NGB Standard

차세대방송표준포럼표준(국문표준)

NGBF-STD-001 제정일: 2013년 11월 26일

모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템; 서비스 모델 및 구조

Downloadable System for Multi-DRM Service of Mobile Broadcasting; Service Model and Architecture

ngB 차세대방송표준포럼

Next-Generation Broadcast Standards Forum

차세대방송표준포럼표준 (국문표준)
NGBF-STD-001 제정일: 2013년 11월 26일

모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템; 서비스 모델 및 구조

Downloadable System for Multi-DRM Service of Mobile Broadcasting; Service Model and Architecture

서 문

1. 표준의 목적

본 표준의 목적은 모바일 멀티미디어 방송 시스템에서 다운로더블 방식을 기반으로 멀티 DRM 을 운영하고자 하는 자에게 필요한 서비스 모델 및 구조에 관한 기술적 정보를 제공하는데 있다.

2. 주요 내용 요약

본 표준은 모바일 멀티미디어 방송 시스템에서 다운로더블 방식을 기반으로 멀티 DRM 을 운영하기 위한 서비스 모델 및 구조에 대해 기술한다.

보다 구체적으로는 모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템의 참조 모델과 DRM 클라이언트 소프트웨어 다운로드 서비스를 위한 동작 프로토콜 흐름을 기술한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 모바일 멀티미디어 방송 시스템에서 멀티 DRM을 운영하기 위한 시스템 구축 및 운영 방법에 사용되며, 본 표준을 이용할 경우 모바일 방송사들은 보다 적은 투자 비용으로 다양한 형태의 모바일 방송 플랫폼에게 유료 방송 콘텐츠를 제공하는 것이 가능하다.

4. 참조 표준(권고)

4.1. 국외 표준(권고)

- 해당사항 없음

4.2. 국내 표준

- 해당사항 없음

5. 참조 표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

- 해당사항 없음

5.2. 참조한 표준(권고)과 본 표준의 비교표

- 해당사항 없음

6. 지적재산권 관련사항

본 표준의 '지적재산권 확약서' 제출 현황은 차세대방송표준포럼 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	2013.11.26	제정 NGBF-STD-001

8.2. 주요 개정 사항

- 해당사항 없음

Preface

1. Purpose of Standard

This standard provides technical information about the service model and architecture for Multi-DRM service according to downloadable scheme in mobile multimedia broadcasting system.

2. Summary of Contents

This standard specifies the service model and architecture for Multi-DRM service according to downloadable scheme in mobile multimedia broadcasting system.

More specifically, this standard includes the definitions of reference system and the specifications of protocol flows for the downloadable Multi-DRM service in mobile multimedia broadcasting system.

3. Applicable fields of industry and its effect

This standard can be used for establishment and operation of downloadable Multi-DRM service in mobile multimedia broadcasting system. This standard also makes mobile multimedia broadcasting service operators can reduce a cost for providing pay-programs to various types of mobile broadcasting platforms.

4. Reference Standards (Recommendations)

4.1. International Standards (Recommendations)

- None

4.2. Domestic Standards

- None

5. Relationship to Reference Standards(Recommendations)

5.1. Relationship of Reference Standards

- None

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

- None

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	2013.11.26	Established NGBF-STD-001

8.2. Revisions

- None

목 차

Contents

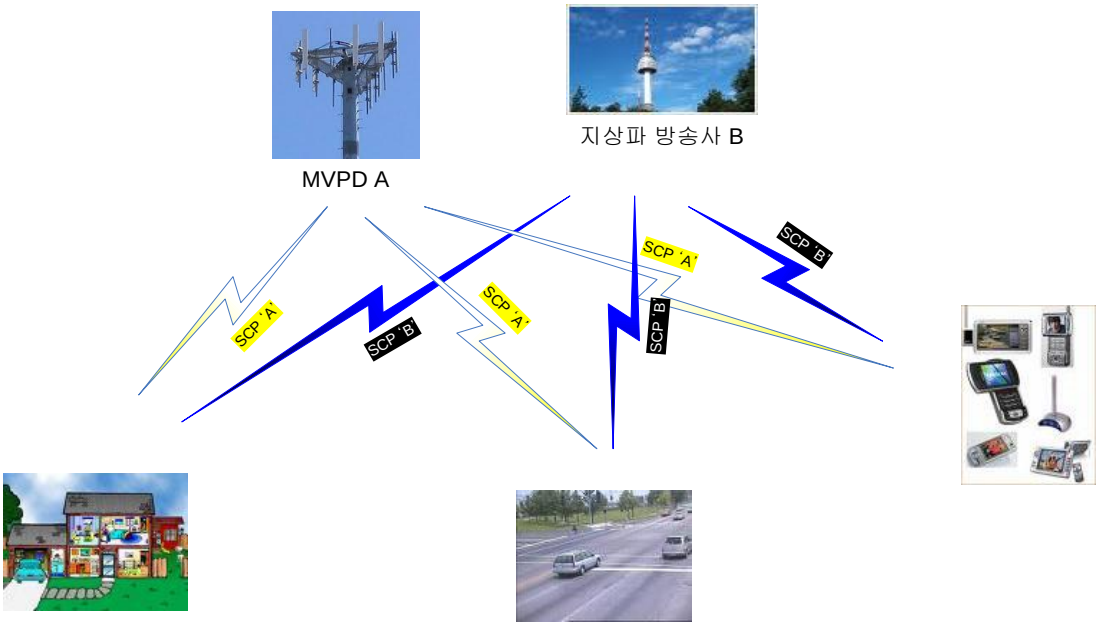
모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템; 서비스 모델 및 구조 (Downloadable System for Multi-DRM Service of Mobile Broadcasting; Service Model and Architecture)

1. 개요

DASH 및 MMT 등 스마트폰 시대에 맞는 차세대 AV 전송 기술에 대한 표준화가 완료 되었고 HTML5 기반의 모바일 방송용 SW 단말플랫폼 표준화 작업이 활발히 진행되고 있다. 이와 더불어 모바일 단말의 고성능화(예, full HD 모바일 디스플레이 패널 등) 현상도 더욱 가속화되고 있다. 이러한 차세대 모바일 방송을 위한 일련의 기술 발달은 일반 품질의 모바일 방송뿐만 아니라 full HD급 이상의 고품질 모바일 방송 서비스들을 앞당기는 역할을 수행할 것으로 예상된다.

모바일 방송 서비스를 제공하기 위해서는 저작권 보호 입장에서 기본적으로 콘텐츠 보호 기술이 필요하다. 특히 일반품질이 아닌 고품질 모바일 방송 서비스를 저작권 문제 없이 원활하게 제공하기 위해서는 더욱 그러하다. 하지만, 현재까지 진행된 차세대 모바일 전송 기술들은 상호 호환성을 염두에 두고 진행된 표준 기술들이 아니며, 각자 고유한 콘텐츠 보호 기술들을 개발하여 사용하고 있다. 또한, 유료방송서비스를 위한 제한수신시스템(Conditional Access System) 사용의 경우를 비추어 볼 때, (그림 1-1)과 같이 모바일 방송사들은 각자 자신들이 선호하는 콘텐츠 보호 기술을 채택하고 사용할 것으로 예상된다. 이러한 상황을 종합적으로 고려해 볼 때, 고품질 모바일 방송 서비스를 제공함에 있어 단일화된 콘텐츠 보호 기술의 사용을 예상하는 것은 매우 어렵다.

복수개의 콘텐츠 보호 기술을 모바일 단말 플랫폼에 적용하여 운영하기 위해서는 크게 세 가지 방법을 고려해 볼 수 있다. 첫 번째 방법은 DRM 클라이언트 소프트웨어 플러그인 (Plug In) 방식으로 제조 시 단말에 탑재하는 방식이다. 두 번째 방법은 DRM 기술 간의 인터페이스 또는 포맷을 공통화 하는 방식이다. 마지막 방법은 방송사에서 DRM 클라이언트 소프트웨어를 다운로드 방식으로 모바일 단말 플랫폼에 탑재하는 방식이다. 각각의 방식은 모두 장점과 단점을 가지고 있지만 모바일 방송 단말 플랫폼의 다양성(예, iOS, 안드로이드, HTML5 등) 및 단말 제조사와 서비스 제공자 간의 독립성 등을 고려할 때 가장 현실적이고 적용 가능성이 높은 방식은 DRM 클라이언트 소프트웨어 다운로드 방식으로 볼 수 있다. 따라서, 본 표준은 복수개의 콘텐츠 보호기술을 모바일 단말 플랫폼에 적용하여 운영하는 세 가지 방법 중 다운로드 방식 기반의 멀티-DRM 서비스 제공을 위한 서비스 모델 및 구조를 정의하고자 한다.



(그림 1-1) 방송사별로 서로 다른 서비스 및 콘텐츠 보호 (SCP) 방식 사용 예

2. 표준의 구성 및 범위

본 표준은 다양한 콘텐츠 보호 기술들이 모바일 방송 플랫폼 내에서 운용되는 데 사용되는 다운로드 기술 기반의 멀티 DRM 서비스 모델 및 구조 규격을 정의한다. 여기서 다운로드 대상은 각 DRM 솔루션 마다 서로 다른 DRM 클라이언트 소프트웨어이다. 단, 본 표준에서는 DRM 클라이언트 소프트웨어 용어 대신 좀더 일반화된 용어인 서비스 및 콘텐츠 보호(Service and Content Protection, SCP) 클라이언트 소프트웨어 용어를 사용한다.

다운로더블 멀티 DRM 서비스를 제공하는 시스템을 본 표준에서는 새롭게 모바일 방송 멀티 DRM 서비스를 위한 다운로더블 시스템(Downloadable system for Multi-DRM service of Mobile Broadcasting, DMMB)으로 정의한다.

3. 참조 표준(권고)

- 해당사항 없음

4. 용어정의

4.1. 액터(Actor)

DMMB 시스템의 역할(Role)과의 상호 작용을 통해 모바일 방송용 멀티 DRM 서비스를 수행하는 행위자를 의미함. 모바일 방송용 멀티 DRM 서비스에서는 '모바일 단말 제조사', '모바일 단말기', 'MVPD 또는 지상파 방송사', 'ADEM 센터' 등 4 가지의 액터(Actor)를 정의함.

4.2. 역할(Role)

모바일 방송용 멀티 DRM 서비스는 'ADE_MSS', 'Application'과 'AA'와 'SCS_ISS'와 'ADE_ISS'와 'CP'와 'SCS_PSS'와 'SCS_MSS'와 같이 총 8 개의 역할(Role)을 정의함. 본 표준에서 역할(Role)은 액터(Actor)와의 상호 작용을 통해 동작되는 DMMB 시스템의 기능을 의미함.

4.3. 다채널 방송 사업자 (Multichannel Video Programming Distributor, MVPD)

지상파 방송사를 제외한 다채널 방송 사업자를 의미하며, DMMB 시스템 액터(Actor) 중의 하나임.

4.4. 응용(Application)

HTML5 웹브라우저 또는 안드로이드 앱 등 비디오 콘텐츠를 디스플레이 하는 기능과 사용자와의 인터페이스를 제공하는 역할을 수행하며, DMMB 시스템 역할(Role) 중의 하나임.

4.5. ADE 에이전트 (ADE Agent, AA)

사용자의 모바일 단말 내에 위치하여 SCP 클라이언트 소프트웨어에 대한 안전한 다운로드 및 초기화 기능을 제공함. ADE 에이전트는 DMMB 운영 시나리오에 따라 모바일 단말 제조 시 탑재 될 수 도 있으며, 사용자가 모바일 단말 운영 중 ADEM 센터를 통해 다운로드 받아 탑재 될 수 있음.

4.6. SCP 클라이언트 소프트웨어 (SCP Client SW, SCS)

DRM 클라이언트 소프트웨어의 보다 일반화된 표현이며, 각 모바일 방송 서비스 제공자마다 고유한 SCP 클라이언트 소프트웨어를 운영함.

4.7. Downloadable system for Multi-DRM service of Mobile Broadcasting (DMMB)

모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템을 의미함. 참고로 DMMB 시스템은 제 3 의 기관으로서의 ADEM 센터가 존재하는 시나리오 상에서 운영될 수도 있으며, ADEM 센터가 존재하지 않는 시나리오 상에서 운영될 수도 있음.

4.8. ADE (Advanced Downloadable security Environment)

모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템 운영 환경을 의미함.

4.9. ADEM 센터 (Advanced Downloadable security Environment Management Center)

MVPD 나 지상파 방송사 외의 제 3 의 기관으로서 ADE 에이전트 다운로드 기능을 포함한 포괄적인 ADE 에이전트 관리 기능을 MVPD 나 지상파 방송사로부터 위탁 받아 수행함. ADEM 센터는 ADE 에이전트 관리에 있어서 기술적 및 법적인 책임을 가짐. 참고로 ADEM 센터가 존재하지 않는 DMMB 운영 시나리오의 경우 MVPD 또는 지상파 방송사가 ADEM 센터 기능을 수행함. DMMB 시스템 액터(Actor) 중의 하나임.

4.10. ADE 에이전트 다운로드 관리 서브 시스템 (Advanced Downloadable security Environment Management Sub-System, ADE_MSS)

이 역할(Role)은 ADEM 센터가 운영되는 시나리오에서는 AA 에 대한 온라인 또는 오프라인 다운로드 관리 기능을 수행하며, ADEM 센터가 운영되지 않는 시나리오에서는 모바일 단말기 제조사를 통한 AA 사전 탑재 기능을 수행함. DMMB 시스템 역할(Role)중의 하나임.

4.11. ADE 에이전트 개인화 서브 시스템(Advanced Downloadable security Environment Initialization Personalization Sub-System, ADE_ISS)

사용자 모바일 단말기에 탑재된 AA 에 대한 개인화 기능을 수행하며, DMMB 시스템 역할(Role) 중의 하나임.

4.12. SCP 클라이언트 소프트웨어 관리 서브 시스템 (SCP Client Software Management Sub-System, SCS_MSS)

SCS_MSS 와 모바일 단말 내 AA 간 보안채널 형성 기능을 수행함. 또한 형성된 보안 채널을 통한 SCS 다운로드 역할 및 SCS Repository 역할을 수행함. DMMB 시스템 역할(Role) 중의 하나임.

4.13. SCP 클라이언트 소프트웨어 개인화 서브 시스템 (SCP Client Software Initialization Personalization Sub-System, SCS_ISS)

모바일 단말에 설치된 SCS 에 대한 개인화 기능을 수행함. DMMB 시스템 역할(Role) 중의 하나임.

4.14. SCP 클라이언트 소프트웨어 정책관리 서브 시스템 (SCP Client Software Policy Sub-System, SCS_PSS)

사용자 시청권한 등급에 따른 차등화된 SCS 다운로드 관리 역할 및 모바일 단말 하드웨어 성능 차이에 따른 SCS 다운로드 관리 기능을 수행함. DMMB 시스템 역할(Role) 중의 하나임.

5. 서비스 모델 및 동작 프로토콜

5.1. 서비스 모델

5.1.1. 참조 모델

모바일 방송용 멀티 DRM서비스를 위한 다운로더블 시스템은 (그림 5-1)과 같이 제3자 인증센터가 존재하지 않는 경우와 제3자 인증센터가 존재하는 경우로 나뉜다. 제3자 인증센터는 AA 설치를 요청하는 가입자가 유효한지 여부를 확인하는 역할을 수행하며 자격권한서버(Authorization Server)와 자격정보(Credentials)들로 구성된다. 본 표준문서

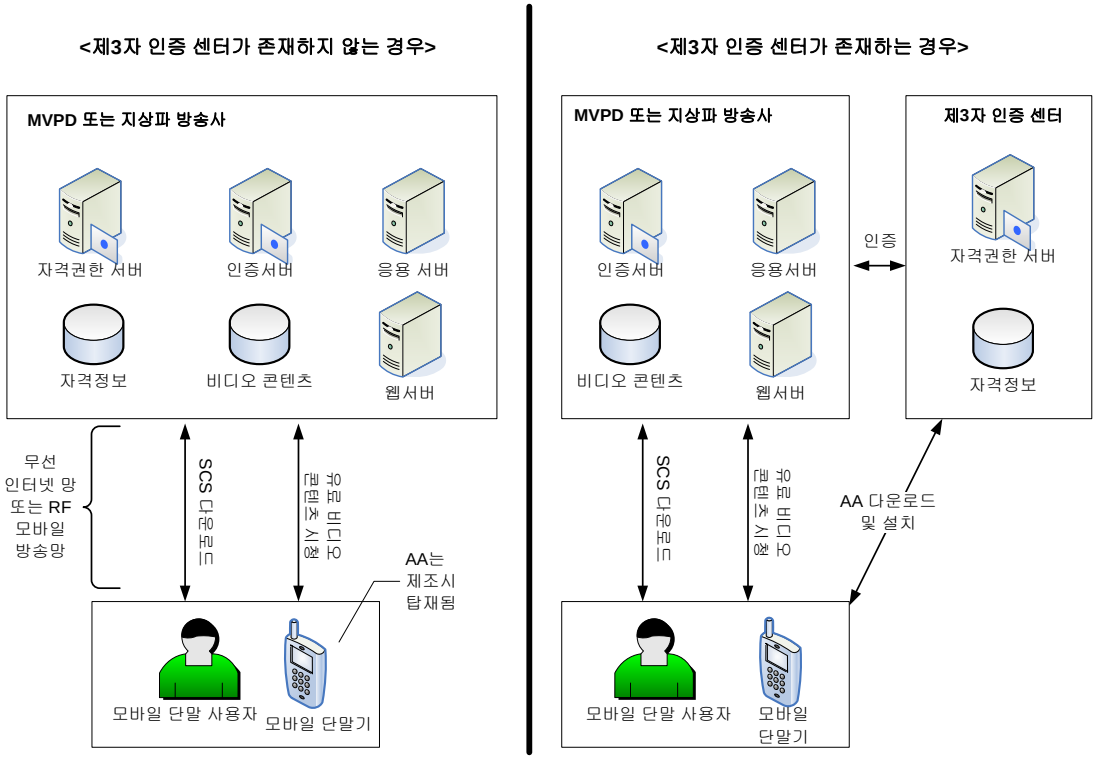
에서는 제3자 인증 센터를 ADEM 센터로 부른다.

제3자 인증센터가 없는 경우에는 자격권한서버와 자격정보들이 MVPD 또는 지상파 방송사 내에서 운영됨을 의미한다. 이때 자격권한서버와 자격정보들은 MVPD 또는 지상파 방송사 내에 존재한다.

제3자 인증센터의 존재 유무에 상관없이 MVPD 또는 지상파 방송사는 모바일 단말기 및 모바일 단말 사용자와 무선 인터넷 망 또는 RF 모바일 방송망으로 연결되어 있다. 이 연결 망을 통해 모바일 단말기는 SCS를 다운로드 받게 되며, 모바일 단말 사용자는 SCS를 다운로드 및 설치한 모바일 단말기를 통해 유료 비디오 콘텐츠를 시청하게 된다.

SCS를 안전하게 다운로드 받기 위해서는 모바일 단말에 AA가 미리 설치 되어 있어야 한다. AA 설치 방법은 제3자 인증 센터의 유무에 따라 다르다. 먼저 제3자 인증 센터가 없는 경우 모바일 단말기 제조사가 AA를 모바일 단말기 제조 시 탑재해야 한다. 이때 AA는 MVPD 또는 지상파 방송사로부터 직접 제공 받거나 MVPD 또는 지상파 방송사가 위임한 제3의 기관을 통해 받을 수 있다.

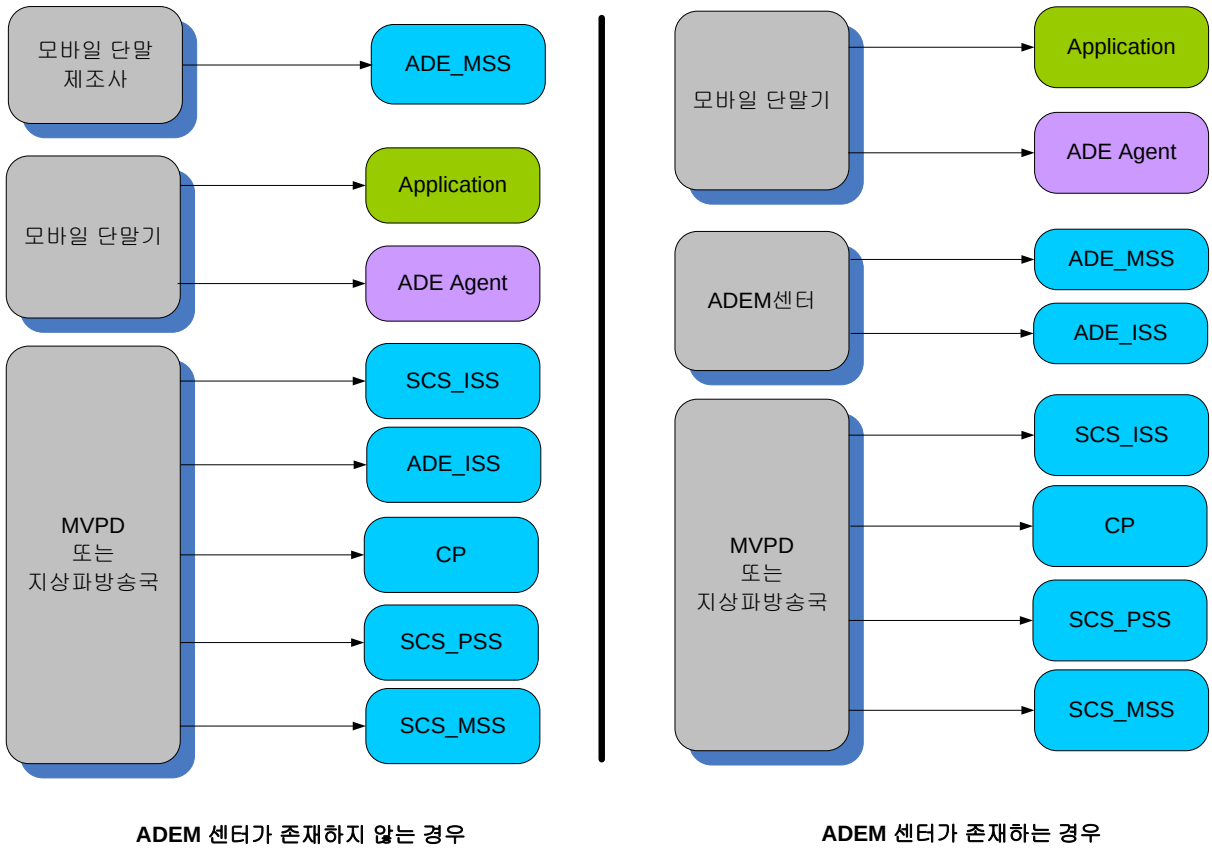
반대로 제3자 인증 센터가 존재하는 경우 AA는 사용자의 모바일 단말기에 온라인 또는 오프라인 방식을 통해 탑재될 수 있다. 온라인 방식을 통해 다운로드 및 설치 되는 경우는 제3자 인증센터와 모바일 단말기간 약속된 통신 프로토콜 방식을 사용해야 하며, AA가 다운로드 되는 동안 해킹되지 않도록 충분한 보안이 제공 돼야 한다. AA를 온라인 방식으로 다운로드 하기 위해 필요한 통신 프로토콜에 대한 정의는 본 표준문서 범위 밖이다. 오프라인 방식으로 AA를 모바일 단말기에 탑재하는 경우는 MVPD 또는 지상파 방송사(MVPD 또는 지상파 방송사로부터 권한을 위임 받은 제3의 기관)를 모바일 단말 사용자가 직접 방문하는 경우에 해당된다. 구체적인 방법 및 절차 역시 본 표준문서 범위 밖이다.



(그림 5-1) DMMB 시스템 참조 모델

5.1.2. 액터(Actor) 및 역할(Role)

모바일 방송용 멀티 DRM서비스를 위한 다운로더블 시스템은 (그림 5-2)에 그려진 바와 같이 액터(actor)들 및 역할(Role)들을 갖는다. 그림의 왼쪽은 ADEM센터가 존재하지 않는 경우에 액터(actor)들과 역할(Role)들간의 관계를 나타내며, 오른쪽은 ADEM센터가 존재하는 경우에 액터(actor)들과 역할(Role)들간의 관계를 나타낸다.



(그림 5-2) 액터(Actor)와 역할(Role)간의 관계

주요 역할(Role)들에 대한 설명은 <표 5-1>에 기술된 바와 같다.

<표 5-1> 역할(Role)

역할	설명
ADE_MSS	• Advanced Downloadable security Environment Management Sub-System의 약어 • ADEM센터가 운영되는 시나리오에서는 AA 온라인/오프라인 다운로드 관리 기능 • ADEM센터를 운영하지 않는 시나리오에서는 제조사를 통해 AA가 사전 탑재기능을 수행
ADE_ISS	• Advanced Downloadable security Environment Initialization personalization Sub-System • AA 개인화(Personalization) 기능 수행

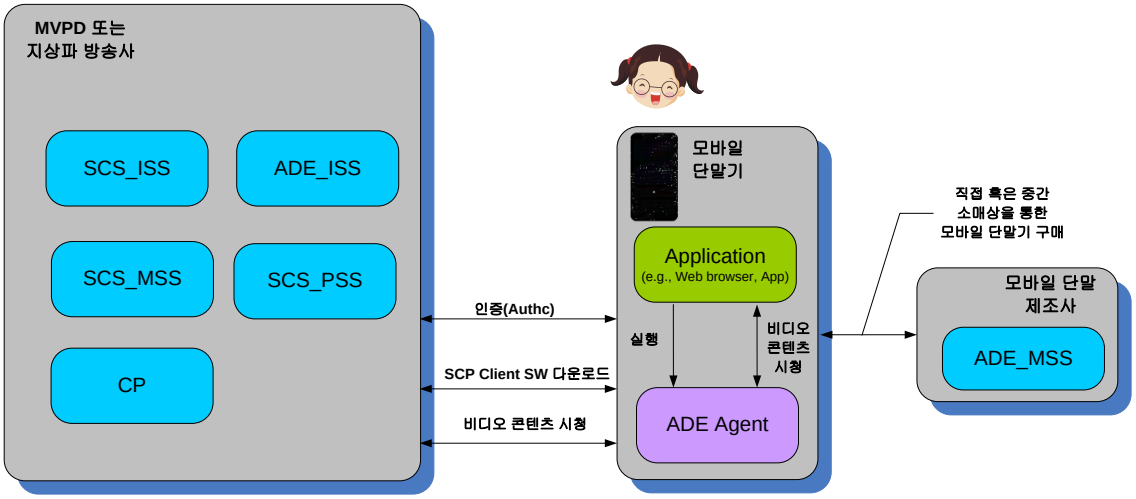
Application	• HTML5 웹브라우저 또는 안드로이드 앱 등 비디오 콘텐츠를 디스플레이 하는 기능과 사용자와의 인터페이스를 제공함
CP	• 콘텐츠 제공자 (Content Provider)의 약자 • 콘텐츠 목록을 단말에 제공하는 기능 수행 (참고로 SCS가 휴대단말에 설치되기 전이라도 사용자는 콘텐츠 목록을 볼 수 있어야 함) • 콘텐츠 저장소 (Content Repository) 기능 수행 • 일반적인 비디오 스트리밍 관리 (video streaming management) 기능 수행
SCS_ISS	• SCP Client Software Initialization personalization Sub-System의 약자 • SCS 개인화 작업 수행
SCS_MSS	• SCP Client Software Management Sub-System의 약자 • SCS_MSS와 모바일 단말 내 AA간 보안채널 형성 기능 수행 • SCS 다운로드 기능 수행 • SCS 저장소(Repository) 기능 수행
SCS_PSS	• SCP Client Software Policy Sub-System의 약자 • 사용자 시청권한 레벨에 따른 차등화된 SCS 다운로드 기능 제공 • 모바일 단말 하드웨어 성능 (hardware capability) 차이에 따른 SCS 관리 기능 제공

5.1.3. 시스템 아키텍처

모바일 방송용 멀티 DRM서비스를 위한 다운로더블 시스템 아키텍처는 ADEM 센터가 존재하지 않는 경우(5.1.3.1절) 와 존재하는 경우(5.1.3.2절)로 나눌 수 있다. 각 경우에 대한 자세한 설명은 이어지는 절들과 같다.

5.1.3.1. ADEM센터가 존재하지 않는 경우

모바일 방송용 멀티 DRM서비스를 위한 다운로더블 시스템에서 ADEM센터가 존재하지 않는 경우에 대한 시스템 아키텍처는 (그림 5-3)과 같으며 수행 절차의 한 예는 <표 5-2>와 같다.



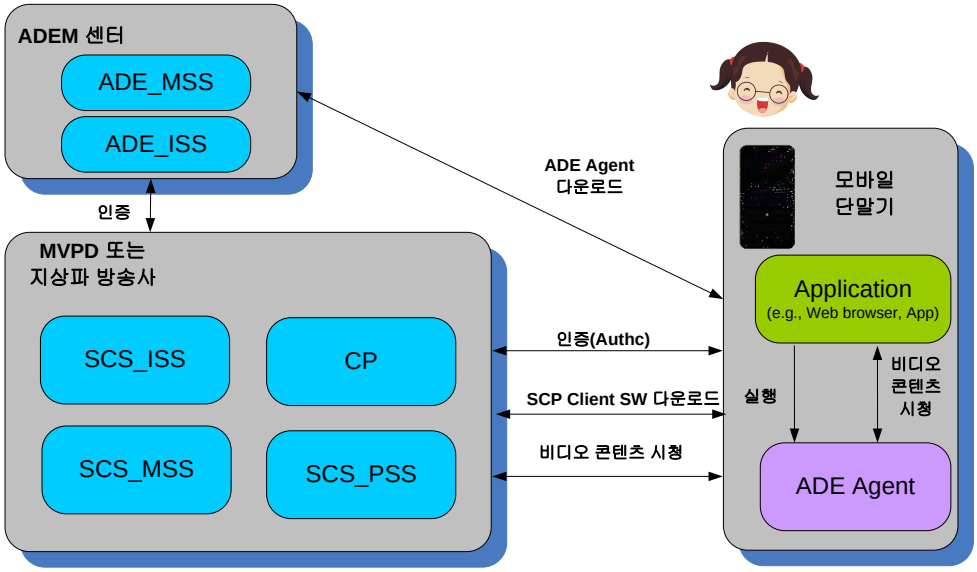
(그림 5-2) ADEM센터가 존재하지 않는 경우에 대한 시스템 아키텍처

<표 5-2> ADEM센터가 존재하지 않는 경우에 대한 기본 동작 절차 (참고사항)

절차	동작	설명	참여 역할(Role)
0	모바일 단말 제조 시 AA 탑재	• 본 시나리오에서는 AA가 모바일 단말 제조사에 의해 이미 모바일 단말에 탑재되어 있는 경우임	
1	AA 실행	• DMMB방식 모바일 방송 서비스 접속 시 Application은 AA 실행 • AA는 모바일 단말기에 탑재되어 있지만 개인화가 이루어지지 않은 경우 AA 개인화 수행	• ADE_MSS • ADE_ISS
2	SCS 다운로드 및 설치	• Application은 AA를 통해 SCS 다운로드 및 설치 • 사용자의 시청 권한 및 단말의 하드웨어 성능에 따라 서로 다른 SCS를 다운로드 받음 후 개인화 과정 수행 • SCS에는 서비스 제공 사업자의 고유한 콘텐츠 보호 방식이 포함되어 있음	• SCS_PSS • SCS_MSS • SCS_ISS
3	콘텐츠 선택 및 시청	• 사용자의 시청 권한으로 볼 수 있는 콘텐츠 목록을 CP로부터 다운로드 받게 되며, 사용자는 그 목록 중 원하는 콘텐츠를 선택한 후 시청	• CP • SCS_PSS

5.1.3.2. ADEM센터가 존재하는 경우

모바일 방송용 멀티 DRM서비스를 위한 다운로더블 시스템에서 ADEM센터가 존재하는 경우에 대한 시스템 아키텍처는 (그림 5-3)와 같으며 수행 절차의 한 예는 <표 5-3>과 같다.



(그림 5-3) ADEM센터가 존재하는 경우에 대한 시스템 아키텍처

<표 5-3> ADEM센터가 존재하는 경우에 대한 기본 동작 절차 (참고사항)

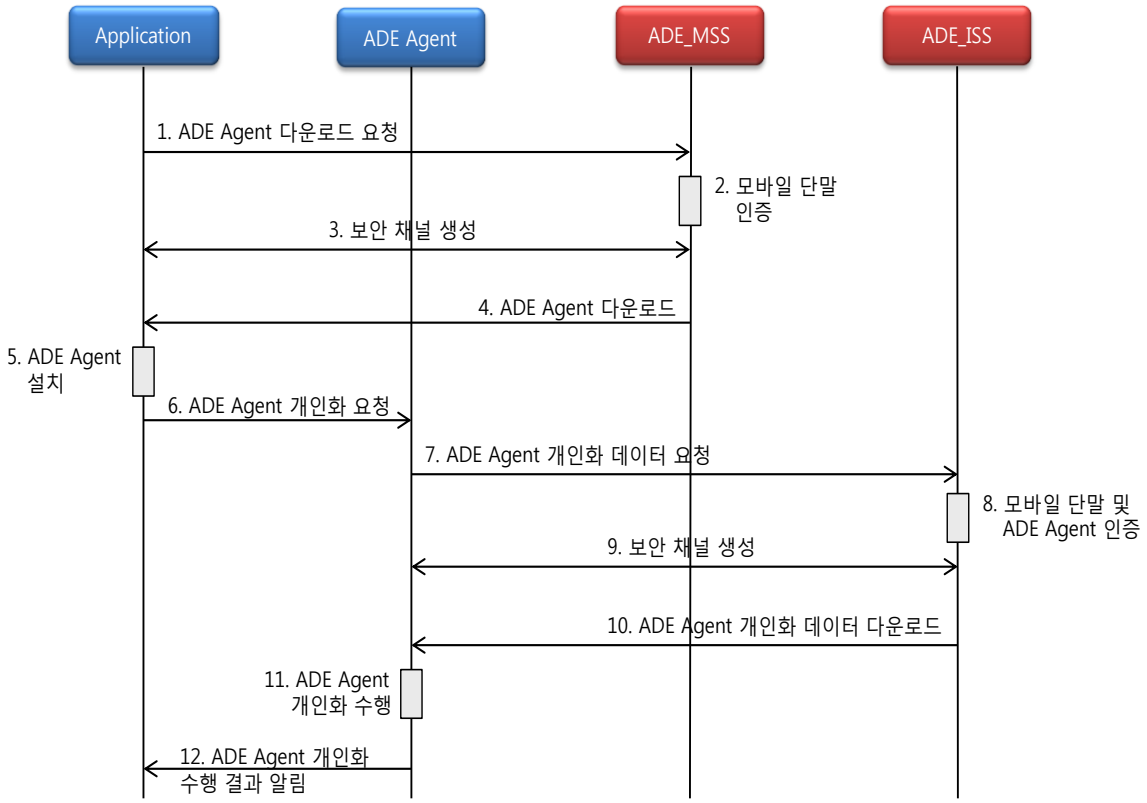
절차	동작	설명	참여 역할(Role)
0	ADEM센터를통한 AA 탑재	• 온라인 또는 오프라인 방식으로 모바일 단말기는 ADEM센터내 ADE_MSS를 통해 AA를 탑재함 • 모바일 단말기와 ADEM센터 간의 구체적인 통신 프로토콜은 본 표준 범위 밖임	
1	AA 실행	• DMMB방식 모바일 방송 서비스 접속 시 Application은 AA 실행 • AA는 모바일 단말기에 탑재되어 있지만 개인화가 이루어지지 않은 경우 AA 개인화 수행	• ADE_MSS • ADE_ISS
2	SCS 다운로드 및 설치	• Application은 AA를 통해 SCS 다운로드 및 설치 • 사용자의 시청 권한 및 단말의 하드웨어 성능에 따라 서로 다른 SCS를 다운로드 받음 후 개인화 과정 수행 • SCS에는 서비스 제공 사업자의 고유한 콘텐츠 보호 방식이 포함되어 있음	• SCS_PSS • SCS_MSS • SCS_ISS
3	콘텐츠 선택 및 시청	• 사용자의 시청 권한으로 볼 수 있는 콘텐츠 목록을 CP로부터 다운로드 받게 되며, 사용자는 그 목록 중 원하는 콘텐츠를 선택한 후 시청	• CP • SCS_PSS

5.2. 서비스 동작 프로토콜

5.2.1. ADE 에이전트 다운로드 및 설치 동작

5.2.1.1.ADE 에이전트 다운로드, 설치, 개인화 수행

본 서비스 동작 시나리오에서는 AA가 모바일 단말에 설치되어 있지 않은 경우 ADE 센터를 통해서 AA를 다운로드 하여 설치하고 개인화를 수행하는 절차에 대해서 기술한다. 본 시나리오는 ADEM센터가 존재하는 경우에만 해당된다.



(그림 5-4) AA 다운로드와 설치 및 개인화 수행 흐름 (ADEM센터가 존재하는 경우)

<표 5-4> AA 다운로드와 설치 및 개인화 수행 단계 (ADEM센터가 존재하는 경우)

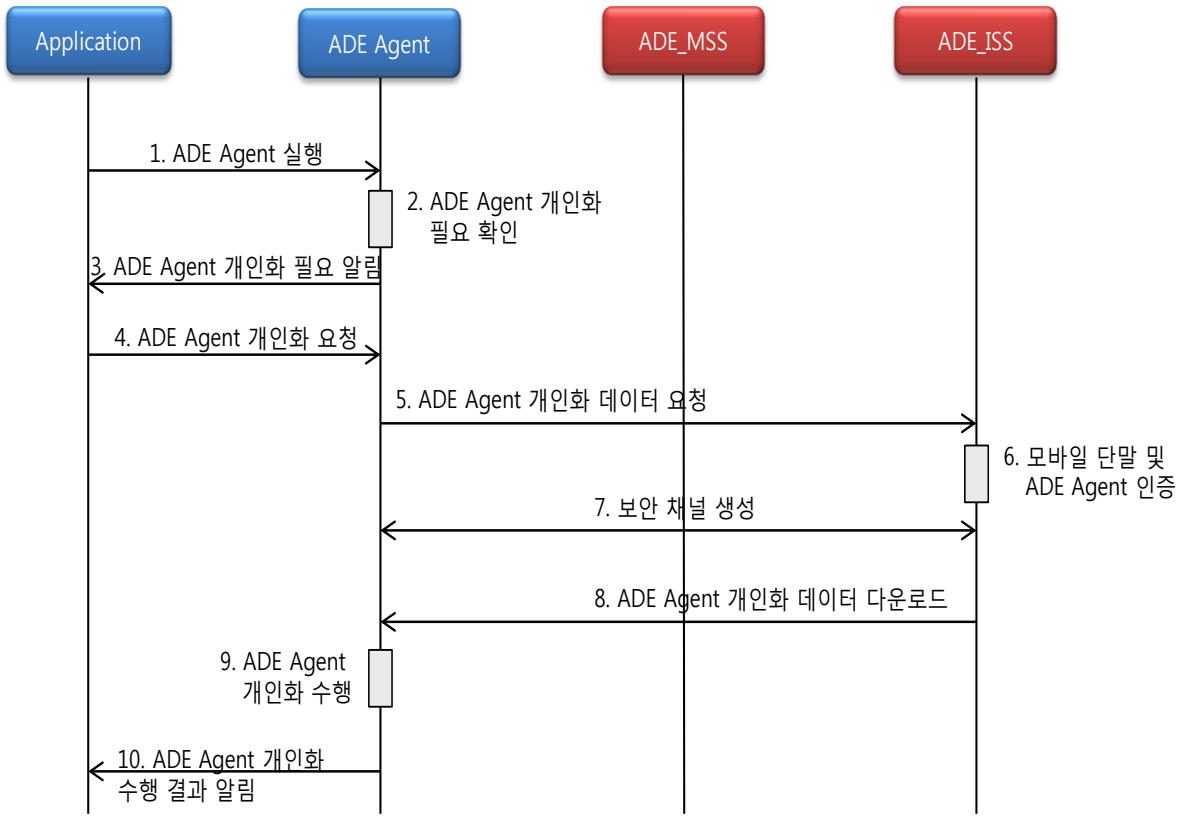
절차	동작	설명
1	AA 다운로드 요청	Application은 AA가 모바일 단말에 설치되어 있지 않음을 인식하고 ADE_MSS로 AA 다운로드 요청 메시지를 전달한다. ADE_MSS의 위치 정보는 모바일 단말 내에 또는 Application에 미리 구성되어 있는 정보를 이용할 수 있다. 다운로드 요청 메시지 전달 시 모바일 단말 수준 또는 Application에서 제공하는 인증 식별자/키 정보, 모바일 단말 정보 등이 전달된다. 단말기 제조사 의존적인 모바일 단말 정보 등의 구성 방식 및 관리 정책에 대한 표준화는 본 문서 범의 밖이다.
2	모바일 단말 인증	ADE_MSS는 AA 다운로드 요청 메시지에 포함된 인증 식별자/키 정보를 이용하여 모바일 단말 인증을 수행한다.
3	보안채널 형성	ADE_MSS는 AA의 안전한 다운로드를 위해 Application과 ADE_MSS 간 보안 채널을 생성한다. 보안 채널은 Application과 ADE_MSS에 대한 실체(Entity) 인증과 다운로드 하는 AA에 대한 메시지(Message) 인증, 기밀성, 무결성을 제공한다.
4	AA 다운로드	ADE_MSS는 보안 채널을 이용하여 모바일 단말에 적합한 AA를 안전하게 다운로드 한다.

5	AA 설치	Application은 다운로드 한 AA를 설치한다. 설치 방법은 각 단말사의 구현에 의존한다.
6	AA 개인화 요청	Application은 설치한 AA에 대해 개인화 수행을 요청한다.
7	AA 개인화 데이터 요청	AA는 개인화를 수행하기 위해 ADE_ISS에 개인화 데이터 요청 메시지를 전송한다. ADE_ISS의 위치 정보는 AA 다운로드 시 함께 제공되거나 AA 구현 내부에 미리 구성될 수 있다. 개인화 데이터 요청 시 모바일 단말 수준 또는 Application에서 제공하는 인증 식별자/키 정보와 설치한 AA에 대한 정보가 함께 전달된다.
8	모바일 단말 및 AA 인증	ADE_ISS는 개인화 데이터 요청 메시지에 포함된 인증 식별자/키 정보 및 AA 정보를 이용하여 모바일 단말 인증을 수행한다.
9	보안채널 형성	ADE_ISS는 개인화 데이터의 안전한 다운로드를 위해 Application과 ADE_ISS 간 보안 채널을 생성한다. 보안 채널은 Application과 ADE_ISS에 대한 실체(Entity) 인증과 다운로드 하는 개인화 데이터에 대한 메시지(Message) 인증, 기밀성, 무결성을 제공한다.
10	AA 개인화 데이터 다운로드	ADE_ISS는 보안 채널을 이용하여 AA로 개인화 데이터(AA 식별자 및 필요 인증서 포함)를 안전하게 전달한다.
11	AA 개인화 수행	개인화 데이터를 수신한 AA는 다운로드 받은 개인화 데이터를 이용하여 개인화를 수행한다.
12	AA 개인화 수행 결과 알림	AA는 Application에게 성공적으로 개인화를 수행하였음을 알린다.

상기 시나리오에서 ADE_MSS와 ADE_ISS가 상호 연동이 되는 경우 AA 다운로드와 개인화 데이터 다운로드를 동시에 수행할 수도 있다.

5.2.1.2. ADE 에이전트 개인화 수행

본 서비스 동작 시나리오에서는 AA가 모바일 단말 제조사에 의해 이미 모바일 단말에 탑재 되어 있지만 개인화가 이루어지지 않은 경우 개인화 수행 절차에 대해 기술한다. ADEM센터가 존재하지 않는 경우에만 해당된다.



(그림 5-5) AA 개인화 수행 흐름 (ADEM센터가 존재하지 않는 경우)

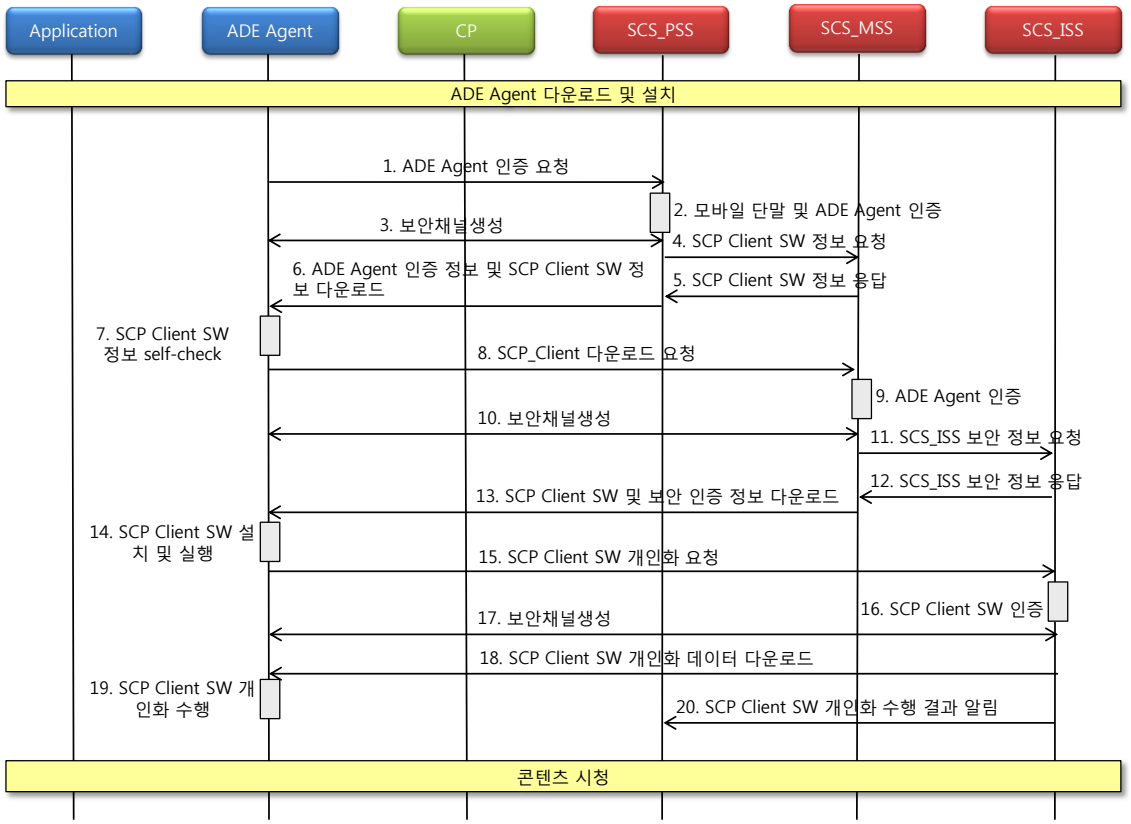
<표 5-5> AA 개인화 수행 단계 (ADEM센터가 존재하지 않는 경우)

절차	동작	설명
1	AA 실행	Application이 AA를 실행 시킨다
2	AA 개인화 필요 확인	AA는 내부적으로 AA가 단말기 제조사에 의해 또는 ADE 센터를 통해 설치된 이후 개인화가 되어 있는지 확인한다. (본 시나리오에서는 개인화가 되어 있지 않은 상태이다.).
3	AA 개인화 필요 알림	AA는 Application에게 AA의 개인화 단계가 필요함을 알린다.
4	AA 개인화 요청	Application은 AA에게 개인화를 수행할 것을 요청한다.
5	AA 개인화 데이터 요청	AA는 개인화를 수행하기 위해 ADE_ISS에 개인화 데이터 요청 메시지를 전송한다. ADE_ISS의 위치 정보는 AA 다운로드 시 함께 제공되거나 AA 구현 내부에 미리 구성되어질 수 있다. 개인화 데이터 요청 시 모바일 단말 수준 또는 Application에서 제공하는 인증 식별자/키 정보와 설치한 AA에 대한 정보가 함께 전달된다.
6	모바일 단말및AA 인증	ADE_ISS는 개인화 데이터 요청 메시지에 포함된 인증 식별자/키 정보 및 AA 정보를 이용하여 모바일 단말 인증을 수행한다.

7	보안채널생성	ADE_ISS는 개인화 데이터의 안전한 다운로드를 위해 Application과 ADE_ISS 간 보안 채널을 생성한다. 보안 채널은 Application과 ADE_ISS에 대한 실체(Entity) 인증과 다운로드 하는 개인화 데이터에 대한 메시지(Message) 인증, 기밀성, 무결성을 제공한다.
8	AA 개인화 데이터 다운로드	ADE_ISS는 보안 채널을 이용하여 AA로 개인화 데이터(AA 식별자 및 필요 인증서 포함)를 안전하게 전달한다.
9	AA 개인화 수행	개인화 데이터를 수신한 AA는 다운로드 받은 개인화 데이터를 이용하여 개인화를 수행한다.
10	AA 개인화 수행 결과 알림	AA는 Application에게 성공적으로 개인화를 수행하였음을 알린다.

5.2.2. SCP Client 다운로드 및 설치 동작

본 서비스 동작 시나리오에서는 AA 다운로드 및 설치가 종료된 이후 SCS의 다운로드 및 설치 동작에 대해서 기술한다. 본 절차는 ADEM센터가 존재하는 경우와 존재하지 않는 경우 모두에 해당된다.



(그림 5-6) SCS 다운로드 및 설치 수행 흐름

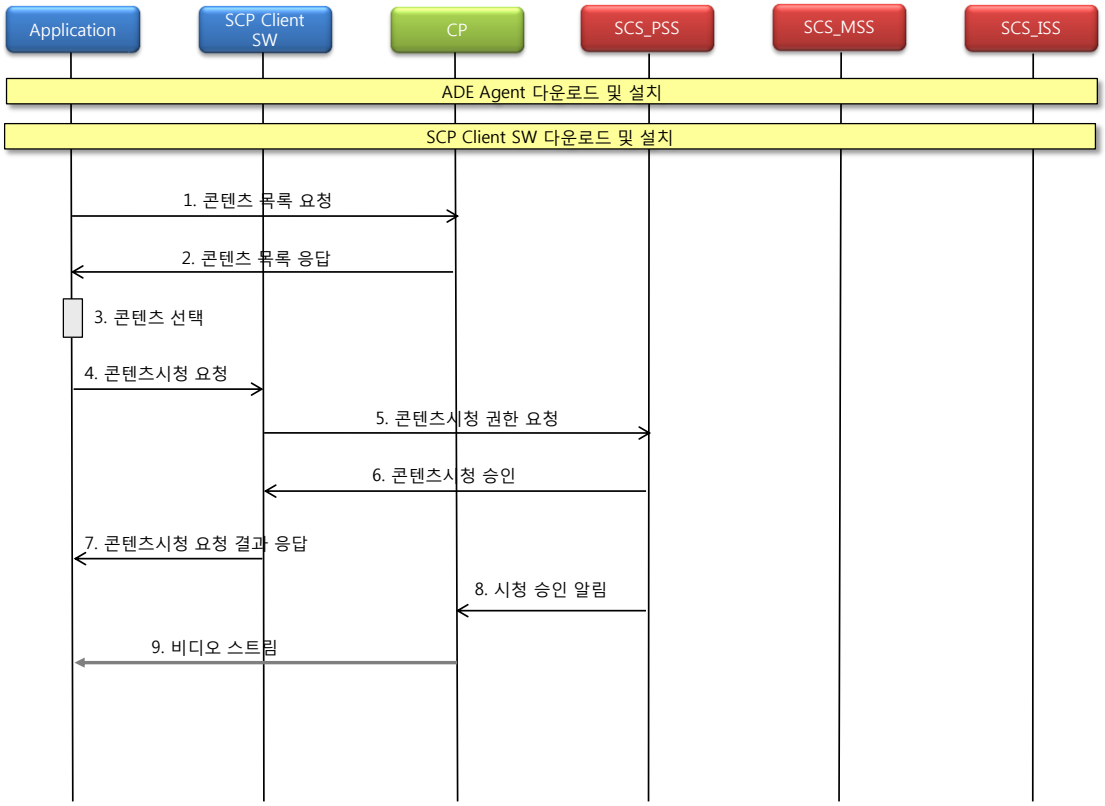
<표 5-6> SCS 다운로드 및 설치 수행 단계

절차	동작	설명
1	AA 인증 요청	AA는 모바일 단말 및 AA를 인증하기 위해 SCS_PSS로 인증 요청 메시지를 전송한다.
2	모바일 단말 및AA 인증	SCS_PSS는 AA 인증 요청 메시지에 포함된 AA 개인화 데이터 및 단말 정보를 이용하여 모바일 단말 및 AA 인증을 수행한다.
3	보안채널생성	SCS_PSS는 AA 인증 정보 및 다운로드 가능한 SCP Client 정보를 안전한 다운로드를 위해 AA 와 보안 채널을 생성한다.
4	SCS 정보 요청	SCS_PSS는 SCS_MSS로 인증 완료된 단말에서 사용 가능한 SCS 정보 요청 메시지를 전송한다. 이때 SCS 정보 요청 메시지에는 AA 인증 정보를 포함한다.
5	SCS 정보 응답	SCS_MSS는 SCS_PSS로 인증 완료된 단말에서 사용 가능한 SCS 정보와 SCS_MSS 보안 인증 정보를 전송한다.
6	AA 인증 정보 및 SCS 정보 다운로드	SCS_PSS는 보안 채널을 이용하여 AA로 다운로드 가능한 SCS 정보와 AA에 대한 SCS_MSS 보안 인증 정보를 안전하게 전달한다.
7	SCS 정보 self-check	AA는 SCS_PSS로부터 전달 받은 SCS 정보를 기반하여 단말에 해당 SCS 의 다운로드 유무를 확인 한다.
8	SCS 다운로드 요청	AA는 해당 단말에서 다운로드 가능한 SCS 를 다운로드 하기 위해 SCS_MSS로 SCS 다운로드 요청 메시지를 전송한다.
9	AA 인증	SCS_MSS는 SCS 다운로드 요청 메시지에 포함된 AA에 대한 SCS_MSS 보안 인증 정보를 이용하여 AA 인증을 수행한다.
10	보안채널생성	SCS_MSS는 SCS의안전한 다운로드를 위해 AA와 보안 채널을 생성한다.
11	SCS_ISS 보안 정보 요청	SCS_MSS는 SCS_ISS로 AA에 대한 SCS_ISS 보안 인증 정보를 요청한다.
12	SCS_ISS 보안 정보 응답	SCS_ISS는 SCS_PSS로 SCS 개인화 정보 요청 시 인증을 위한 SCS_ISS 보안 인증 정보를 전송한다.
13	SCS 및 보안 인증 정보 다운로드	SCS_MSS는 보안 채널을 이용하여 SCS 와 AA에 대한 SCS_ISS 보안 인증 정보를 안전하게 전달한다.
14	SCS 설치 및 실행	AA는 안전하게 다운로드 한 SCS 를 설치하고 실행한다.
15	SCS 개인화 요청	SCS 는 개인화를 수행하기 위해 SCS_ISS에 개인화 데이터 요청 메시지를 전송한다.
16	SCS 인증	SCS_ISS는 SCS 개인화 요청 메시지에 포함된 SCS_MSS 보안 인증 정보를 이용하여 SCS 인증을 수행한다.
17	보안채널생성	SCS_ISS는 SCS 개인화 데이터를 안전한 다운로드를 위해 SCS 와 보안 채널을 생성한다.
18	SCS 개인화 데이터	SCS_ISS는 보안 채널을 이용하여 SCS 로 개인화 데이터를

	다운로드	안전하게 전달한다.
19	SCS 개인화 수행	개인화 데이터를 수신한 SCS 는 다운로드 받은 개인화 데이터를 이용하여 개인화를 수행한다.
20	SCS 개인화 수행 결과 알림	SCS_ISS는 SCS_PSS에게 성공적으로 개인화를 수행하였음을 알린다.

5.2.3. 콘텐츠 시청 동작 (참고사항)

본 서비스 동작 시나리오에서는 '5.2.1 AA 다운로드 및 설치 동작' 및 '5.2.2 SCS 다운로드 및 설치 동작'이 종료된 이후 콘텐츠 시청 동작 흐름에 대해서 기술한다. 본 흐름은 본 표준규격 범위 밖일 뿐만 아니라 실제 서비스 제공자에 따라 상이하게 제공될 가능성이 높은 내용이므로 참고사항이다.



(그림 5-7) 콘텐츠 시청 동작 흐름 (참고사항)

<표 5-7> 콘텐츠 시청 동작 단계 (참고사항)

절차	동작	설명
1	콘텐츠 리스트 요청	Application는 CP에게 콘텐츠 리스트를 요청한다. 이 과정은 Application에 따라 SCS 다운로드 이전에 수행될 수 있다.
2	콘텐츠 리스트 응답	CP는 Application에게 콘텐츠 리스트를 전송한다.
3	콘텐츠 선택	시청자는 CP로부터 전달받은 콘텐츠 리스트로부터 콘텐츠를 선택한다. 이때 권한에 따라 선택 가능한 콘텐츠 리스트가 달라 질 수 있다.
4	콘텐츠 시청 요청	Application은 SCS 로 선택한 콘텐츠에 대한 시청 요청을 한다.
5	콘텐츠 시청 권한 요청	SCS 은 SCS_PSS로 선택한 콘텐츠에 대한 시청 권한을 요청한다.
6	콘텐츠 시청 승인	SCS_PSS에서는 시청 권한 요청 메시지에 포함된 휴대 단말 하드웨어 성능을 확인하고 해당 단말에서의 시청 가능 여부를 응답한다.
7	콘텐츠 시청 요청 결과 응답	SCS는 Application로 선택한 콘텐츠에 대한 시청 가능 여부에 대한 정보를 전달한다
8	시청 승인 알림	선택한 콘텐츠의 시청이 가능한 경우 SCS_PSS는 CP로 시청 요청을 보낸다.
9	비디오 스트림	CP는 선택된 콘텐츠의 비디오 스트림을 Application에 송출한다.

차세대방송표준포럼표준(국문표준)

모바일 방송용 멀티 DRM 서비스를 위한 다운로더블 시스템;
서비스 모델 및 구조
(Downloadable System for Multi-DRM Service of Mobile Broadcasting;
Service Model and Architecture)

발행인 : 차세대방송표준포럼 의장
발행처 : 차세대방송표준포럼
135-703, 서울시 강남구 테헤란로 7 길 22 본관 610 호
(역삼동 한국과학기술회관)
Tel : 02-568-3556, Fax : 02-568-3557
http://www.nextb.or.kr/
발행일 : 2013.11.26