VOD 의 액세스 제어 기법

염 흥 열*, 이 종 형**
순천향대학교 전자공학과*, 충남대학교 컴퓨터공학과**

Access Control Techniques for VOD

Heung-Youl, Youm*, Jong-Hyeong, Lee**
Dept. of Electronics Eng., Soonchunhyang Univ.*,
Chungnam Univ.**

- 요약 -

본 고에서는 DAVIC 에서 권고 중인 VOD (video-on-demand) 시스템에 대한 액세스 제어 기법을 분석하고, 이를 바탕으로 국내 VOD 시스템에 적용 가능한 액세스 제어 기법을 제시한다. 이를 위하여 DAVIC 의 VOD 시스템에서의 보안 기법을 분석하고, 보안 시스템을 위한 참조 모델과 요구되는 서비스 및 보안 메카니즘을 분석한 후, 국내 VOD 시스템에 적용 가능한 액세스 제어 시스템 실현 방안과 정보보호 메카니즘을 제시한다. 그리고 방송용 서비스에 적용 가능한 ECM 채널을 DES, MD5, 그리고 RSA 알고리즘을 이용하여 C 언어로 구현하고 관련 동작을 시뮬레이션한다. 시뮬레이션 결과 ECM 채널이 정상 동작됨을 확인한다. 제시된 방안은 국내 VOD 시스템 실현시 유용하게 활용될 수 있다.

제1장 서론

비디오 신호를 디지탈 신호로 변환하기 위한 국제 표준 방식은 JPEG, MPEG1, 그리고 MPEG2 등이 있다. JPEG 은 정지 화상을, MPEG1 은 1.5Mbps VCR 정도의 품질을 갖는 화상을, MPEG2 는 11 개의 레벨을 가지며 NTSC 신호를 4-15Mbps 의 디지탈 신호로 변환하는 MPML (main profile at main level) 과 HDTV 신호 품질의 40-50Mbps 신호을을 갖는 MPHL (main profile at high level) 등으로 구성된다. 디지탈 비디오 신호에 바탕을 둔 멀티 미디어 신호는 광대역 ISDN 을 통해 활발히 유통되거나 저장 매체를 통해 저장될 예정이다. 최근 DAVIC (digital audio-visual council) 에서는 쌍방향 비디오 서비스 제공이 가능한 VOD (video on demand) 시스템에 대한 국제 표준화에 대한 연구를 수행하고 있다. VOD 에서의 가장 핵심적인 기능 중의 하나는 비인가자에 대한 비디오 신호의 액세스를 제한하는 액세스 제어 기술이다. 이는 크게 가입자측 장비인 STU, 각 가입자의 액세스 제어 기능을 수행하는 스마트 카드 형태로 실현될 보안 장치, 그리고 서비스 제공자의 자격 관리 및 제어 기능을 담당하는 액세스 제어 장치 등을 이용

하여 실현될 것이다. 스마트 카드의 외부 장치와의 인터페이스 표준은 ISO 권고안을 따르도록 권고하고 있다. 광대역 ISDN 이 구축되면서, VOD 서비스에 대한 요구는 급증할 추세이다. VOD 서비스에서 핵심적인 기능을 담당할 액세스 제어 기술은 광대역 ISDN 을 통한 VOD 서비스의 조기 구축의 관건이 될 것이다.[1,2,3,4]

본 고에서는 DAVIC 에서 권고중인 VOD 시스템에 대한 액세스 제어 기법을 분석하고, 이를 바탕으로 국내 VOD 시스템에 적용 가능한 액세스 제어 기법을 제시한다. 이를 위하여 DAVIC VOD 시스템에서의 보안 기법을 분석하고, 보안 시스템을 위한 참조 모델과 요구되는 서비스 및 보안 메카니즘을 분석한 후, 국내 VOD 시스템에 적용 가능한 액세스 제어 시스템 실현 방안과 정보보호 메카니즘을 제시한다. 그리고 방송용 서비스에 적용 가능한 ECM 채널을 DES, MD5, 그리고 RSA 알고리즘을 이용하여 C 언어로 구현하고 관련 동작을 시뮬레이션한다.

제2장 VOD 시스템 분석

본 장에서는 DAVIC 의 VOD 시스템 개요, 액세스 제어를 위한 메시지 구조, 그리고 액세스 제어를 위한 STU 내의 인터페이스를 정의한다.[1]

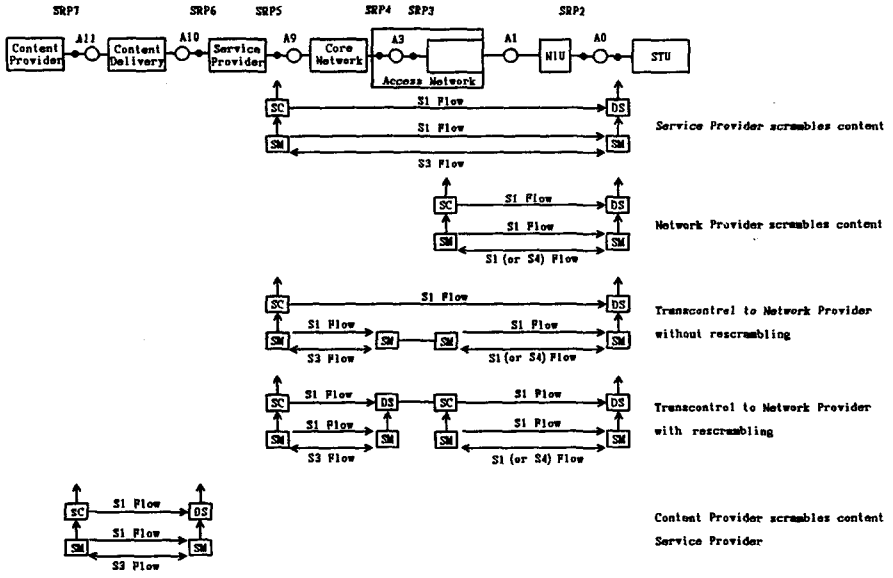

그림 2.1 간략화된 액세스 시스템 참조 모델

2.1 VOD 시스템의 개요

DAVIC 시스템은 5 개의 시스템 개체들로 구성된다. 이는 내용 제공자 시스템 (content provider system), 서비스 제공자 시스템 (service provider system), 서비스 고객 (service client), 내용 제

공자와 서비스 제공자를 연결하기 위한 전달 시스템 (delivery system), 그리고 서비스 고객과 서비스 제공자를 연결하기 위한 또 다른 전달 시스템으로 구성된다. DAVIC 시스템에서의 각 시스템 개체 간의 정보 흐름은 주 서비스 계층 (principal service layer) 용 S1 정보 흐름, 응용 서비스 계층 (application service layer) 용 S2 정보 흐름, 세션 및 트랜스포트 서비스 계층 (session/transport service layer) 용 S3 정보 흐름, 그리고 망 서비스 계층용 S4 정보 흐름 등이 있다. VOD 보안 서비스를 위한 스크램블링은 S1 정보 흐름 계층에서, 인증 기능은 S3 정보 흐름 계층에서 수행된다. DAVIC 에서 간략화된 액세스 제어 시스템 참조 모델 (reference model) 은 그림 2.1과 같다. SRP1-SRP7 은 보안 관련 기능이 발생하는 보안 참조 점 (security reference point) 이며, SC 는 스크램블링 (scrambling) 을, DS 는 디스크램블링 (descrambling) 을, SM (security management) 은 보안 관리 기능을 수행하는 개체를 각각 의미한다. 보안 기능은 보안 세션 협상, 스크램블링 알고리즘 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.

2.2. MPEG-2 트랜스포트 스트림 부호화 구조 및 파라메타

VOD 에서의 기밀성을 위한 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 스트림으로 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 패이로드에는 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) 을 위한 정보 및 표현 타임 스탬프등에 관한 정보를 포함한다.

트랜스포트 패킷(transport packet) 에는 13 비트의 PID (packet identifier) 를 포함한다. PID 는 PSI (program specific information) 테이블을 이용하여 규정된 트랜스포트 패킷이 담고 있는 데이타의 종류를 확인한다. 동일한 PID 을 갖는 트랜스포트 패킷은 하나의 기본 스트림을 전달한다. 여러 개의 트랜스포트 패킷들로 구성되는 트랜스포트 스트림의 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_byte 는 "0100 0111" 패턴이다. transport_error_indicator 는 한 비트 플래그로서, '1' 인 경우 교정이 불가능한 에러가 발생했음을 의미한다. payload_unit_start_indicator 는 1 비트 플래그로서, PES 와 PSI 패킷에 대해 의미를 갖는다. transport_priority 는 한 비트의 표시자로서 '1' 인 경우 우선 순위가 높은 패킷이다. PID 는 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 경우 유보되어 있고, 나머지 값은 PSI 를 통해 또 다른 기본 스트림에 할당된다. transport_scrambling_control 은 트랜스포트 패킷 페이로드의 스크램블링 상태를 나타낸다. adaptation_field_control 은 2 비트 필드로서 adaptation 필드의 존재 여부를 나타낸다. continuity_counter 는 4 비트 필드로서, 동일한 PID 를 갖는 트랜스포트 패킷이 전달될 때마다 1 씩 증가한다. data_byte 는 PID 에 의해 확인되는 PES 스트림, PSI 테이블, 또는 private data 로부터의 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 2.1 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_prefix 는 24 비트 부호로서, PES 패킷의 시작 부분을 확인하기 위하여 "0x000001" 패턴이다. stream_id 는 표 2.1과 같이 기본 스트림의 종류를 규정하고 있다. PES_packet_length 는 PES 패킷의 바이트 단위의 갯수로서 16 비트 필드이다. PES_stream_control 은 표 2.2와 같이 PES 패킷 페이로드의 스크램블링 모드를 나타낸다. PES_priority 는 페이로드의 우선순위를 나타내는 1 비트 표시자이다. PES_packet_data_byte 는 패킷의 stream_id 에 의해 확인되는 기본 스트림으로 부터의 연속적인 데이타를 의미한다.

packet_data_byte 의 길이 N 은 PES_packet_length 이며, PES_packet_length 의 마지막 바이트에서 PES_packet_data_byte 까지의 첫 바이트까지의 바이트의 수를 뺀 값이다. Padding_byte 는 8 비트 패턴으로서, "1111 1111" 이다.

표 2.2 PES_stream_control 필드

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

PSI (program specific information) 은 디코더에서 프로그램의 역다중이 가능케 하는 MPEG 정규 데이타 (normative data) 와 private data 를 포함한다. 프로그램은 하나 이상의 기본 스트림들로 구성되며, 각각의 기본 스트림은 고유의 PID 를 갖는다. 프로그램, 기본 스트림 등은 한정 액세스되어야 한다. PSI 는 스크램블링되지 않는다. PSI 는 표 2.3 과 같은 4 가지 테이블로 구성된다. 이중 conditional access table 은 CA 시스템과의 관계와 EMM 스트림을 제공한다.

표 2.3 PSI

구조 이름	스트림종류	PID 번호	내용
program association table	MPEG	0x00	프로그램 번호와 program map table 의 PID 를 연관시킴
program map table	MPEG	PAT_PID로 할당	하나 이상의 프로그램 요소에 대한 PID 값 규정
network information table	private	network PID 로 할당	FDM 주파수와 수신기의 갯수 등의 물리적 망 변수
conditional access table	MPEG	0x01	하나 이상의 EMM 에 특정의 PID 값 할당

PAT (program association table) 는 프로그램 번호와 프로그램 정의를 전달하는 트랜스포트 패킷의 PID 값을 전달하며, 이에 대한 PID 값은 "0x00" 이다. 프로그램 번호 0x0000 은 network PID 용으로 설정되었다. PAT 는 PID = "0x00" 인 트랜스포트 패킷으로 전달되며, 해당 프로그램 정보를 전달하는 트랜스포트 패킷의 program_map PID 를 전달한다.

PMT (program map table) 은 프로그램과 이를 구성하는 기본 스트림간의 관계를 나타내며, 기본 스트림의 PID 를 전달한다. 이는 TS program map section 으로 전달된다.

CAT(conditional access table) 은 하나 이상의 CA 시스템과 CA 시스템의 EMM 채널을 전달하는 트랜스포트 패킷의 CA_PID 를 전달한다.

2.3 액세스 제어을 위한 STU 내의 인터페이스 정의

STU 는 그림 2.2 와 같이 한정 액세스 유닛 (conditional access unit), 역다중(demux), 그리고 디코더(decoder) 부로 구성되어 있다. 한정 액세스 유닛은 디스크 샘플링 및 필터링 부와 암호 유

닛 (즉, 보안장치) 으로 구성된다. STU 에는 한정 액세스를 위해 2 개의 인터페이스가 정의되어 있다. CA0 인터페이스는 STU 내의 한정 액세스 유닛과 나머지 부분과의 인터페이스 점이며, CA1 은 한정 액세스 유닛 내의 디스크램블러 및 필터 부와 암호 유닛 간의 인터페이스 점이다.

디스크램블러 및 필터는 트랜스포트 스트림 레벨에서 동작되며, 스크램블링된 트랜스포트 패킷을 미리 합의된 스크램블링 알고리즘으로 디스크램블링하며, 스크램블러의 비밀키인 제어 워드는 송수신단과 공유되는 비밀 정보이다. PES 헤더부의 stream_id 필드는 ECM 및 EMM 을 구분한다. 디스크램블러와 필터링은 트랜스포트 스트림으로 부터 CA_PID 를 갖는 트랜스포트 스트림을 통해 전달되는 EMM 및 ES_PID 을 갖는 트랜스포트 스트림을 통해 전달된다. ECM 등의 보안 관련 명령들을 추출하여, 보안 관련 명령을 보안 장치로 전달한다. 여러 개의 ECM 및 EMM 메시지들을 수신한 필터링 부는 특정의 보안 유닛과 관련된 보안 정보 만을 전달한다. STU 와 보안 장치와의 인터페이스는 케릭터/블럭 단위의 비동기식 인터페이스가 적용 가능하다. STU 와 보안장치간의 기능 분담은 현재의 기능 수준으로 보아 고속 디스크램블링 기능과 필터링 기능은 STU 에서 수행하고 나머지 디지탈 서명, 무결성 서비스, 공개키 암호 알고리즘은 보안 장치에서 수행하도록 해야 할 것이다.

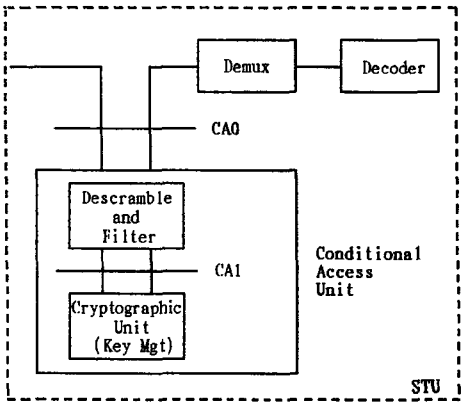

그림 2.2 STU 내의 인터페이스 정의

각 보안 유닛은 그룹 주소와 개별 주소로 구별된다. 보안 메시지는 유일하고도 구별 가능한 식별자로서, 첫 6 디지트는 산업체, 국가, 그리고 발행자등을 나타내는 디지트들이며, 12 디지트는 각 보안 유닛 또는 계정 확인자이고, 1 디지트는 검사 디지트이다. 발행자 식별자는 6 디지트 즉, 24 비트이며, 트리 구조로 생성되며, 트리의 레벨 수는 6 이며, 각 레벨당 출력 수는 최대 100 이다. 서브 트리 단위나 개별 주소를 나타낸다. 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 메시지의 구조는 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
                } }
```

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

table_id 는 8 비트 필드이며 표 2.4 와 같으며, 최대 9 개의 CA message descriptor bytes 가 주소 필터링을 위해 할당된다. section_syntax_indicator 는 한 비트 표시자로서, 항상 '0' 으로 리셋된다. CA_section_length 는 12 비트 필드이며, CA_section_length 에서 끝까지의 바이트 단위의 길이를 나타낸다. CA_message_descriptor_byte 는 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.

한정 액세스 정보를 갖는 CA_message_section 에 유용하며, ECM 데이타 전송을 위한 table_id 는 0x80 와 0x81 이다. ECM 의 table_id 의 변화가 ECM 의 내용 변화를 의미한다. 즉, odd 및 even CW 의 전달을 의미한다. 이의 문법은 다음과 같다.

```
CA_message_descriptor(){
        ca_unit_id
```

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.

표 2.5 ECM과 EMM 채널

이름	CLA	INSTR	P1	P2	Lc	Le
ECM	0x8c	0x30	0x00	0x00	length of descriptor	0x10
EMM	0x8c	0x32	0x00	0x00	length of descriptor	-

표 2.6 인증 정보에 대한 파라메타 값

CLA	0x0c
INS	0x88
P1	인증 알고리듬의 종류
P2	key reference
Lc	데이타 필드의 길이
CA_data_byte	인증 관련 데이타(예, challenge)
Le	최대 응답 길이

암호 유닛으로 전달되는 방송 키 관리 명령은 CA1 인터페이스를 통해 전달되며, ECM/EMM 섹션의 descriptor 부분을 전달한다. EMM 메시지는 올바른 그룹이나 개인 주소를 가진 특정의 보안 장치로 CA1 인터페이스를 통해 전달된다. 그리고 현재의 프로그램과 관련된 ECM 메시지 만이 CA1 인터페이스를 통해 보안 유닛으로 전달된다. EMM, ECM 메시지는 안전한 방법으로 전달되어야 한다. ECM과 EMM 채널은 표 2.5와 같은 변수를 이용하여 구분된다.

ECM 명령에 응하여 보안 유닛은 16 바이트의 get response 를 이용해 CAI 인터페이스를 통해 그 결과를 응답해야 한다. 이의 내용은 복구된 odd 및 even parity 의 CW 값이다. EMM 명령에 대한 응답은 없다.

인증 명령은 특정의 보안 유닛으로 전달되며, 특정 보안 유닛의 구별은 개별 ID 또는 그룹 ID 로 구별된다. 보안 장치의 주소는 STU 내에서 별도의 파일에 저장되며, 읽기가 가능하다. 보안 유닛에 대한 사용자 인증은 CA1 인터페이스를 통해 수행되며, 내부 인증 명령으로 수행된다. 인증 정보에 대한 파라메타 값은 표 2.6 과 같다.

제3장 VOD 에서의 보안 서비스

3.1 VOD에서 요구되는 보호 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) 등이 있다.[1]

3.2 보호 서비스를 위한 요구사항

정보보호 메카니즘은 암호 이론에 바탕을 두며, 키 관리 서비스와 함께 제공된다. 액세스 제어는 최종 사용자, 시스템 제공자, 그리고 서비스 제공자에 의해서 함께 관리되는 사용자 프로필을 바탕으로 수행된다. 세 가지 일반적인 원칙들이 보안을 위해 채용되었다.

첫째는 장기간 암호키 (long term cryptographic key) 는 절대로 누출되지 않아야 한다는 것이다. 이를 위해서는 특정 사용자에 한정되고 간섭이 불가능하며 교환이 가능한 보안 장치의 사용이 요구된다. 보안 장치는 서명용 및 암호용의 다른 2개의 비대칭형 암호키 쌍을 비밀리에 보관하고 있어야 한다. 둘째는 최종 사용자 인증은 보안 장치 내에 비밀리에 보관 중인 비밀 정보를 이용하여 실현되어야 한다는 것이다. 즉, 보안 장치 내의 비밀 정보만을 이용하여 인증이 수행되어야 한다. STU는 서비스 제공자가 최종 사용자를 인증하기 위하여 요구되는 일체의 비밀 정보도 가지지 않아야 한다. 보안 장치만이 인증을 위한 비밀 정보를 보유하고 있어야 한다. 이렇게 함으로서 최종 사용자의 위치에 무관하게 관련 보안 서비스들을 제공할 수 있기 때문이다. 셋째는 믿을 수 있는 제삼자를 사용하여 개별 사용자의 ID와 공개키를 연결하는 수단을 이용해야 한다는 것이다. 믿을 수 있는 제삼자를 도입함으로서 최종 사용자는 하나의 공통 한정 액세스 유닛을 사용하여 여러 다른 서비스 제공자의 서비스 제공자를 액세스할 수 있다.

3.3 보안 서비스

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, 내용 제공자와 전달 시스템 등의 구성 요소 들간에 수행되어야 한다.

데이타 발신처 인증은 단일 메시지의 발신처를 검증할 필요가 있을 때 요구된다. 메시지 발신처 인증은 방송 응용에서 세션키의 교환 시에 응용될 수 있다. 이는 보안 장치와 요금 시스템, 고객의 보안 장치와 서비스 제공자, 서비스 제공자와 고객의 보안 장치, 그리고 전달 시스템과 고객의

보안 장치 들간에 이루어진다. 이는 디지탈 서명시스템으로 실현된다.

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 장치 와 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 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 내용 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 디지탈 서명 메카니즘으로 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 일시적인 변화를 가능케 한다. 키 관리는 키 관리 메카니즘과 인증 메카니즘이 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 제삼자에게도 익명성이 보장되도록 수행되어야 한다.

3.4 보호 서비스 실현을 위한 보호 메카니즘

보안 기법으로는 스크램블링 기법, 키 관리 기법, 인증 기법, 그리고 보안 장치로 구분된다.

3.4.1 스크램블링 시스템

스크램블링 시스템은 비디오, 오디오, 그리고 부호화된 데이타 등의 내용 정보를 조직적으로 변경함으로서 불법 사용자는 그 내용을 알 수 없지만 합법 사용자는 원래의 내용 정보를 복구할 수 있도록 하는 기법이다.[12]

스크램블링 시스템은 모든 사용자에게 정보를 방송하는 경우 필요치 않다. 그러나 내용이 선택된 특정 사용자들에게만 분배되는 경우는 반드시 스크램블링 시스템을 이용해야 한다. 내용 제공자 또는 서비스 제공자는 선택된 사용자들로 만의 내용의 분배가 자신들의 이익에 필수적이기 때문에 스크램블링 시스템에 대한 요구 사항들을 규정해야 한다. 내용 제공자, 서비스 제공자, 그리고 망 제공자는 스크램블링 툴을 소지해야 한다.

제어 워드(control word : CW) 는 MPEG-2 트랜스포트 스트림 패킷에서의 스크램블링된 페이로드를 디스크램블링하는데 이용된다. 제어 워드는 자격 제어 메세지(ECM) 를 통해 암호화된 형태로 MPEG 트랜스포트 패킷을 통해 각 사용자에 분배된다. CW 의 수명은 수초 정도이다. CW 는 암호화되어 전달되기 때문에 정당한 사용자들만이 복구할 수 있다. CW 에 대한 실시간 변경을 용이하게 하기 위하여 우수 패리티를 갖는 CW 와 기수 패리티를 갖는 CW 로 알려진 두개의 서로 다른 CW 를 사용한다.

표 3.1 transport scrambling control 필드

부호값	의미
00	스크램블링 않됨
01	예비용(reserved)
10	even CW 로 스크램블링
11	odd CW 로 스크램블링

MPEG2 트랜스포트 패킷 헤더에는 패킷 페이로드를 스크램블링하는데 이용된 CW 의 패리티 및 상태 정보를 나타내는 transport_scrambling_control 필드를 이용한다. 이 필드는 스크램블링 시스템의 사용 여부를 나타내는데 이용된다. 이 필드의 값이 "00" 일 경우, 스크램블링 되지 않은 상태를 의미한다. 이의 구체적인 의미는 표 3.1과 같다.

트랜스포트 헤더 부와 적응 필드는 스크램블링되지 않아야 한다. 이는 보호 과정 없이 트랜스포트 제어와 역다중 및 재다중을 가능케 하기 위함이다. 여러 스크램블링 알고리즘들이 사용될 수 있으므로, 실제 적용되는 알고리즘은 확인 가능해야 한다. 스크램블링 알고리즘은 서비스를 개시하기 이전에 세션 계층에서 수행되거나 MPEG-2 스크램블링 서비스가 전달되는 동안 PMT (program map table) 의 CA descriptor 에 표시되어야 한다.

현재까지 고려중인 스크램블링 알고리즘은 DVB 스크램블링 알고리즘, DES, triple-DES, 그리고 FEAL 등이다. 채널의 변경은 최소 시간내에 가능해야 하고, 복호 역시 큰 지연 없이 복호을 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 대칭

형 암호 알고리즘은 입력의 길이가 8 바이트의 정수배가 되도록 하는 것을 요구한다. 이를 요구하는 알고리즘을 위하여 적응 필드의 길이에 제한을 두어 패킷 페이로드의 크기가 8 바이트의 배수가 되도록 해야 한다. 각각의 패킷은 서로 독립적으로 스크램블링되어야 한다. 이는 패킷 손실시에 정보의 잘못된 디스크램블링이 연속적으로 되는 것을 방지할 수 있다.

3.4.2 키 관리 기법

키 관리는 계층적 키에 바탕을 두고 있다.[13] 계층의 최상 노드에서는 비대칭형 암호 알고리즘을 사용한다. 최상 레벨의 키는 키 분배를 제공하는데 이용된다. 계층의 하부 계위는 대칭형키 암호에 바탕을 두고 있다. 대칭형키 암호는 오직 키 계층의 하위 계위만을 실현 가능하다. 이는 모든 서비스 제공자와 최종 사용자들의 임의의 결합을 포함하는 모든 통신 주체들 간에 대칭형 키의 안전한 분배를 요구한다.

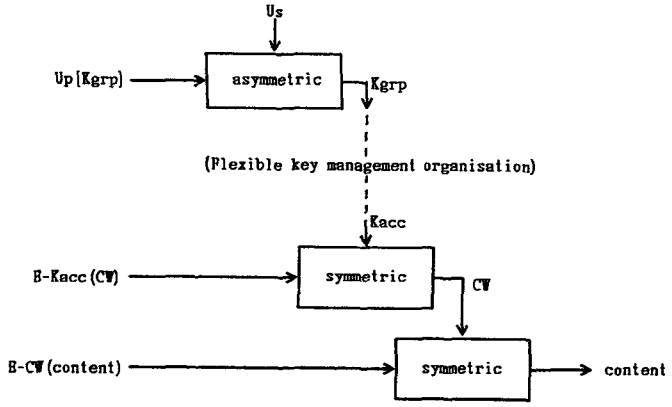

그림 3.1 키 분배 계층

키 계층은 다음과 같다. 방송 응용은 많은 사용자들에게 동일한 CW 의 안전한 분배를 요구한다. CW 는 내용을 디스크램블링하는데 사용되므로 장기간 암호키보다 훨씬 더 노출될 가능성이 높다. 따라서 CW 는 수분 또는 수초 차원으로 자주 변경되어야 한다. 키 계층의 사용은 방송 응용을 위한 키 관리 과정을 간단하게 한다. 계층에서의 계위의 수는 제한되어 있지 않다. 그림 3.1 은 키 분배 계층을 나타낸다.

여기서 Up 는 사용자의 공개키, Us 는 사용자의 비밀키, Up[I] 는 사용자의 공개키 Up 로 암호화된 정보 I, E-K(data) 는 대칭형 암호알고리즘의 비밀키 K 로 암호화된 데이타, Kgrp 는 응용 및 서비스 별로 할당된 서비스 관리 키, Kacc 는 CW 에 대한 액세스를 허용하는 키, 그리고 CW 는 내용을 스크램블링하는데 이용되는 제어 워드이다.

수신자는 스크램블링된 내용 정보를 CW 을 이용하여 디스크램블링한다. CW 는 모든 사용자에

공통이고 수 초 단위로 자주 변한다. 규칙적으로 전송되는 새로운 CW 는 암호화되어 보호되어야 한다. 키 Kacc 는 CW 을 액세스하는데 이용된다. 특정 서비스는 될 수 있는 한 작은 수의 Kacc 를 가져야 한다. 방송 응용은 별도의 자격 관리 메세지 (ECM : entitlement control message) 형태로 새로운 CW 들을 여러 다른 서비스 관리 키 Kacc 들로 암호화한 복사판들을 송신한다. 보안 장치는 특정의 Kacc 를 소지하고 있으므로 암호화되어 있는 CW 의 특정 실체를 복호화하여 CW 을 복구한다. CW 는 자주 변해야 한다. 왜냐하면 보안 장치는 STU 로 평문 형태의 CW 을 보내고 STU 는 이를 이용하여 내용을 복호한다. 만약 CW 변경 주기가 길다면 합법적인 사용자가 STU 와 보안 장치간의 CW 을 이용하여 비합법적인 사용자에 넘기는 공격이 가능하다. Kacc 는 보안 장치내에 비밀스럽게 보관되어야 한다. Kacc 가 암호 공격으로 노출되었을 경우 Kacc 는 변경되어야 한다. Kacc 의 수명은 보통 수주 또는 수달 정도이므로 CW 의 수명보다 훨씬 길다. 융통성있는 키 관리 계층이 Kacc 를 생성하기 위하여 도입될 수 있다. 사용자의 비대칭형 비밀키가 궁극적으로 서비스 내용을 복호하는 키를 보호한다.

Kacc 는 그룹키 Kgrp 에 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 CW 을 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 비밀스럽게 저장되어야 한다. 이는 비밀키 쌍의 최상단의 비밀키를 포함한다. 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. ECM 에는 데이타와 시간 정보를 포함해야 한다. 자격 데이타는 ECM 채널로 전달된다. ECM 은 새로 연결된 사용자의 빠른 액세스를 가능케 하고 CW 의 주기적 변경을 위하여 충분히 자주 사용자로 방송된다. 보안 모듈이 CW 을 계산할 수 있고 충분한 동기를 보장할 수 있도록 CW 변경 주기는 충분히 길어야 한다. 그러나 CW 의 수명은 충분히 짧아야 한다. CW 계산은 보안 모듈에서 수행된다. ECM 은 액세스 조건 등의 메세지에 대한 무결성을 검증하기 위한 디지탈 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 CW 을 복구하고 STU 로 CW 로 전달한다.

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

3.4.3 인증 기법

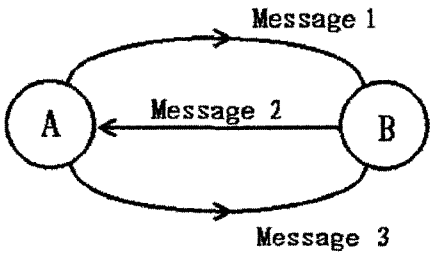

그림 3.2 인증 정보

인증은 상대방의 정체를 확인하기 위한 메카니즘이다. 인증은 동위 개체 인증과 데이타 발신처 인증 으로 구분된다. 현재 표준화가 고려 중인 인증 기법은 공개키 암호 기법에 바탕을 둔 X.509 인증 방식과 영지식 상호 증명 기법이다. 인증 기법으로 X.509 에 규정되어 있는 강력 인증 기법이 고려되고 있다. 이 메카니즘은 인증 정보 교환을 보호하기 위한 비대칭형 암호 기법에 바탕을 두고 있다. 이 메카니즘을 실현하기 위하여 요구되는 핵심 요소 기술은 PIN 으로 보호된 보안 장치, 적당한 해쉬 함수, 그리고 디지탈 서명 알고리즘 등이다. X.509 는 일회 (one-way), 이회 (two-way), 삼회 (three-way) 로 알려진 세 가지의 인증 과정들을 규정하고 있다. 이회와 삼회 인증은 동위 개체 인증에 이용된다. X.509 인증 프로토콜은 동위 개체 인증과 메세지 발신처 인증을 제공하기 위하여 사용된다.[4,7]

그림 3.2는 X.509 인증 과정을 위해 두 개체 A, B 간에 요구되는 교환되어야 할 인증 정보를 나타낸다. 이 정보는 메세지 1 (Message 1), 메세지 2 (Message 2), 메세지 3 (Message 3) 이라 명

명된다. 이 메세지들은 두 개체간에 번호 순서대로 교환된다. 이 세 메세지의 구조는 다음과 같다.

```
Message1        ::= SEQUENCE {
        certification_path              Certification Path  OPTIONAL
        token1                          Token1 }

Token1          ::= SIGNED { SEQUENCE {
        time_stamp                      TimeStamp OPTIONAL      (TA)
        random_1                        BIT STRING OPTIONAL     (RA)
        name                            DistinguishedName       (IB)
        data                            ANY OPTIONAL }}

Message2        ::= SIGNED { SEQUENCE {
        time_stamp                      TimeStamp OPTIONAL      (TB)
        random_1                        BIT STRING OPTIONAL     (RA)
        name                            DistinguishedName       (IA)
        random_2                        BIT STRING              (RB)
        data                            ANY OPTIONAL }}

Message3        ::= SIGNED { SEQUENCE {
        random_2                        BIT STRING              (RB)
        name                            DistinguishedName       (IB)
                }}

TimeStamp       ::= SEQUENCE {
        generation                      UTCTime OPTIONAL
        expire                          UTCTime }
```

일회 인증에서는 Message1 만이 사용자 A에서 사용자 B 로 전달된다. 이회 인증에서는 Message1 과 Message2 가 교환된다. 그리고 삼회 인증에서는 모든 메세지들이 교환된다.

Message1 에는 B 에서 A 로의 인증 경로, token1 의 생성 시간과 해제 시간을 포함하는 timestamp(T_A), 재생 공격을 방지하기 위하여 사용자 A 에 의해 생성되는 난수(R_A), B 의 구별 가능한 이름(I_B), 사용자 B 의 공개키로 암호화된 세션키 분배를 위한 데이타 부로 구성된다. Message2 에는 Message2 의 생성 시간과 해제 시간을 포함하는 timestamp(T_B), Message1 에 포함되어 사용자 A 에서 B 로 전달된 난수(R_A), A 의 구별 가능한 이름인 이름(I_A), 사용자 B에 의해 생성되는 난수(R_B), 데이타 발신처 인증이 제공되는 데이타부로 구성된다. Message3 에는 B 가 A 로 보낸 난수(R_B)와 B 의 구별 가능한 이름(I_B)을 포함한다.

영지식 증명 기법을 이용한 인증 방식의 표준화가 고려되고 있다. 대표적인 영지식 인증 기법은 GQ 의 이증 기법과 FS 의 인증 기법 등을 들 수 있다.[5,6,8.9.10,14]

인증 서비스를 위하여 두 개체는 동일한 알고리즘을 가지고 있어야 한다. 인증 알고리즘은 RSA,

DSS, 그리고 Gillou-Quisquater 영지식 증명 방식 등이다. 인증 메카니즘은 인증 서비스의 속도를 향상하기 위하여 보안 장치에서 작은 연산 능력을 갖는 알고리즘으로 선택될 것이다.

3.4.4 보안 장치

보안 장치와 STU 간의 기능 분배는 다음 3 가지 레벨로 실현된다.

① 보안 기능이 STU 내에만 수행된다. 디스크램블링, CA 메세지의 필터링, 그리고 키 관리 기능 모두가 STU 에 의해 내부적으로 처리된다.

② 디스크램블링과 CA 메세지의 필터링은 STU 내에서 수행되며, 키 관리는 부가적인 보안 장치에 의해 수행된다. 부가적인 보안 장치는 스마트 카드가 될 것이다.

③ 모든 액세스 기능이 부가적인 장치에 의해 수행된다.

가장 실현 가능한 방법은 ② 이다.

3.5 보안 시스템 구조

본 절에서는 보안을 위한 기본 구성을 규정한다. 이 법칙은 보안 서비스와 관련되므로 시스템의 구조를 정의하는데 도움이 된다.

① 스크램블링은 모든 계약 소지자에게 유용해야 한다. 스크램블링 기법이 모든 계약 소지자에 언제나 서비스되어야 함을 의미한다. 따라서 서비스 제공자의 어떤 스크램블링 서비스도 계약 소지자에 의해 제공되는 스크램블링을 제외해서는 안된다.

② 스크램블링은 시스템내의 임의의 위치에서 수행될 수 있으나, 스크램블링이 수행되는 계층은 MPEG2 트랜스포트 시스템 레벨 계층에서만 수행되어야 한다. 디스크램블링 역시 MPEG2 트랜스포트 시스템 레벨 계층에서 수행되어야 한다. 즉, MPEG2 트랜스포트 패킷을 이용한다. 스크램블링은 서비스 제공자와 STU 에서 협상에 의해 선택된 유용한 알고리즘을 이용하여 패킷의 페이로드부에만 적용되어야 한다. 그리고 패킷의 헤더 부는 평문 형태로 전달되어야 한다. 서비스는 동일한 MPEG2 데이타 다중 레벨과 독립적으로 제공되므로 스크램블링 서비스는 데이타 다중 내에서 독립적으로 스크램블링되어야 한다. STU 는 자신이 제공 가능한 스크램블링 알고리즘을 보안 장치에 STU 프로필로 전달할 수 있다.

③ 스크램블링의 제어는 서비스 제공자 또는 중간 서비스 제공자 영역에서 수행될 것이다. 정보의 스크램블링는 키 관리와 CW 을 전달하는 세션까지를 제어하는 능력을 갖는다. 스크램블링은 MPEG2 신호의 접근이 가능한 시스템내의 임의의 위치에서 적용될 수 있지만 핵심망(core network) 의 입력에 위치한 모듈에서 스크램블링을 제어한다.

④ 스크램블링과 보안 서비스는 최종 서비스 제공자와 중간 서비스 제공자에서 제공될 것이다. 중간 서비스 제공자에 의해 보안 서비스가 제공되는 경우, 중간 서비스 제공자는 신호를 디스크램블링하고 새로운 CW 로 재스크램블링하며, 동일한 CW 을 전달하기 위하여 별도의

ECM 과 EMM 을 사용자에 제공하는 과정들을 수행함으로서 스트림을 재구성한다.

⑤ 보안 서비스는 반드시 STU 까지 수행되어야 한다. 망종속 장치인 NIU 와 망 독립 가입자 장치인 STU 간의 인터페이스는 A0 인터페이스이다. A0 인터페이스를 갖는 STU 에서는 안전하고 갱신 가능한 디바이스를 이용하여 디스크램블링과 액세스 처리 기능을 수행한다. 이는 인터페이스 A0 상의 VASP (value added service provider) 내용 정보는 안전해야 하며, NIU 는 망종속 장치이고 STU 는 망에 무관하다. 한정 액세스는 망에 무관하므로 보안 장치는 STU 에 있어야 하고, STU 상에 한정 액세스 기능을 두는 것은 보안 장치와 STU 간에 안전한 신호 처리를 가능케 한다. 디스크램블링과 한정 액세스 기능이 다른 액세스 형태를 갖는 STU 내에서 실현되어야 하기 때문이고, 서비스 제공자는 NIU 을 제어하는 것이 아니라 STU 를 제어한다. 이는 VSAP 입장에서 STU 측에 CA 기능이 실현되는 것이 바람직함을 의미한다.

⑥ 하향 전달을 위하여 ECM에 포함 되는 실시간 보안 정보는 S1 스트림을 통해 전달된다.

3.6 방송형 서비스를 위한 보호 시스템 구성

방송 서비스는 CW 를 분배하기 위한 ECM 채널과 CW 을 암호화하는 AK(authorization key) 을 분배하기 위한 EMM 채널에 바탕을 두고 있으며, EMM 은 서비스 제공자와 각 사용자의 액세스 카드가 공유하고 있는 가입자의 분배키와 서명문을 위한 일차 검증키를 이용하여 생성된다.[11]

송신자는 임의로 CW 을 선택할 수 있다. ECM 및 EMM 으로 부터 유용한 정보의 추출은 가입자측 보안 장치에 의해 수행되며, 이는 이차 카드라 불린다.

CW 는 ECM 형태로 가입자에 전달된다. ECM 은 CW 를 AK 로 암호화한 암호문과 제어 파라메타에 대한 서명문을 쇄상하여 생성된다. 각 보안 장치는 ECM 으로 부터 CW 를 복구하고 제어 메세지의 정당성을 서명 알고리즘을 이용하여 검사한 후, 메세지가 정당하면 CW 을 디스크램블러로 전달한다. AK 의 분배는 EMM 을 이용한다. EMM 은 각 사용자의 분배키로 AK 를 암호화한 암호문과 사용자의 자격을 나타내는 자격 정보를 사용자의 일차 검증키로 서명한 이용하여 서명문을 쇄상하여 생성된다. 각 사용자의 액세스 카드에서는 분배키를 이용하여 AK 를 복구하고 자격 메세지를 검사하여, 자격이 있다면 AK 를 ECM 제어부로 전달한다. 이 방식은 서비스 제공자와 사용자가 비밀리에 분배키와 서명용 일차 검증키를 공유하고 있다는 사실에 바탕을 두고 구축된다. 서비스 제공자 측의 안전성을 향상하기 위하여 ECM 생성용 제어 카드와 EMM 생성용 관리 카드를 이용한다. 매 10 초마다 새로운 AK 가 자격 관리 메세지를 통해 각 사용자 또는 그룹에 전달된다. 서비스 제공자가 $E_{Di}(AK)$ 를 각 사용자에 전송하지 않으면 각 사용자는 절대로 AK 를 복구할 수 없다.

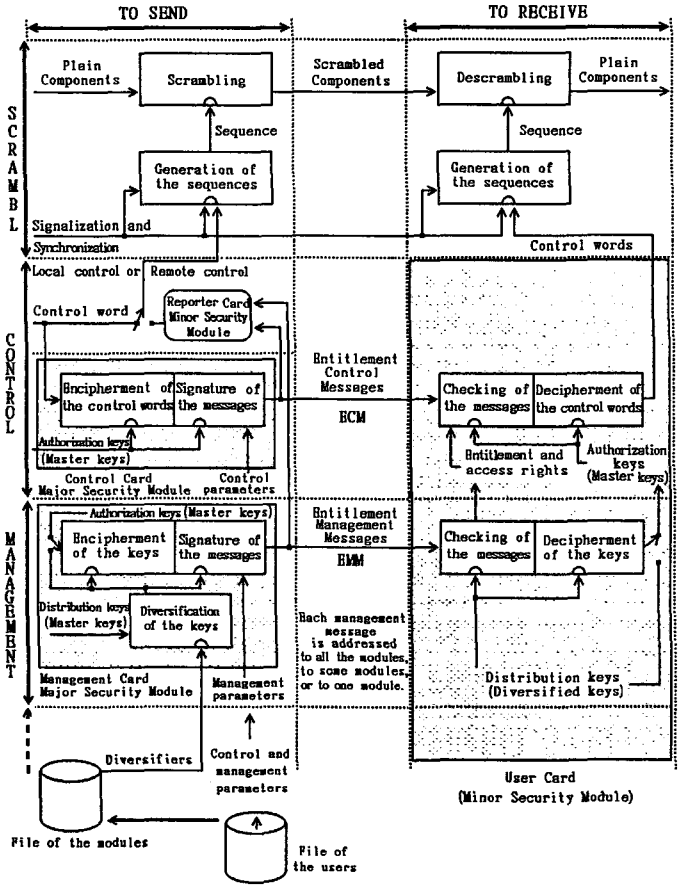

그림 3.3 인증 분배를 갖는 향상된 방식

서비스 제공자는 제어용 일차 카드을 이용하여 CW 의 암호문과 액세스 조건을 전달하기 위한 ECM 메세지를 생성하고, 자격과 인증키 전달을 위한 EMM 메세지를 관리용 일차 카드를 이용하여 생성하며, 사용자는 CW 와 AK 를 복구하기 위하여 이차 카드를 이용한다.

제어 및 관리 동작을 위하여 스마트 카드에 전송되어야 할 메세지는 연속적인 데이타 객체 들의 스트링으로 구성된다. 첫 번째 객체는 모든 카드, 그룹 카드, 또는 개별 카드 등을 나타내는 수신 개체를 의미한다. 그리고 CW 전달용 ECM, 자격 분배용 EMM, 또는 AK 분배용 EMM 등을 나타내는 특정 동작의 목적을 나타내는 객체도 포함된다. 두 번째 객체는 액세스 조건, 자격, 그리고 암호문 등의 객체이다. 세 번째 객체는 메세지 부에 대해 수행된 디지탈 서명문을 나타내는 객체이다. 이들 세 객체를 수신한 사용자 카드는 제일 먼저 디지탈 서명문을 검사한다. 서명문이 유효하면 요구된 동작을 수행하고, 유효하지 않으면 사용자 카드는 이 후의 일체의 요구된 동작

을 중단한다.

보안 장치는 ECM 용 키와 EMM 용 키를 별도로 사용한다. 하나의 스마트 카드는 다른 서비스 제공자가 전달한 여러 개의 비밀키를 저장하고 있을 수 있다. 스마트 카드의 구조는 모든 서비스에 공통적으로 적용되는 MF(master file) 부와 특정 서비스에만 적용되는 DF(dedicated file) 부로 구성된다. 카드는 DF 상호 간, 또는 MF와 DF 사이에 독립성이 보장되도록 설계되어야 한다.

3.7 대화형 서비스를 위한 인증 방식을 위한 공개키 증명서

공개키 증명서의 구성 정보는 사용자의 공개키와 사용자의 구별 가능한 이름, 공개키 증명서의 유효 기간 등이며, 공개키 증명서는 상기 구성 신호를 CA 의 비밀키로 서명한 $D_{CA_S}(ID_A, PK_A)$ 이다. 공개키 증명서의 검증은 CA 의 공개 정보를 이용하여 수행되며, CA 의 공개 정보는 각 사용자가 변경 불가능한 영역에 보관해야 한다. CA의 공개 정보의 누출은 CA 에 의해 검증된 사용자간의 정보의 무결성에 심각한 영향을 미치기 때문이다. 따라서 CA 의 공개 정보 저장 매체는 스마트 카드가 바람직한다. 공개키 증명서의 일반적 구조는 다음과 같다.[4]

```
공개키 증명서 :: =
    {
      일련번호(serial number);
       서명 알고리즘 확인자(signature algorithm identifier);
       발행자 이름(issuer name);
       유효 기간(validity period);
       사용자 이름(subject name);
       사용자 관련 정보 (subject information);
       상기 정보에 대한 해쉬 결과 값의 디지탈 서명문(digital signature)
    }

유효기간(validity period) :: =
   {
       개시일자(start date);
       종료일자(finish date)
   }

사용자 관련 정보(subject information) :: =
   {
       사용자 공개키(subject public key);
       공개키 알고리즘 확인자(public key algorithm identifier)
   }
```

공개키 증명서 경로는 DIT 에서의 노드들의 경로이며, 서로 다른 CA 들의 관할 하에 있는 사용자간의 통신시 이용된다. 개체 A 의 공개키 증명서 Cert(A) 는 믿을 수 있는 제삼자인 인증 센타 (CA : certification authority) 가 발행하며, CA 는 모든 개체가 신뢰할 수 있는 개체이다. 각 개체는 CA 의 공개키 CAP 를 스마트 카드에 비밀스럽게 저장해야 한다.

개체 A 가 믿는 CA 를 CA_A 라 하고, 개체 B 가 믿는 CA 를 CA_B 라 하면, 두 개체에 대한 인증 센타들이 서로 다를 경우, 각 CA 가 공통적으로 믿을 수 있는 상위의 CA 를 구한 후, 각 개체는 공통의 CA 을 통해 상대방의 공개키 증명서를 얻는다. 공개키 증명서는 위조가 불가능하게 하기 위해 인증 센타 CA 의 비밀 서명키로 서명한 개체의 ID 와 공개키를 의미하며 식 (3.1)과 같다.

Cert(A) = {SN,AL,CA,A,PKA,TA, CAS[h(SN,AL,CA,A, PKA,TA)]} (3.1)

여기서, SN 은 공개키 증명서의 일련 번호, AL 은 CA가 공개키 증명서의 서명을 생성하는데 이용한 서명 알고리즘의 종류와 일방향 해쉬함수 알고리즘의 종류를, CA 는 CA 의 이름 (distinguished name), A 는 개체 A 의 이름 (distinguished name), PKA 는 개체 A 의 공개키, TA 는 공개키 증명서의 유효한 개시일과 마지막 날로 구성된 유효 기간, CAS[h] 는 데이타 블럭 h 와 CA 의 비밀키에 의해 암호화된 내용, 즉, CA 의 h 에 대한 디지탈 서명, h(I) 는 데이타 블럭 I 를 단방향 해쉬 함수에 대입하여 얻은 결과이다. X.509 공개키 증명서는 공개키 증명서의 유효성을 확인하기 위해 식 (3.2) 의 만족 여부를 확인하고 TA 가 최종 시간 내에 있는가를 확인한 후 검증된다.

h(SN,AL,CA,A,PKA,TA) =? CAP{CAS[h(SN,AL,CA,A,PKA,TA)]} (3.2)

식 (3.2) 의 좌측은 CA(A) 의 좌측에 있는 SN, AL, CA, A, PKA, TA 를 단방향 해쉬함수 h 에 직접 대입하여 얻은 결과이고, 식 (3.2)의 우측은 CA(A) 의 우측에 있는 CAS[h(SN, AL, CA, A, PKA, TA)] 를 CA 의 공개키로 복호한 결과이다.

3.8 국내 VOD 의 액세스 제어 시스템에 적용 가능한 정보보호 메카니즘

VOD 에서의 서비스는 크게 대화형 서비스와 방송형 서비스로 구분된다.

방송형 서비스에서 요구되는 서비스는 MPEG2 트랜스포트 레벨 패킷에서의 페이로드에 대한 스크램블링 서비스, 스크램블링 서비스를 가능케 하는 CW 을 전달하는 기능 등을 수행하는 ECM 채널 서비스, 그리고 EMM 채널 서비스로 구분될 수 있다. 방송형 서비스를 위한 키 계층은 2 단 이상으로 한다. 스크램블링을 위한 스크램블링 기법은 DES 를 이용하는 방법, FEAL 을 이용하는 방법, IDEA 를 이용하는 방법, 그리고 독립적인 스트림 암호 방식을 채용하는 방법 등이 고려될 수 있다. ECM 채널을 위한 정보보호 메카니즘은 CW 을 분배하기 위한 DES 암호 알고리즘과, 액세스 조건 등을 서명하기 위한 해쉬 함수와 서명 알고리즘이 요구된다. 해쉬 함수는 MD5 해쉬 함수를 이용하며, 서명 알고리즘은 RSA 또는 미국의 표준 서명 알고리즘인 DSS 알고리즘을 이용한다. EMM 채널을 위한 정보보호 메카니즘은 CW 를 암호화하는 AK 을 전달하기 위한 비대칭형 암호 알고리즘인 RSA 알고리즘과 액세스 조건 전달을 위한 조건 정보를 서명하기 위한 해쉬 함수와 서명 알고리즘이 요구된다. 해쉬 함수는 MD5 해쉬 함수를 이용하며, 서명 알고

리즘은 RSA 또는 미국의 표준 서명 알고리즘인 DSS 알고리즘을 이용한다.

대화형 서비스를 위한 정보보호 서비스는 세션 개시시에 통신 상대의 정체를 확인하기 위한 등위 개체 인증 서비스, 스마트 카드가 사용자를 인증하기 위한 사용자 인증 서비스, 개체 인증 중에 수행되는 세션 키 분배 서비스, 공유된 세션키를 이용하여 CW 을 전달하기 위한 ECM 채널 서비스, 그리고 ECM 채널용 암호키를 분배하기 위한 EMM 채널 서비스로 구분될 수 있다. 스크램블링을 위한 스크램블링 기법은 DES 를 이용하는 방법, FEAL 을 이용하는 방법, IDEA 를 이용하는 방법, 그리고 별도의 스트림 암호 방법을 채용하는 방법이 있다.

등위 개체 인증 서비스는 ITU X.509 의 인증 기법을 이용한다. 인증에 이용되는 암호 알고리즘은 RSA 암호 알고리즘을 이용한다. 세션 키 분배는 Diffie-Hellman 의 키 분배 방식 또는 ISO 에서 권고 중인 세션 키 분배 방식을 이용한다. 사용자 인증은 패스워드를 이용한 인증 기법을 사용한다. 이를 이용함으로서 스마트 카드의 분실시에 불법 사용을 방지할 수 있다. ECM 채널을 위한 정보보호 메카니즘은 CW 을 분배하기 위한 DES 암호 알고리즘과, 액세스 조건 등을 서명하기 위한 해쉬 함수와 서명 알고리즘이 요구된다. 해쉬 함수는 MD5 해쉬 함수를 이용하며, 서명 알고리즘은 RSA 또는 미국의 표준 서명 알고리즘인 DSS 알고리즘을 이용한다. CW 를 암호화하는 AK 는 등위 개체 인증 과정과 함께 수행되는 세션키 분배 과정에서 얻어지는 인증키를 이용한다. 이 AK 는 해당 세션에 대해서만 유효하다.

스마트 카드가 저장해야 할 비밀 정보는 방송형 서비스의 EMM 채널을 전달하기 위한 각 보안 장치마다 고유하게 할당된 512 비트의 RSA 비밀키 및 합성수, 서비스 제공자의 서명용 512 비트 서명 검증용 공개키 및 합성수이다. 그리고 대화형 서비스를 위한 저장해야 할 비밀 정보는 ECM 채널을 위한 64 비트 DES 비밀키와 서명 검증용 512 비트 RSA 공개키와 합성수이다.

3.9 ECM 채널 시뮬레이션

ECM 채널은 CW 와 자격 정보를 암호화하여 전송하는 채널이다. 실현된 기능은 DES, RSA, 그리고 MD5 해쉬 함수이다. 시뮬레이션을 위한 언어는 C 언어이다. CW 을 암호화하기 위한 알고리즘은 DES 을 이용했으며, 동작 모드는 CBC 모드이다. 디지탈 서명 방식은 RSA 을 이용했으며, 해쉬 함수는 MD5 해쉬 함수를 사용하였다. RSA 의 공개키중 합성수 n, 서명용 비밀키 d, 그리고 서명 검증용 공개키 e 은 식 (3.3) 과 같다.

```
d = 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00e9
e = 0000 3ce1 5403 f820 8c69 1d99 177e 8b34 11e9 6149 bbb2 8bee affe 681e c144 d4cd
    0c09 0b9d baee 460f a166 b987 9acb 275d ace4 317b 220b aa30 8dec 4721 0404 11e5
n = 0000 c250 f39c 7325 41e9 ceb0 869a e9e5 51b7 cd51 09f0 3ce1 4a48 10b6 53d4 ae3a
    5104 ca26 97b0 dc90 b1b9 e728 697a c7c2 0817 f1be ab0c 028c ea56 eba4 5739 7a75
                                                                          (3.3)
```

CW = "0123456789ABCDEF" 로, 자격 변수 (EI:entitlement information) 는 "FEDCBA987654

3210" 로 가정한다. 해쉬 함수의 입력 데이타와 자격 변수를 MD5 해쉬 함수에 대입하여 구한 해쉬 값은 식 (3.4) 와 같다.

해쉬함수의 입력 메시지 :
[fedcba98] [76543210] [80000000] [00000000] [00000000] [00000000] [00000000] [00000000]
[00000000] [00000000] [00000000] [00000000] [00000000] [00000000] [00000000] [00000040]
해쉬 결과 값 :
[cb1e10ee] [42d9fda5] [a625e889] [53f6e097] (3.4)

EMM 채널을 통해 전달된 CW 를 암호화하기 위한 암호키 DK 는 "3456789ABCDEF012" 로, 초기키는 "123456789ABCDEF0" 으로 전달받은 것으로 가정하였다. 식 (3.4) 와 같은 해쉬 결과 값을 식 (3.3) 과 같은 RSA 서명용 비밀키로 서명한 결과와 CW 와 자격 정보를 쇄상하여 DK 로 암호화한 결과는 그림 3.4와 같다. 시뮬레이션 결과 ECM 채널의 구조 및 정상 동작을 확인하였다.

E_{DK}[CW || EI]		D_S(H(EI))
9e93cc00 095e9ff8	227b4047 b1eb7f4b	0000 1908 209d 0081 72dd cbd3 61dd f084 5bb9 d23f daf2 e3a2 d391 2c06 0f0a f707 dc9f 36ad 9861 5654 a15f 18aa 0e30 8844 3f36 3067 d819 2689 62de 0096 5af5 f598
← 64 비트 →	← 64 비트 →	← 512 비트 →

그림 3.4 시뮬레이션 결과 값

제4장 결론

VOD 에서의 서비스의 종류는 크게 방송형과 대화형 서비스로 구분된다. 본 고에서는 국내 VOD 시스템의 액세스 제어 기능을 실현하기 위하여 DAVIC VOD 시스템의 한정 액세스 기법을 분석했고, 스크램블링이 적용되는 MPEG 트랜스포트 패킷 및 관련 테이블 패킷의 구조를 분석했으며, 또한 자격 관리 및 검사 채널의 구조를 분석하고 기능을 정의하였다. 그리고 이를 바탕으로 국내 VOD 에 적용 가능한 액세스 제어 방안 및 정보보호 기법을 제시하였다. 제시된 액세스 제어 기법은 국내 VOD 의 액세스 제어 시스템 설계시 적극적으로 활용될 수 있을 것이다. 그리고 방송용 서비스에 적용 가능한 ECM 채널을 DES, MD5, 그리고 RSA 알고리즘을 이용하여 C 언어로 구현하였고 관련 동작을 시뮬레이션하였다. 시뮬레이션 결과 관련 동작이 정상적으로 수행될 수 있음을 확인하였다.

- 참 고 문 헌 -

(1) DAVIC, DAVIC 1.0 Specifications Revision 3.0, 1995. 9., Hollywood
(2) ISO/IEC 13818-2, Information Technology - General Coding of Moving Pictures and

Association Audio, Committee Draft, ISO/IEC JTC1/SC29, 1993., Seoul

(3) ISO/IEC IS 9798-3, Entity Authentication Mechanisms - part 3 : Entity Authentication Using a Public-key Algorithm, ISO, Geneva, Switzerland, 1993.

(4) ITU Rec. X.509, The Directory - Authentication Framework, ITU, Geneva, Switzerland, 1993.

(5) G.J. Simmon, Contemporary Cryptology, IEEE press, 1992.

(6) Man Young Rhee, Cryptography and Secure Communications, Mcgraw-Hill, 1992.

(7) R.A. Rueppel and P.C.V. Oorschot, "Modern Key Agreement Techniques," Computer Communications, Vol.17, No.7, pp.458-465, 1994.

(8) A. Fiat and 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.

(9) T.Beth, "Efficient Zero Knowledge Identification Scheme for Smart Cards," Proc. Eurocrypt'88, pp.77-84, 1988.

(10) W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. on Info. Theory, Vol. IT-22, No.6, pp.644-654, 1976.

(11) L.C. Guillou and J.L. Giachetti, "Encipherment and Conditional Access," SMPTE Journal, pp.398-406, June, 1994.,

(12) HeungYoul Youm and ManYoung Rhee, "Correlation-immune Random Sequence Generator Using GMW Sequences," Proceeding of Joint Workshop on Information Security and Cryptography'95, Japan, 1995.

(13) 염 흥열, "컴퓨터 통신망에서의 암호키 생성, 분배, 그리고 관리 방식," 한국통신정보보호학회 학회지, Vol.1, N0.1, pp.83-93, 1991.

(14) 염 흥열, "스마트 카드에서의 인증 방식," 데이타보호 기반 기술 워크샵 논문집, 한국통신정보보호학회, pp.239-258, 1992.