FBMF Standard

미래방송미디어표준포럼표준 (국문표준)

FBMF-STD-002 제정일: 2017 년 5 월 15 일

IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처

Architecture of Multi-CA/DRM Content Protection System in IP-based Broadcasting Environment

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-002
표준 초안 작성자	구한승	ETRI	책임연구원	방송콘텐츠보호기술WG 의장	
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 ECI 등을 종합하여 한국 상황에 맞는 IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호를 위한 시스템 아키텍처 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)의 시스템 아키텍처를 명시한다. 비록 CPE가 콘텐츠와 관련된 CA/DRM 클라이언트를 갖지 않더라도, 다운로드 가능한 멀티 CA/DRM 서비스를 활용함으로써 시청 자격을 가진 시청자들은 CA/DRM이 관리하는 방송과 광대역 콘텐츠를 시청할 수 있다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

본 표준은 아래의 참조 표준 문서들을 기반으로 하여 한국 지상파 방송 현황에 맞춰서 콘텐츠 보호 시스템의 아키텍처를 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.
- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스 케이스 및 요구사항”, 2016

3.2 인용 표준과 본 표준의 비교표

FBMF-STD-002	참조 표준	비고
6. IMCP 시스템 기술 개념	ITU-T J.1010, ETSI ISG ECI Part 1	준용
7. 신뢰 환경	ITU-T J.1010, ETSI ISG ECI Part 1	준용

Preface

1 Purpose

The purpose of this standard is to define the architecture of 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 system architecture of 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 contents that require DRM and/or CAS client even though a CPE does not have content-related CA/DRM client at the beginning service stage.

3 Relationship to Reference Standards

3.1 Relationship of Reference Standards

This standard specifies the architecture 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.
- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스 케이스 및 요구사항”, 2016

3.2 Differences between Reference Standards and this Standard

FBMF-STD-002	Reference Standard	Remarks
6. The technical concept of the IMCP System	ITU-T J.1010, ETSI ISG ECI Part 1	modified
7. Trust Environment	ITU-T J.1010, ETSI ISG ECI Part 1	modified

목 차

IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처

Architecture of Multi-CA/DRM Content Protection System in IP-based Broadcast Environment

1 적용 범위

CA(Conditional Access)와 DRM(Digital Rights Management) 솔루션은 디지털 방송에서 콘텐츠 소유자와 네트워크 및 PayTV 운영자의 사업 모델들을 보호하는 데 있어 필수적이다. 개념적으로 CA는 네트워크를 통해 분배되는 방송 콘텐츠에 대한 접근제어 메커니즘을 제공하는 데 초점을 두고 있는 반면, DRM은 콘텐츠 라이센스에 기반하여 콘텐츠 재생과 저장 그리고 분배 등을 제어하는 데 초점을 두고 있다.

기존의 디지털 방송과 IPTV 및 새로운 OTT(Over-The-Top) 서비스들에 사용되는 대부분의 CA와 DRM 시스템들은 적절한 고유 보안 관련 요소를 바인딩하여 CPE를 식별한다. 그 결과, 네트워크 A 또는 플랫폼 A 환경에 맞춰 설정된 CPE는 네트워크 B 또는 플랫폼 B에서 사용할 수 없다. 그 반대의 경우도 마찬가지이다. 그러므로, 디지털 TV 소비자 시장은 표준이 지역뿐만 아니라 플랫폼마다 다른 특징 때문에 아직도 분할되어 있다. 분리 가능한 CA/DRM 모듈들은 완전한 솔루션을 제공하지 않는다. 가격이 저렴하지 않으며, 주로 케이블이나 위성 TV에 사용되고, 물리적인 인터페이스가 없는 태블릿과 같은 최신형 장치에 사용될 수 없다.

현재 구현된 임베디드 또는 분리 가능한 하드웨어 CA/DRM 솔루션들은 시장에서 종속 효과를 초래한다. 이 솔루션들은 디지털 멀티미디어 콘텐츠 시장에서 많은 회사들의 자유를 심각하게 제한한다. 그러나 기술적인 개선 덕분에, 혁신적이고 소프트웨어 기반의 CA/DRM 솔루션들이 실현 가능하게 되었으며, 높은 수준의 보안을 유지하면서 모듈의 상호 호환성을 최대화하는 것이 폭넓은 소비자의 선택과 새로운 사업을 원하는 미래의 시장 요구를 충족시키게 되었다.

소비자들은 그들이 구매했던 CPE들을 계속 사용할 수 있을지에 관심이 있다. 예를 들면, 이사 또는 네트워크 사업자의 변경 후에 장치를 다른 상업 비디오 포탈

의 서비스에 이용할 수 있는지를 궁금해 한다. 이는 적절한 보안 아키텍처를 기반으로 한 CA와 DRM 관련 CPE들의 상호 호환성이 보장되어야만 가능하다. 즉 교환가능CA/DRM 시스템을 보장해 줌으로서 CPE 시장의 분열을 막을 수 있고 더 많은 회사 간의 경쟁이 독려될 것이다.

본 표준은 IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 (IP-based Multi-CA/DRM Content Protection, IMCP) 아키텍처를 정의한다. 헤드엔드와 IMCP 클라이언트들을 포함하고 있는 CPE와의 관계를 정의하고, CPE가 복수 개 존재하는 경우 CPE 내 IMCP 클라이언트들 간의 구조적 관계도 정의한다. 마지막으로 IMCP 클라이언트를 포함하는 IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템용 CPE 구조를 정의한다.

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.

2.2 국내 표준

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

3 용어 정의

3.1 키 래더 모듈 (Key Ladder Module)

IMCP 클라이언트를 위한 하드웨어와 소프트웨어로 강화된 보안 기능을 제공하는 IMCP를 준수하는 CPE의 기능.

3.2 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 허용하고, IMCP를 준수하는 다른 CPE 장치와의 상호 호환성을 제공하는 아키텍처와 시스템.

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 제공함. 또한, IMCP 클라이언트는 소비자가 사용하는 권리나 자격 같은 조건을 받고 다양한 암호화된 메시지와 콘텐츠를 해석하기 위한 키를 수신함.

3.4 IMCP 클라이언트 로더 (IMCP Client Loader)

IMCP 호스트의 IMCP 컨테이너에 새로운 IMCP 클라이언트 소프트웨어를 다운로드, 검증 및 설치할 수 있게 하는 IMCP 호스트의 소프트웨어 모듈 파트.

3.5 IMCP 컨테이너 (IMCP container)

CA/DRM 호스트로부터 CA/DRM 클라이언트를 완전히 분리하는 호스트와 클라이언트간의 소프트웨어 인터페이스들의 묶음. 인터페이스의 권한 설정을 통해 CA/DRM 클라이언트의 상호 호환성을 보장함. IMCP 컨테이너는 소프트웨어 형태의 가상머신(Virtual Machine)으로 구성될 수 있음.

3.6 IMCP 호스트 (IMCP Host)

IMCP와 관련된 기능들을 갖고 IMCP 클라이언트와의 인터페이스를 갖는 CPE의 하드웨어 및 소프트웨어 시스템. IMCP 호스트는 CPE 펌웨어의 한 부분.

3.7 IMCP 호스트 로더 (IMCP Host Loader)

새로운 IMCP 호스트 소프트웨어를 CPE에 설치, 인증 및 다운로드 할 수 있게 하는 소프트웨어 모듈.

3.8 Trust Authority (TA)

IMCP 시스템 관련 호환되는 구성 부품을 제조하는 업체에게 증명서와 키를 제공하는 기술 서비스 제공자.

4 약어 및 규약

4.1 약어

본 표준은 다음 약어들을 사용한다.

API	Application Programming Interface
CA	Conditional Access
CENC	Common Encryption
CI	Common Interface
CPE	Customer Premises Equipment
DRM	Digital Rights Management
ECI	Embedded Common Interface
HD	High Definition
HTTP	Hypertext Transfer Protocol

iDTV	integrated Digital TV
IMCP	IP-based Multi-CA/DRM Content Protection
IP	Internet Protocol
IPTV	TV using the IP protocol
ISO	International Standards Organization
LA	License Agreement
OS	Operating System
OSD	On Screen Display
OTT	Over-The-Top
PIN	Personal Identification Number
ROM	Read Only Memory
SI	Service Information
SoC	System on Chip
TA	Trust Authority
TEE	Trusted Execution Environment
TV	Television
UI	User Interface
VM	Virtual Machine

4.2 규약

본 표준에서는 다음과 같이 규약을 정의한다:

- "**의무**": 어떠한 경우에도 예외 없이 필수적인 항목 (영어의 SHALL에 해당)
- "**권고**": 아주 명백한 사유가 있지 않는 한 "의무"인 항목 (영어의 SHOULD에 해당)
- "**선택**": 추가적으로 허용될 수 있는 항목 (영어의 MAY에 해당)

5 IMCP 시스템 소개

본 표준에서 다루는 IMCP시스템의 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 적용 가능
- 멀티 스크린 환경의 지원
- 솔루션 종속 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 보장해 주는 교체 가능성에 목표를 두고 있으며, 소비자를 위해 가능한 저비용을 목표로 하고 디지털 콘텐츠 시장에서 회사의 목표 상품 개발에 필요한 CA /DRM에 대한 규제 완화를 목표로 한다. 그러므로, IMCP는 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 가상머신(VM) 또는 TEE와 같은 격리 모듈 상에서 동작된다.
- 하나의 CPE에는 복수 개의 개별 IMCP 컨테이너가 포함된다. 각 컨테이너는 가상머신(VM) 또는 TEE와 같은 격리 모듈의 인스턴스를 소유하며 그 인스턴스에서 실행된다.
- 안전한 표준 로더(loader) 개념 하에 다른 CPE 소프트웨어와 독립적으로 IMCP 클라이언트가 설치된다.
- 콘텐츠 보호를 지원하고, 권한이 없는 콘텐츠에 대한 접근을 막을 수 있는 키 래더 모듈 기능(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 뿐만 아니라 현대의 OTT 기반 시스템에도 적합함.

IMCP는 기존 관련 분야 솔루션에 비해 다음의 차이점들이 존재한다.

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

결론적으로, CA/DRM 구성요소는 훨씬 쉽게 교체할 수 있고, 비싼 모듈로의 교체 없이도 종단 사용자의 CPE가 다양한 운영자로부터 폭넓은 서비스를 받을 수 있다.

6 IMCP 시스템 기술 개념

6.1 기본 고려 사항

본 문서는 같은 호스트에서 돌아가는 다른 IMCP 클라이언트들에 독립적으로 언제라도 IMCP 클라이언트의 다운로드, 업그레이드, 제거 및 교체를 할 수 있는 시스템 아키텍처를 명시하고 있다. IMCP 호스트는 최소 두 개 이상의 IMCP 클라이언트를 위한 런타임 환경을 제공할 수 있어야 한다. 호스트에서 IMCP 클라이언트들은 병렬로 돌아가야 하며 동시에 다른 운영자들로부터 오는 다른 콘텐츠 스트림의 복호화 및 재암호화를 할 수 있어야 한다.

본 문서에 명시된 기술적인 개념은 CENC 호환 DRM 시스템 모두에서 적용될 수 있다.

CPE는 IMCP 클라이언트들의 통합성과 인증을 보호하기 위한 필수 보안 기능을 갖춘 특별한 로더(loader)를 관리한다. 이 로더(loader)는 다른 IMCP 클라이언트를 인증하고 다운로드하기 위해 언제라도 호출되어 동작될 수 있다.

각 IMCP 클라이언트는 각자의 가상머신(VM) 인스턴스와 함께 분리된 소프트웨어 컨테이너에 설치된다.

IMCP 컨테이너는 CA/DRM 기능 전용이다. CPE와의 인터페이스는 다양한 CA/DRM 기능들에 필요한 요청과 데이터 교환을 가능하게 한다. 이러한 요청과 데이터 교환은 IMCP 클라이언트와 호스트, 같은 호스트에 있는 두 개의 IMCP 클라

이언트, 또는 서로 다른 호스트에 있는 두 개의 IMCP 클라이언트 사이에서 이루어진다.

TV 중심의 장치들은 칩셋 안에서 MPEG-2 트랜스포트 스트림을 처리할 수 있는 장치로 정의한다. IMCP는 그 칩셋들이 IMCP호환 키 래더 모듈 기능들을 구현하도록 요구한다. 키 래더 모듈 개념은 모든 IMCP 클라이언트들이 필요 시에 서로 독립적으로 동시에 동작하기 위한 기능을 사용할 수 있게 한다.

IPTV와 태블릿, 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 보안 등의 기능이 필요하다.

키 래더 모듈 기능은 CPE에서 동작하는 모든 IMCP 클라이언트에서 동시에 이용할 수 있다. IMCP 클라이언트들은 multi-crypt 모드에서 동작하는 CENC 호환 DRM 시스템들의 서버 쪽이 각자의 최신 표준에 호환 가능하면, 그 플랫폼 안에 구성될 수 있다.

6.2 시스템 아키텍처 개요

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 비호환 클라이언트로 동작하는 방식으로 구현될 수 있다.

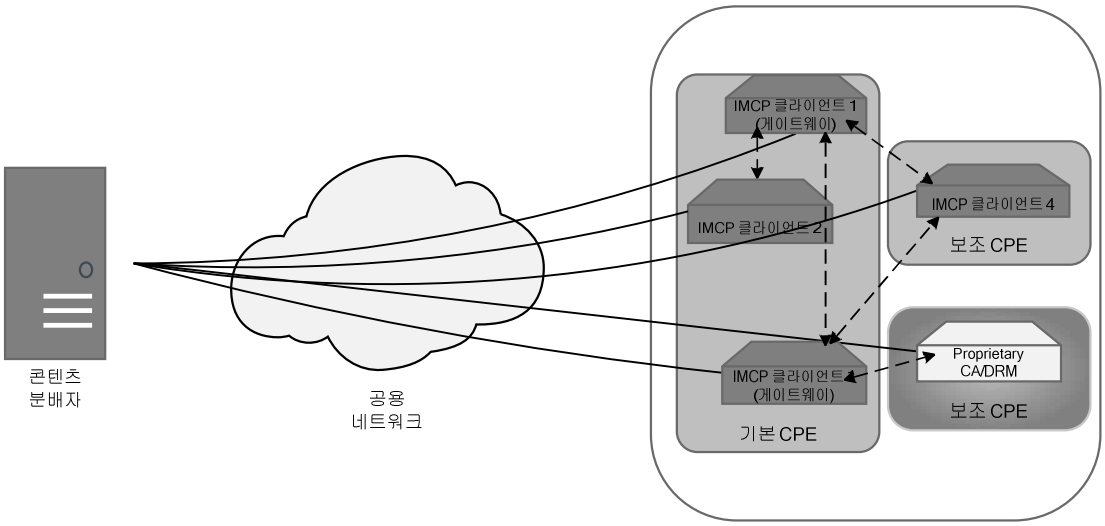

그림 1. 단일 시청자 도메인 상의 IMCP 클라이언트

IMCP 표준은 주로 IMCP 컨테이너와 IMCP 호스트 간의 인터페이스를 정의하고 있다. 그림 2는 IMCP 컨테이너와 통신하는 IMCP 호스트 내의 다른 기능들과 IMCP 컨테이너를 포함한 CPE의 블록 다이어그램을 나타낸다. 이 기능들 중 몇 가지는 선택적이다. IMCP 클라이언트를 설치하고 기동시키는 과정에서 호스트는 IMCP 클라이언트가 이용 가능한 관련 기능들을 명시한다.

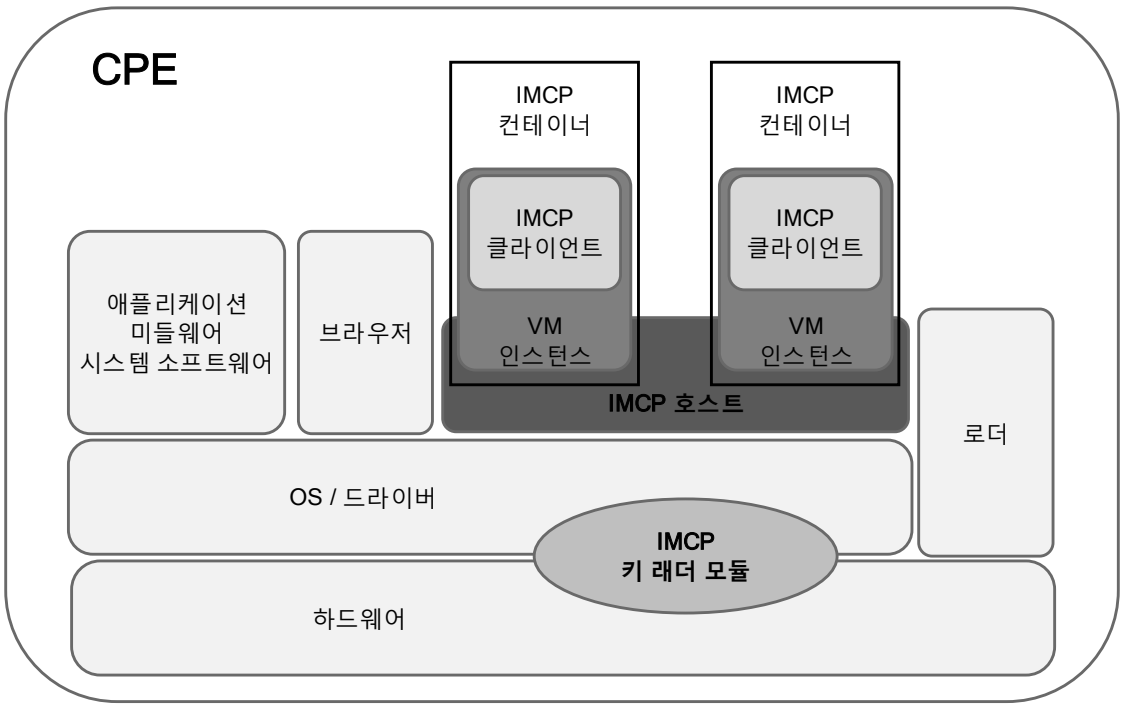

그림 2. 각자의 IMCP 컨테이너와 가상머신(VM) 인스턴스를 포함하는 IMCP 클라이언트와 CPE의 블록다이어그램

IMCP 시스템에서 로더(loader)의 개념은 칩 기반 로더(loader), 시스템 소프트웨어 로더(loader) 및 IMCP 클라이언트 로더(loader)로 구성된 계층적 로더(loader) 개념을 기반으로 한다.

IMCP 호스트 로더(loader)는 IMCP 호스트 소프트웨어를 로딩한다. 로딩 시, 키 래더 모듈 구성요소로 접근하기 위한 가상머신(VM)과 IMCP 클라이언트 로더(loader)와 같은 다른 요소들도 포함시켜 로딩한다. IMCP 호스트는 독립적이고 서로 분리되어 동작하는 가상머신(VM) 인스턴스들에 다중 IMCP 클라이언트들을 로딩할 수 있다.

시스템에 IMCP 클라이언트를 로딩 할 때, IMCP 클라이언트가 로딩된 곳에 가상머신(VM) 인스턴스가 생성된다. 이 가상머신(VM) 인스턴스는 IMCP 클라이언트와 호스트 사이에서 샌드박스(보호된 영역 안에서 프로그램을 작동시키는 보안 소프트웨어) 역할을 한다. IMCP 클라이언트와 가상머신(VM) 인스턴스 간의 인터페이스는 IMCP 시스템의 키 인터페이스이다.

IMCP 호스트 자체는 제조사의 구현에 따라 다르다. IMCP 호스트는 OS 및 드라이버 계층과 접속하고 IMCP 클라이언트 인터페이스 표준에서 정의한 모든 기능들을 제공한다. IMCP 호스트는 IMCP에 명시되어 있지 않지만, IMCP 클라이언트 인터페이스 규격과의 호환을 보장하기 위해 TA의 인증이 필요하다.

6.3 IMCP 호환 장치의 의무 기능

그림 1처럼 IMCP는 다양한 시나리오에 사용될 수 있다. 따라서, IMCP는 iDTV, STB, PVR, IPTV, 태블릿, 스마트폰 등과 같은 다양한 장치와 호환이 되어야 한다. 이러한 장치들은 각자 서로 사양이 다르지만 IMCP는 다양한 장치와 호환되는 보안 프레임워크를 제공해야 한다.

TV 중심의 장치들은 칩셋 안에서 MPEG-2 트랜스포트 스트림을 처리할 수 있는 장치로 정의한다. IMCP는 그 칩셋들이 IMCP 호환 키 래더 모듈 기능들을 구현하도록 요구한다.

IPTV와 태블릿, 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 보안 등의 기능이 필요하다.

6.4 IMCP 호스트와 클라이언트 간 필수 인터페이스

IMCP 컨테이너는 가상머신(VM)과 IMCP 클라이언트를 나머지 CPE 요소들로부터 분리하고 보호하기 위해 가상머신(VM)과 IMCP 클라이언트를 합친 기술적인 개념이다. 가상머신(VM)은 IMCP 호스트의 기능이다. IMCP 클라이언트를 로딩함으로써 IMCP 호스트는 가상머신(VM) 인스턴스를 생성한다. 가상머신(VM)은 IMCP 클라이언트에 대한 필수 인터페이스를 제공하고, IMCP 클라이언트들을 IMCP 호스트에 연결한다. IMCP 표준은 가상머신(VM)과 IMCP 클라이언트 간의 인터페이스를 정의한다. 인터페이스는 특정 API를 제공하고 보안 통신 채널을 수립한다.

중요한 소프트웨어 인터페이스들은 다음과 같다:

- IMCP 호스트와 IMCP 클라이언트 간의 성능 정보 교환을 위한 인터페이스
- CPE의 입력 및 출력 신호를 처리하기 위한 인터페이스
- 키 래더 모듈 하드웨어/드라이버 블록과의 인터페이스
- 로더(loader) 기능들 과의 인터페이스
- 사용자 상호작용을 지원하기 위한 인터페이스
- 암호 및 복호 기능과의 인터페이스
- 워터마킹 같은 특정 보안 기능들 과의 인터페이스
- 로컬 저장장치와의 인터페이스

IMCP 클라이언트의 모든 인터페이스는 가상머신(VM)을 통해 제공된다.

보안 통신을 위한 추가적인 통신 프로토콜이 인터페이스 상에 존재한다.

CPE는 어떠한 종류의 네트워크든 상관없이 동시에 여러 개의 네트워크와 단방향 및 양방향으로 연결될 수 있다. 하지만 항상 네트워크에 연결되어 있을 필요는 없다.

6.5 사용자 인터페이스와 디스플레이의 최소 기능

사용자와의 통신을 위해, 최소한의 UI와 OSD 기능은 IMCP 컨테이너에서 이용가능해야 한다. UI와 OSD 기능은 사용자를 위해 CA/DRM 시스템을 사용할 때 발생되거나 보내지는 메시지들을 디스플레이 하기 위해 사용된다. 또한 이 기능은 PIN과 같은 사용자 입력을 허용한다. 사용자는 IMCP 클라이언트를 통해 CA/DRM 시스템과 소통한다.

6.6 가상머신(Virtual Machine)

IMCP 클라이언트는 표준화된 가상머신(VM) 상에서 동작한다. 설치된 각 IMCP 클라이언트는 고유의 VM 인스턴스를 가진다. VM 인스턴스는 CA 커널이나 DRM 클라이언트 애플리케이션을 실행하기 위한 보안 환경을 제공한다. IMCP 호스트 환경에 대한 리소스가 표준화된 방법으로 접근될 수 있을 때, VM은 API들을 제공한다.

6.7 키 래더 모듈 기능

IMCP는 안전한 콘텐츠 보호 시스템을 빌드하기 위해 요구되는 최소한의 필수 보안 기능들을 정의한다. IMCP는 하드웨어 요소 기반의 개선을 요구한다. 이는 TV 중심의 장치들에서 TV 전용의 특정 키 래더 모듈 기술을 통해 전달된다. 이는 SoC에서 “Key Ladder Block”으로 명시된다. 키 래더 모듈 기능의 필수 임무는 콘텐츠 보호 키들이 CPE 내 IMCP 클라이언트에서 콘텐츠 복호 기능으로 전송되는 동안 또는 보호 콘텐츠를 한 IMCP 클라이언트에서 다른 IMCP 클라이언트로 전송되는 동안 키들을 보호하는 것이다 (그림1 참조). 키 래더 모듈 시스템은 동시에 서로 다른 제어 단어(Control Word) 스트림과 동시에 IMCP 클라이언트 서비스를 요구하는 다수의 IMCP 클라이언트들을 지원한다. 또한 키 래더 모듈 기능은 호스트와 IMCP 클라이언트들을 위한 소프트웨어의 다운로드를 확인하는 데 큰 역할을 한다.

IPTV와 태블릿, 스마트폰 등과 같은 장치들은 일반적으로 소프트웨어 내에서 더 많은 기능들을 구현하고 양방향 IP 통신으로 연결된다. IMCP는 동일한 키 래더 모듈 개념과 메커니즘을 명시하지만, 각 장치의 보안 아키텍처에 따라 서로 다르게 매핑할 것이다.

6.8 리스크램블링(Re-scrambling)

IMCP 호환 CPE를 통해 수신한 보호 콘텐츠는 바로 소비되지 않을 것이다. 다음 기능들은 IMCP 호환 장치들과 같이 이용할 수 있다:

- 로컬 저장장치
  - CPE가 제어함
  - CA 또는 DRM 클라이언트가 제어함
- 게이트웨이
  - DRM 클라이언트의 관리 하에 외부 장치로 보호 콘텐츠 요소를 전달

- 같은 CPE 내부 또는 CPE와 호환이 되는 다른 IMCP에서 돌아가는 다른 IMCP 클라이언트로 보호 콘텐츠 요소를 전달

이 기능들을 지원하기 위해 IMCP 호환 장치는 콘텐츠를 리스크램블링 할 수 있어야 한다. IMCP 시스템은 전송 메커니즘, 저장장치를 위한 이용 가능한 DRM 기능들이나 다른 장치로의 보호 콘텐츠의 전송을 명시하지 않는다.

6.9 IMCP 로더(loader) 기능

IMCP 호환 CPE는 로더(loader) 기능들을 제공해야 하고, 이 기능들은 로딩, 설치뿐만 아니라 IMCP 시스템 관련 소프트웨어 모듈의 무결성 보장 및 경쟁 보호가 가능하도록 해야 한다.

칩 안에 내장된 로더(loader)는 처음에 시스템 소프트웨어 로더(loader)를 로딩한다. 이 임베디드 로더(loader)는 오직 보증된 시스템 소프트웨어 로더(loader)만이 설치되고 동작될 수 있도록 보장한다. 시스템 소프트웨어 로더(loader)는 IMCP 호스트 로더(loader)를 포함하므로, TA의 승인이 필요하다. 시스템 소프트웨어 로더(loader)는 IMCP 기능에 관련되지 않고 시스템에 보안 관련 요소와 연관이 없는 다른 시스템 소프트웨어를 위한 로더(loader)를 포함할 수 있다. IMCP 호스트 소프트웨어는 요청에 따라 IMCP 클라이언트를 로딩 할 수 있는 IMCP 클라이언트 로더(loader)를 포함한다.

IMCP 클라이언트를 설치하고 기동시키는 과정에서 IMCP 클라이언트는 IMCP 호스트로부터 IMCP 컨테이너를 통해 기록 기능, HD 기능, 워터마킹 기능, 네트워크 등과 같은 기능을 포함하는지에 대한 정보를 받는다.

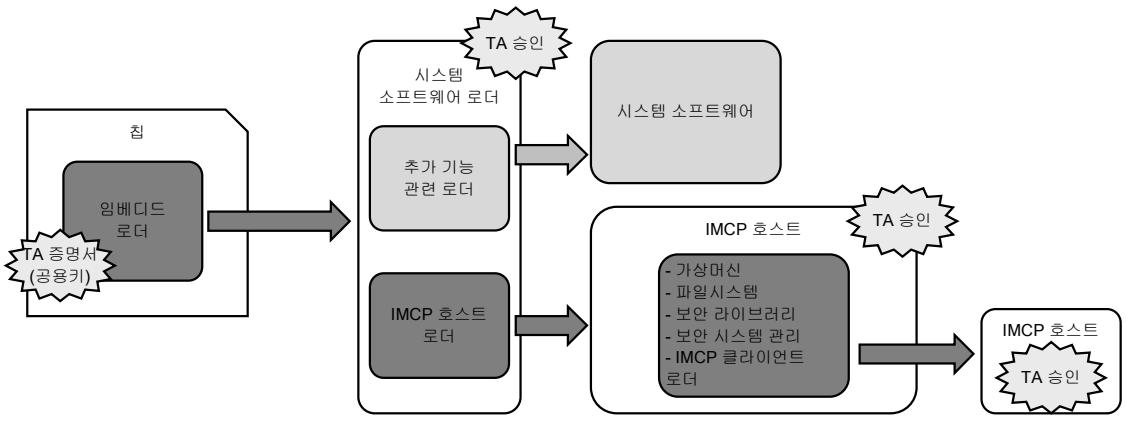

그림 3. 로더(loader)의 계층적 개념

6.10 폐기(Revocation)

TA는 블랙 리스트에 특정 제조업체의 하나의 CPE, 다양한 종류의 CPE, 한 종류의 CPE 또는 모든 CPE를 포함시킬지 결정할 수 있다. 콘텐츠 제공자나 운영자는 블랙 리스트 관련 CPE나 CPE들에 대해 그들의 서비스를 폐기할 것이다.

폐기는 운영자나 콘텐츠 제공자가 블랙 리스트 관련 CPE에 모든 서비스 또는 일부 서비스의 제공을 차단할 수 있다.

7 신뢰 환경(Trust Environment)

IMCP기반 시스템 구축을 위해서는 신뢰 환경이 기본적으로 준비되어야 한다. 신뢰 환경에 대한 세부 항목들은 본 표준의 범주에서 벗어난다.

IMCP 시스템 이해관계사는 다음과 같다:

- CPE 제조업체
- CA/DRM (IMCP 클라이언트) 제조업체
- 칩셋 제조업체. 칩셋 구성요소들은 호스트와 CA/DRM 호환 시스템 사이의 상호작용을 위해 필요한, 바뀔 수 없는 보안 프로세스 키와 증명서를 포함한다.
- 플랫폼 운영자; 플랫폼 운영자는 CA/DRM 시스템의 모든 필수 요소들을 관리하는 단체이다. 플랫폼 운영자들의 예로는 서비스 제공자나 네트워크 운영자가 있다.
- 해당 애플리케이션 제공자

TA는 IMCP 시스템 관련 요소를 제조하는 업체에 증명서와 키를 제공하는 기술적 서비스 제공자이다.

TA는 신뢰 관계의 기반을 형성하므로 상품(칩과 CPE), 동작(보안 IMCP 클라이언트의 다운로드와 활성화) 및 제어 수단(예를 들어, 폐기)을 아우르는 전체 처리과정에 포함되어야 한다.

7.1 운용상의 필수 작업 흐름 (Work Flow)

본 절에서는 서로 다른 시장 참여자가 IMCP 기술 기반의 비지니스를 구현하기

위해 필요한 운용상의 작업 흐름(Work Flow)에 대한 개요를 제공한다. 이 작업 흐름(Work Flow)들은 IMCP 시스템 구현을 위해 필요한 필수적인 기술적 요소에 기반을 둔다. 그림 4는 기술적인 구성요소와 관련 시장 참여자들 간의 상호작용을 나타낸다.

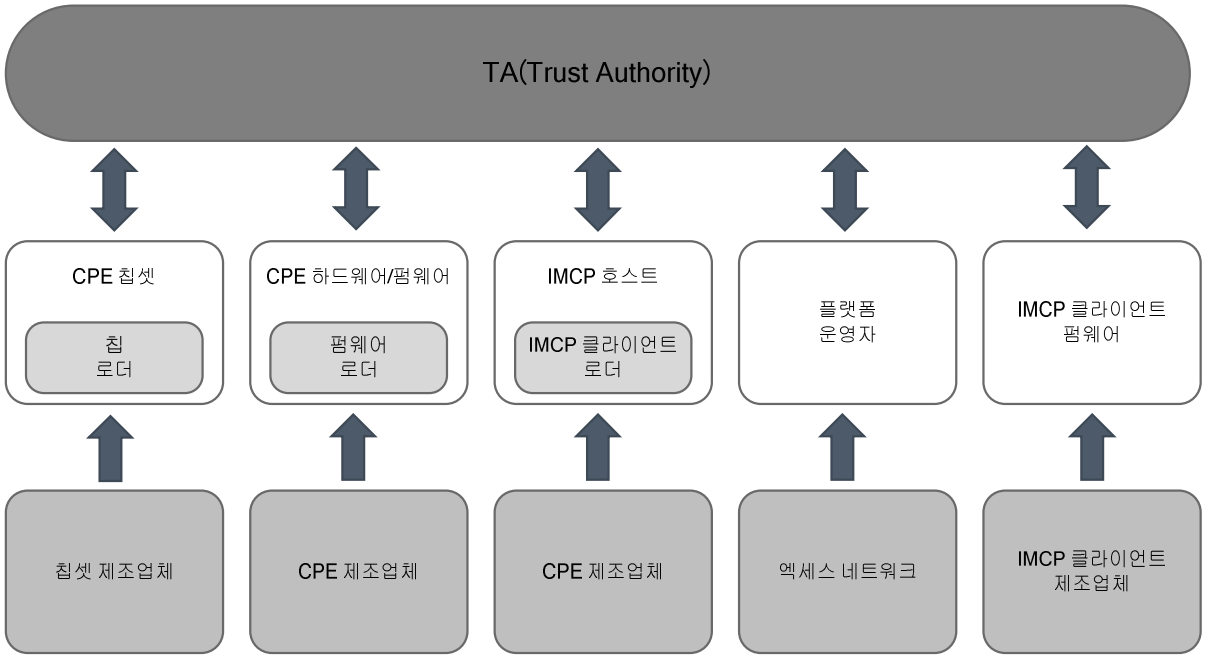

그림 4. TA와 관련 시장 참여자들 간의 필수 신뢰성 관리

그림 4에서 양방향 화살표로 표시된 신뢰 환경을 위한 운용상의 이슈들은 다음과 같다:

1) 무결성(Integrity)

무결성은 한 시장 참여자가 다른 시장 참여자가 제공하는 하드웨어/소프트웨어 구성요소가 비공인 파티에 의해 수정되었는지 여부를 확인할 수 있어야 하고, 표준과 무결성 규칙들을 만족하는지에 대한 요구사항이다. 이 요구사항은 TA로부터 제공되는 테스트 자격을 기반으로 한 테스트, 서명과 적절한 자격을 통해 만족시킬 수 있다.

2) 진의성(Authenticity)

진의성은 모든 하드웨어/소프트웨어 구성요소가 TA와 계약 상의 파트너인 업체로부터 만들어지고, 필수적인 검증과 증명 과정을 통과하여 복제된 어떠한 구성 요소와도 구별될 수 있음을 의미한다. 모든 하드웨어/소프트웨어 관련 구성요소의 진의성은 모든 IMCP 시스템에 의해 입증된다.

3) 대응책(Remedies)

IMCP 시스템의 하드웨어/소프트웨어 구성요소가 더 이상 호환되지 않는 경우, TA는 적당한 기간 안에 에코시스템의 무결성을 다시 설립하는 것을 목표로 그 구성요소 제공자를 위한 절차를 설립한다.

그림 4의 필수적 기술 구성요소들은 다음과 같다:

1) CPE 칩셋

기존의 플랫폼 운영자와 콘텐츠 제공업체의 요구사항에 의해 일반적으로 SoC에 포함되는 CPE 하드웨어에서 CPE 칩셋은 주된 구성요소이다. 또한 보통 칩 로더(loader)는 CPE 칩에 포함된다.

2) CPE 하드웨어

안전한 CPE 칩셋 구현, 저장 요소(플래시, 롬)로의 권한이 없는 어떠한 접근 방지 및 인터페이스의 보호는 필수적인 이슈이다.

3) 다양한 로더(loader)

CPE의 하드웨어/소프트웨어 환경설정에 따라 칩 로더(loader)는 다양한 부가적인 로더(loader)들을 다운로드 한다.

4) CPE 펌웨어

CPE 펌웨어는 IMCP 클라이언트와 모든 관련 CPE 하드웨어 인터페이스와 다양한 상호작용을 한다.

5) IMCP 클라이언트

IMCP 클라이언트는 CPE의 입력 단으로부터 전달된 모든 CA와 DRM 관련 정보를 뽑아내고 CPE 장치(디스크램블러, 인터페이스)의 관련 설정을 게시한다.

부 속 서 A

(본 부속서는 표준 내용의 일부임)

IMCP 호환 신뢰 시스템의 구현

IMCP 기반 기술 비즈니스를 구현하기 위해 부속서 A는 시장이 다른 경쟁 업체들의 요구를 수용하는 필수 동작 워크플로우에 대한 개요를 제공한다. 작업 흐름(Work Flow)는 IMCP 시스템 구현을 위해 필요한 기술적인 부품에 기반을 둔다. 그림 A-1는 기술적인 구성요소와 시장 이해관계 업체들 간의 상호작용을 보여준다.

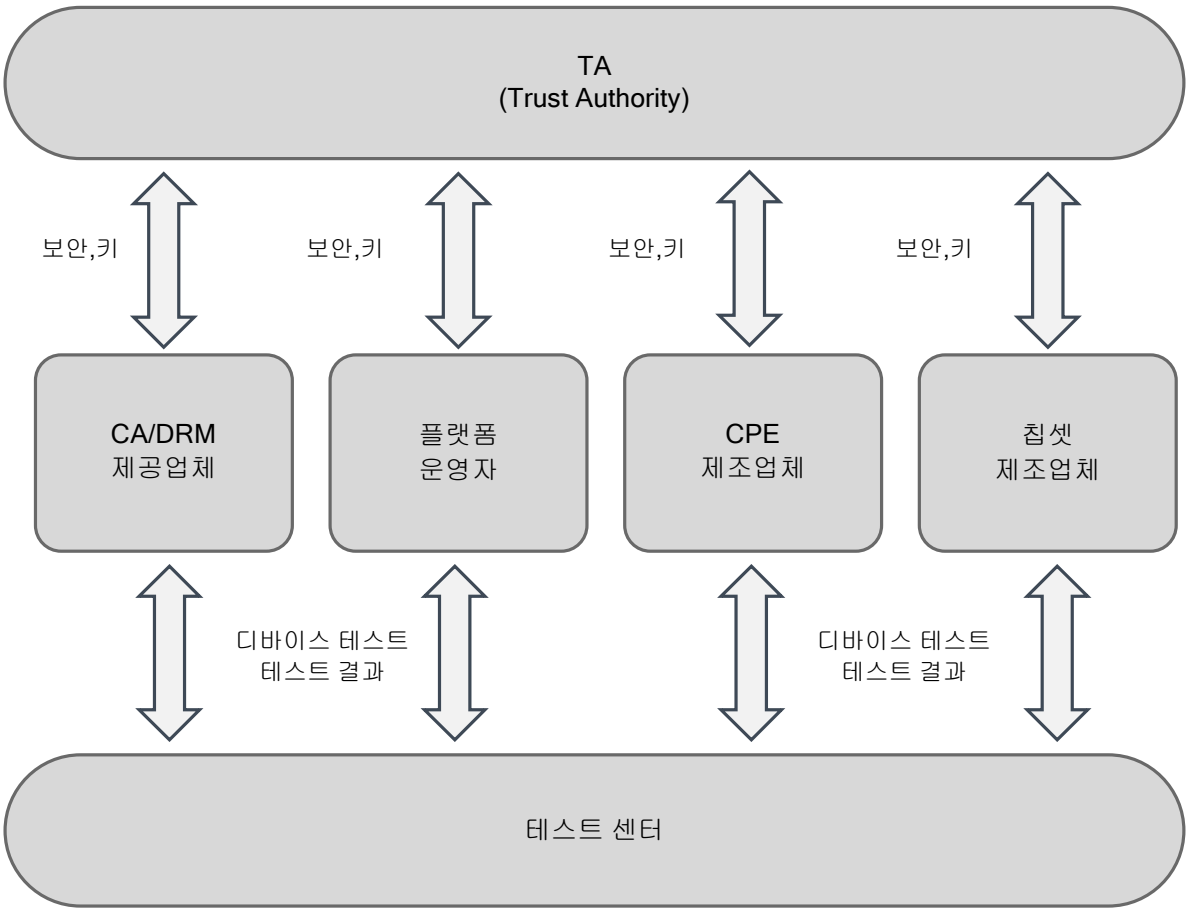

그림 A-1. 일반적인 작업 흐름 (Work Flow) 개요

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.

상기 표준은 본 표준에서 다루고 있는 IMCP 시스템의 유스케이스 및 요구사항을 정의하고 있다.

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ETSI GS ECI 001-3: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation".

[2] ETSI GS ECI 001-4: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine".

[3] ETSI GS ECI 001-5: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System".

[4] ETSI GS ECI 001-6: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: The Trust Environment".

[5] ETSI GS ECI 001-7: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Use cases and Requirements, extended Requirements".

[6] ETSI ISG ECI: "Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions, White paper".

[7] CENELEC EN 50221 (1997-02): "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications".

[8] ETSI TS 101 699 (V1.1.1) (1999-11): "Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification".

[9] CI Plus Specification (V1.3.1) (2011-09): "Content Security Extensions to the Common Interface".

[10] Recommendation ITU-T H.222.0 (2006)/ISO/IEC 13818-1:2007: "Information technology -- Generic coding of moving pictures and associated audio information: Systems".

[11] ETSI EN 300 468 (V1.13.1) (2012-08): "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[12] ETSI TS 103 205: "Digital Video Broadcasting (DVB); Extensions to the CI Plus™ Specification".

[13] ETSI TS 103 162 (V1.1.1) (2010-10): "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification".

[14] ISO 7816: "Information Technology Identification Card Integrated Circuit Cards with contacts".

[15] ETSI ISG ECI: Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions.

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	2017.5.15	제정 FBMF-STD-002	-	UHDTV분과위원회
오류정정				
오류정정				
제2판				