通信情報保護學會誌
第8卷 第3號, 1998. 9

공개키 기반 구조 응용 분석 및 디지털 방송 한정 수신 시스템

PKI Applications and CAS for Digital Broadcasting

이 강 석*, 염 흥 열*, 윤 이 중**

요 약

인터넷의 급속한 확산과 전세계 통신서비스의 확장으로 인해 세계는 정보의 공유와 다양한 삶의 변화를 가져오고 있다. 교통수단의 발달로 전세계가 일일생활권에 접어들었다면 인터넷과 통신수단의 발전으로 인해 세계는 동일문화권을 형성하고 있다. 주체할 수 없이 수많은 정보와 서비스 속에서 살고 있지만, 아직도 좀더 편리하고 안전한 정보의 공유와 윤택한 삶을 영유하기 위한 많은 문제점이 있으며, 이러한 발전 속에서 더 많은 문제점들이 나타나고 있는 것이 현실이다. 또한 이러한 문제점들을 해결하기 위한 다양한 해결책들이 쏟아져 나오고 있다.

본 고에서 다루게 될 내용은 전체적인 공개키 기반구조를 살펴보고 이를 디지털 위성방송 한정수신 시스템에 적용한다. 공개키 기반구조에 대해서는 인터넷에서 사용자를 인증하기 위한 X.509 인증서에 대해 살펴보고, 인증서를 이용한 서비스들에 대해 살펴본다. 또한 최근 각 나라별 공개키 기반구조 표준안의 진행 상황을 알아보고 IETF의 PKIX 표준안으로서 공개키 관리 프로토콜, CRL, CRL 확장, 인증서, 그리고 인증서 확장에 대해 살펴본다. 곧 실현될 디지털 위성방송의 유료화 서비스는 가입자 인증과 서비스에 대한 접근 통제가 가능해야 한다. 따라서, 가입자에 대한 관리부분에 공개키 기반구조를 적용함으로서 가입자에 대한 인증과 서비스 및 접근 통제를 가능하게 한다.

1. 공개키 기반구조

많은 인터넷 프로토콜들과 응용 서비스는 보안을 유지하기 위해 공개키 기술을 도입하고 있으며, 이에 따라 폭넓게 산재하고 있는 사용자나 시스템들을 위하여 자신의 공개키를 안전하게 관리하고 전달하기 위한 공개키 기반 구조에 바탕을 둔 키관리 체계가 요구되고 있다. 인증서는 사용자의 공개키와 사용자의 ID를 인증기관의 서명용 비밀키로 서명한 서명문이다. X.509는 ITU에 의해 제안된 인증서에 대한 기본 구조를 정의한 규격이다. 이 구조에서는 인증서의 데이터 형식들과 인증기관에 의해 인증서를 통한 공개키의 효율적인 분배를 정의하고 있다. 초기 X.509 버전에 이어 X.509 버전 2에서는 인증서 폐지 목록(CRL:

* 순천향대학교 공과 대학 전자 공학과
** 한국전자통신연구원

Certificate revocation list)을 포함시켰고, 버전 3에서 인증서를 정의하는 다양한 환경에 맞는 조건과 서명 알고리듬들이 선택이 가능하도록 확장영역을 추가하였다. 공개키 기반 구조를 이용하는 서비스들은 PEM(Privacy Enhanced Mail), PGP(Pretty Good Privacy), S/MIME (Security Multipurpose Internet Mail Extensions), MOSS(MIME Object Security Service), GSS-API(Generic Security Service - Application Protocol Interface), IPSEC(IP security protocol) 프로토콜, 전자 지불 프로토콜, 그리고 WWW(World Wide Web) 프로토콜들이 있다. 이들 서비스의 인증서에 사용되는 기본 핵심 보안 메커니듬은 공개키 암호 방식에 기초한 디지털 서명 메카니듬과 MAC를 위한 해쉬 알고리듬이다.

디지털 서명은 메시지의 소유자가 누구인지를 증명할 수 있는 메시지에 대한 전자 서명문이며 메시지 인증을 위해 이용된다. 서명 과정은 일반적으로 메시지를 해쉬 함수에 적용하여 구한 결과인 메시지 지문을 생성한 후, 이 값을 서명용 비밀키로 암호하여 원래의 메시지와 함께 수신자에 전달한다.

이 코드가 디지털 서명문이다. 수신자는 서명문을 송신자의 서명용 공개키로 복호하여 해쉬 함수 결과 값을 얻고, 수신된 메시지에 송신단과 동일한 해쉬 함수를 적용하여 다른 해쉬 함수 결과를 생성한다. 두 해쉬 함수 결과 값이 일치하면 수신자는 메시지가 중간에 변경되지 않았음을 확신한다. 이 서비스를 부인 방지 서비스와 무결성 서비스라 한다.

공개키 기반 구조(PKI: Public Key Infrastructure)는 인터넷상에서 서로 초면인 사용자간에 민감한 데이터를 안전하게 교환함으로서, 금융 거래를 전자적으로 가능케 하기 위하여 인증서를 분배하고 전달하는 시스템이라고 정의할 수 있다. PKI를 이용하면 기밀성(Privacy), 접근제어(Access Control), 무결성(Integrity), 인증(Authentication), 그리고 부인봉쇄(Non-repudiation) 서비스를 제공받을 수 있다. 이들 서비스는 전자 상거래 응용들과 결합하여 전자 상거래의 재정적 거래를 지원한다. 또한 PKI는 공개키와 비밀키 쌍들을 생성하고, 분배하며, 그리고 이를 관리한다. 또한 공개키에 대한 인증서를 이용하여 사용자의 공개키를 게시판(Open Bulletin Board)에 공개한다. PKI는 공개키에 대응되는 비밀키(Private Key)를 안전하게 저장하고 특정 공개키와 특정 비밀키가 정확히 연결되도록 한다. PKI 인증기관(CA: Certificate Authority)은 계층 구조로 구성된다. 각 사용자에 대한 공개키와 사용자의 ID는 인증서에 포함된다. CA는 사용자의 ID와 공개키를 CA의 비밀키로 서명하여 인증서를 생성하고, 다른 사용자들은 공개적으로 엑세스가 가능한 게시판(X.500 디렉토리)을 통해 다른 사용자의 인증서를 구하여 통신하고자 하는 다른 사용자의 공개키를 확신한다. 그러므로 어떤 사용자도 다른 사용자들의 공개키를 공개 게시판(Public Directory)으로부터 가져올 수 있고, CA의 서명용 공개키를 이용해 인증서에 있는 CA 서명문을 확인함으로서 사용자의 공개키에 대한 정당성을 검증할 수 있다. 계층에서 제일 위층에 위치한 CA는 하위 CA 디렉토리의 공개키를 포함하는 인증서들을 서명하고 서명을 받은 인증기관들은 다시 아래의 인증서들을 서명한다. 이 과정은 공개키들이 검증된 CA들의 하부구조에서 다른 CA들을 서명하도록 한다. 이를 통해 하부구조에 있는 CA들간에 신뢰구조가 형성된다.

2. 공개키 인증서의 응용 분야

PKI 의 바탕이 되는 공개키 인증서의 응용예는 다음과 같다.

2.1 PGP(Pretty Good Privacy)[1]

PGP는 필립 짐머만(Philip Zimmermann)에 의해 1991년에 제안된 전자 우편용 보안 프로토콜이다. 이것은 메시지를 속도가 빠른 대칭 알고리듬을 사용해 암호하며, 대칭 알고리듬에 사용된 비밀키를 공개키 암호방식을 이용해 암호화하여 전달하는 키 분배 방식을 사용하고 있다. 대칭 알고리듬은 IDEA를 사용하며, 공개키 암호 방식은 RSA를 이용한다.

사용자는 PGP를 이용하여 통신할 상대인 다른 사용자의 공개키들을 관리하는 공개키 링을 관리해야 한다. PGP는 인증기관을 활용하지 않기 때문에 상대의 공개키와 신뢰 정도를 나타내는 신뢰 정보를 이용하여 통신할 상대의 공개키를 확신한다. 각 사용자는 상대에 대한 공개키 링과 자신에 대한 비밀키 링을 유지한다. 비밀키 링에는 타임 스탬프, 키 ID, 서명용 공개키, 자신의 패스 프레이즈(Pass-phase) 로 암호화된 비밀키, 그리고 사용자의 ID 항목으로 구성되어 있다. 각 사용자의 공개키 링에는 타임 스탬프, 상대에 대한 공개키 ID, 상대의 공개키, 공개키 사용자에 대한 신뢰 정도를 나타내는 사용자 신뢰 필드(Owner Trust), 상대방 사용자의 ID, 상대의 공개키와 사용자의 ID에 대한 바인딩(Binding)에 대한 신뢰 정도를 나타내는 PGP에 의해 계산되는 키 적법성(Key Legitimacy) 필드, 그리고 다른 사람의 공개키를 서명한 상대의 신뢰 정도를 나타내는 서명문 신뢰(Signature Trust) 필드로 구성된다. 즉, 키 적법성 필드는 PGP가 서명문 신뢰 정도 필드를 조사하여 계산하며, 이는 통신할 사용자의 공개키에 대한 신뢰 정도를 나타낸 값이다. 적법성 신뢰의 수준이 높을수록 공개키 링에 있는 사용자 ID와 공개키가 강하게 결합되어 있음을 의미한다. 또한 공개키 링에는 공개키를 다른 사용자의 서명키로 서명한 공개키에 대한 인증서 역할을 하는 공개키에 대한 서명문들이 존재한다. 각 서명은 서명 신뢰 필드와 연관되며, 이것은 PGP 사용자가 상대의 공개키의 믿음의 정도인 키 적법성 필드를 계산할 때 사용된다. 즉, 키 적법성 필드는 실제적으로 공개키 링에서 서명문 신뢰 필드들을 조사하여 PGP가 계산함을 의미한다. 이외에도 공개키 링에는 특정 사용자의 공개키를 저장하는 공개키 필드와 특정 사용자에 대한 믿음의 정도를 나타내는 공개키 사용자 신뢰 필드를 가지고 있다. 특정 사용자의 신뢰 정도는 해당 사용자에 의해 할당된다.

PGP는 공개키 링을 주기적으로 관리한다. 본질적으로 이것은 탑-다운 절차로 진행된다. PGP는 각 소유자의 신뢰 필드마다 해당 소유자에 의해 작성된 모든 서명문에 대한 서명 신뢰 필드를 소유자 신뢰 필드로 갱신한다. 그 다음 키 적법성 필드를 서명문 신뢰 필드 값을 이용하여 계산한다. 그림 1은 PGP에서 사용하고 있는 서명문 신뢰 필드와 키 적법성 필드와의 관계를 나타내고 있다.

각 PGP 사용자는 상대방의 공개키를 소유자로부터 직접 얻거나 키 서버 같은 제삼자로부터 얻을 수 있다. 그림 1에서 "You" 라고 레이블된 노드는 사용자에 대응되는 공개키 링에서의 사용자 ID등의 구성 요소에 대응된다. 이 레벨에서의 공개키는 적법하고 소유자 신뢰는 최고 값이다. 키 링에서 다른 노드들의 소유자 신뢰 값은 사용자가 어떤 값을 부여하지 않았다면 정의되지 않은 상태 값을 갖는다. 이 그림은 사용자 "You"는 사용자 d, e, f, l에 의해 서명되어 있는 공개키를 완전히 신뢰함을 의미한다. 사용자 "You"는 사용자 a, b에 의해 서명되어 있는 공개키를 부분적으로 신뢰함을 의미한다. 트리구조는 어느 키가 어느 사용자에 의해 서명되었는지를 나타낸다. 사용자는 자신의 비밀키에 대한 크래킹이 의심되거나 오래 동안 동일한 암호키를 사용하는 것을 방지하기 위해서 현재의 공개키를 폐

지할 수 있다. 사용자는 현재의 공개키를 폐지하기 위하여 자신의 서명키로 서명한 폐지 인증서를 발행하여 배포한다. 폐지 인증서는 보통의 서명 인증서와 동일한 형태이지만 이 인증서의 목적이 현재의 공개키의 사용을 폐지하는 것이라는 옵션 표시가 들어 있다.

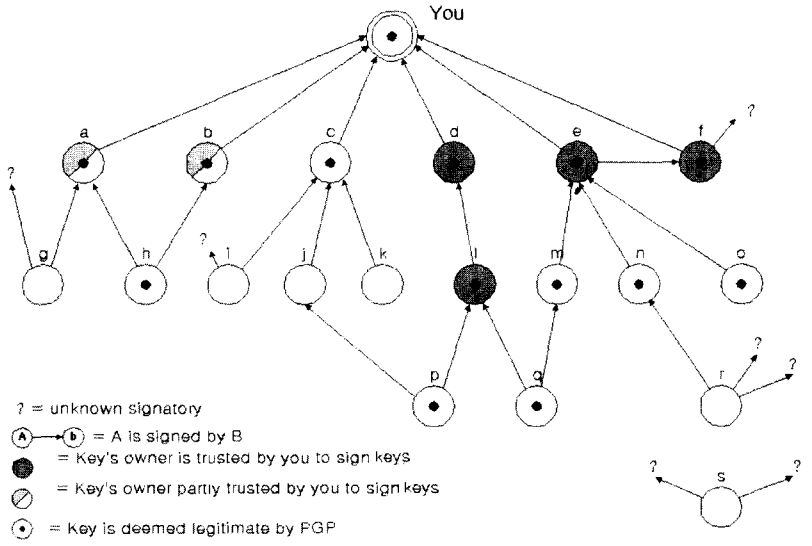


그림1 PGP 사용자 공개키 신뢰 모델

2.2 PEM(Privacy Enhanced Mail) [1][2]

PEM은 IETF에 의해 고안된 인터넷 보안 전자 우편 프로토콜이다. PEM도 PGP와 비슷한 방식으로 메시지를 암호하고 서명한다. 이용되는 보안 알고리듬은 대칭 암호 알고리듬으로 DES를 사용하며, 공개키 암호 알고리듬으로 RSA를 사용한다. PEM은 인증기관을 갖고 인증기관에서 인증서를 발행한다. PEM은 인터넷 표준으로 완벽한 보안 시스템인 반면 사용이 어렵다는 점 때문에 상대적으로 보안성이 떨어지는 PGP가 널리 사용되고 있다. PEM은 X.509 인증서 형식을 사용한다. 인증기관은 계층적으로 구성되어 있으며, 그림 2와 같이 PRA, PCA, CA의 세 레벨로 계층화된다.

인증기관의 계층 구조에서의 루트는 IPRA이다. IPRA는 PEM 환경에서의 인증을 위한 총괄 정책을 설정한다. IPRA의 기능은 다음과 같다.

- **PCA 등록** : 각 PCA는 IPRA에 등록되어야 하며, 보안 정책은 파일의 문서로 기술된다. IPRA는 자신이 서명한 문서의 사본을 PEM MIC-ONLY(메시지 검사 부호만 포함된 PEM 메시지) 메시지 형태로 발행한다. 이것은 PEM 사용자가 PCA 정책에 대한 인증된 메시지로 액세스할 수 있게 하기 위함이다.
- **PCA 이름의 고유성과 정확성에 대한 검증** : IPRA는 모든 PCA와 CA 이름이 고유하고 정확하다는 것을 보장해야 한다.
- **CRL 관리** : IPRA는 모든 인증서 철회 목록에 대한 관리 책임을 진다. IPRA는 자신이 인증하고 보장하는 모든 PCA들에 대한 CRL을 관리하고, 각 PCA는 자신이 인증하는 모든 PCA들에 대한 CRL을 관리한다.

각 PCA는 사용자에 대한 등록 규정을 구축

하고 발표한다. CA는 사용자와 다른 계층의 CA들에 대한 인증서를 관리한다. PEM은 세 가지 유형의 CA를 갖는다.

- **기관형(Organizational)** : 초기 대부분의 사용자는 기관형 CA에 등록된다. 기관형 CA에는 상업, 정부, 교육계, 비영리, 그리고 전문가 협회를 포함한다.
- **거주형(Residential)** : 어떤 조직적인 기관과는 독립적으로 가입하고자 하는 사용자는 거주형 CA를 이용할 수 있다. 이 CA들은 특정한 지역의 사용자를 인증하는 지방 정부 기관과 연관될 수 있다.
- **PERSONA** : PERSONA CA는 사용자가 익명으로 인증서를 발급 받을 수 있게 한다. 익명으로 등록된 사용자는 자신의 신분을 숨기고 PEM 보안 서비스를 사용할 수 있다. 이 경우, CA는 개인 신분 확인을 보장하지 않을 것이다.

그림 2는 PEM 인증서의 계층적 구조를 나타낸다. 최상위 CA는 많은 PCA들을 인증하는 IPRA 이다. 각 PCA는 하부의 여러 CA들을 인증하며 각 CA는 사용자와 다른 CA를 인증한다. 다음의 경우, 사용자는 만료일이 지나지 않은 인증서를 폐기할 수 있다.

- 사용자의 비밀키가 손상되었다고 추정되는 경우
- 사용자는 더 이상 CA에 의해 인증되지 않는 경우
- CA의 인증서가 손상되었다고 추정되는 경우

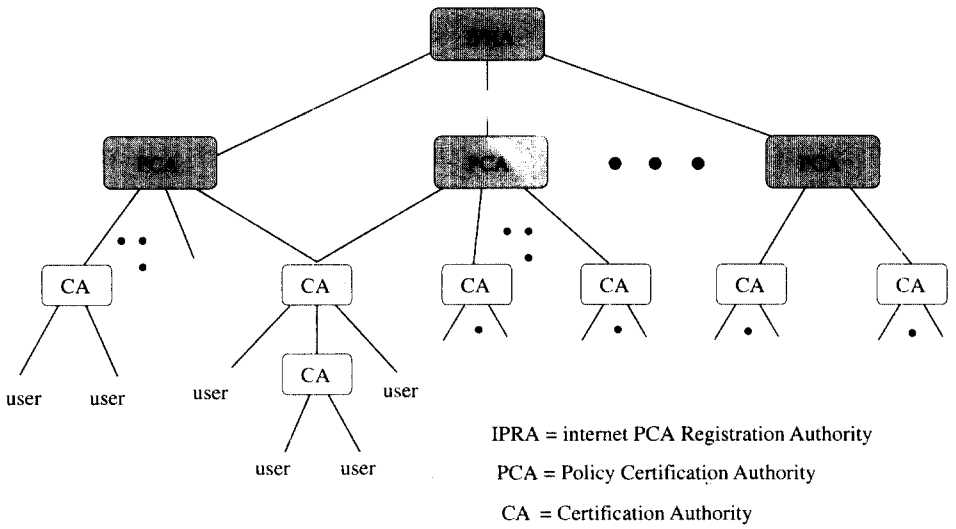


그림2 PEM의 CA 신뢰모델

CA는 다른 CA들의 폐지된 인증서와 자신의 인증서 폐지 목록을 관리해야만 한다. 이러한 CRL은 CA의 서명용 비밀키로 서명된다. PEM은 X.509와 동일한 방법으로 CRL을 관리한다.

2.3 PKCS(Public Key Encryption Standards)[3]

PKCS는 공개키 암호화를 위해 RSA에서 제안한 표준 프로토콜이다. APPLE,

MicroSoft, DEC, Lotus, Sun, MIT 등이 PKCS를 채택하여, 콘소시엄을 구성하고 있다. 현재(1998년 10월) 전체 사양은 PKCS#1에서 PKCS#15로 구성되어 있다. PKCS#2와 PKCS#4는 PKCS#1에 통합되었고, PKCS#1은 "RSA 암호화 표준", PKCS#3은" Diffie-Hellman 키동의 표준", PKCS#5는 "패스워드 기반 암호 표준", PKCS#6는 "확장된 인증서 구문 표준", PKCS#7은 "암호화 메시지 구문 표준", PKCS#8은 "개인키 정보 구문 표준", PKCS#9는 "선택된 속성 타입", PKCS#10은 "인증서 요구 구문 표준", PKCS#11은 "암호 토큰 인터페이스 표준", PKCS#12는 "개인정보 교환 구문 표준", PKCS#13은 "Elliptic Curve Cryptography 표준", 그리고 드래프트로 발표된 PKCS#15는 "스마트 카드 파일 형식"을 정의하고 있다. PKCS는 공개키 암호화 알고리듬, 비밀키 암호화 알고리듬, 그리고 메시지 다이제스트 알고리듬에 바탕을 두고 구축되고 있다.

2.4 S/MIME(Security Multipurpose Internet Mail Extensions)와 MOSS[4][5]

MIME(Multipurpose Internet Mail Extensions)는 다양한 형태의 데이터도 처리할 수 있도록 SMTP(Simple Mail Transfer Protocol)를 확장한 메일 프로토콜이다. MOSS는 MIME에 PEM에서 이용된 보안 기능을 부가한 것으로, PEM-MIME이라고 불리어 진다. S/MIME은 RSA사에 의해 발표된 PKCS에 기반을 둔 강력한 암호 기능과 유연성 있는 확장 능력을 갖고 있는 대표적인 MIME 프로토콜이다.

2.5 GSS-API(Generic Security Service - Application Protocol Interface)[6][7][8][9]

GSS-API는 IETF에 의해 제안된 보안 인터페이스로서, Kerberos에 기반을 둔 방식과 X.509 방식의 공개 키 방법에 기반을 둔 방식이 혼용되어 업계 표준으로 제정되었다. GSS-API에서는 암호에 대한 사전 지식이 없는 사용자에게 편리한 보안 서비스를 제공하기 위하여 규격화된 보안 인터페이스 규격을 정의하고 있다. GSS-API는 하부 메커니듬이나 하부 통신 프로토콜에 독립적으로 동작한다. 전형적인 GSS-API를 호출하는 개체는 통신 프로토콜이며, 이는 GSS-API와 거래를 통해 상호 인증, 무결성, 그리고 선택적인 기밀성 보안 서비스들을 제공받아 클라이언트와 서버간의 메시지를 안전하게 교환한다. GSS-API는 호출자, 응답자, 그리고 자국 및 원격국 GSS-API 실현들로 구성되어 있다. GSS-API 호출자는 자국 GSS-API 와 거래를 통해 제공되는 토큰을 원격 시스템의 등위(Peer)에게 전달하고, 상대 등위는 수신된 토큰을 자신의 자국 GSS-API 로 전달하여 자국 GSS-API에서 수신 메시지를 처리한 후, 처리된 결과를 수신하도록 구성되어 있다. GSS-API는 신임장(Credential)을 설정하는 단계, 등위들 간에 보안 컨텍스트를 설정하는 단계, 데이터 발신처 인증 및 데이터 무결성 서비스를 제공하는 단계, 그리고 메시지를 암호 및 복호하는 단계들로 구성된다. 이와 유사한 것으로는 Crypto-API, GCS-API 등이 있다. 여기서도 공개키 인증서를 사용하고 있다.

2.6 IPSEC 프로토콜(IP Security Protocol)[10]

IPSEC는 인터넷의 IP 계층을 보호하기 위한 보안 프로토콜이다. IPSEC는 인증, 무결성, 접근제어, 그리고 부인 봉쇄 서비스들을 지원

한다. IP 계층 보안 메커니듬은 캡슐화 메커니듬과 키관리 메커니듬으로 조합하여 실현된다. IPSEC에서의 키관리는 공개키 암호 기술을 사용하고 공개키 기반 메커니듬을 지원하고 있다.

2.7 전자 지불 프로토콜[11]

SET(Secure Electronic Transaction)은 1996년 2월 비자와 마스터 카드사가 연합하여 인터넷과 같은 공개된 통신망에서 안전하게 상거래를 할 수 있도록 하기 위해 개발한 보안 프로토콜로서, 일상 생활에서 이용되고 있는 신용 카드에 기반을 두고 있다. SET은 이용자(Card Holder)와 상인(Merchant) 사이의 인증, 정보의 기밀성, 데이터의 기밀성, 서비스의 상호 유용성을 구현할 목적으로 개발되었다. SET의 가장 큰 장점은 암호화 기술을 이용하고 있다는 점이다. SET가 사용하고 있는 암호화 방법은 지불 정보를 64-비트 대칭형 암호화 알고리듬을 이용해 암호화하고, 대칭형 알고리듬에 이용되는 세션키를 다시 1024-비트의 RSA 공개키 알고리듬으로 암호화하여, 암호문과 세션키를 암호한 암호문을 동시에 전송하도록 구성되어 있다. 매 트랜잭션마다 일회용 암호키를 사용한다.

SET 프로토콜은 지불 메시지에 대한 암호화를 하거나 카드 소지자를 인증할 수 있는 인증서를 채용함으로서, 인터넷에서 안전한 전자 상거래가 이루어질 수 있도록 하고 있다. 또한 SET 규격은 관련 업계에 공개 사양으로 배포되었으며, 어떠한 지불 서비스에도 적용이 가능하고, 어느 소프트웨어 업체도 응용 프로그램을 개발할 수 있다. SET에 참여하는 참여자들은 카드 소지자, 발행사, 가맹점, 매입사, 그리고 인증기관으로 구성되어 있다.

- 카드 소지자: 카드 회사(발행사) 에서 발행한 카드를 갖고 있는 카드 소지자
- 발행사, 또는 발행 은행: 카드를 발행하는 금융 기관
- 가맹점, 또는 상점: 카드를 수령하여 대금을 결제하고 상품이나 서비스를 제공하는 업체
- 매입사, 또는 매입 은행: 가맹점과 계약에 의해 지불카드의 인증과 대금결제를 처리하는 금융기관
- 지불 게이트웨이(Payment Gateway): 가맹점의 지불 메시지를 처리하기 위해 매입사, 혹은 제삼자에 의해 설계 및 구현된 창치
- 인증기관: 카드소지자, 가맹점, 지불 게이트웨이에 인증서를 배포하는 기관

SET은 크게 다섯 가지의 주요 보안 기술로 구성된다. 이 보안 기술은 공개키에 대한 인증서 기술, 암호화 기술, 디지털 서명, 지불시스템과의 연결, 그리고 운용 규칙의 설정 등이다. SET에서 이용되는 공개키 인증서는 다음과 같은 방식으로 동작된다. 인증기관은 PG, 발행 은행, 매입 은행에게 인증서를 각각 발행해 주고, 발행 은행은 카드 소지자에게 인증서를 발행하고, 매입 은행에서 상인에게 인증서를 발행한다. CA는 보다 상위의 CA로부터 인증서를 발급 받고, 최상위에는 루트 CA가 존재한다. CA에서 발급한 인증서는 일방향 함수에 기초한 암호기술을 사용하므로 CA 이외의 어떤 개체도 인증서의 내용을 수정할 수 없으며 인증서는 CA에서만 발행할 수 있다. 인증서는 거래자 상호간의 신분을 확인하는데 이용되며, 인증서에는 거래시 필요한 최소한의 정보를 갖고 있다.

2.8 인터넷 보안 프로토콜들[12][13]

보안 프로토콜로는 SSL(Secure Socket Layer)과 SHTTP(Secure Hyper Text

Protocol) 등이 있다. SSL과 SHTTP는 인터넷 상에서 상업적 기밀 통신을 제공한다. SSL 프로토콜과 SHTTP는 데이터의 기밀성, 인증 및 무결성, 그리고 부인 봉쇄 등의 보안 서비스를 통해 도청과 위조로부터 안전하게 데이터를 전송하는 안전한 통신 메커니듬이다. SSL은 그림 3과 같이 응용 프로토콜(HTTP, SMTP, Telnet, NNTP, FTP 등) 과 TCP/IP사이에 존재하여 소켓 계층 역할을 수행한다.

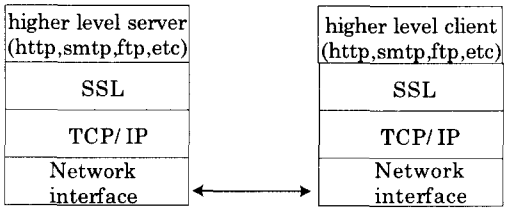


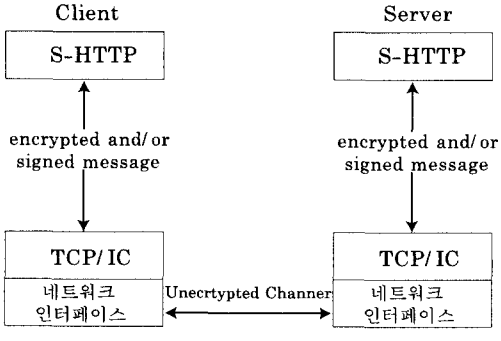
그림 SSL 계층 위치

SSL은 메시지들의 길이, 종류, 내용 필드 등을 다루고 있다. SSL은 메시지를 블록 단위로 분할하고, 선택적으로 압축하며, 이에 대한 MAC(Message Authentication Code)를 계산하고, 이를 암호한 후 그 결과를 상대방에 전송한다. 수신된 데이터는 복호화, MAC 검증, 압축 풀기, 역분할의 과정을 거쳐 상위 계층의 개체로 전달된다.

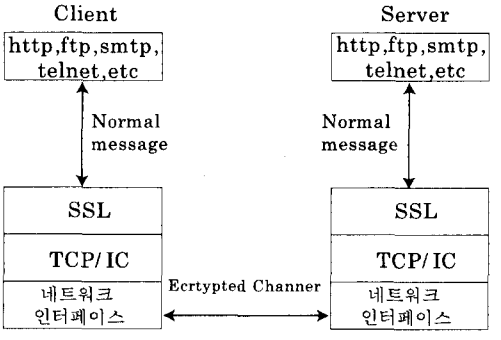
SHTTP는 HTTP 프로토콜에 바탕을 두고 보안 측면에서 보완한 것이다. 즉, SHTTP는 HTTP에 붙여서 사용하기 위해 고안된 통신 프로토콜이며 HTTP 메시지 모델과 함께 존재하고, 쉽게 HTTP 응용에 결합되도록 고안되었다. SHTTP는 헤더를 통해 각 거래마다 상대방들 사이에 옵션 협상을 하고, 이 협상을 통한 다중 직교 동작 모드, 키관리 메커니듬, 신뢰 모델, 암호 알고리듬 그리고 캡슐화 형식을 지원하는 융통성 있는 프로토콜을 제공한다. SSL이 연결 레벨 보안을 지원하고 S-HTTP가 응용층 레벨 보안을 지원하기 때문에 이들의 연합구조도 고려되고 있다. 그림 4는 SSL과 S-HTTP의 보안 레벨 구조를 보여준다.

2.9 전자 수표[14]

대표적인 전자 수표는 미국 재정 서비스 기술 컨소시엄(FSTC:Financial Services Technology Consortium)에 의해 개발되고 있다. 전자수표는 네트워크 상에서 안전한 가계



(a) S-HTTP : 응용층 레벨 보안



(b) SLL : 연결 레벨 보안

그림 4 S-HTTP와 SSL 의 채널 비교

수표의 사용을 가능케 하는 전자 수표 시스템이며, WWW의 환경에서 스마트 토큰을 이용하여 실현되고 있다. 전자수표는 근본적으로 디지털 서명 방식을 사용하므로 공개키 인증서를 이용해야 한다. 공개키 인증서는 X.509 인증서를 채용하고 있으며, 디지털 서명 시스템은 DSS(Digital Signature Standard) 서명 방식을 사용한다. 이 전자 수표에 대한 데모는 1995년 9월 21일 미국의 샌프란시스코 아메리카 은행에서 시행되었으며, 이 컨소시엄에 참여하고 있는 주요 은행은 미국 은행, 보스턴 은행, 몬트리올 은행, Bank one, 화학 은행 등이며, 전자화폐를 실현하는 기술을 지원하는 회사는 IBM, Sun Microsystems, Telequip 사, 그리고 Bellcore 등이다. 전자수표의 대표적인 흐름은 그림 5와 같다.

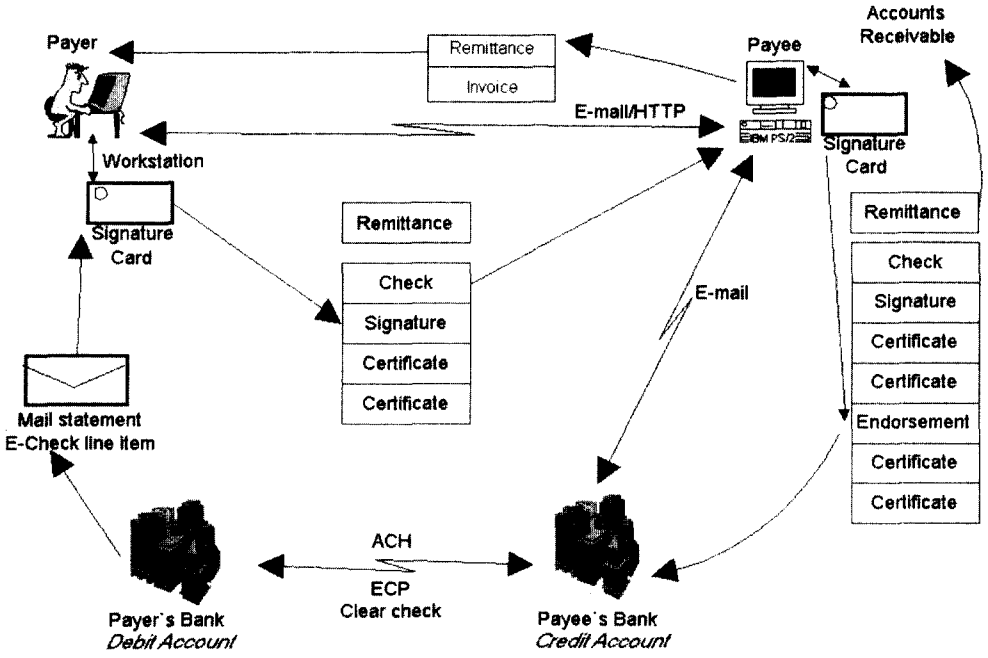


그림5 전자 수표의 흐름

먼저 수표 발행자 또는 지불자는 수표 수신인 또는 수표 수취인으로부터 수표의 발행을 요구하는 송장(Invoice)을 수신한 후 자신의 스마트 토큰에 저장되어 있는 서명용 비밀키로 전자 수표를 발행하고, 발행된 디지털 서명문과 자신의 서명용 공개키에 대응되는 공개키 인증서를 전자 우편으로 전자 수표 수취인에게 전송하며, 전자 수표 수취인은 자신이 거래하는 은행으로 전자 수표 발행자의 서명문과 공개키 인증서를 함께 보낸다. 은행은 전자 수표를 처리하고, 수취인의 은행과 지불자의 은행은 금융 거래를 정리한다. 이와 같은 전자 수표의 장점은 실현 비용이 낮고, 실현이 용이하다는 점이다.

3. 국내외 PKI 연구 동향

3.1 미국[15]

NIST는 AT&T, BBN, Certicom, Cylink, DynCorp, IRE, Motorola, NT, Spyrus, 그리고 Verisign 사와 컨소시엄을 구성하여 1977년에

자국 공개키 기반 구조를 제안했다. NIST는 DSA 만을 이용하는 FIPS186 규정안을 확장하여 여러 서명 알고리듬들이 포함되도록 연방정부를 위한 새로운 PKI 방식을 제안했다. 여기서 이용되는 서명 알고리듬은 DSA, RSA, 그리고 Elliptic Curve Digital Signature Algorithm(ECDSA) 이다. PKI는 ITU X.509v3 인증서를 채용하고 있다. 기본적으로 하나의 CA는 하나의 서명 알고리듬만을 이용한다. 만약 하나의 CA가 다른 서명 알고리듬을 이용하려 한다면 다른 CA 이름으로 공개키 인증서를 발급해야 한다. NIST에서 사용하고 있는 대표적인 알고리듬은 해쉬 알고리듬으로 SHA-1, 서명 알고리듬으로 DSS, 기밀성 알고리듬으로 DES 또는 AES(Advanced Encryption Standard), 인증 알고리듬으로 공개키 알고리듬에 바탕을 둔 개체 인증 알고리듬 등이다. NIST에서 상호 동작을 위한 최소로 요구되는 규격안은 CA, ORA(Organizational Registration Authority), 인증서 소지자 규격, 고객 규격 등을 포함하는 기반 구성요소 규격과, 인증서 형식, 인증서 폐지 목록(CRL), 인증 경로 유효성, 거래 메시지 형식, PKI 거래 등을 담고 있는 데이터 형식으로 구분되어 있다.

IBM 은 PKI 구성 요소를 크게 PKI 서버와 PKI 고객으로 구분하며, PKI 서버는 인증서 서버, 디렉토리 서버, 키 복구 서버 등으로 구성되며, PKI 고객은 WWW 서버, WWW 브라우저, 안전한 전자우편 고객, 파일 응용들로 구분하고 있다. CA는 인증서를 발행하고 관리하고 폐지하는 기능을 수행한다. 디렉토리 서버는 사용자 관련 속성 정보를 관리하는 기능을 수행한다. 키 복구 서버는 암호키를 복구하고 백업하며, 유사시에 잃어버린 암호키를 복원한다. 키 복구 시스템은 암호키를 분실한 암호화된 파일을 안전하게 복구하는데 유효하다. 서버는 비밀키에 대한 에스크로우(Escrow) 기능을 제공한다.

3.2 캐나다[16]

캐나다는 GoC(Government of Canada) PKI를 표준안으로 마련 중에 있으며 1998년까지 모든 PKI 서비스를 실현하려 하고 있다.

캐나다 PKI의 목적은 자국민에게 더 효율적인 보안 서비스를 제공하고, 전자상거래에서의 기밀성 서비스를 제공하며, 또한 정부에서 이용되는 정보에 대한 기밀성을 향상시킨다는 것에 있다. 캐나다의 PKI 기본 구조는 그림 6과 같다.

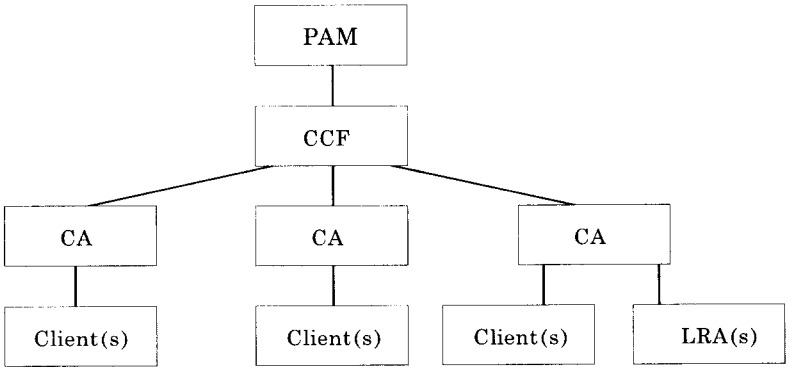


그림6 캐나다의 PKI 구조

캐나다 정부는 1998년 PKI에 대한 보고서를 발표했다. 캐나다 PKI는 키관리, 디지털 서명, 기밀성을 위한 키 인증 서비스를 제공하고, 정책 관리국(PMA:Policy Management Authority)은 PKI 정책에 관한 사항을 총괄한다. 캐나다 PKI는 전자상거래 분야와 공공분야의 안전한 정보 관리를 위하여 공개키 인증서, 스마트 카드 등의 여러 보안 기술들에 바탕을 두고 있다. 여기서는 공개키 인증서, 제삼자 상호 인증(Cross-Certification) 으로 구성된 공개키 기반 구조 정의, PKI 실현 방안, 산업체의 참여 현황, 기밀성 알고리듬, 보안 알고리듬, 통신 프로토콜, 네트워크 등으로 구성된 공개된 표준, 전자정보의 안전성과 관련된 법적 문제들, 미래 발전 방향, 실현 예, 그리고 PKI 의 활용 이점 등의 내용을 포함하고 있다.

3.3 호주[17]

호주는 1997년 1월 자국의 PKI 정책을 발표했다. 호주의 PKI 보안 규격은 512 비트와 1024 비트의 RSA 서명 알고리듬을 사용하며, 키 생성, 인증서 검증, 비밀키 보관 루틴을 공개적으로 제공하고 있다. 기본적으로 X.509v3 인증서를 사용한다. 사용자에게 제공되는 서비스는 하나의 인증키쌍, 하나의 인증용 공개키 인증서, 하나의 기밀성키 쌍, 하나의 기밀성 공개키 인증서를 제공한다.

3.4 유럽[18]

덴마크(DK-CA), 이태리(Italian CA), 노르웨이(UNINETT CA), 영국(UK Academic CA), 독일(DFN-PCA), 슬로베니아(SI-CA)는 연합하여 1995년부터 ICE-TEL 프로젝트를 수행하여 유럽의 최상위 레벨 CA를 구축하였다. 현재는 4차의 유럽 CA 기반 구조로 발전하여 왔다.

3.5 IETF[19]

IETF에서는 1977년 인터넷 X.509 공개키 기반 구조에서의 서명알고리듬을, 1998년 3월 인터넷 공개키 기반 구조에서의 인증서 및 CRL (Certificate Revocation List) 프로필 구조를, 1998년 4월 인터넷 X.509 공개키 기반 구조 인증서 정책과 인증 실현 프레임워크, 1998년 4월에 인터넷 X.509 공개키 기반 구조에서의 공개된 CRL 분배 절차, 1998년 3월 인터넷 X.509 공개키 기반 구조에서의 온라인 인증서 상태 조회 프로토콜, 1998년 4월에 인터넷 X.509 공개키 기반 구조에서의 고객이 온라인으로 인증서의 상태를 조회하기 위한 프로토콜을, 1998년 2월에 인터넷 X.509 공개키 기반 구조에서의 인증서 관리 프로토콜, 1998년 2월에 인터넷 X.509 공개키 기반 구조에서의 인증서 관리 메시지 형식, 1998년 2월에 인터넷 X.509 공개키 기반 구조에서의 인증서 요청 메시지 형식, 1998년 3월에 인터넷 X.509 공개키 기반 구조에서의 CMS (Cryptographic Message Syntax) 상에서 인증서 관리 메시지를 발표하였다. 이는 초안으로서 앞으로 지속적인 연구가 수행되어 최종안이 발표될 예정이다.

4. PKI 보안 알고리듬

공개키 기반 구조를 이루고 있는 핵심 보안 알고리듬은 해쉬 알고리듬, 암호 알고리듬, 서명 알고리듬으로 분류된다. 표 1은 공개키 기반 구조에 이용 가능한 보안 알고리듬을 각 나라와 크기를 비교하여 나타내었다.

X.509는 인증서를 서명하기 위한 알고리듬으로 RSA, DSA, ECDSA, KCDSA를 사용한다. 이들 알고리듬들은 공개키를 이용할 경우에도 사용된다. 이들 알고리듬들은 CA와 최종

객체간에 검증이 되어야 하며 최소한 하나를 사용할 수 있어야 한다. 디지털 서명을 하기 위해서는 인증 알고리듬인 일방향 해쉬 함수와 함께 결합되어 사용된다.

표1 PKI에 이용되는 핵심 보안 알고리듬

분류	알고리듬	암호키 크기	국 가
대칭 키 암호	CAST	128비트	캐나다,
	DES	64비트	캐나다,미국(NIST),호주,유럽(IEC-TEL)
	IDEA	64비트	유럽(IEC-TEL)
	Triple DES	192비트	캐나다
	RC2	가변	캐나다
	RC4	가변	캐나다
	AES	128비트	미국
디지털 서명/해쉬 알고리듬	RSA/MD5	512/1024비트	캐나다,미국(NIST),호주,유럽(IEC-TEL)
	RSA/SHA-1	512/1024비트	캐나다,미국(NIST),유럽(IEC-TEL)
	DSA/SHA	512/1024비트	캐나다, 미국(NIST)
	ECDSA	512/1024비트	미국(NIST)
	KCDSA	512/1024비트	한국

5. PKIX

여기에서는 IETF 표준안[19]을 중심으로 X.509를 이용한 PKI(PKIX)를 설명한다.

5.1 Internet X.509 PKI 인증서 관리 프로토콜

프로토콜 메시지들은 인증서 생성과 관리에 대해 정의하고 있다. 인증서는 X.509v3을 이용한다. 인증서 관리 프로토콜에는 PKI 관리 메시지의 데이터 구조와 PKI 관리 기능을 정의하고 PKI 메시지 전송을 위한 프로토콜을 설명한다. 관리 프로토콜은 PKI 요소들 사이에 온라인 상호작용을 지원해야 한다. 상호 작용을 위한 개체들에는 최종개체, 인증기관, 등록기관으로 구성된다.

개체는 응용의 사용자나 또는 응용이다. 인증기관은 최종개체(EE)와 다른 CA들에게 인증서를 발행하는 신뢰된 개체이다. 최종개체가 직접 신뢰하는 CA를 "루트 CA"라고 한다. 최종개체와 CA외에, 다양한 환경들을 위해 등록기관(RA)이 존재한다. RA는 개인 인증, 토큰 분배, 철회보고, 이름 할당, 키 생성, 키 쌍 기록 등을 수행한다. RA가 존재하지 않을 땐, CA가 RA 기능들을 대신하게 된다. 모든 RA들은 최종개체를 인증할 수 있고, 서명용 개인키를 가지고 있다고 가정한다. RA는 특정한 CA에 의해 인증되어져야 한다고 규정하지 않음으로서, 하나의 RA가 여러 개의 신뢰된 CA와 동작할 수 있도록 한다. RA가 존재하여도 최종개체는 CA와 직접적으로 통신할 수 있다. 초기 등록과 초기 인증시에 최종개체의 주체는 자신의 RA를 이용 할 것이다. 그러나 자신의 인증서를 갱신하기 위해서는 CA와 직접적으로 통신할 것이다.

5.2 PKI 관리 요구 사항

여기에서 사용되는 프로토콜은 다음과 같은

요구 사항을 만족해야 한다.

- PKI 관리는 ISO 9594-8 표준과 관련된 수정안을 따라야만 한다.
- 정기적으로 키쌍을 갱신 할 수 있어야 한다.
- PKI 관리 프로토콜에서 기밀성의 사용은 최소화되어야 한다.
- PKI 관리 프로토콜은 서로 다른 표준 보안 알고리듬을 사용할 수 있어야 한다.
- PKI 관리 프로토콜은 관련된 EE, RA, 또는 CA의 인증서 공표를 지원해야 한다.
- PKI 관리 프로토콜은 CRL(Certificate Revocation Lists) 생성을 지원해야 한다.
- PKI 관리 프로토콜은 mail, http, TCP/IP, ftp와 같은 다양한 전송 메커니즘에서 이용할 수 있어야 한다.
- 인증서 생성에 대한 최종 권위는 CA에게 있다.
- 협상되지 않은 CA 키쌍의 갱신이 자연스럽고 계획적으로 이루어져야 한다. 새로운 CA 공개키를 포함하는 PSE의 최종개체는 증명 가능한 이전의 공개키를 이용하여 인증서를 증명할 수 있어야 한다. 이전의 CA 키쌍을 신뢰하는 최종개체는 새로운 CA 개인키로 서명된 인증서를 증명해야 한다.
- RA의 기능들을 CA가 수행할 수 있어야 하며, RA와 통신하든지 CA와 통신하든지 간에 관계없이 최종개체는 동일한 프로토콜을 이용 할 수 있도록 설계되어야 한다.
- 최종개체가 인증서를 요구할 경우, 최종개체는 공개키에 대응되는 개인키를 증명해 보여야 한다. 이것은 인증서 요구의 형태에 따라서 다양한 방법으로 수행될 수 있다.

5.3 PKI 관리 동작

초기 등록 및 인증은 최종개체, 등록기관, 또는 인증기관 중에 어느 것이든 먼저 시작할 수 있다. 최종개체 메시지 인증은 out-of-band 방법을 통해 얻어진 비밀 값(초기 인증키)과 참조값(거래를 검증하기 위해 사용된 값)으로 인증기관이나 등록기관에 의해 이루어진다. 키는 최종개체, 등록기관, 인증기관 어디서든지 생성될 수 있고, 키 생성 요청 및 응답 프로토콜에 의해 전송된다.

다음 그림 7은 PKI 관리 동작을 보여준다.

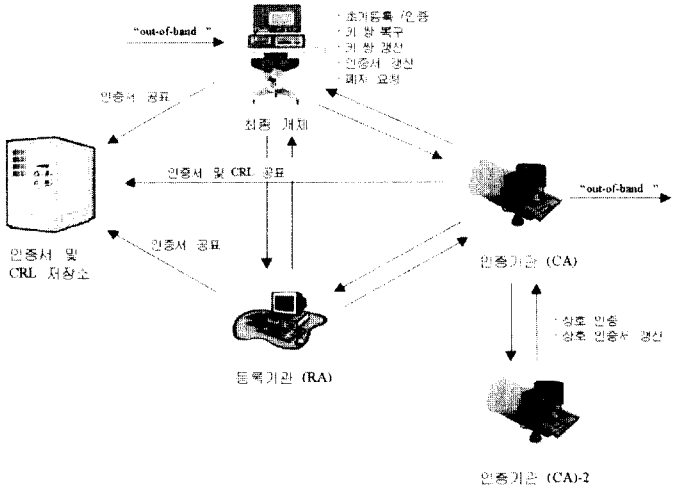


그림 7 PKI 관리 동작

5.4 PKI X.509 인증서

인증서는 공개키 인증서라고도 하며, 공개키와 사용자를 바인딩 함으로서 사용자를 인증한다. 공개키를 사용하는 사용자는 공개키와 관련된 개인키가 올바른 주체의 것임을 확인하고 이들이 암호와 디지털 서명을 할 수 있음을 확인하게 된다. 이러한 신뢰는 인증서를 통해 이루어지며, 이 공개키 인증서는 공개키 값들과 주체들을 바인딩 한다.

ITU-T X.509 또는 ISO/IEC/ITC 9594-8은 표준 인증서 포맷인 X.509를 정의한다. 1988년에 발표된 인증서 포맷은 버전 1(v1) 포맷이다. 1993년 X.500이 개정되었을 때, 두 개의 필드가 추가되었고, 결과로서 버전 2(v2) 포맷이 나왔다. 이 두 필드는 디렉토리 접근 제한을 지원하기 위한 것이다. 1993년에 공개된 PEM(Privacy Enhanced Mail)은 X.509 v1 인증서에 기반한 PKI에 대한 명세서를 포함하고 있다. X.509 v1과 v2를 사용하면서 더 많은 필드가 요구되어졌고, 결국 ISO/IEC/ITU와 ANSI X9는 발전된 X.509 버전 3(v3) 인증서 포맷을 내어놓게 되었다. 버전 3은 버전2에 확장필드들을 추가한 것이다. 특별한 확장 필드 타입들은 표준에 명시되거나 또는 어떤 조직이나 공동체에 의해 등록되고 정의될 것이다. 1996년 6월에 X.509 v3 포맷의 표준이 완성되었다. ISO/IEC/ITU와 ANSI X9는 버전 3 확장 필드에 사용될 표준 확장들을 계속 발전시켜 왔다. 이 들 확장들은 부가적인 주체 신분 정보, 키 속성 정보, 정책 정보, 그리고 인증 경로 구속력과 같은 데이터를 운반할 수 있다. 그러나 ISO/IEC/ITU와 ANSI X9 표준 확장들은 매우 광범위하므로 인테넷에서 X.509 v3을 사용하기 위해서는 호환성 있는 X.509 v3 시스템으로 발전시켜야 했다. 따라서, X.509 v3 확장들을 인터넷, 전자메일, 그리고 IPsec 응용들에서 사용하기 위해 이들에 대한 규정이 요구되고 있다.

5.4.1 X.509 v3 인증서

그림 8은 X.509 v3 인증서 구조를 보여준다.

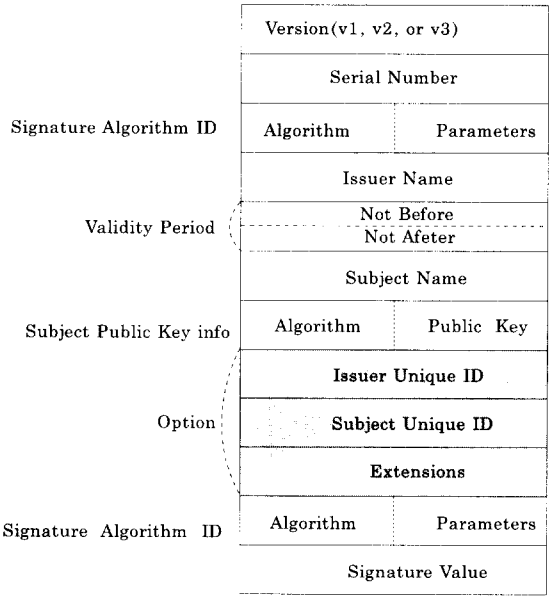


그림8 X.509 v3 인증서

인증서 필드는 인증서, 서명알고리듬, 서명값의 세 필드로 구성되어 있다. 인증서 필드는 개체와 발생사의 이름들, 개체와 관련된 공개키, 유효기간, 그리고 그 외 관련 정보들이 포함된다. 서명 알고리듬 필드는 서명알고리듬과 파라메터들이 있으며 이것은 인증서 필드에 있는 서명 알고리듬 식별자와 동일해야 한다. 서명값은 ASN.1 DER 인코딩된 값으로, 인증서 필드를 해쉬한 후 서명알고리듬을 이용해 계산된 값이다.

인증서 확장영역은 표준화된 확장영역과 인터넷을 위한 확장영역으로 구분된다. 표준화된 확장영역은 키와 정책 정보, 주체와 발행자 속성, 인증경로 구속력, 그리고 CRL 식별자 확장의 4가지로 분류될 수 있다. 인터넷을 위한 확장에는 어떻게 인증서의 발행자를 위한 서비스들과 CA 정보에 접근할 것인지에 대한 정보가 포함된다. 정보와 서비스들은 온라인 유효 서비스들과 CA 정책 데이터들을 포함한다.

5.4.2 CRL과 CRL 확장 규정

X.509 v2 CRL 규정의 목적은 재사용 가능하고 호환성 있는 인터넷 PKI의 개발에 있다. 이 목적을 이루기 위해, 확장들의 사용에 대한 지침들이 정의되고, CRL에 포함된 정보의 성질에 대한 몇 가지 가정들이 세워졌다. CRL들은 폭넓은 환경과 응용들에 사용될 것이다. 이 규정은 폭넓은 호환성을 요구하는 일반적인 응용들을 위한 일반 기준선을 설정하며, 모든 CRL에서 예상될 수 있는 정보의 기준선 세트를 정의한다. 또한 흔히 사용된 속성들에 대해 CRL내에 일반적인 위치뿐만 아니라 이들 속성들을 위한 일반적인 설명까지도 정의한다.

발행하는 CA들은 X.509 인증서 버전 2 CRL들을 발행해야 하고, CA들은 다음 CRL이 nextUpdate 필드, CRL 번호 확장, 그리고 인증키 증명자 확장에서 발행될 날짜를 포함해야 한다. 확실한 응용들은 프로세스 버전 1과 2 CRL들에서 요구된다. 그림 9는 X.509 v2의 구조를 보여준다.

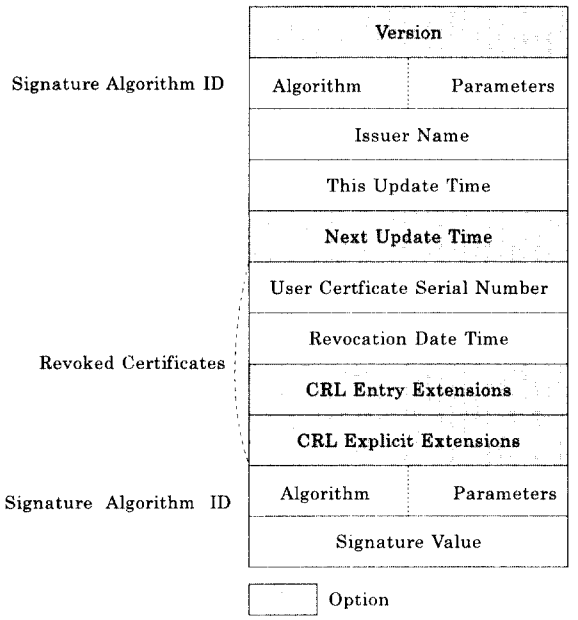


그림9 X.509 v2 CRL

X.509 v2 CRL은 인증서 필드, 서명알고리듬필드, 서명값 필드의 세 필드로 구성된다. 인증서 필드는 발행자의 이름, 발행 날짜, 다음 리스트의 발행 날짜, 철회된 인증서들의 리스트, 그리고 선택적인 CRL 확장들을 포함한다. 철회된 인증서 리스트상의 각각의 엔트리는 사용자 인증서 시리얼 번호, 철회 날짜, 그리고 선택적 CRL 엔트리 확장들을 정의하고 있다. 서명 알고리듬필드는 서명하기 위한 알고리듬 식별자이다. 이 필드 역시 인증서 필드에 있는 서명알고리듬 식별자와 동일한 알고리듬 식별자이어야 한다. 서명값은 인증서 필드를 서명한 값이다.

X.509 v2 CRL들에 대한 ANSI X9와 ISO/IEC/ITU에 정의된 확장들은 CRL들과 부가적인 속성들에 대한 결합 방법을 제공한다. X.509 v2 CRL 포맷은 공동체에 독특한 정보를 운반하기 위해 공동체가 비밀 확장을 정의하도록 허용한다. CRL에 있는 각 확장은 critical 또는 non-critical로 구분된다.

6. 유료방송을 위한 한정 수신 시스템 [20][21][22]

스크램블링 및 디스크램블링 기능, 인증을 위한 가입자 신분 확인(Authentication) 기능, 그리고 접근 제어 기능은 유료 방송시스템을 실현하기 위한 핵심 기능 중의 하나이다. 한정 수신 시스템은 시청료를 지불한 시청자만이 수신 측에서 스크램블된 형태로 전달된 신호를 디스크램블하여 원하는 프로그램을 시청할 수 있게 하는 시스템이다. 한정 수신 시스템을 실현하기 위해서는 스크램블링의 강도가 어느 정도 높아야 하고, 스크램블링 및 디스크램블링을 위한 관련 파라메터들은 암호학적으로 안전한 알고리듬을 사용하여 수신단으로 안전하게 전달되어야 한다. 방송망에 적용 가능한 한정 액세스는 크게 스크램블러의 비밀키인 제어워드(CW: Control Word)를 분배하는 기능과 CW를 암호화하여 전달하는데 이용되는 인증키(AK)를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현될 수 있다. CW를 인증키로 암호화하여 전달하는 메시지를 ECM 이라고 하고 인증키를 전달하기 위한 메시지를 EMM 이라고 한다.

기존의 케이블 망용 한정 액세스 시스템은 케이블에 연결되어 있는 사용자만이 비디오 및 오디오 신호를 수신할 수 있고, 별도의 블랙 박스(Set top box)를 부가하여 특정 프로그램의 액세스를 제한하며, 사용자의 액세스 빈도를 저장하는 계수기를 포함하여 과금을 처리하며, 교환기가 사용자의 요구에 응하여 선택적으로 프로그램을 분배한다는 원칙 하에 설계되었다.

방송 환경에서는 반드시 스크램블링 기법이 요구되며, 여러 가지 다양한 스크램블링 기법이 적용될 수 있다. 적용되어야 할 스크램블링 기법은 안전성이 높아야 하며, 스크램블링의 도입으로 인하여 방송서비스 신호의 질을 저하하지 않도록 설계되어야 한다.

스크램블러에 이용될 수 있는 PRBS (Pseudo Random Binary Sequence) 생성기는 주기가 될 수 있는 한 길어야 하고, 출력 비트간의 상관(Correlation)이 작아야 하며, 난수계열의 일부분으로부터 스크램블러의 비밀 정보인 초기치를 유도할 수 없어야 한다는 특성을 가져야 한다.

기존의 CAS는 디코더를 이용한 인증과 키 분배였었지만, 디코더의 단점을 보완하고 보안성을 위해 스마트 카드를 이용한 CAS 구조가 제안되었으며 서버 측의 안전성을 향상시키기 위하여 ECM 생성용 제어 카드와 EMM 생성용 관리 카드를 도입하였다. 그림 10은 스마트 카드를 이용한 CAS를 보여준다.

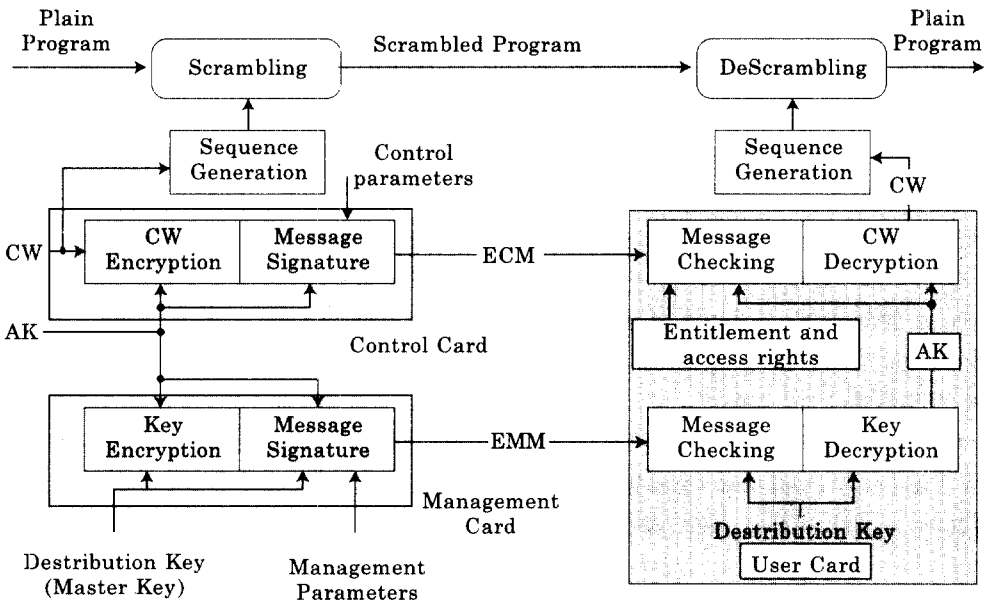


그림10 스마트 카드를 이용한 CAS

이 방식은 CW를 분배하기 위한 ECM과 CW를 암호화하는데 이용되는 인증키를 분배하기 위한 EMM에 바탕을 두고 있으며, EMM은 서버와 각 사용자의 액세스 카드가 공유하고 있는 가입자의 분배키와 서명문을 위한 일차 검증키를 이용하여 생성된다. 가입자측 IC 카드는 ECM 및 EMM 으로부터 해당 정보를 도출한다. CW는 ECM 형태로 암호화되어 가입자에 전달된다. ECM은 CW를 인증키로 암호화한 암호문과 이에 대한 서명문을 쌍상한 구조를 갖는다. 각 가입자는 ECM으로부터 CW를 복구하고 제어 메시지의 정당성을 서명 알고리듬과 무결성 알고리듬으로 검사한 후, 메시지가 정당하면 CW 를 디스크램블러로 전달한다. 인증키의 분배는 EMM을 통해 전달되며, EMM은 각 사용자의 분배키로 인증키를 암호화한 암호문과 사용자의 자격을 나타내는 자격 정보를 사용자의 일차 검증키(Primary Verification Key)로 서명한 서명문으로 생성된다. 각 사용자의 액세스카드는 분배키를 이용하여 인증키를 복구하고 자격 메시지를 검사하며, 인증키를 ECM 제어부로 전달한다. 이 방식은 서버와 사용자가 비밀리에 분배키와 서명용 일차 검증키를 공유하고 있다고 가정한다.

보통 ECM은 수초에 한번씩 전송되면 EMM은 한 달에 한번씩 특수채널이나 우편을 통해 전송되어 스마트 카드에 내장된다.

7. PKIX를 이용한 디지털 방송 한정수신 시스템

현재, 제한 수신 시스템은 스마트 카드를 이용한 디지털 유료 방송 서비스에 적용 가능한 한정 수신 시스템이 개발되어 있고, 스크램블링 알고리듬 역시 일부 표준화되어 있다. 한정수신시스템은 수신료를 시청시간 및 시청한 프로그램에 따라 차등적으로 적용하는 등 다

양한 서비스를 제공할 수 있으나, 이를 실현할 경우에 발생하는 여러 가지 해결해야할 문제점이 남아있다. 즉, 일반적으로 관리상에서 발생할 수 있는 서비스 가입 등록, 서비스 가입자 관리, 서비스 관리 등과 제한 수신시스템 상에서 발생할 수 있는 키 생성 속도 및 전달 시간, 전용선 Capacity, 시스템 용량 등의 문제들을 고려해야 할 필요성이 있다. 따라서, 앞으로 디지털 방송 유료 서비스의 질을 개선하고, 효율적으로 상용화하기 위해서는 위의 문제점들이 해결되어야 할 것이다.

현재 인터넷을 통한 방송이 일부 실시되고 있지만, 전송속도와 용량으로 문제점이 되고 있다. 속도가 느리기 때문에 자주 끊김 현상이 나타나고 화질도 좋지 않다. 앞으로 전송속도가 향상되거나, 압축기술등의 기술적인 면이 향상되지 않는 한 인터넷을 통한 방송서비스는 많은 어려움이 있을 것으로 보이며, 따라서, 이는 새로운 형태로의 접근이 필요하다.

기존의 디지털 방송에 관리상의 문제점을 해결하기 위해 앞에서 살펴본 PKIX를 적용한다. PKIX를 이용하여 서비스 가입과 등록, 서비스 가입자 관리, 그리고 서비스 관리를 하게 된다.

PKI 메시지를 이용한 디지털 방송 한정수신 시스템 서비스의 전체 구성도는 그림 11과 같다.

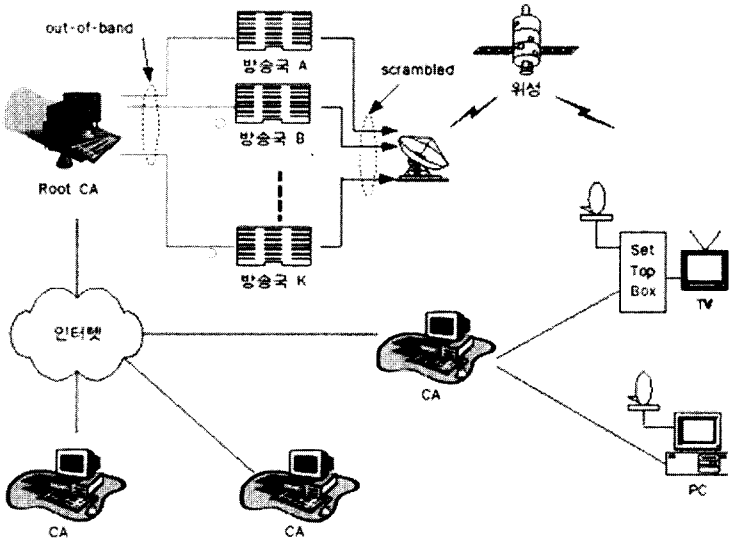


그림11 PKI를 이용한 디지털 방송 한정 수신 시스템 서비스

앞에서 살펴본 바와 같이 방송 프로그램을 스크램블링하고 디스크램블링하는데는 ECM과 EMM 메시지가 필요하다. 여기에서는 스크램블링된 방송 프로그램과 ECM메시지를 동시에 보내는 구조를 생각한다. 그리고 EMM 메시지는 PKI를 이용해 안전하게 가입자에게 전달되도록 한다.

루트 CA나 CA는 키 관리국을 의미하며, 키 관리국은 가입자 인증 및 관리를 하게 된다. 루트 CA는 방송국과 로컬 CA들을 직접적으로 인증해야 하며, out-of-band로 인증서를 발행해야 한다. 로컬 CA들을 둠으로서 키관리에 대한 부하를 최소화한다. 인증서는 디렉토리에 공개하지 않는다.

7.1 루트 CA와 방송국 및 로컬 CA

루트 CA는 방송국들에게 out-of-band 방식으로 인증서를 발행한다. 방송국은 프로그램을 스크램블링하기 위해 AK(Authorization Key)가 필요하다. 인증서는 루트 CA에 의해 자가 서명된다. AK는 주기적으로 변경되어야 하기 때문에 루트 CA는 AK를 변경한 후 방송국에 분배한다. 루트 CA와 로컬 CA들도 동일한 방법으로 인증서와 AK들을 전달하게 된다. 다음 그림 12는 루트 CA와 방송국 A의 인증서와 AK 분배를 보여주고 있다.

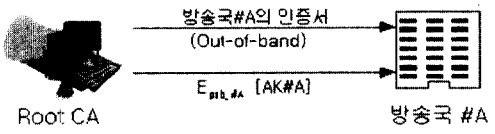


그림12 방송국과 루트 CA간의 키 분배

다음 그림 13은 루트 CA와 로컬 CA의 방송국들의 AK 분배를 보여주고 있다. 루트 CA는 모든 방송국의 AK를 각 로컬 CA의 공개키를 이용해 분배한다.

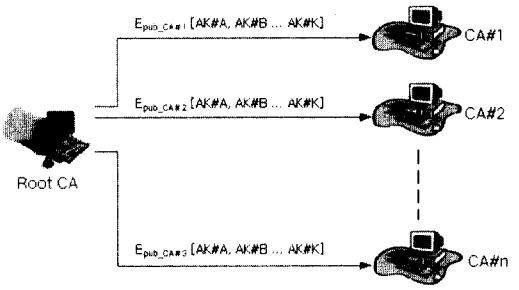


그림13 루트 CA와 로컬 CA의 키 분배

7.2 로컬 CA와 가입자

다음은 로컬 CA와 가입자간의 AK 분배 과정을 설명한다. 가입자는 스마트 카드를 이용해 Out-of-band 방식으로 비밀 메시지를 분배받는다. 가입자는 스마트 카드를 이용해 인증서를 요청하게 된다. 인증서 요청은 PKI 관리 메시지 구조와 동일하다. 다음 그림 14는 인증서 요청을 보여준다.

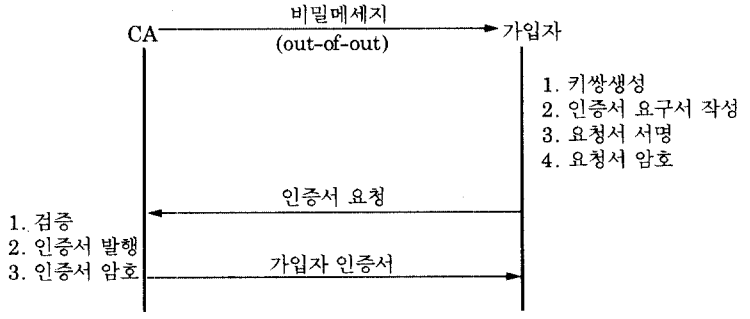


그림14 가입자의 인증서 발급

여기서, 비밀메시지는 가입자가 키쌍을 생성할 수 있는 파라메터와 CA의 공개키가 포함된다. 가입자가 인증서를 받은 후에는 스크램블된 프로그램을 디스크램블링하기 위해 AK를 수신해야 한다. AK를 수신하기 위한 방법은 다음 그림 15와 같다.

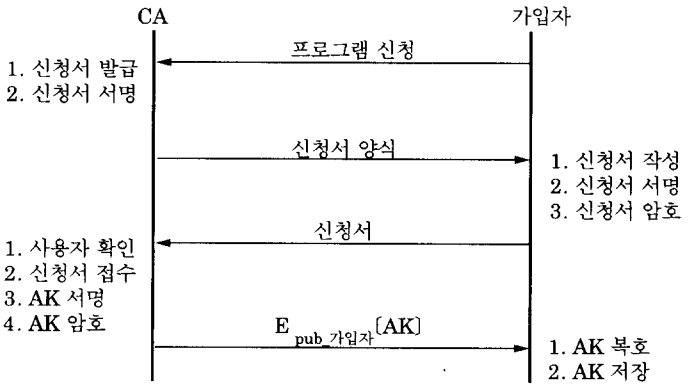


그림15 가입자의 프로그램 신청과 AK 분배

가입자는 CA에 프로그램 신청을 하고, CA로부터 신청서 양식을 받게 된다. 신청서에는 프로그램 서비스 타입과 방송국을 지정할 수 있는 다양한 옵션이 있을 수 있다. 로컬 CA는 가입자를 별도로 관리하며 전적으로 로컬 CA로 관리가 이루어 질 수 있다. AK를 수신한 가입자는 스마트 카드에 AK를 저장하고, 프로그램을 디스크램블링하여 시청이 가능하게 된다.

8. 결 론

인터넷의 발달과 함께 서비스의 형태들이 인터넷을 중심으로 인터넷과 연결되어 발전해 나가고 있다. 이러한 서비스들은 각 사용자들을 위한 보안을 위해 공개키 암호 방식을 이용한 공개키 기반구조를 사용하고 있다. 공개키 기반구조를 이용한 사용자 관리는 X.500 디렉토리나 X.509를 표준으로 발전하고 있으며, 선진 외국에서는 공개키 기반구조의 표준에 대한 발빠른 움직임들을 보이고 있으며, 각 인터넷 표준 그룹들에서도 PKI의 표준안을 제안하고 있다. 정보보호 관련 기반구조인 공개키 기반 구조는 현재 미국, 호주, 캐나다, 독일 등에서 공개키 기반구조 구축을 추진 중에 있다. 국내에서도 전자 상거래를 국가 전략 사업으로 추진하고 있으며, 공개키 기반구조 시범 시스템이 구축되고 있다. 공개키 기반 구조는 특성상 상호 연동 가능성이 가장 중요한 요소이며, 이를 위해 공개키 키관리 체계 표준이 시급히 요구되고 있다. 이러한 공개키 기반구조의 이용으로 인해 전자상거래는 물론 대부분의 서비스들이 인증서를 기반으로 하는 공개키 기반구조를 채택하고 있다.

본 고에서는 공개키 기반구조에 관해서 인증서 활용 서비스를 도출, 국가별 공개키 기반구조의 표준화 동향, 공개키 기반 구조에 요구되는 기본 요구사항과 요소 분석, 그리고 응용 메커니듬과 서비스들을 분석하였으며, 디지털 방송을 위한 한정수신 시스템에 대해 살펴보았다.

위의 분석한 결과를 토대로 공개키 기반구조를 디지털 방송 한정수신 시스템에 도입함으로서 가입자의 관리와 키 분배에 효율적인 방안을 제시했다.

참고 문헌

[1] William Stallings, "Network and Internetwork Security", Prentice Hall International Editions, 1995.

[2] Linn, J., "Privacy Enhanced for Internet Electronic Mail: Part I: Message Encryption and Authentication Proced ures", RFC1421, IETF PEM WG, Feb, 1993.

[3] RSA Labatories, PKCS: http://www.rsa.com/rsalabs/pubs/PKCS/index.html

[4] RSA Labatories, S/MIME Message Specification, July, 1997.

[5] J. Galvin, S. Murphy, S. Croker, N. Freed, Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted, RFC1847, Oct, 1995.

[6] J.Linn, "Generic Security Service Application Program Interface", IETF, RFC 2078, Jan, 1997

[7] Carlisle Adams, The Simple Public-Key GSS-API Mechanism, RFC 2025, October, 1996

[8] National Security Agency, "Security Service API : Cryptographic API Recommendation," NSA Cross Organization CAPI Team, 12 Jun 1995.

[9] 염흥열, 윤호선, 김락현, 류대현, "공개키 방식을 이용한 GSS-API 시스템 설계", 제1회 개방형보안기술과 응용 워크샵, pp 196-206, 1997.11.

[10] IP Security Working Group Twenty-Ninth IETF March 31, 1994

[11] SET(Secure Electronic Transaction) Specification Book 1 : Business Description

[12] 이강석, 김상필, 염흥열, " 전자 상거래에 적용 가능한 SSL의 분석", 호서지부전자공학회, 1997. v1. n1, pp. 13-18.

[13] E. Rescorla, A. Schiffman Terisa Systems, Inc., "The Secure HyperText Transfer Protocol--SHTTP/1.2", draft-ietf-wts-shttp-03.txt, July 1996.

[14] FSTC, "Electronic Check Proposal : Public Document," Financial Services Technology Consortium, 1995.

[15] William Burr, Donna Dodson, Noel Nazario, W.Timothy Polk, MISPC, Version 1, September, 1997.

[16] Government of Canada, Communications Security Establishment(CSE), "Government of Canada Public Key Infrastructure-White Paper" 1998

[17] Certificates Australia, http://www.secdom.com.au/certserv.htm

[18] ICE-TEL Project, http://www.darmstadt.gmd.de/ice-tel/

[19] PKIX Working Group draft-ietf-pkix, 1997-1998

[20] CCIR "Conditional-Access Broadcasting System", Recommendation 810, 1992.

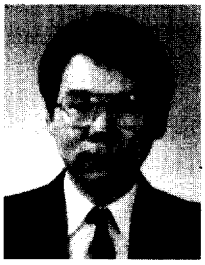
[21] General Characteristics of a Conditional Access Broadcasting System-Report CCIR 1079-1.

[22] 김경신, 김승주, 원동호, "스마트카드를 이용한 유료 방송 한정수신 시스템", JCCI'96, 1996.

[23] 조현숙, 임춘식, " DigiPass - KoreaSat DBS의 Conditional Access System", 전자공학회지 제22권 제7호, 1995년 7월, pp768-775

[24] 조현숙, 임춘식, " Pay-TV 서비스를 위한 스마트카드", 위성통신과 우주산업회지, 1995년 8월, pp58-65

□ 著者紹介

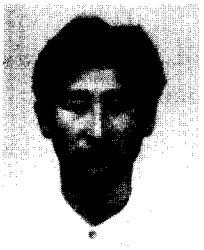


염 흥 열

1981년 한양대학교 전자공학과 졸업(학사)
1983년 한양대학교 대학원 전자공학과 졸업(공학석사)
1990년 한양대학교 대학원 전자공학과 졸업 (공학박사)
1982년 12월 ~ 1990년 9월 한국전자통신연구소 선임연구원
1990년 3월 ~ 현재 순천향대학교 공과대학 전기전자공학부 부교수
1997년 3월 ~ 현재 순천향대학교 산업기술연구소 소장
1997년 3월 ~ 현재 한국통신정보보호학회 총무이사

※ 주관심분야: 암호이론, 부호이론, 이동통신 분야

□ 著者紹介

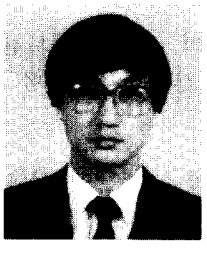


이 강 석

1997년 2월 순천향대학교 전자공학과 졸업(학사)
1997년 3월 ~ 현재 순천향대학교 전자공학과 석사과정

※ 주관심분야: 공개키 기반구조, 네트워크 보안, 전자상거래

□ 著者紹介



윤 이 중

1988년 인하대학교 전자계산학과(학사)
1990년 인하대학교 전자계산학과(석사)
1998년 한국전자통신연구원 근무

※ 주관심분야: 정보보호 시스템 개발, Public Key Infrastructure 개발