通信情報保護學會誌
第 7卷 第1號, 1997. 3

DAVIC 에서의 보안 기법

DAVIC Security

염 흥 열*

요 약

본 고에서는 DAVIC(Digital Audio-Visual Council)에서 권고 중인 액세스 제어 기법을 분석한다. 이를 위하여 DAVIC 보안 기법을 분석 및 제시하고, 보안 시스팀을 위한 참조 모델과 요구되는 서비스 및 보안 메카니듬을 분석한다. 현재 DAVIC에서는 보안을 위해 표준화를 진행 중에 있으므로 현재까지 표준화되고 있는 내용을 중심으로 기술한다.

1. 서 론

멀티미디어 신호는 광대역 ISDN을 통해 활발히 유통되거나 저장 매체를 통해 저장될 예정이다. 최근 DAVIC에서는 쌍방향 비디오 서비스에 대한 국제 표준화에 대한 연구를 수행하고 있다. 이들 비디오-오디오 시스템에서의 핵심 기능은 비인가자에 대한 비디오 신호의 액세스를 제한하는 액세스 제어 기술이다. 액세스 제어는 가입자측 장비인 STU(Set-top Unit), 가입자당 보안 기능을 수행하는 스마트 카드 형태로 실현될 보안 장치, 그리고 서비스 제공자의 자격 관리 및 제어 기능을 담당하는 한정 액세스 장치 등을 이용하여 실현될 것이다. 보안 모듈과 STU와의 인터페이스는 ISO-7816 권고안을 따르는 CA1 인터페이스와 별도의 독립적인 인터페이스를 따르는 CA0 인터페이스가 있다. 광대역 ISDN이 구축되면서, 디지탈 오디오 및 비디오 서비스에 대한 요구는 급증할 추세이다. 본 고에서는 DAVIC 에서 권고중인 액세스 제어 기법을 분석한다. 이를 위하여 DAVIC에서의 보안 기법을 분석하고, 보안 시스팀을 위한 참조 모델과 요구되는 서비스 및 보안 메카니듬을 분석한다. 2장에서는 액세스 제어를 위한 일반 방식을 분석하고 3장에서는 CA1 인터페이스를 정의하였다.

* 순천향대학교 전기전자공학부

2. DAVIC에서의 액세스 제어 방식 분석

여기에서는 DAVIC의 최종 사용자, 전달 시스템, 서비스 제공자, 그리고 내용 제공자에 의해 사용되는 기본 보안 서비스(Security Service) 의 집합을 정의한다. 이를 위하여 DAVIC 보안을 위한 기본 요구 사항, 일반 보안 서비스, 보안 서비스를 위한 보안 기법, 그리고 보안 시스템 구조 등을 분석한다.[1,2,3,4,5,6]

2.1 DAVIC 시스템

DAVIC 시스템은 그림 2.1과 같이 5 개의 시스템 개체들로 구성된다. 이는 내용 제공자 시스템(Content Provider System), 서비스 제공자 시스템(Service Provider System), 서비스 고객(Service Client), 내용 제공자와 서비스 제공자를 연결하기 위한 전달 시스템(Delivery System), 그리고 서비스 고객과 서비스 제공자를 연결하기 위한 또 하나의 전달 시스템으로 구성된다. DAVIC 시스템에서의 각 시스템 개체 간의 정보 흐름은 주 서비스 계층(Principal Service Layer)을 위한 S1 정보 흐름, 응용 서비스 계층(Application Service Layer)을 위한 S2 정보 흐름, 세션 및 트랜스포트 서비스 계층(Session/Transport Service Layer)을 위한 S3 정보 흐름, 그리고 망 서비스 계층을 위한 S4 정보 흐름 등이 있다. VOD 보안 서비스를 위한 스크램블링은 S1 정보 흐름 계층에서, 인증 기능은 S3 정보 흐름 계층에서 수행된다.

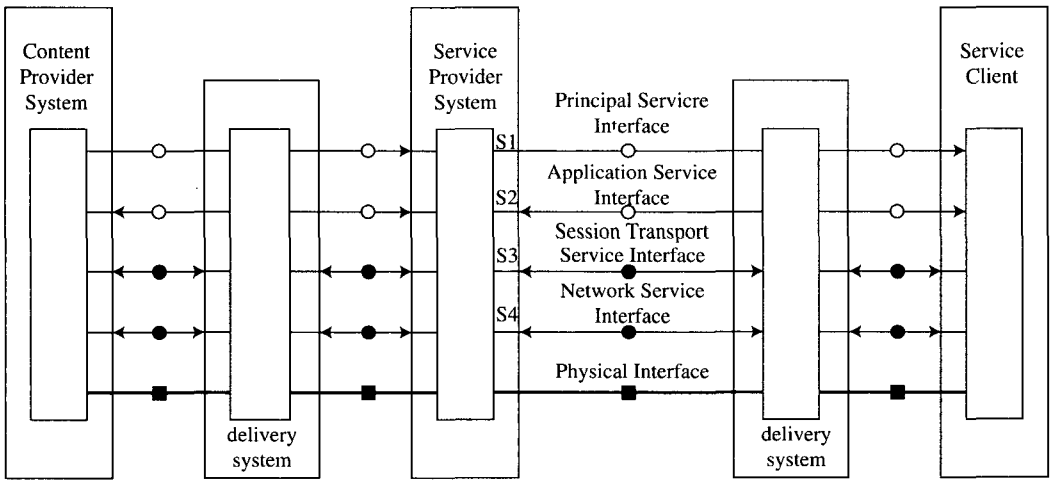


그림 2.1 일반적인 DAVIC 시스템

2.2 DAVIC 정보 흐름 및 프로토콜 스택

DAVIC 에서의 S1 정보 흐름은 내용(Content) 정보 흐름으로서 서버로 부터 사용자로의 정보 흐름이다. S1 정보 흐름은 인증이 완료된 후, 사용자로 전송되어야 한다. S1 정보 흐름은 ATM 기본 전송 시스템에 바탕을 두는 경우, 그림 2.2와 같은 같은 프로토콜 스택을 갖는다.

내용 정보에는 MPEG 비디오 및 오디오 정보를 포함한다. 기타 데이타는 파일, DSM-CC DownloadDataBlock, DVB 서비스 정보(Service Information), 영상, 그리고 실시간 그래픽 정보를 포함한다. MPEG2 PSI(Program Specific Information)에는 PAT(Program Association Table), PMT(Program Map Table), CAT(Conditional Access Table), 그리고 NIT(Network Information Table) 등을 포함한다.

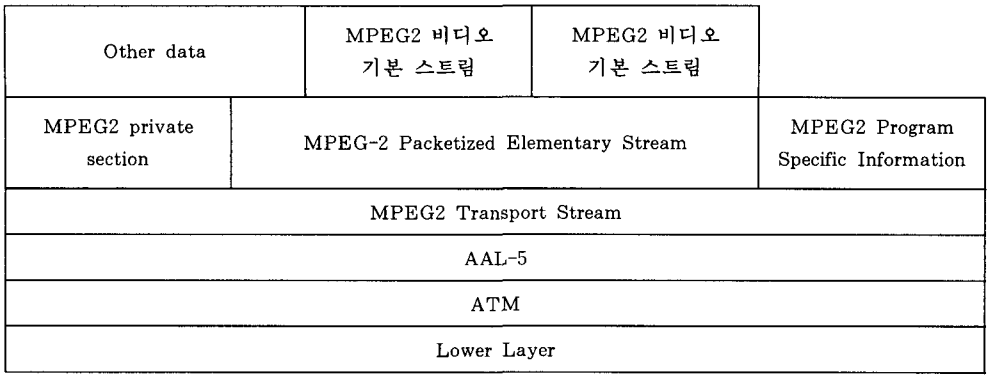


그림 2.2 S1 정보흐름을 위한 프로토콜 스택

PSI(Program Specific Information)는 디코더에서 프로그램의 역다중을 가능케 하기 위한 정보이다. 프로그램은 하나 이상의 기본 스트림들로 구성되며, 각각의 기본 스트림은 고유의 PID 를 갖는다. 프로그램과 기본 스트림은 한정 액세스 되어야 한다. PSI 정보는 스크램블링되지 않은 형태로 전달된다. PAT(Program Association Table)는 프로그램 번호와 프로그램 정보를 전달하는 PMT(Program Map Table)의 PID 값을 전달하며, PAT 의 PID 값은 "0x00"이다. 프로그램 번호 "0x0000"은 망 PID 용으로 설정되었다. PMT 는 프로그램과 이를 구성하는 기본 스트림간의 관계를 나타내며, 주로 기본 스트림들의 PID로 전달한다. 이는 Program Map Table Section 으로 전달된다. CAT는 하나 이상의 CA 시스템과 CA 시스템의 EMM 채널을 전달하는 트랜스포트 패킷의 CA_PID 를 전달한다.

표 2.1 PSI(Program Specific Information)

MPEG2 PSI	스트림	PID 번호	내 용
PAT	MPEG	0x00	프로그램 번호와 Program Map Table 의 PID 를 전달함
PMT	MPEG	PAT_PID 로 할당	하나 이상의 프로그램 요소에 대한 PID 값 규정
CAT	MPEG	0x01	하나 이상의 EMM 에 특정의 PID 값 할당
NIT	private	network PID 로 할당	FDM 주파수와 수신기의 개수 등의 물리적 망 변수

2.3 전달 시스템

전달 시스템은 그림 2.3과 같이 핵심 망, 액세스 망, 그리고 댁내 망(In House Network) 등으로 분류될 수 있다.

액세스 노드(Access Node)는 핵심 망과 액세스 망을 구분하기 위한 노드이며, NT(Network Termination) 는 액세스 망과 댁내 망을 구분하는 노드이다. 핵심 망은 서비스 제공자, 내용 제공자, 그리고 액세스 망내의 개체간의 신뢰성

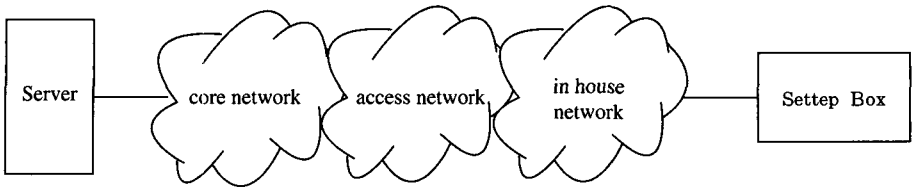


그림 2.3 전달 시스템 구성

있는 정보의 전달을 담당하고, 두 개체간의 연결의 설정 및 해제를 위한 교환 기능을 담당한다. 액세스 망은 최종 사용자로의 내용 분배를 담당한다.

액세스 망은 특정 지역의 사용자들을 위한 서비스 및 응용 정보 흐름에 대한 전송, 다중, 집선, 그리고 방송 기능을 수행하며, 관련 제어 및 관리 기능을 수행하며, 여타의 전화, 아날로그 TV, 그리고 N-ISDN(Narrowband Intergated Service Data Network) 서비스 등의 서비스를 제공한다. 액세스 망의 구조는 전송 매체에 따라 다음과 같이 구분될 수 있다.

- 완전 구리선 액세스 망
- 반은 광섬유이고 나머지 반은 동축 케이블이거나 트위스트-페어인 FTTC(Fiber To The Curb)
- 반은 광섬유이고 나머지 반은 동축 버스를 제공하는 HFC(Hybrid Fiber Coax)
- 전체가 광섬유인 FTTH(Fiber To The Home)

완전 구리선 액세스 망은 높은 속도의 트래픽을 처리하기 위하여 그림 2.4와 같이 ADSL (Asymmetric Digital Subscriber Line)모뎀을 이용한다. ADSL 모뎀은 가입자로 향하는 채널의 속도는 매우 높고, 반대로 가입자에서 망으로 향하는 채널의 속도는 매우 낮은 비대칭적 디지틀 가입자 선로를 이용한다. 중심국 ADSL 모뎀은 액세스 망에 존재하고 다른 쪽 ADSL 모뎀은 Set-Top Box에 위치한다.

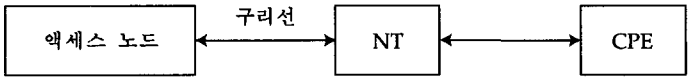


그림 2.4 ADSL 완전 구리선 액세스 망

FTTC 액세스 망은 그림 2.5와 같이 액세스 노드와 ONU(Optical Network Interface), 그리고 NT(Network Termination)로 구성된다.

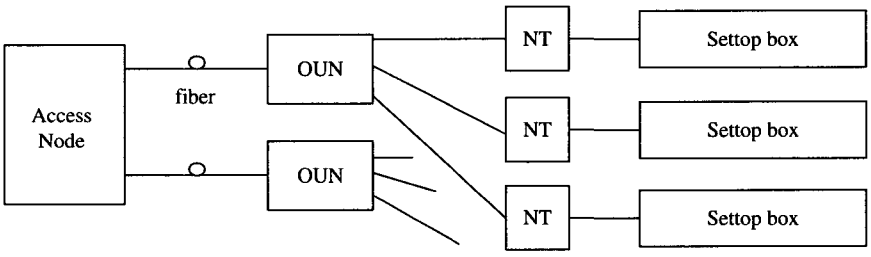


그림 2.5 FTTC 액세스 망

FTTC 액세스 망은 길 또는 큰 건물에 있는 수십 가입자용 ONU(Optical Network Unit)까지는 광섬유를 이용하고, ONU에서 NT까지는 수백 미터 정도의 트위스트-페어나 동축 케이블을 이용한다. ONU에서는 광 신호를 전기적 신호로 변환하고 NT에서는 신호를 트위스트-페어에 적합한 신호로 변환하는 기능을 수행한다.

HFC는 그림 2.6과 같이 인접 노드(Neighbourhood Node)까지는 광섬유를 사용하고 인접 노드에서 가입자까지는 동축 케이블을 이용한다. 하나의 인접 노드는 100 ~ 500 정도의 가입자들을 수용한다. 인접 노드에서 가입자까지의 망 구성은 버스 형태이며, 하나의 동축 케이블을 이용하여 연결된다. 따라서 각 가입자의 NT는 버스 형태로 매체를 공유한다. 매체를 공유하므로 매체 액세스 제어 기법과 프라이버시 보호 기법이 적용되어야 한다.

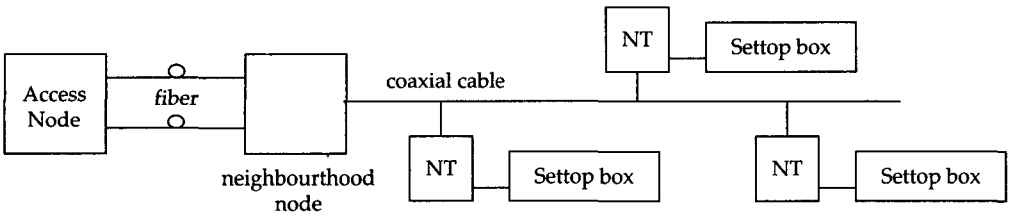


그림 2.6 HFC 액세스 망

FTTH에서는 그림 2.7과 같이 액세스망에서 가입자 댁내 망(Customer Premise Network) 까지를 광섬유를 이용한다. 광 액세스 망(Optical Access Network)은 NT가 종단하며, 가입자 댁내 망은 광섬유나 동축 케이블을 이용한다. 하나의 FTTH는 PON(Passive Optical Network)에 바탕을 두고 구축된다. 즉, 하나의 광섬유는 여러 가입자로 수동적으로 분할된다. 이는 여러 가입자가 하나의 고속 광섬유 능력을 공유함을 의미한다. 따라서 Passive Split로 인한 특별한 보안 및 프라이버시 대책이 요구된다. 상향 신호 전송 시에는 매체 액세스 기법이 요구된다.

댁내 망은 NT와 STU 사이에 존재한다. 댁내 망은 단순한 선로에서부터 회선 연결 기능을 갖는 완전한 댁내 망 구조를 가질 수 있다. NOD(Network Ownership Decoupling) 기능은 액세스 망과 댁내 망 간의 경계를 구분하기 위하여 설정된 기능 블럭이다. TTD(Transmission Technology Decoupling)는 한 매체의 신호를 다른 매체에 적합한 신호로 변환한다. FTTH의 경우 광 신호를 종단하고 트위스트-페어 케이

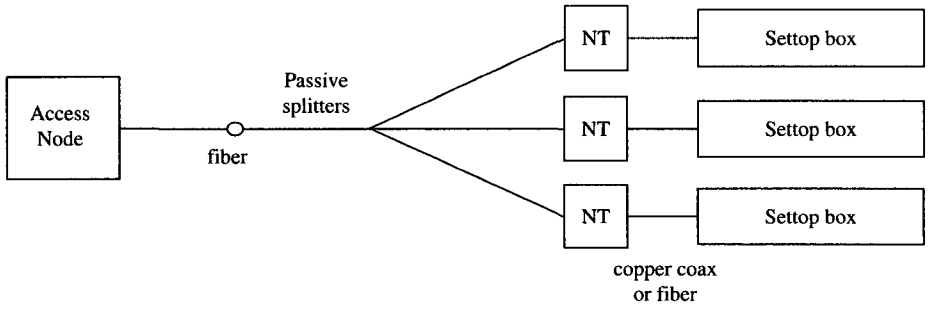


그림 2.7 FTTH 액세스 망

블에 적합한 새로운 신호를 생성하여 매체에 삽입한다. NIU(Network Interface Unit)는 망 종속 신호를 망 독립 신호로 변경한다.

댁내 망은 세가지 구조를 갖는다. STB(Set Top Box)는 STU와 NIU로 구성된다. NOD 기능은 NT 에 존재하며, NIU 기능은 STB 내에 존재한다. 그리고 TTD 기능은 선택 사항이다. 매체의 변경이 없다면 TTD 기능도 요구되지 않는다. TTD가 NT와 STB 사이의 별도의 장치에 존재하면, 이 장치는 UPI(User Premise Interface)라 불린다. UPI 는 사용자 장치로서 액세스 망과 댁내 망을 연결하는 게이트웨이(Gateway) 기능을 수행한다. 그림 2.8은 TTD 기능이 없는 댁내 망의 구조이다. 전송 기술의 변경이 없으므로 댁내 망은 단순히 액세스 망의 연장으로 볼 수 있다. NOD는 NT에 존재하며 망과 가입자의 관리 책임을 구분한다.

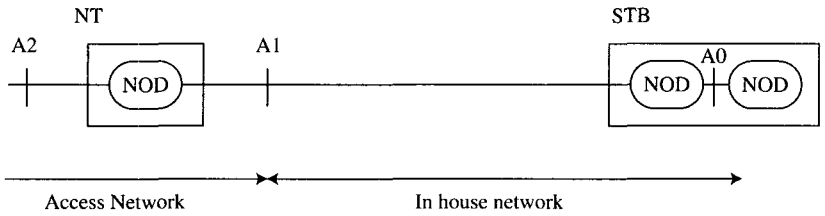


그림 2.8 TTD 기능이 없는 댁내 망

그림 2.9는 TTD와 NOD 기능을 갖는 NT와, NIU 와 STU 기능을 갖는 STB 로 구성된 댁내 망의 참조 모델이다. 댁내 망은 액세스 망과 다른 전송 기술을 이용한다.

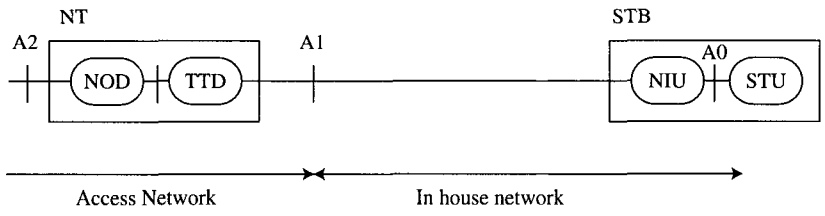


그림 2.9 NT가 TTD 기능을 갖는 댁내 망 참조 모델

그림 2.10은 TTD가 NT와 STB 사이에 존재하는 UPI에 존재하는 댁내 망의 참조 모델이다.

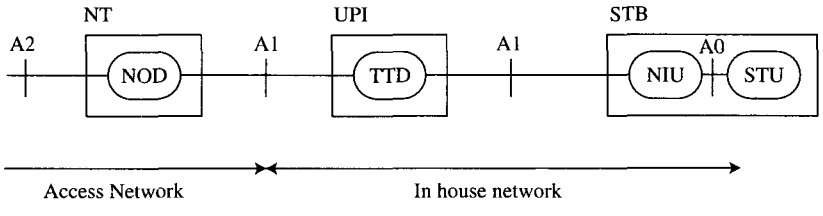


그림 2.10 TTD가 UPI에 있는 댁내 망의 참조 모델

2.4 NIU 와 STU

STU와 인터페이스 되는 NIU는 여러 망에 적용될 수 있도록 각 망에 적합한 형태로 따로 개발될 것이다. 단일 DS 구조가 나타날 가능성이 거의 없으므로 STU는 여러 망에 적용되는 NIU 와 인터페이스 해야 할 것이다.

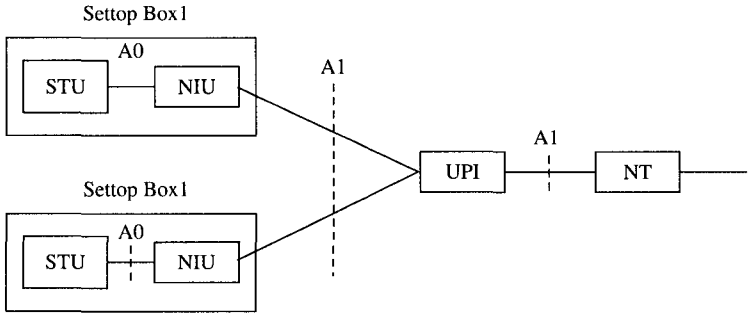


그림 2.11 STU 참조 구조(reference architecture)

NIU는 특정의 DS 시스템과 연동할 수 있는 액세스 망 종속 하드웨어를 포함해야 한다. 그러나 STU는 망 독립이다. 따라서 NIU와 STU 간의 표준화된 인터페이스는 망에 독립인 STU의 개발이 가능하다는 측면에서 매우 중요하다. DAVIC에서는 이를 위하여 A0와 A1 인터페이스를 갖는 NIU를 정의했으며, A1 인터페이스만을 갖고 STU와 NIU의 결합인 STB(Set Top Box) 를 정의하였다. 그림 2.11은 STU 주변 장치와 관련 참조 구조를 정의하였다. NIU 는 참조점 A1* 에서 UPI(User Premise Interface)와 인터페이스한다. UPI는 NT와 A1 참조점에서 인터페이스한다. 그리고 STU와 NIU는 참조점 A0에서 인터페이스한다.

참조점 A0는 STU를 망에 독립적으로 동작케 하며, A0 인터페이스에 대한 논리적, 전기적, 기계적, 그리고 물리적 규정을 정의하고 있다. A0 인터페이스 신호는 고속 하향 데이터 버스, ATM 양방향 데이터 버스, 그리고 자국 제어용 데이타 버스로 구성되는 3가지 논리 데이터 버스와, 리셋 상태, 선택 신호인 아날로그 통과 신호, 그리고 NIU 를 위한 전력 공급 신호 등이 있다. 그림 2.12는 A0 인터페이스의 논리적 기술이다.

2.5 STU 에서의 보안 인터페이스

STU는 디스크램블러(Descrambler), MPEG 복호기, 역다중화기, 그리고 보안 관리 기능(Security Management Functions) 으로 구성되어 있으며, NIU에서는 망 관련 보안 기능을 수행한다. DAVIC에서의 보안 장치는 암호 장치의 설치 및 수출에 엄격한 제한이 있고, 보안 위협 요소는 너무 다양하여 다양한 공격 방법으로 위협받으며, 보안 장치가 안전하다고 확신하기가 매우 어렵고, 또한 실제로 완전히 안전한 보안 장치를 실현하는 것은 불가능하다는 이유로 세계 표준 단일 보안장치로 표준화되지 않을 전망이다. DAVIC STU는 그림 2.13과 같이 수신 신호를 검출하는 수신기 및 복조기, 스마트 카드로의 CA 메세지을 전달하기 위한 필터부, 암호화되어 수신된 MPEG-2 스트림을 복호하기 위한 디스크램블러, 수신된 MPEG-2 신호를 역다중하기 위한 역다중화기, 그리고 MPEG 복호기 등으로 구성되어 있다. 따라서 STU는 보안 기능을 수행하기

위하여 하나 이상의 부가적인 보안 모듈(Detachable Security Module)과 인터페이스한다.

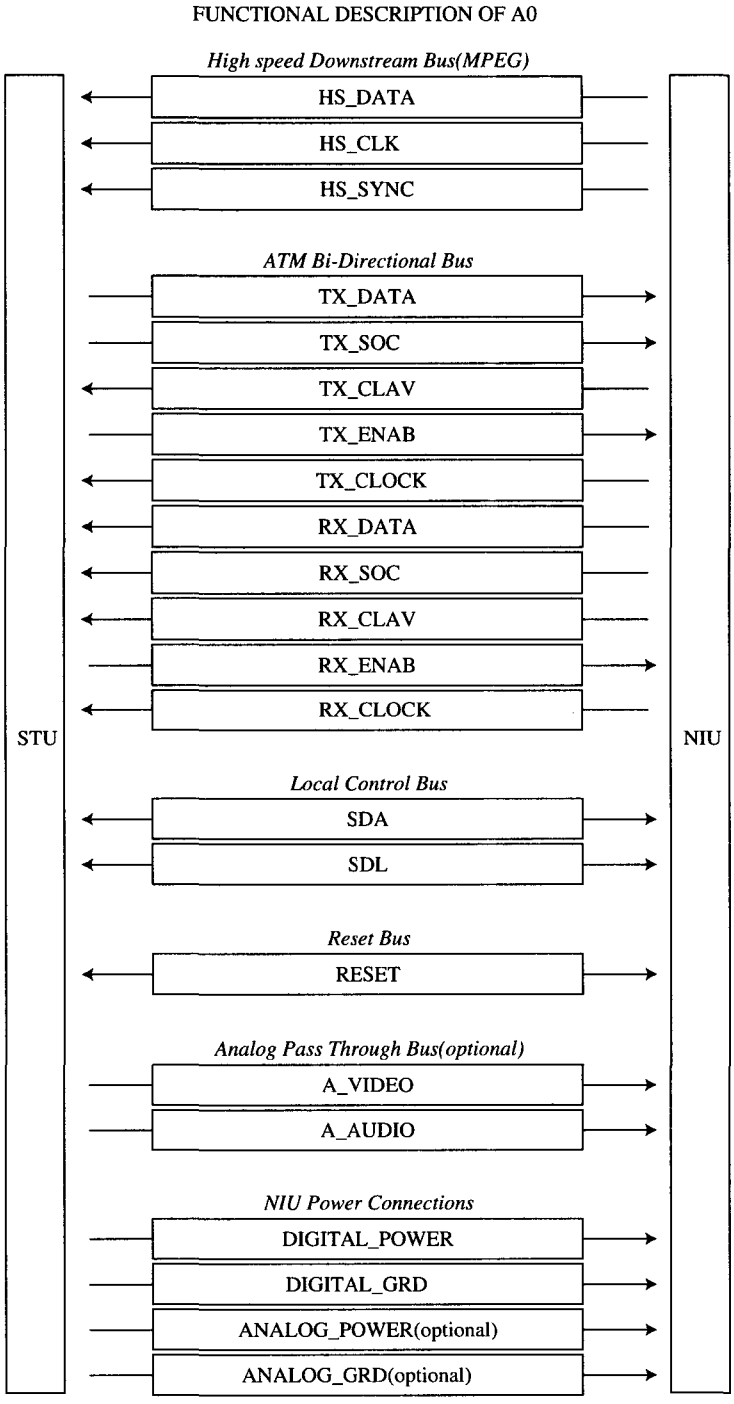


그림 2.12 A0 인터페이스의 논리적 기술

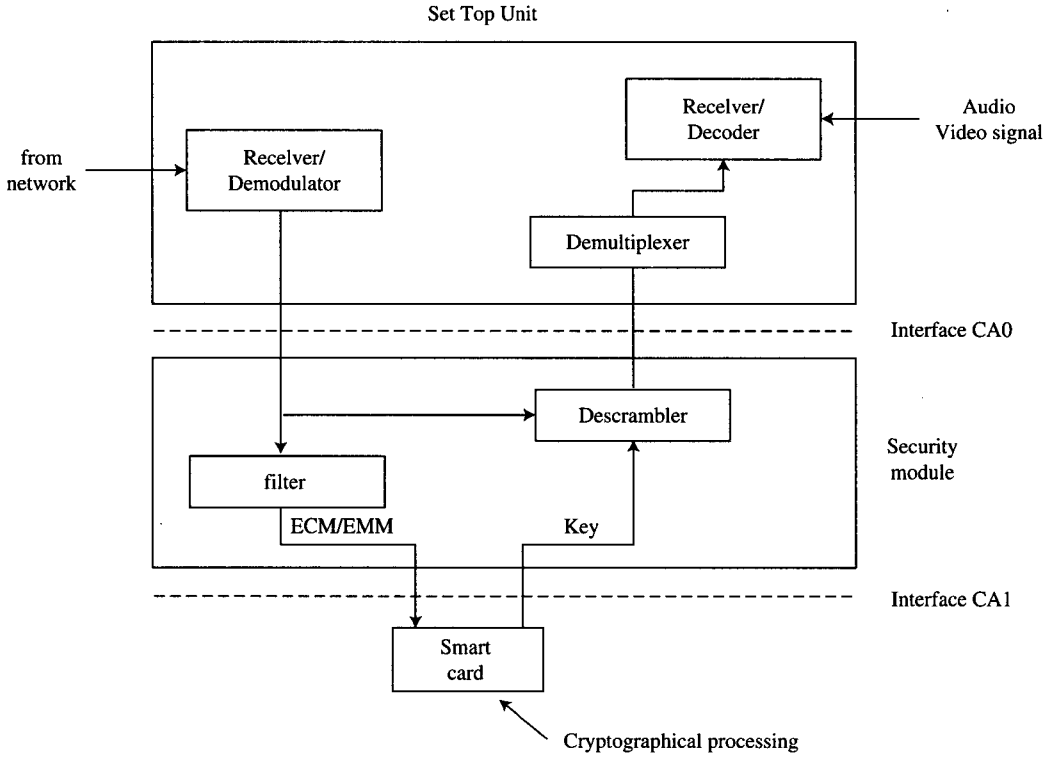


그림 2.13 STU 기능 블럭도

사용자 댁내 장치(Customer Premises Equipment) 는 STU와, 스마트 카드와 디스크램블러로 구성되는 부가적인 보안 장치로 구성될 수 있다. 보안 모듈은 암호 알고리듬에 대한 공격이 성공했을 경우 쉽게 대체될 수 있고, STU에 가입자 관련 정보를 제거하여 STU의 일반화가 가능하며, STU의 쉬운 변경 및 재사용이 가능케 한다. STU 와 보안 모듈간의 인터페이스는 CA0 인터페이스로, 보안 모듈과 스마트 카드간의 인터페이스는 CA1 인터페이스로 정의되어 있다. CA0는 STU 와 고속의 디스크램블링 기능 및 필터 기능 차원에서 인터페이스하며, 저속의 키 관리 정보 역시 송수신할 수 있어야 한다. CA1은 저속이며, CA0 인터페이스는 고속이다. CA1 인터페이스는 저속의 보안 관리 기능만을 수행하는 저속 스마트 카드와 인터페이스한다. CA1 인터페이스 호환성 여부는 STU와 서비스 제공자간에 사용되는 스크램블링 알고리듬의 종류 및 공통의 필터의 적용 여부에 좌우된다.

CA1 인터페이스는 다음과 같은 특성이 있다. 디스크램블러, 역다중화기, 복호기를 하나의 칩으로 집적화할 수 있으므로 스마트 카드의 복잡도를 감소시킬 수 있다. 또한 보안 알고리듬의 공격 성공, 새로운 서비스의 도입, 새로운 서비스 제공자로의 액세스 등을 가능케 한다. 그리고 디지틀 정보에 대한 보호가 용이하다는 것이다. CA0 인터페이스는 인터페이스를 통하여 복구된 디지틀 스트림이 전달되므로 도청이 가능하다. 그러나 CA1 인터페이스에서는 복구된 디지틀 스트림이 STU 내에 포함되므로 사용자가 도청하는 것을 어렵게 한다. 만약 디스크램블링 기능과 복호가 하나의 칩에서 수행된다면 디지틀 스트림에 대한 보호는 더욱 용이해진다.

2.6 액세스 제어 시스템 참조 모델

DAVIC 에서 간략화된 액세스 제어 참조 모델(Reference Model)은 그림 2.14와 같다. SRP1-SRP7은 보안 관련 기능이 발생하는 보안 참조점(Security Reference Point)이며, SC 는 스크램블링을, DS는 디스크램블링을, SM(Security Management)은 보안 관리 기능을 수행하는 개체를 각각 의미한다. 보안 기능은 보안 세션 협상, 스크램블링 알고리듬 협상, 일방향 방송에서의 메시지 인증, 등위 개체 인증 , 그리고 안전한 거래 등을 포함한다. 스크램블링 기능은 서비스 제공자와 사용자 고객, 전달 시스템과 사용자 시스템, 그리고 내용 제공자와 사용자 시스템간에 제공된다. 스크램블링의 제어는 사용자 고객과의 제어를 위해서는 서비스 제공자에서 또는 전달시스템에서 수행된다.

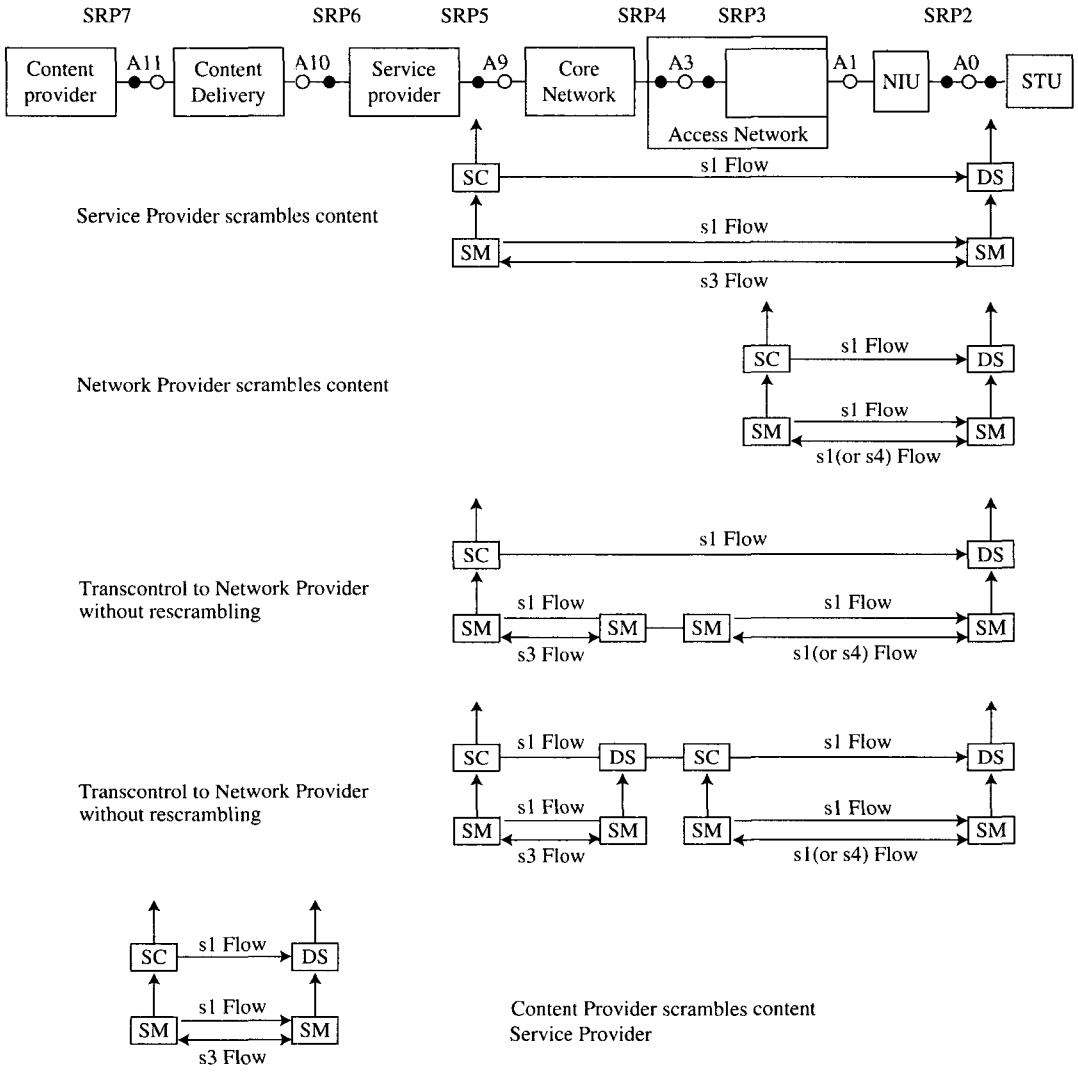


그림 2.14 간략화된 액세스 시스템 참조 모델

2.7 MPEG2 트랜스포트 스트림

DAVIC에서의 스크램블링은 MPEG2 트랜스포트 스트림 레벨에서 수행된다. 기본 스트림(Elementary Stream)은 부호화된 비디오, 오디오, 또는 다른 용도의 부호화된 비트 스트림 중의 하나를 나타내는 용어이다. 그룹은 하나 이상의 기본 스트림들로 구성된다. 프로그램은 공통의 시스템 클럭 주파수 타임 기준을 갖는 기본 스트림들의 그룹이다. 트랜스포트 스트림 부호화 계층은 하나 이상의 그룹들로 구성된다. MPEG2 트랜스포트 스트림은 하나 이상의 프로그램들이 다중화되어 있다. 비디오 기본 스트림의 표현 단위는 화상(Picture)이고, 음성의 표현 단위는 음성을 표본화한 샘플이다. 화상에 대한 액세스 단위는 화상을 위한 모든 부호화된 데이타를 포함한다. 액세스는 표현 단위별로 수행되며, 기본 스트림은 액세스 단위들로 구성된다.[2]

기본 스트림 데이타는 PES(Packetized Elementary Stream) 패킷을 이용하여 전달된다. PES 패킷은 PES 패킷 헤더와 PES 패이로드로 구성된다. PES 패킷 페이로드에는 하나의 가변 길이의 연속적인 기본 스트림 데이터로 구성된다. PES 패킷은 트랜스포트 패킷(Transport Packet)을 이용하여 전달된다. PES 패킷 헤더는 패킷 데이타의 시작을 확인해 주는 32-비트 패킷 시작 부호로 시작되며, 복호(Decoding)를 위한 표현 타임 스탬프등에 관한 정보를 포함한다.

트랜스포트 패킷(Transport Packet)에는 13 비트의 PID(Packet Identifier)를 포함한다. PID는 PSI(Program Specific Information) 테이블에서 규정된 트랜스포트 패킷이 담고 있는 데이타의 종류를 확인하기 위하여 이용된다. 동일한 PID를 갖는 트랜스포트 패킷은 하나의 기본 스트림을 전달한다. 여러 개의 트랜스포트 패킷들로 구성되는 트랜스포트 스트림은 다음과 같은 문법을 갖는다.

```
MPEG_transport_stream(){
        do{
            transport_packet()
        } while(nextbits() == sync_byte)
        }
```

트랜스포트 패킷의 구조는 다음과 같다.

```
transport_packet(){
  sync_byte                        8    bslbf
  transport_error_indicator        1    bslbf
  payload_unit_start_indicator     1    bslbf
  transport_priority               1    bslbf
  PID                             13    uimsbf
  transport_scrambling_control     2    bslbf
  adaptation_field_control         2    bslbf
  continuity_counter               4    uimsbf
  if(adaptation_field_control == '10' ||
    adaptation_field_control == '11') {
          adaptation_field()
          }
  if(adaptation_field_control == '01' ||
    adaptation_field_control == '11') {
          for(i=0;i<N;i++){
              data_byte
                  }
          } }
```

sync_byte는 "0100 0111" 패턴이다. transport_error_indicator는 한 비트 플래그로서, '1'인 경우 교정이 불가능한 에러가 발생했음을 의미한다. payload_unit_start_indicator는 1 비트 플래그로서, PES와 PSI 패킷에 대해 의미를 갖는다. transport_priority는 한 비트의 표시자로서 '1'인 경우 우선 순위가 높은 패킷이다. PID는 13 비트 필드로서, 패킷 페이로드가 담고 있는 데이타의 종류를 나타낸다. PID = "0x0000"인 경우 프로그램

연관(Program Association) 테이블용으로, PID = "0x0001"인 경우 한정 액세스 테이블용으로, PID = '0x0002-0x000F'인 경우를 유보되어 있고, 나머지 값은 PSI를 통해 또 다른 기본 스트림에 할당된다. transport_ scrambling_control은 트랜스포트 패킷 페이로드의 스크램블링 상태를 나타낸다. adaptation_field_control은 2 비트 필드로서 adaptation 필드의 존재 여부를 나타낸다. continuity_counter는 4 비트 필드로서, 동일한 PID를 갖는 트랜스포트 패킷이 전달될 때마다 1 씩 증가한다. data_byte는 PID에 의해 확인되는 PES 스트림, PSI 테이블, 또는 private data 로 부터의 연속적인 데이타이다. PES 패킷은 다음과 같은 구조를 갖는다.

```
PES_packet(){
  packet_start_code_prefix          24    bslbf
  stream_id                          8    uimsbf
  PES_packet_length                 16    uimsbf
  if( (stream_id != private_stream_2) && (stream_id != padding_stream_2) ) {
    "10"                             2    bslbf
    PES_scrambling_control           2    bslbf
    PES_priority                     1    bslbf
    ...
    for(i=0;i<N;i++){
      PES_packet_data_byte           8    bslbf
    }
  else if( stream_id == private_stream_2 ) {
    for(i=0;i<PES_packet_length;i++){
      PES_packet_data_byte           8    bslbf
    }
  else if( stream_id == padding_stream ) {
    for(i=0;i<N;i++){
      padding_byte                   8    bslbf
    } }
```

표 2.2 stream_id 의 의미

stream_id	스트림의 종류
1011 1100	program stream map
1011 1101	private_stream_1
1011 1110	padding_stream
1011 1111	private_stream_2
110x xxxx	MPEG audio stream - number xxxxx
1110 xxxx	MPEG vidio stream - number xxxx
1111 0000	ECM
1111 0001	EMM
1111 0010	DSM CC (digital storage media command and control)
1111 0011	MHEG
1111 xxxx	reserved data stream xxxx
1111 1111	program stream directory

packet_start_code_prefix는 24 비트 부호로서 PES 패킷의 시작 부분을 확인하기 위한 "0x000001" 패턴이다. stream_id는 표 2.2와 같이 기본 스트림의 종류를 규정하고 있다. PES_packet_length는 PES 패킷의 바이트 단위의 갯수로서 16 비트 필드이다. PES_stream_control은 표 2.3과 같이 PES 패킷 페이로드의 스크램블링 모드를 나타낸다. PES_priority는 페이로드의 우선순위를 나타내는 1 비트 표시자이다. PES_packet_data_ byte는 패킷의 stream_id 에 의해 확인되는 기본 스트림으로부터의 연속적인 데이타를 의미한다. packet_data_byte의 N은 PES_packet_length 이며, PES_packet_ length의 마지막 바이트에서 PES_packet_ data_byte까지의 첫 바이트까지의 바이트의 수를 뺀 값이다. Padding_byte는 8 비트 패턴으로서, "1111 1111"이다.

표 2.3 PES_stream_control 필드

부호값	의미
00	스크램블링됨
01	사용자 정의
10	사용자 정의
11	사용자 정의

2.8 액세스 제어를 위한 보안 유닛의 주소

각 보안 유닛은 그룹 주소와 개별 주소를 갖는다. CA_unit()은 유일하고도 구별 가능한 식별자로서, 첫 6 디지트는 산업체, 국가, 또는 발행자 등을 나타내는 발행자 식별자(issuer_identification_number) 디지트들이며, 다음 12 디지트는 보안 유닛 또는 계정 확인자이고, 마지막 1 디지트는 검사 디지트이다. 발행자 식별자는 6 디지트(24 비트)이며, 트리 구조로 생성된다. 트리의 최대 레벨 수는 6 이며, 각 레벨당 최대 출력 수는 100 이다. 보안 유닛의 주소는 다음과 같은 문법을 갖는다.

```
CA_unit(){
  issuer_identification_number   24   bslbf
  reserved                        4   bslbf
  unit_id_length                  4   uimsbf
  for(i=0;i<N;i++){
      unit_identifier_ls_digit    4   uimsbf
      unit_identifier_ms_digit    4   uimsbf
      }
  }
```

보안 관련 메시지인 CAT(Conditional Access Table) 는 다음과 같은 문법을 갖는다.

```
CA_message_section(){
  table_id                        8   uimsbf
  section_syntax_indicator        1   bslbf
  DVB_reserved                    1   bslbf
  ISO_reserved                    2   bslbf
  CA_message_section_length      12   uimslf
  for(i=0;i<N;i++){
      CA_message_descriptor_byte  8   bsblf
            } }
```

Table_id는 8 비트 필드이며 표 2.4와 같으며, 9 개의 CA message descriptor bytes가 주소 필터링을 위해 할당된다. section_syntax_indicator는 한 비트 표시자로서, 항상 '0'으로 리셋된다. CA_section_length는 12 비트 필드이며, CA_section_length에서 끝까지의 바이트 단위의 길이를 나타낸다. CA_message_descriptor_byte는 CA 정보 전송을 위한 8 비트 필드이며, 첫 9 바이트는 주소 필터링을 위해 할당된 바이트이다. 16 개의 table_id 값이 여러 다른 한정 액세스 정보를 전달하기 위하여 설정되었다.

표 2.4 Table_id

Table_id 값	의미
0x00-0x02	MPEG specified
0x03-0x3f	MPEG_reserved
0x40-0x72	V2-SI specified
0x73-0x7f	DVB_reserved
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82-0x8f	CA-message_section, CA system private
0x90-0xfe	private
0xff	ISO-reserved

한정 액세스 정보를 갖는 CA_message _section에 유용하며, ECM 데이타 전송을 위한 table_id값은 "0x80" 또는 "0x81"이다. ECM을 위한 table_id의 변화는 ECM의 내용 변화를 의미하며, 이는 odd 및 even CW가 전달되었음을 의미한다. 이에 대한 문법은 다음과 같다.

```
CA_message_descriptor(){
  ca_unit_id                    8   uimsbf
  class                         8   uimsbf
  instruction                   8   uimsbf
  parameter_1                   8   uimsbf
   parameter_2                  8   uimsbf
  data_length                   8   uimsbf
  response_length               8   uimsbf
  for(i=0;i<N;i++){
     CA_data_byte               8   bslbf
        }   }
```

데이타 길이 필드와 응답 길이 필드(data length field and response length field)는 한 옥텟 필드이며, 최대값은 255 이다.

2.9 보안 관련 개체들에 대한 요구사항

각 개체간에 설정된 정보에 대한 보안 요구사항은 매우 중요하다. DAVIC 에서의 개체들은 그림 2.15와 같이 서비스 제공자(Service Provider), 논리적 망(Logical Network), 그리고 서비스 사용자(Service User) 로 구성된다. 서비스 제공자의 정보원과 사용자의 정보싱크간의 S1 정보 흐름에 대한 보안 요구 사항(R1)은 제 삼자에 의한 서비스 제공자 또는 서비스 사용자를 가장하는 것을 방지해야 하고, 내용 정보 및 키 정보에 대한 도청을 예방해야 하며, 전달된 스트림의 비인가된 액세스에 대해 보호되어야 하고, 다운로드된 SW의 비인가된 변경에 대한 보호 및 내용의 비인가된 복사에 대한 보호, 그리고 서비스 제공자에 의한 거부에 대한 대책이 있어야 한다.

서비스 제공자의 종점간 제어 개체와 서비스 사용자의 종점간 제어 개체간의 S2 정보 흐름에 대한 보안 요구 사항(R2)은 서비스 제공자나 서비스 사용자의 가장에 대한 보호, 민감한 서비스 제공자와 사용자간의 대화에 대한 도청 예방, 서버 개체의 비인가된 액세스에 대한 보호, 다운로드된 SW의 비인가된

변경에 대한 보호, 위조에 대한 보호, 그리고 서비스 사용자에 의한 거부에 대한 대책이 있어야 한다.

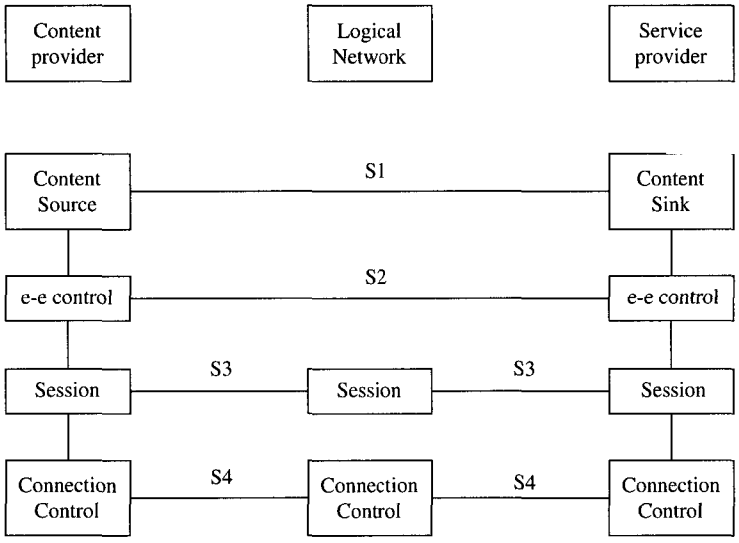


그림 2.15 DAVIC 개체들

2.10 S2 또는 S3 상에서의 보안 메카니듬

S2 정보 흐름상에서의 통신을 보호하기 위한 보안 메카니듬은 인증 메카니듬, 무결성, 그리고 암호 메카니듬이 있다. 인증 방식은 ITU X.509에서 표준화된 삼방향 인증 메카니듬을 이용한다. 이는 상대 개체를 서로 인증하는 양방향 인증 방식이며, 동기화된 클럭을 제거할 수 있으며, 인증 프로토콜 수행과 동시에 추후의 무결성 및 암호 통신을 위한 세션키를 공유할 수 있는 방식이다.

인증 방식에서 이용되는 정보 채널의 구조는 DSM-CC 사용자간 메시지에서의 Auth-Request_T 구조를 사용한다. 인증 과정의 개시는 사용자에 의해 수행된다. 이에 응하여 서버는 인증이 필요치 않을 경우, 사용자에게 No-Auth exception 정보를 전달한다. 이는 서버에서 사용자로 향하는 No-Auth exception이며, 이의 파라메타에는 일방향, 이방향, 그리고 삼방향 인증을 나타내는 인증 방식의 종류 정보와, RSA, ElGamal, FS, 그리고 GQ 등의 채용한 서명 기법을 나타내는 서명 방식의 종류 정보가 포함된다.

2.11 S2 또는 S3 상에서의 인증 프로토콜과 변수

DAVIC 인증을 위한 참조 모델은 그림 2.16과 같다. 인증 정보 교환을 위한 흐름은 DSM-CC U-U 정보를 이용하여 실현된다. 여기서 이용될 수 있는 알고리듬은 RSA 서명 알고리듬, GQ의 서명 알고리듬, 또는 그외의 영지식 서명 알고리듬 등이 있다.

S2 상에서의 인증 프로토콜은 그림 2.17과 같으며, 이는 ITU X.509의 공개키증명서 방식을 이용한다. 인증 프로토콜은 넌스(Nonce)와 공개키 암호 시스템에 바탕을 두고 있다.

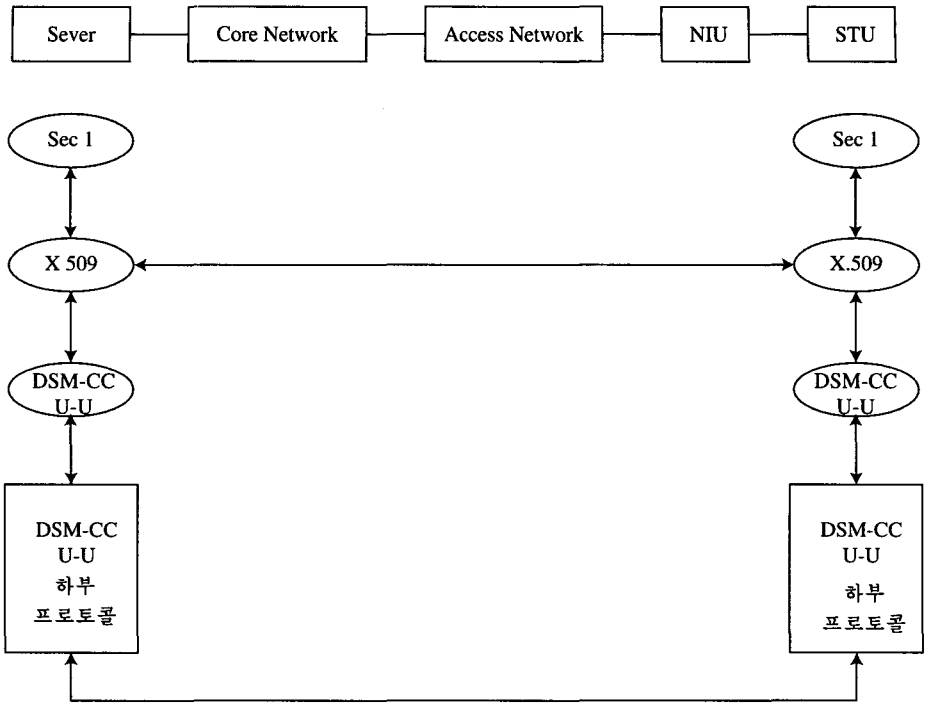


그림 2.16 인증 참조 모델

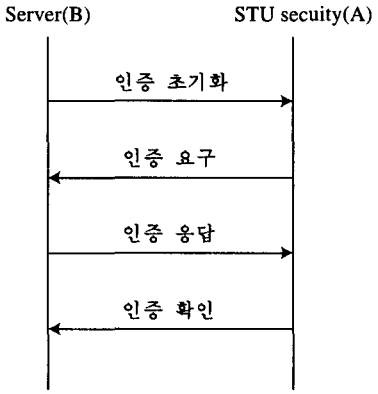


그림 2.17 인증을 위한 정보 흐름

인증 프로토콜은 인증을 받는 사용자 또는 증명자(Prover)와 이를 검증하는 서버 또는 검증자(Verifier) 간에 수행된다. 인증 프로토콜에서 이용되는 인증 정보는 그림 2.17과 같이 인증 초기화(Authentication Initialization), 인증 요구(ARQ : Authentication Request), 인증 응답(ARS : Authentication Response), 인증 확인(AC : Authentication Confirm), 그리고 선택적으로 인증 성공 확신(CONFIRM-AP)으로 구성된다. 이밖은 장애 상태의 발생을 상대국에 전달하기 위한 FAULT 정보가 있다. 인증 초기화 정보는 인증 과정을 개시하기 위하여 서버에서 사용자로 전달되는 인증 정보이다. 인증 요구 정보는 사용자가 서버로 사용자의 이름 A, 사용자의 공개키 증명서 C_A, 추후 암호 통신에 이용될 무결성 알고리듬의 종류를 나타내는 IntAlgs와 암호 알고리듬의 종류를 나타내는 ConfAlgs, 서버의 이름 B, 선택적으로 타임 스템프 T_A, 그리고 사용자 넌스 N_A를 사용자의 비밀키로 암호화한 파라메타를 전달한다. 인증 요구 정보는 식 (2.1)과 같다.

$$\text{ARQ} : A,\ D_{Sa}[B,\ N_A,\ T_A(\text{Opt.}),\ \text{IntAlgs},\ \text{ConfAlgs}],\ C_A \qquad (2.1)$$

ARQ를 수신한 서버는 사용자의 C_A의 유효성을 확인하고 이로 부터 서명용 공개키를 복구한 후, 서명용 공개키를 이용하여 $D_{Sa}[B,\ N_A,\ T_A(\text{Opt.}),\ \text{IntAlgs},\ \text{ConfAlgs}]$를 복호하여 $B,\ N_A,\ T_A(\text{Opt.}),\ \text{IntAlgs},\ \text{ConfAlgs}$를 복구한다. 그리고 자신으로 향하는 정보인가를 B로 확인하고, 넌스 N_A를 추후의 ARS를 위해 저장한다.

인증 응답 정보는 서버에서 사용자로 향하는 정보 흐름이다. ARS는 서버의 이름 B와 서버의 공개키 증명서 C_B, 그리고 사용자로 부터 제안된 내용을 바탕으로 선택된 추후의 무결성 알고리듬인 IntAlgs와 암호 알고리듬인 ConfAlgs, 사용자의 이름 A, 선택적으로 타임 스템프 T_B, 자신의 기밀성용 공개키로 추후 무결성 서비스를 위한 세션키 K^I_{AB}를 암호화한 $E_{Pa}[K^I_{AB}]$, 자신의 기밀성용 공개키로 추후 기밀성 서비스를 위한 세션키 K^{-C}_{AB}를 암호화한 $E_{Pa}[K^C_{AB}]$, 그리고 서버의 Nonce N_B를 서버의 서명용 비밀키로 서명한 서명문을 묶어서 전달한다. 인증 응답 정보는 식 (2.2)와 같다.

$$\text{ARS} : B, D_{Sb}[A, N_A, N_B, T_B(\text{Opt}), \text{IntAlgs}, \text{ConfAlgs}, E_{Pa}[K^I_{AB}], E_{Pa}[K^C_{AB}]], C_B \qquad (2.2)$$

ARS를 수신한 사용자는 C_B의 유효성을 검증하고 서버의 서명용 공개키를 구한 후, 이를 이용하여 $D_{Sb}[A, N_A, N_B, T_B(\text{Opt}), \text{IntAlgs}, \text{ConfAlgs}, E_{Pa}[K^I_{AB}], E_{Pa}[K^{-C}_{AB}]]$를 복호하여, $A, N_A, N_B, T_B(\text{Opt}), \text{IntAlgs}, \text{ConfAlgs}, E_{Pa}[K^I_{AB}], E_{Pa}[K^C_{AB}]$를 복구한다. 복구된 A를 이용하여 자신으로 향한 정보인가를 확인하고, 수신된 N_A와 송신된 N_A가 동일한가를 확인함으로서 서버의 정체를 인증하고, 협상된 무결성 알고리듬과 기밀성 알고리듬의 종류를 확인한다. 그리고 $E_{Pa}[K^I_{AB}]$와 $E_{Pa}[K^C_{AB}]$를 자신의 비밀키를 이용하여 서버에서 전송된 무결성 서비스용 키 K^I_{AB}와 기밀성용 키 K^C_{AB}를 복구한다.

인증 확인 정보는 사용자에서 서버로 향하는 정보로서, 사용자의 이름 A와 서버의 이름인 B및 서버로 부터 수신된 넌스 N_B를 사용자의 서명용 비밀키로 서명한 결과를 전달한다. 상기 과정들을 수행함으로서 양방 인증이 수행될 수 있다. 인증 확인 정보는 식 (2.3)과 같다.

AC : A, D_{Sa}[B, N_B] (2.3)

그림 2.18은 CA0 인터페이스를 갖는 STU와 보안 모듈간의 프로토콜 스택을 나타내고 있으며, 그림 2.19는 CA1 인터페이스를 갖는 STU와 스마트 카드간의 프로토콜 스택을 나타내고 있다. 기본적으로 국내에서는 CA1 인터페이스를 갖는 인증 참조 모델을 채용하는 것이 현실적이라 판단된다.

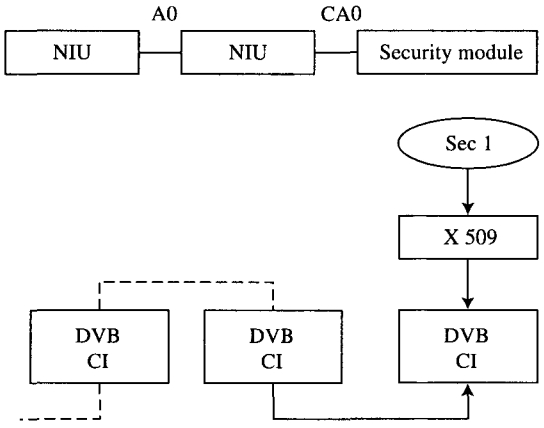


그림 2.18 CA0 인터페이스를 갖는 STU 와 보안 모듈간의 프로토콜 스택

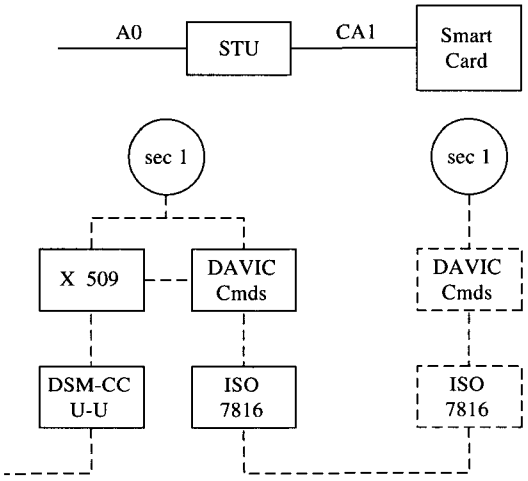


그림 2.19 CAI 인터페이스를 갖는 STU 와 보안 모듈간의 프로토콜 스택

2.12 VOD 를 위한 인증 프로토콜 설정 및 스택

VOD 서비스는 네트워크 계층에서 수행되는 S3 상에서의 인증과 서버와 STU 간의 종점간에 수행되는 S2 상에서의 인증을 포함해야 한다. S3 또는 S4 정보 흐름을 이용한 사용자(Client)와 세션과 자원을 집중 관리하는 SRM(Session and Resource Manager) 간의 인증을 위해 개입되는 프로토콜 스택은 그림 2.20과 같다. 인증은 UDP(User Datagram Protocol) 상위 계층에서 실현된다.

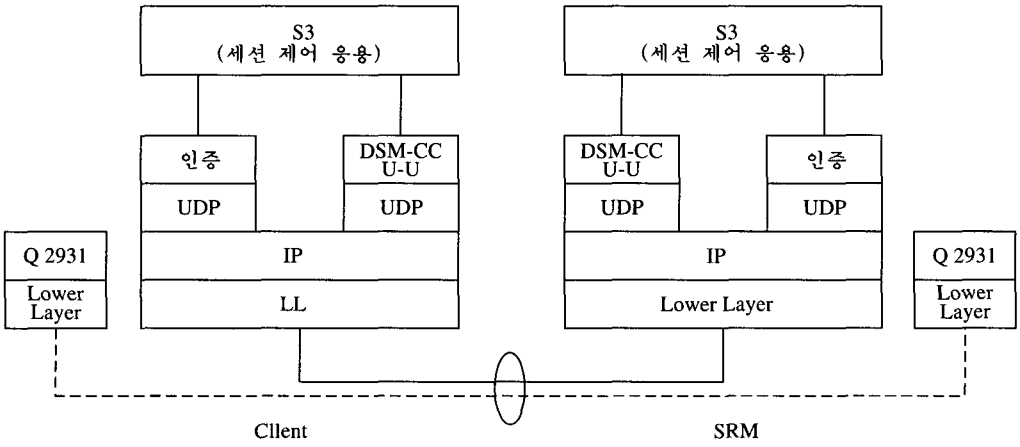


그림 2.20 고객과 SRM 간의 인증을 위한 프로토콜 스택

또한 SRM 과 서버간의 인증을 위해 개입되는 프로토콜 스택은 그림 2.21과 같다. 이는 TCP 상위 계층에서 수행된다.

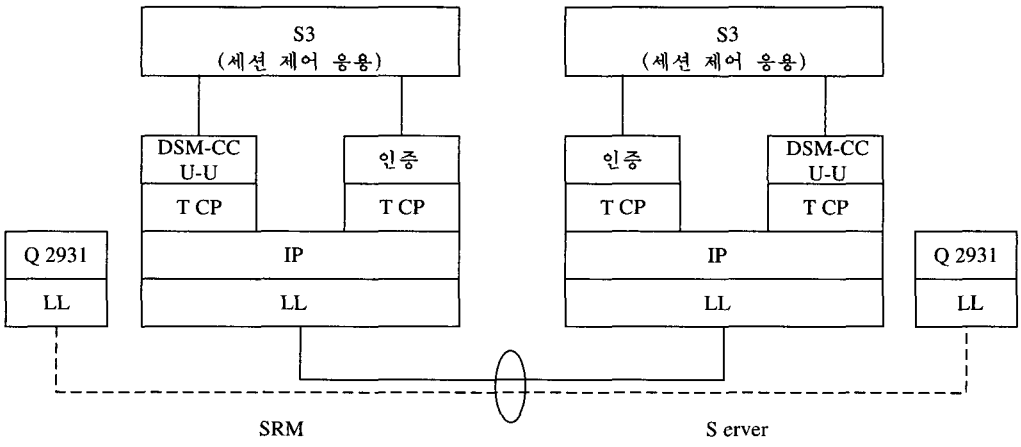


그림 2.21 SRM과 서버간의 인증을 위한 프로토콜 스택

또한 고객측에서의 인증을 위한 프로토콜 스택은 그림 2.22와 같다. 인증은 TCP 또는 UDP 상위 계층에서 수행됨을 알 수 있다. 따라서 TCP/UDP 계층과의 인증 정보 교환은 기존의 프리미티브를 이용하여 실현될 수 있다.

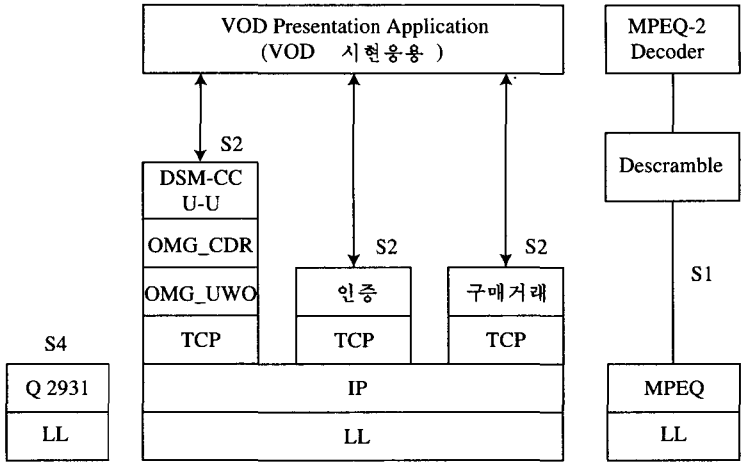


그림 2.22 고객측에서의 인증을 위한 프로토콜 스택

VOD 세션 서비스를 위한 전체 과정은 그림 2.23과 같다. 첫 단계에서는 고객과 SRM 간의 세션 설정을 위한 과정이다. 고객은 SRM 으로 사용자를 위한 configuration 파라메타를 요청하는 UNConfigRequest 정보를 전송하고, SRM은 고객으로 UNConfigConfirm을 전송함으로서, 고객과 SRM은 서로의 NSAP(Network Service Access Point)와 IP 연결을 확인한다. 이후, UDP를 통한 인증 정보를 교환함으로서, 고객과 SRM 간의 인증 기능을 수행한다. UDP는 인증 정보 교환을 위한 DSM-CC UN 정보의 전달 메카니듬을 제공한다. 그리고 SRM과 고객은 서비스를 선택하기 위한 다운로드 과정과 협상 과정을 수행한다. 이를 완수하면 고객은 서비스를 선택하고 SRM을 통하여 서버로 연결되기 위하여 세션의 Id인 sessionId 필드, 요구된 특정 서버를 지적하는 serverId 필드, 고객의 고유 Id를 포함하는 clientId 필드를 포함하는 CientSessionSetup-Request를 SRM에 전달한다. 이를 수신한 SRM은 서버와 인증 정보를 교환하여 서로의 신분을 확인한 후, 세션 협상 과정을 수행한다. 이를 위하여 SRM은 서버로 sessionId, serverId, clientId 등을 포함하는 ServerSessionSetupIndication 정보를 전송하고, 서버는 SRM으로 ServerAddResourceRequest를 전송하며, SRM은 서버로 ServerAdd ResourceConfirm을 전송하며, 서버는 SRM으로 ServerSession-SetupResponse을 전송한다. 이를 수신한 SRM은 고객으로 세션내내 이를 확인하는 sessionID 필드, 세션 요구의 상태를 나타내는 response 필드, 그리고 서버 ID인 serverId 필드 등으로 구성된 ClientSessionSetupConfirm을 전송함으로서, 서버와 고객은 SRM의 중재로 상대방의 NSAP을 알고 서로의 IP 연결을 설정한다. 여기서 여러개의 TCP 연결이 인증, 구매 요구, DSM-CC UU 정보 교환을 위하여 설정되며, S1 정보 교환을 위한 MPEG-2 TS가 설정된다. 이후 고객과 서버는 서로의 신분을 확인하고 추후의 암호 통신을 위한 세션과 무결성을

위한 세션키를 공유하며, VOD 서비스가 최종적으로 제공하기 이전에 수행되어야 할 구매대화, 그리고 S1 정보를 통한 영화 내용 교환, 그리고 DSM-CC U-U 구조를 이용한 비디오 및 오디오 제어 신호의 교환 과정 등을 수행한다. VOD 서비스가 완료되면 고객은 SRM으로 해제를 요청하는 sessionID 필드와 해제 이유를 나타내는 reason 필드를 포함하는 ClientReleaseRequest를 전송하고, 이를 수신한 SRM은 ServerRelease-Indication을 서버로 전

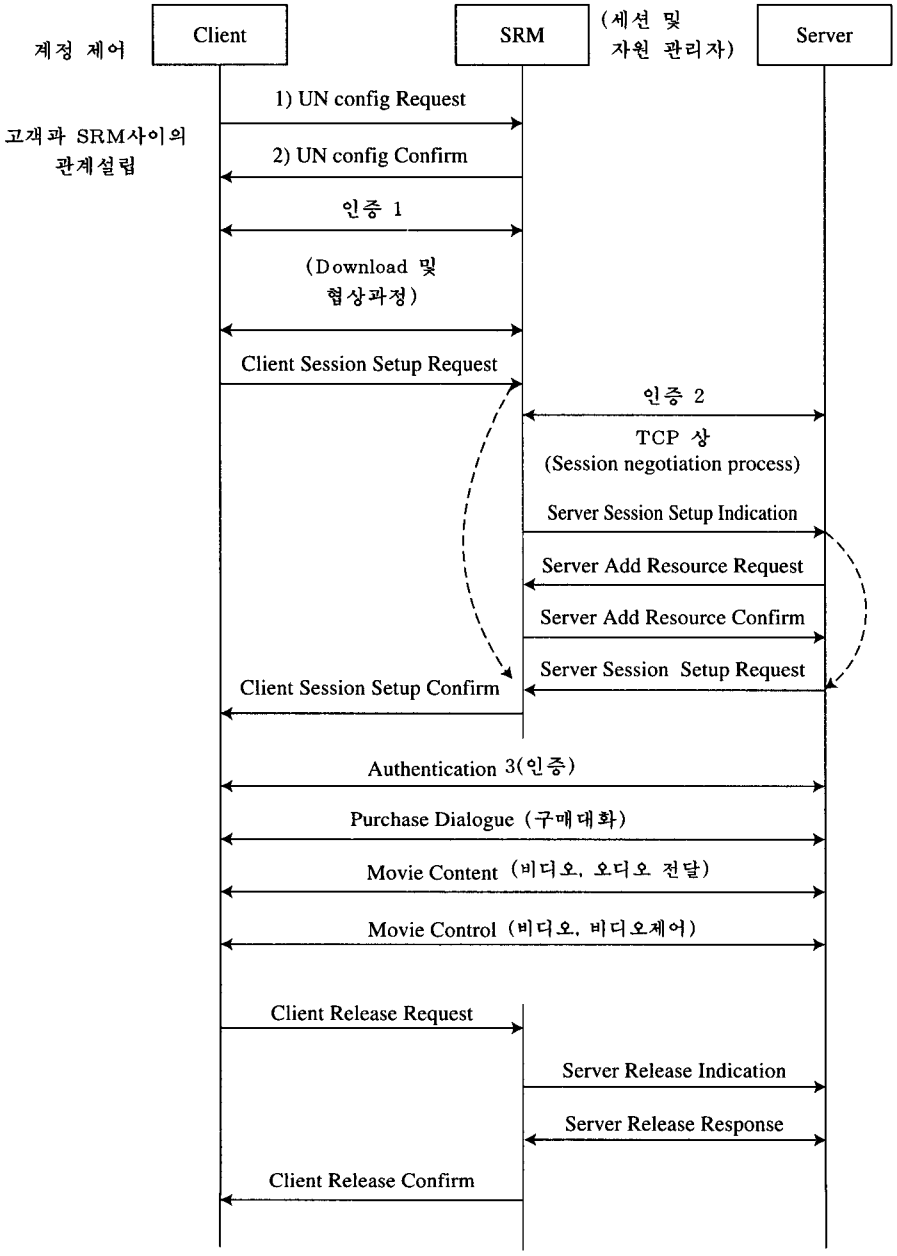


그림 2.23 VOD 세션에 응용된 예

달하며, 서버는 Server-ReleaseResponse를 SRM으로 전달하며, 마지막으로 SRM은 고객에 ClientReleaseConfirm 을 전달한다.

2.13 보안 서비스

보안 서비스는 등위 개체 인증(Peer Entity Authentication), 데이타 발신처 인증(Data Origin Authentication), 무결성(Integrity), 액세스 제어(Access Control), 부인 봉쇄(Non-Repudiation), 키 관리(Key Management), 감시(Audit), 그리고 익명성(Anonymity) 서비스 등이 있다.

등위 개체 인증은 대화형 서비스를 제공하기 위한 두 개체들 간에 세션을 설정할 때 수행되며, 최종 사용자는 서비스를 수신하기 전에 서비스 비용의 올바른 지불을 위하여 등위 개체 인증을 통해 서비스 제공자 또는 전달 시스템에 자신의 신분을 확인 받아야 한다. 등위 개체 인증은 보안 장치와 STU, 보안 장치와 전달 시스템, 보안 장치와 서비스 제공자, 서비스 제공자와 전달 시스템, 내용 제공자와 서비스 제공자, 그리고 내용 제공자와 전달 시스템 등의 구성 요소 들간에 수행되어야 한다.

- 보안 장치와 STU : STU는 등위 개체 인증 후에 보안 장치의 사용을 가능케 한다.
- 보안 장치와 전달 시스템 : 전달 시스템이 보안의 일부를 취급하는 경우, 전달 시스템은 보안 장치를 인증한 후 서비스를 전달한다.
- 보안 장치와 서비스 제공자 : 서비스 제공자는 세션을 설정하기 이전에 먼저 사용자의 신분을 인증해야 한다.
- 보안 장치와 다른 사용자의 보안 장치 : 한 사용자가 다른 사용자와 비디오 전화나 비디오 회의를 하기 위해서는 먼저 다른 사용자에 대한 등위 개체 인증을 수행한 후에 세션을 설정한다.
- 서비스 제공자와 전달 시스템 : 전달 시스템이 보안의 일부를 취급하는 경우, 전달 시스템은 서비스 제공자를 등위 개체 인증을 한후에 서비스를 전달한다.
- 내용 제공자와 서비스 제공자 : 서비스 제공자는 내용의 전달을 제공자를 개체 인증한 후에 세션을 설정한다.
- 내용 제공자와 전달 시스템 : 전달 시스템이 보안의 일부를 취급하는 경우, 전달 시스템은 내용 제공자를 개체 인증한 후에 서비스를 전달한다.

통신망이 STU를 개체 인증하는 것은 중요하지 않다. DAVIC 액세스 제어 시스템의 안전성은 STU에 독립이어야 한다. STU는 ID(identity)을 가질 수 있으나, STU에 대한 인증은 요구되지 않는다. 인증 과정은 STU의 참여하에 수행될 수 있지만, 근본적으로 보안 장치에 의해 수행되어야 한다. 보안 장치는 사용자의 비밀키의 누설 없이 인증 과정을 수행할 수 있는 충분한 기능을 가지고 있어야 한다.

데이타 발신처 인증은 단일 메시지의 발신처를 검증할 필요가 있을 때 요구된다. 메시지 발신처 인증은 방송 응용에서 세션키의 교환시에 응용될 수 있다. 이는 보안 장치와 과금 관리 시스템, 고객의 보안 장치와 서비스 제공자, 서비스 제공자와 고객의 보안 장치, 그리고 전달 시스템과 고객의 보안 장치 들간에 이루어진다. 이는 디지틀 서명 기법으로 실현된다.

- 고객의 보안 장치와 과금 시스템 : 고객이 지불을 수락할 때(payment request)
- 고객의 보안 장치와 서비스 제공자 : 고객이 서비스 개시를 요구할 때
- 서비스 제공자와 고객의 보안 장치 :

authorization decision(액세스 허용 판단)

- 전달 시스템과 고객의 보안 장치 : 전달 시스템이 제어 워드를 변경하려 할 때

데이타 기밀성은 권한 없이 서비스 내용이 액세스 되지 않도록 보호하기 위하여 사용되거나 여러 통신 주체 들간에 신호 정보와 제어 정보를 보호하기 위하여 사용된다. 제어 및 신호 정보에는 암호키의 교환을 위한 교환 정보를 포함한다. 기밀성은 전달 시스템과 보안 장치, 서비스 제공자와 보안 장치, 전달 시스템과 STU, STU/보안 장치와 STU/보안 장치, 서비스 제공자와 전달 시스템, 내용 제공자와 서비스 제공자, 내용 제공자와 전달 시스템, 그리고 서비스 제공자와 서비스 제공자 간에 요구될 수 있다. 데이타 기밀성은 스크램블링 툴로 실현된다.

- 전달 시스템과 보안 장치 : 전달 시스템이 보안의 일부를 취급하는 경우, 전달 시스템이 세션키를 보안 장치로 전달하려고 할 때
- 서비스 제공자와 보안 장치 : 서비스 제공자가 세션키를 전달하려고 할 때
- 전달 시스템과 STU : 전달 시스템이 보안의 일부를 취급하는 경우, 전달 시스템이 STU로 제어 정보(control information)를 전달하려고 할 때
- 서비스 제공자와 STU : 서비스 제공자가 STU 로 내용을 전송할 때
- STU/보안 장치와 STU/보안 장치 : 두 STU 간의 비디오 회의를 원할 경우
- 서비스 제공자와 전달 시스템: 전달 시스템이 보안의 일부를 취급하는 경우, 서비스 제공자가 전달 시스템으로 제어 정보를 전송할 때
- 내용 제공자와 서비스 제공자 : 내용 제공자가 서비스 제공자로 내용을 전달할 때
- 내용 제공자와 전달 시스템 : 전달 시스템이 보안의 일부를 취급하는 경우, 내용 제공자가 전달 시스템으로 제어 정보를 전달할 때
- 서비스 제공자와 서비스 제공자 : 서비스 제공자간에 내용을 전달하려고 할 때

데이타 무결성 서비스는 데이타가 변경되지 않았다는 것을 증명하기 위하여 사용된다. 데이타 발신처 인증이 하나의 데이타 단위를 보호하기 위하여 사용되는 반면, 데이타 무결성은 세션 동안 내내 사용된다. 데이타 무결성 서비스는 등위 개체 인증 서비스를 사용하여 설정이 완료되어 있는 세션 동안에 사용될 것이다.

액세스 제어는 시스템 개체에 특정 응용을 액세스하는 능력, 변경 또는 관찰의 목적으로 특정 유형을 액세스하는 능력, 그리고 읽고 쓸 목적으로 시스템 정보에 액세스하는 능력을 부여하거나 거절하는데 이용된다. 서비스 제공자나 전달 시스템은 사용자의 과거 신용 상태를 기초로 특정 응용으로의 사용자의 액세스를 허용하거나 거부할 수 있는 액세스 제어 시스템을 채용한다. 또한 최종 사용자는 자신이 지배하고 있는 하부 사용자에 대한 서비스로의 액세스를 허용하거나 거부할 수 있다.

부인 봉쇄는 메세지의 수신 및 메세지의 근원지를 증명하는데 중요하다. 이를 이용하면 송신자는 자신이 보낸 메세지를 거부할 수 없고 수신자는 수신되었다는 사실을 거부할 수 없다. 이는 디지틀 서명 메카니듬으로 실현된다. 부인 봉쇄는 금융 거래나 고부가 가치의 서비스를 주문하는 경우 매우 유용하다.

키 관리는 다른 보안 서비스들을 보조하기 위하여 요구된다. 키 관리의 주요 목적은 통신 개체들 간의 대칭형 세션키의 안전한 분배 문제이다. 방송 서비스의 경우, 키 관리는 여러 사용자들이 사용하고 있는 키의 동시적인 변

화를 가능케 한다. 키 관리는 키 관리 메카니듬과 인증 메카니듬이 결합되어 실현된다.

서비스 제공자, 전달 시스템, 그리고 청구서 작성 시스템은 보안 감시 기능을 수행해야 한다. 이는 보안 서비스의 취약점을 검출하고 분석하며 동시에 청구서 관련 분쟁을 보조한다.

모든 사용자들의 동작은 다른 제삼자에는 익명성을 보장해야 한다. 사용자에 의해 수행된 동작 정보를 인식하는 것은 매우 어렵다. 그리고 제삼자는 다른 사람의 신원을 확인하거나 데이타를 보내고 수신하는 서비스 제공자의 신원을 알 수 없도록 해야 한다.

2.13. S1 정보를 위한 스크램블링 시스템

스크램블링 시스템은 내용 정보(S1, Content Information)의 표현(Representation)을 변경하여, 인정받은 사용자는 변경된 내용으로 부터 내용 정보를 복구할 수 있지만, 인정받지 못한 사용자는 내용 정보를 복구할 수 없도록하는 암호학적 툴이다. DAVIC에서의 스크램블링 시스템은 선택 사항이며, 내용 정보가 모든 사용자에게 가용한 경우, 스크램블링 시스템은 요구되지 않는다. 그러나 내용의 분배가 특정 사용자에게만 한정되기를 원하는 경우 스크램블링 시스템이 이용 가능하다. 내용 제공자, 서비스 제공자, 그리고 망 제공자는 스크램블링 시스템을 실현할 것이다.

스크램블링은 시스템내의 임의의 위치에서 발생되며, MPEG2 트랜스포트 시스템 레벨 계층에서 수행될 것이다. 스크램블링은 페이로드에만 적용된다. 스크램블링 알고리듬은 내용 제공자, 서비스 제공자, 또는 망 제공자에서 실현된다.

스크램블링은 시스템 내의 임의의 위치에서 수행되며, 이는 MPEG2 트랜스포트 시스템 레벨에서 행해진다. 디스크램블링 역시 MPEG2 트랜스포트 시스템 레벨에서 행해질 것이다. 스크램블링은 페이로드에만 수행되며, 스크램블링 알고리듬은 카드 소지자와 STU에서 제공 가능한 알고리듬이 선택될 것이다. MPEG2의 헤더 부는 평문 형태로 유지되어야 한다. 특정의 세션마다 스크램블링을 위한 하나 또는 하나 이상의 일련의 세션키가 제공되어야 한다. 이는 세션키 설정 절차를 따라 제공된다. STU는 STU의 프로파일의 일부로서 STU에서 유용 가능한 보안 서브 시스템과 스크램블링 알고리듬을 보안 모듈 또는 서버로 전달할 수 있다.

제어 워드(Control Word)는 MPEG2 트랜스포트 스트림 패킷을 디스크램블링 하는데 이용될 수 있다. 제어 워드는 MPEG2 트랜스포트 패킷으로 ECM(Entitlement Control Message) 형태로 전달되거나 보안 장치 내에서 유도된다. CW의 주기는 보안을 위하여 수초 정도의 매우 짧은 주기를 갖는다. 세션키는 인증된 사용자만이 복구할 수 있다. 제어 워드의 실시간 변화를 가능케 하기 위하여 even 제어 워드와 odd 제어 워드로 알려진 2개의 서로 다른 제어 워드를 저당하고 있어야 한다.

MPEG 트랜스포트 패킷은 패킷 페이로드를 스크램블링 하는데 이용되는 odd 또는 even 제어 워드를 나타내는 트랜스포트 스크램블링 제어 필드를 포함하고 있다. 이의 값은 표 2.7과 같다.

표 2.7 transport_scrambling_control 필드

부호값	의 미
00	스크램블링됨
01	예비용(reserved)
10	even CW로 스크램블링
11	odd CW로 스크램블링

MPEG2 트랜스포트 패킷 헤더에는 패킷 패이로드를 스크램블링하는데 이용된 CW의 패리티 및 상태 정보를 나타내는 transport__scrambling__control 필드를 이용한다. 이 필드는 스크램블링 시스템의 사용 여부를 나타낸다. 이 필드의 값이 "00" 일 경우, 스크램블링되지 않은 상태이다.

트랜스포트 헤더부와 적응 필드는 스크램블링되지 않아야 한다. 이는 보호 과정 없이 중간 망요소에서 트랜스포트 제어와 역다중 및 재다중을 가능케 하기 위함이다. 여러 스크램블링 알고리듬들이 사용될 수 있으므로, 실제 적용되는 알고리듬은 확인 가능해야 한다. 적용되고 있는 스크램블링 알고리듬의 종류는 서비스를 개시하기 이전에 세션 계층에서 결정되거나 MPEG-2 스크램블링 서비스가 전달되는 동안 PMT(Program Map Table)의 CA descriptor 에 표시되어야 한다.

스크램블링 시스템을 실현하기 위한 스크램블링 알고리듬의 안전성은 중간 공격자나 해커가 내용 정보를 가로챌 수 없도록 충분히 강력해야 한다. 최소한으로 DAVIC 에서 이용되는 스크램블링 알고리듬은 ISO, ITU, 또는 ETSI에서 표준안으로 수용되어야 한다.

DAVIC의 여러 개체들은 각자의 스크램블링 시스템 툴을 실현할 것이다. 따라서 하나의 스크램블링 알고리듬에 대한 선택은 법적 문제와 상용화의 제한 등의 문제점이 있으므로 단일 스크램블링 알고리듬으로의 표준화는 거의 불가능하다. 그러나 이용되는 스크램블링 알고리듬의 갯수는 될 수 있는 한 작아야 한다.

스크램블링 알고리듬은 수출의 제한이 작아야 하고, MPEG 스트림 내의 가변 길이 필드들을 스크램블링할 수 있어야 하며, 적당한 시간 내에 깨지지 않아야 하며, 알고리듬의 안전성이 입증되고 표준화되어야 한다.

적용 가능한 스크램블링 알고리듬은 DVB 스크램블링 알고리듬, DES, triple-DES, 그리고 FEAL 등이다. 채널의 변경은 최소 시간 내에 가능해야 하고, 복호 역시 큰 지연 없이 복호를 시작할 수 있어야 한다. 따라서 패킷 단위로 암호화를 수행하는 것이 바람직하다. 이는 최선의 액세스 점 조각을 제공한다. 즉, 스트림 시작점에 대한 최소의 대기 시간을 제공한다. 일반적으로 대칭형 암호 알고리듬은 입력의 길이가 8 바이트의 정수 배가 되도록 하는 것을 요구한다. 이를 요구하는 알고리듬을 위하여 적응 필드의 길이에 제한을 두어 패킷 패이로드의 크기가 8 바이트의 배수가 되도록 해야 한다. 각각의 패킷은 서로 독립적으로 스크램블링되어야 한다. 이는 패킷 손실 시에 정보의 잘못된 디스크램블링이 연속적으로 되는 것을 방지할 수 있다.

스크램블링 시스템 툴의 실현은 반드시 키 관리 툴과 연동되어야 한다. 왜냐하면 키 관리 툴은 스크램블링된 내용 정보를 수신할 수 있는 권한이 부여된 사용자만이 내용 정보를 디스크램블링하는데 요구되는 CW를 소지하는 것을 가능케 하며, 궁극적으로 이 사용자만이 내용 정보를 액세스할 수 있을 것이다.

2.15 키 관리

키 관리는 계층적 키에 바탕을 두고 있다. 계층의 최상 노드에서는 비대칭형 암호 알고리듬을 사용한다. 최상 레벨의 키는 키 분배를 제공하는데 이용된다. 계층의 하부 계위는 대칭형키 암호에 바탕을 두고 있다. 대칭형키 암호는 오직 키 계층의 하위 계위에서만 적용된다. 이는 모든 서비스 제공자와 최종 사용자들의 임의의 결합을 포함하는 모든 통신 주체들 간에 대칭형 키의 안전한 분배를 요구한다.

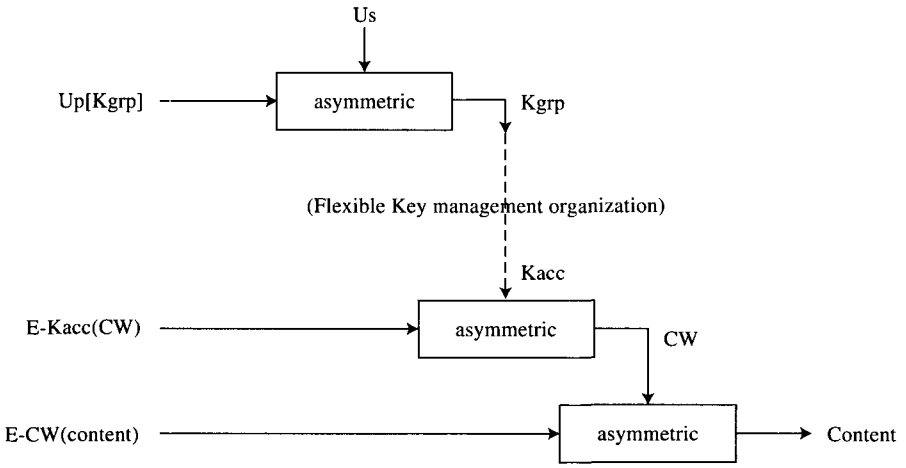


그림 2.24 키 분배 계층

키 계층은 다음과 같다. 방송 응용 서비스의 경우, 많은 사용자들에게 동일한 CW의 안전한 분배를 요구한다. CW는 내용을 디스크램블링하는 비밀키이므로 장기간 암호키보다 훨씬 더 노출될 가능성이 높다. 따라서 CW는 수분 또는 수초 차원으로 변경되어야 한다. 키 계층의 사용은 방송 응용을 위한 키 관리 과정을 간단하게 한다. 계층에서의 계위의 수는 제한되어 있지 않다. 그림 2.24는 키 분배 계층을 나타낸다. 여기서 Up는 사용자의 공개키, Us는 사용자의 비밀키, Up[I]는 사용자의 공개키 Up 로 암호화된 정보 I, E-K(data)는 대칭형 암호알고리듬의 비밀키 K로 암호화된 데이타, Kgrp는 응용 및 서비스 별로 할당된 서비스 관리키, Kacc는 CW에 대한 액세스를 허용하는 키, 그리고 CW는 내용을 스크램블링하는데 이용되는 제어 워드이다.

수신자는 스크램블링된 내용 정보를 CW를 이용하여 디스크램블링한다. CW는 모든 사용자에 공통이고 수 초 단위로 자주 변한다. 규칙적으로 전송되는 새로운 CW는 암호화되어 보호되어야 한다. 키 Kacc 는 CW를 액세스하는데 이용된다. 특정 서비스는 될 수 있는 한 작은 수의 Kacc를 가져야 한다. 방송 응용은 별도의 자격 관리 메세지 (ECM : Entitlement Control Message) 형태로 새로운 CW들을 여러 종류의 서비스 관리 키 Kacc들로 암호화한 복사판들을 송신한다. 보안 장치는 특정의 Kacc를 소지하고 있으므로 암호화되어 있는 CW를 복호하여 CW를 복구한다. CW는 자주 변해야 한다. 왜냐하면 보안 장치는 STU로 평문 형태의 CW를 보내고 STU는 이를 이용하여 내용을 복호한다. 만약 CW 변경 주기가 길다면 합법적인 사용자가 STU 와 보안 장치간의 CW를 이용하여 비합법적인 사용자에 넘기는 공격이 가능하다. Kacc는 보안 장치 내에 비밀스럽게 보관되어야 한다. Kacc가 암호 공격으로 노출되었을 경우 Kacc는 변경되어야 한다. Kacc의 수명은 보통 수주 또는 수달 정도이므로 CW의 수명보다 훨씬 길다. 융통성있는 키 관리 계층이 Kacc를 생성하기 위하여 도입될 수 있다. 사용자의 비대칭형 비밀키가 궁극적으로 서비스 내용을 복호하는 키를 보호한다.

Kacc는 그룹키 Kgrp에 의하여 보호될 수 있다. 각 그룹에는 작은 수의 사용자들이 있고 여러 개의 그룹들이 존재한다. 작은 수의 사용자를 위한 그룹키는 보안 장치 내에 저장된다.

그룹키를 변경할 필요가 있는 경우, 온라인으로 수행되어야 한다. 새로운 그룹 키는 사용자의 공개키로 새로운 CW을 암호화하여 각 사용자에 송신함으로서 새로운 그룹 키를 온 라인으로 각 사용자들에게 분배할 수 있다. 이 그룹화 계획은 그룹 키가 탈로 났을 때 재분배할 사용자의 수를 줄일 수 있는 융통성을 부여한다.

키 계층의 최상 단에 있는 복호키는 합법적인 최종 사용자에게도 알려지지않으며, 이는 스마트카드의 비밀 영역에 비밀스럽게 저장되어야 한다. 하나의 보안 장치만으로 여러 다양한 서비스 제공자들과 접속이 가능케 하기 위해서는 공개키 증명서를 이용해야 한다. 이는 믿을 수 있는 제삼자가 사용자의 공개키를 서명한 공개키 증명서를 이용하며, 공개키 증명서를 보안 장치로 분배하여 쉽게 실현될 수 있다.

키 분배를 위한 ECM/EMM 구조는 다음과 같다. 키는 자격 관리 메세지와 자격 제어 메세지 형태로 분배된다. 자격 검사 기능은 서비스를 액세스하기 위한 조건(Conditions)을 전달한다. 액세스 변수(Access Parameter)는 조건의 일부이다. 액세스 변수로는 프로그램의 ID, 프로그램 번호, cost per view, cost per time, cost per level, 그리고 주제 등의 프로그램을 액세스하기 위해 요구되는 조건들을 포함한다. ECM에는 데이타와 시간 정보를 포함해야 한다. 자격 데이타는 ECM 채널로 전달된다. ECM은 새로 연결된 사용자의 빠른 액세스를 가능케 하고 CW의 주기적 변경을 위하여 충분히 자주 사용자로 방송된다. 보안 모듈이 CW을 계산할 수 있고 충분한 동기를 보장할 수 있기 위하여 CW변경 주기는 충분히 길어야 한다. 그러나 CW의 수명은 충분히 짧아야 한다. CW 계산은 보안 모듈에서 수행된다. ECM은 액세스 조건 등의 메세지에 대한 무결성을 검증하기 위한 디지틀 서명 기법을 채용해야 한다. 대화형 서비스의 경우, 비밀키는 세션의 개시 시에 계산되며, 이의 사용은 해당 세션으로 한정된다. 보안 장치는 수신된 액세스 파라메타와 자신의 자격 정보를 비교하여, 일치하면 CW을 복구하고 STU로 CW를 전달한다.

자격 관리 기능은 수신자에 자격을 분배하거나 소비에 대한 정보를 분배한다. 가입은 다양한 선택으로 이루어진다. 이 선택에는 주제별, 레벨별, 사전 예약, impulsive pay-per-view, 시간별, 그리고 프로그램별 등이 있다. 이 데이타는 EMM(entitlement management message)라 불리는 전용 채널로 전달된다. EMM은 신호 전송 채널 또는 다른 채널 상에서 경로 배정된다. 기밀성이 요구되지 않으면 새로운 권한에 대한 무결성을 검사하기 위한 디지틀 서명 기법만이 요구된다. EMM이 각 가입자의 비밀키를 변경하고 분배하는 채널로 이용된다면 기밀성 기법이 반드시 이용되어야 한다.

2.16 DAVIC 공개키 증명서

각 사용자의 공개키는 믿을 수 있는 제삼자인 인증 센타가 발행해야 한다. 개체 A 의 공개키 증명서는 모든 객체들이 믿을 수 있는 인증센타 (CA:Certification Authority)가 발행하며, CA는 모든 개체가 신뢰할 수 있는 개체(Entity)이다. 공개키 증명서의 구성 정보는 사용자의 공개키와 사용자의 구별 가능한 이름, 공개키 증명서의 유효 기간 등이며, 공개키 증명서는 기본적으로 ID와 PKA를 CA의 비밀키로 서명한 DCAs(IDA,PKA)이다. 공개키 증명서의 검증은 CA의 서명용 공개 정보를 이용하여 수행되며, CA의 공개 정보는 각 사용자가 변경 불가능한 영역에 보관해야 한다. CA의 공개 정보의 누출은 CA에 의해 검증된 사용자간의 정보의 무결성에 심각한 영향을 미치기 때문이다. 따라서 CA의 공개 정

보 저장 매체는 스마트 카드가 바람직한다. 공개키 증명서의 일반적 구조는 다음과 같다.

```
DAVIC-Certificate ::= SEQUENCE
  { to be signed SEQUENCE {
    version                 INTEGER DEFAULT 1,
    certificateNumber       PrintableString,
    namingAuthority         Name,
    signatureAlgorithm      AlgorithmIdentifier,
    issuer                  Name,
    timeOfIssue             UTCTime,
    validity                Validity,
    subject                 Name,
    firstSubjectKeyInfo     PublicKeyInfo,
    secondSubjectKeyInfo    PublicKeyInfo  OPTIONAL,
                            }
    signature               OCTET STRING
}

Validity ::= SEQUENCE {
    notBefore               UTCTime,
    notAfter                UTCTime
            }

PubKeyInfo ::= SEQUENCE {
    subjectAlgorithm        AlgorithmIdentifier,
    subjectPublicKey        OCTET STRING }
```

버전은 DAVIC 공개키 증명서 버전의 번호이고, certificateNumber 는 알파벳을 허용하기 위한 printablestring 이며, 공개키 증명서를 유일하게 확인하기 위한 식별자이다. naming-Authority 는 공개키 증명서의 소유자가 속해 있는 보안 영역을 책임지는 기관의 이름이다. signatureAlgorithm은 CA가 서명문 생성을 위해 사용한 알고리듬이다. issuer 는 공개키 증명서 발행자의 유일한 이름이다. timeOfIssue 는 공개키 증명서가 발행되는 시간을 의미한다. validity는 공개키 증명서의 유효 기간을 나타내며, 유효 시작 일시와 유효 종료 일시를 포함한다. subject는 공개키 증명서 소유주의 DistinguishedName이다. firstSubjectKeyInfo와 secondSubjectKeyInfo는 이용되는 보안 알고리듬의 종류와 각 보안 서비스를 위한 공개키 값을 포함하고 있다. signature는 상기 구성 정보를 CA의 서명용 비밀키로 서명한 결과이다.

3. CA1 인터페이스

DAVIC에서는 스마트카드와 인터페이스되는 CA1과 보안 모듈과 인터페이스되는 CA0 인터페이스의 2가지 인터페이스를 정의하고 있다. 본 장에서는 경제성 및 간단성 특성을 갖는 CA1 인터페이스 규격을 분석한다. DAVIC 보안 시스템을 위한 도구는 ISO-7816에 기반을 둔 CA1 인터페이스를 통해 실현될 수 있다.

3.1 CA1 인터페이스를 위한 요구사항

CA1 인터페이스를 위한 일반적인 요구사항은 다음과 같다.

① 단일 STU는 여러 다른 CA 시스템을 지원해야한다.
② 분리 가능한 보안 요소는 경제적으로 실현되어야 한다.
③ 인터페이스는 CA0 인터페이스를 실현하는 경우에 비해 경제적으로 실현될 수 있어야 한다.
④ 둘 또는 그 이상의 보안 요소를 동시에 사용 가능하도록 구성되어야 한다.
⑤ 어떤 보안 요소도 다른 어떤 보안 요소의 동작이나 기능에 방해받지 말아야 한다.

⑥ 모든 보안 요소의 부재 시에도 모든 비 액세스 제어 서비스는 STU에서 유용하게 서비스되어야 한다.

⑦ 모든 보안 요소의 부재 시에 STU는 넓은 범위에서 그것의 자원 모두를 제어할 수 있어야 한다.

⑧ 사용자가 친숙하도록 구성되어야 한다.

⑨ 인터페이스는 전세계적인 규격의 적용으로 인한 경제적 규모가 크도록 실현되어야 한다.

⑩ 인터페이스는 분리 가능한 보안 요소의 쉬운 재생 및 변경이 가능하도록 구성되어야 한다.

ⓐ 인터페이스는 보안 요소의 정보와 인증에 관한 사항을 제시할 수 있도록 구성되어야 한다.

ⓑ 인터페이스는 STU에서 녹음 방지 기능의 논리적 기능을 제어할 수 있어야 한다.

ⓑ STU와 보안 요소간에 통신 속도의 상한선이 정의되어야 한다.

3.2 CA1 인터페이스 규격

부착 가능한 보안 모듈(즉, 스마트 카드)은 STU에 적은 가격의 추가로 실현 가능해야 하고, 소비자가 쉽게 사용할 수 있어야 하며, 운반이 용이해야 하고, 기존의 표준안에 바탕을 두고 실현되어야 한다. CA1 참조 모델은 물리적 계층은 ISO/IEC 7816-1,2의 물리/전기적 특성에, 프로토콜과 데이터 구조는 ISO 7816-3,4에 기반을 두고 실현된다. 이를 위하여 다음의 사항을 가정한다.

- 각 CA 시스템은 그것의 CA__System__ID 에 의해 확인되어진다.
- 하나의 STU는 하나 이상의 CA 시스템과 작동 될 것이다.
- 각 CA 시스템은 하나 이상의 CA 운용자로 실현되어 질 것이다.
- CA1은 망에 독립적인 인터페이스이다.

귀환 채널(Return Channel)은 스마트카드와 서버간의 통신 링크를 제시한다. EMM 메세지는 개인의 보안 요소나 보안 요소의 그룹 단위로 전송된다. 이의 속도는 수 Mbps 이고, EMM 처리는 암호화 연산이 요구되므로, 하드웨어 필터가 암호화 프로세서에서의 처리율을 줄이기 위해 요구된다. 카드에 유용한 CA 메시지를 추출하기 위해 하드웨어 필터가 요구된다. 이의 필터링 영역은 카드에 의해 제어된다. 일반적으로 CA__Message__Section 은 다음과 같다.

```
CA-Message-Section(){
        table-id
        section-syntax-indicator
        DVB-reserved
        ISO-reserved
        CA__message-section-length
        for (i=0; i<N; N++) {
                CA-message-descriptor-byte
                } }
```

필터링 대상 필드는 CA__Message__Section 의 table__id와 CA-message-descriptor-byte 의 처음에서 일정한 offset를 갖는 7 바이트에 대해 수행된다. offset 이 있는 처음 7 바이트는 필터 영역(Filterable Area)이라 한다. 필터는 원하는 ECM/EMM 메세지를 추출하여, 이를 CA1 인터페이스를 통해 스마트카드로 전달한다. 필터 영역은 다음과 같은 구조를 갖는다.

```
CA__unit(){
        issuer Id                24
        reserved                  4
        unit-id-length            4
```

```
for (i=0; i<N; I++){
    unit-Id-ls--digit        4
    unit-Id-ms-digit         4
                }
```

동일한 구조를 갖는 N개의 필터 집합은 다음과 같은 레지스터 들로 구성되며, 프로그램 가능하다.

① 필터 영역과 동일한 길이의 Target 레지스터
② 필터 영역과 동일한 길이의 Mask 레지스터
③ CA Section의 table id와 비교되는 Target 레지스터
④ CA Section의 table id와 비교되는 Mask 레지스터

STU는 위의 4 필터 레지스터를 이용하여 특정 조건이 만족될 경우에만 필터 영역과 CA Section 패이로드로 구성되는 CA Section 내용을 CA1 인터페이스를 통해 스마트 카드로 전달한다. 입력 필터 가능한 패턴을 마스크 레지스터의 비트가 "1"인 비트만에 대해 target 레지스터 패턴과 비교되며, 또한 table ID를 위한 target 레지스터와 마스크 레지스터도 동일한 방법으로 비교되며 필터된다.

3.3 명령(Command)

명령은 스마트카드에 적당한 파일의 선택하거나 파일 데이터를 읽기 위하여 사용된다. 이의 종류는 다음과 같다.

- Select__File, Send__CA__Message, Read__record, Modify__Password, Verify__Password
- Modify__Maturity__Rating, Get__Response, Get__Data, Put__Data, Get__Status

Select__File 명령은 DF나 EF등의 특정 파일을 선택하기 위해 사용된다. 이는 그림 3.1과 같은 구조를 갖는다.

CLA	미정
INS	0XA4
P1	00 : file ID 에 의한 선택 04 : DF 이름에 의한 직접 선택
P2	
Lc field	ID Length
Data	file ID or DF name

그림 3.1 Select__File 명령 및 응답

CA 메세지는 ECM, EMM, 그리고 구매 메세지(Purchase Message)등을 포함한다. ECM 은 하나 또는 다수의 암호화된 제어문과 프로그램 요소의 어떤 특성을 전달한다. 이는 프로그램 요소와 동기화 되어 전송된다. EMM은 자격 관리 정보를 수반하며, 특정 카드나 카드 그룹에 전달된다. 구매 메세지는 사용자의 어떤 프로그램에 대한 구매 요구나 카드에 구매 정보를 저장하는 것을 허용한다. Send__CA__Message 명령은 그림 3.2와 같다.

CLA	미정
INS	미정
PI	00
P2	00
Lc field	다음 데이터 필드의 길이
Data	CA 메세지 (EMM or ECM)
Le field	Empty

그림 3.2 Send__CA__Message 명령

Read_Record 명령은 그림 3.3과 같이 스마트카드로부터 현재 선택된 파일 내용물의 내용 조회를 위해 사용된다.

CLA	미정
INS	0XB2
P1	레코드 번호
P2	02 다음 레코드 03 이전 레코드 04 P1 에 의해 주어진 레코드 번호
P3	ID Length
Data	없음
Le	읽을 바이트 수

그림 3.3 Read_Record 명령

Get_Response 명령은 처리 결과에 관한 정보를 얻기 위하여 사용된다. Get_Response 명령의 부호화된 형태는 그림 3.4와 같다.

CLA	미정
INS	C0
PI	00
P2	00
Lc	없음
Data	무
Le field	응답시 기대되는 최대 바이트 수

그림 3.4 Get_Response 명령

Modify_Password 명령은 스마트 카드에 있는 패스워드를 바꾼다. 임의의 DF나 선택된 EF에서도 사용될 수 있다. Modify_Password 명령은 그림 3.5와 같은 구조를 갖는다.

Verify_password 명령은 패스워드를 검증하는데 사용하며, 어떤 DF나 선택된 EF로 사용될 수 있다. 명령 메시지는 그림 3.6과 같다.

CLA	미정
INS	미정
PI	00
P2	00
Lc field	다음 데이터 필드의 길이
Data field	old_password new_password
Le field	응답시 기대되는 최대 바이트 수

그림 3.5 Modify_Password 명령

CLA	?
INS	20
PI	00
P2	00
Lc field	다음 데이터 필드의 길이
Data field	패스워드
Le field	Empty

그림 3.6 Verify_Password 명령

Put_Data 명령은 하나의 원시 데이터 객체나 구성된 데이터 객체에 포함된 하나 또는 그이상의 데이터 객체들의 저장을 위해 사용된다. Put_Data 명령은 그림 3.7과 같다.

CLA	미정
INS	DA
P1-P2	Table 55
P2	00
Lc field	다음 데이터 필드의 길이
Data field	Parameter + 쓰여진data
Le field	Empty

그림 3.7 Put_Data 명령

Get_Data 명령은 하나의 원시 데이터 객체의 복구나 구성된 데이터 객체에 포함된 하나 또는 그 이상의 데이터 객체들의 조회를 위해 사용된다 명령 메세지는 그림 3.8과 같다.

CLA	미정
INS	CA
P1-P2	Table 55
Lc field	Empty
Data field	Empty
Le field	응답시 기대되는 바이트들의 수

그림 3.8 Get_Data 명령

Get_Status 명령은 STU가 스마트 카드 상태를 규칙적으로 폴링하는 것을 가능하게 한다. 상태의 규칙적인 폴링은 필수 사항이다. 상태 객체는 이 명령에 대한 응답으로 되돌려 받을 것이다. Get_Status 명령은 그림 3.9와 같다.

CLA	미정
INS	C0
P1	00
P2	00
Lc field	Empty
Data field	Empty
Le field	응답시 기대되는 데이터의 최대 길이.

그림 3.9 Get_Data 명령

3.4 귀환 채널(Return Channel)

귀환 채널은 카드를 사용하기 위해 인증한 CA 운용자 서버에 관한 정보의 조회하거나, 카드와 서버간의 인증 정보의 교환 등의 통신을 위한 메시지의 전송을 위해 이용된다. 구체적인 인증 관련 객체의 구조 및 명령의 구조는 추후 연구되어져야 한다.

4. 결 론

멀티미디어 서비스가 초고속 통신망을 통해 널리 유통될 예정이다. 이를 실현하기 위한 핵심 기술중 하나는 액세스 제어 기술이다. 본고에서는 DAVIC에서 권고 중인 액세스 제어 기법을 분석하였다. 이를 위하여 먼저 5개의 시스템 개체를 참조 모델로 하여, DAVIC 정보 흐름 및 프로토콜 스택을 정의하였다. 그리고 전달 시스템을 분석하고, STU와 NIU의 인터페이스를 분석하였다. 그리고 STU에서의 보안 인터페이스를 정의하였고, 액세스 제어 시스템을 위한 참조 모델과 보안 관련 참조점을 분석하였다. 그리고 MPEG2 트랜스포트 스트림을 분석하였으며, 액세스 제어를 위한 보안 메시지 구조를 제시하였다. 또한 보안 관련 개체들간의 요구사항을 분석하고, S2 또는 S3 상에서의 보안 메카니듬과 S2 또는 S3 상에서의 인증 프로토콜 및 변수를 분석하였다. 그리고 액세스 제어를 위한 보안 서비스를 분석하고, S1 정보를 위한 스크램블링 시스템의 동작을 제시하였다. 또한 암호키 관리 방식과 공개키 증명서 방식을 제시하였다. 또한 DAVIC CA1 인터페이스를 위한 요구사항, CA1 참조 모델, 명령 규격, 그리고 귀환 채널 등을 분석하였다.

참 고 문 헌

[1] DAVIC, DAVIC 1.2 Baseline Documents, 1996. 6., Newyork

[2] Man Young Rhee, Cryptography and Secure Communications, Mcgraw-Hill, 1992.

[3] ISO/IEC 13818-2, Information Technology - General Coding of Moving Pictures and Association Audio, Committee Draft, ISO/IEC JTC1/SC29, 1993., Seoul

[4] ISO/IEC IS 9798-3, Entity Authentication Mechanisms-Part 3 : Entity Authentication Using a Public-key Algorithm, ISO, Geneva, Switzerland, 1993.

[5] ITU Rec. X.509, The Directory-Authentication Framework, ITU, Geneva, Switzerland, 1993.

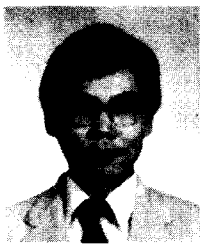
[6] NBS, Data Encryption Standard, FIPS Pub-46, 1977.

[7] A. Fiat, A. Shamir, "How to prove Yourself : Practical Solutions to Identifications and Signature Problems," in Advances in Cryptology Crypto'86, Proceedings, Springer-Verlag, pp.186-194, 1987.

[8] T.Beth, "Efficient Zero Knowledge Identification Scheme for Smart Cards," Proc. Eurocrypt'88, pp.77-84, 1988.

[9] J.Simmons, "An Impersonation-proof Identity Verification Scheme" Advances in Cryptology : Proceedings of Crypto'87, Springer-Verlag, pp.211-215, 1988.

□ 著者紹介



염 흥 열(정회원)

1981년 漢陽大學校 電子工學科 卒業(學士)
1983년 漢陽大學校 大學院 電子工學科 卒業(工學碩士)
1990년 漢陽大學校 大學院 電子工學科 卒業(工學博士)
1982년 12월 ~ 1990년 9월 韓國電子通信研究所 先任研究員
1990년 3월 ~ 현재 順天鄕大學校 工科大學 電子工學科 副教授

※ 관심분야 : 암호이론, 부호이론, 이동통신 분야