호 등

[R 08] IMCP 는 홈 도메인 또는 홈 네트워크 상에서 적법하게 획득한 보호 콘텐츠의 다른 터미널로의 외부 출력을 지원할 수 있어야 한다 **(의무)**. 이는 하나의 IMCP 클라이언트가 같은 CPE 내의 또 다른 IMCP 클라이언트와 통신할 수 있는 인터페이스가 필요함을 의미하며, 이와 같은 기능은 각 콘텐츠 소유자들이 발행하는 URI 내용 안에서만 가능해야 한다 **(의무)**.

[R 9] IMCP 클라이언트는 보호 콘텐츠를 IMCP 비호환 장치로도 출력할 수 있도록 구현 될 수 있다 **(선택)**. 이와 같은 기능은 각 콘텐츠 소유자들이 발행하는 URI 내용 안에서만 가능하다.

7.3. 사용자 관련 요구사항

[R 10] IMCP 는 사용자에게 뛰어난 사용성과 편리한 UI 조작을 위해 사용자 인터페이스 구현을 위한 API 를 제공해야 한다 **(권고)**.

[R 11] IMCP 는 IMCP 를 사용하는 서로 다른 CA/DRM 시스템을 두 개의 채널 (서비스)에서 사용하는 경우라 할지라도 비슷한 CA/DRM 솔루션에 견주어 현격한 추가적 지연이 발생되지 않아야 한다 **(권고)**. 단, 일반적인 채널 (서비스) 전환 상황에서 CA/DRM 시스템이 변경되는 경우는 고려하지 않는다.

[R 12] 모든 IMCP 관련 동작들은 (예, 정상 동작, IMCP 클라이언트 다운로드) 사용자 경험 및 성능에 현격한 영향을 주지 않아야 한다. **(권고)**

7.4. IMCP 클라이언트 교체 관련 요구사항

[R 13] IMCP 는 CA/DRM 제조사, 장치 제조사, 플랫폼 또는 서비스 운영자들의 허락 없이도 신규 CA/DRM 서비스 제공자로의 변경을 허용해야 한다 **(의무)**.

[R 14] IMCP 클라이언트 변경 시 서비스 간섭에 대한 영향은 최소화 해야 한다 **(의무)**.

[R 15] IMCP 클라이언트 변경 후 scrambled PVR 콘텐츠와 같이 변경 전에 합법적으로 획득된 보호 콘텐츠에 대한 시청이 사용자 입장에서 복잡한 절차 없이 가능해야 한다 **(의무)**.

[R 16] IMCP 는 시장의 요구에 의해 CA/DRM 사업자들이 다른 교환 가능한 호환 IMCP 클라이언트의 개발을 특별한 이유 없이 제한하지 않아야 한다 **(의무)**.

7.5. IMCP 시스템 보안 관련 요구사항

[R 17] IMCP 시스템은 CPE 상에서 IMCP 클라이언트에 대한 안전한 다운로드 및 설치는 표준화된 방식을 기반으로 이루어 져야 한다 **(의무)**.

[R 18] CPE 는 모든 종류의 IMCP 클라이언트에 대해 통일화된 추상 인터페이스를 제공하는 소프트웨어 형식 (예: VM) 또는 하드웨어 형식 (예: TEE)의 컨테이너를 제공해야 한다 **(의무)**.

[R 19] IMCP 클라이언트들과 호스트 시스템은 언제라도 자신들의 신뢰성을 입증할 수 있어야 한다 **(의무)**.

[R 20] IMCP 시스템 운영을 위해 Trust Authority 의 설립 및 운영이 필요하다 **(의무)**.

[R 21] IMCP 는 현존하는 특정 하드웨어 및 운영체제에 종속되어서는 안 된다 **(의무)**. 다만 특정 칩 개발사의 향상된 보안 시스템이 공개적으로 널리 이용되고 있다면, 본 요구사항의 제한을 받지 않는다.

[R 22] IMCP 시스템은 기존 CA/DRM 시스템들이 IMCP 시스템으로 이동(migration)하는 것을 허용해야 한다 **(의무)**.

[R 23] IMCP 는 향후 추가 개발될 수 있는 IMCP 에 대한 역호환성을 제공해야 한다 **(의무)**. 기존 IMCP 구현들은 CPE 나 IMCP 클라이언트 성능이 확장됨에 따라 향후에 나타날 수 있는 추가 기능들에 대한 usage right 들을 처리할 수 있어야 한다 **(의무)**.

[R 24] IMCP 는 보안 장치로써 스마트카드를 사용하거나, 사용하지 않는 시스템 모두를 지원할 수 있다 **(선택)**.

[R 25] IMCP 는 서로 다른 CA/DRM 시스템 어플리케이션들이 요구하는 모든 레벨의 콘텐츠 보호 기능들을 지원해야 한다 **(의무)**.

[R 26] IMCP 는 IMCP 클라이언트 변경 시 어떠한 하드웨어 구성품에 대한 변경을 요구해서는 안 된다 **(의무)**. 만약 스마트카드 기반 CA/DRM 시스템의 스마트카드 변경에 대한 경우, 본 요구사항은 예외이다.

[R 27] IMCP 는 최소한 AES 암호화를 지원해야 한다 **(의무)**. IMCP 호스트는 최소한 ISOBMFF / CENC 가 적용된 미디어 콘텐츠 처리 기능을 지원해야 한다 **(의무)**.

[R 28] IMCP 는 IMCP IMCP 컨테이너와 IMCP 호스트 간 적절한 인터페이스를 통해 폭넓은 usage right 들을 지원할 수 있어야 한다 **(의무)**.

[R 29] IMCP 는 기존 CA/DRM 클라이언트들의 URI 를 새로운 URI 로 변경할 수 있어야 한다 **(권고)**.

[R 30] IMCP 는 동일 장치 내, 또는 다른 장치들 사이에서 IMCP 클라이언트 간 보안 통신 채널을 제공할 수 있어야 한다 **(의무)**.

(뒷 표지)

차세대방송표준포럼표준(국문표준)

IP 기반 방송 환경에서 멀티디바이스 콘텐츠보호 시스템 유스케이스 및 요구사항
(Use cases and Requirements of Multi-CA/DRM Content Protection System in IP-based Broadcasting Enviroment)

발행인 : 차세대방송표준포럼 의장
발행처 : 차세대방송표준포럼
135-703, 서울시 강남구 테헤란로 7 길 22 신관 1108 호
(역삼동 한국과학기술회관)
Tel : 02-568-3556, Fax : 02-568-3557
http://www.nextb.or.kr/
발행일 : 2016.08
