主題

PKI 기술

한국전자통신연구원 조영섭, 진승헌, 윤이중, 조현숙

차 례

요 약

통신과 컴퓨터 기술의 비약적인 발전에 따른 인터넷의 급속한 확산은 일상적인 상거래를 인터넷 상에서 전자적으로 수행할 수 있도록 하는 전자상거래의 급속한 확장을 가져오고 있다. 전자상거래는 시·공간적인 제약을 받는 기존 상거래를 대체하며 현재 활발히 확산되고 있다. 그러나 인터넷 상의 전자상거래가 더욱 활성화 되기 위해서는 거래에 대한 인증, 무결성, 기밀성, 부인봉쇄 기능을 제공하여 전자거래의 안전성과 신뢰성을 확보해야 한다. 최근 이러한 전자 상거래의 안전성을 제공하기 위해 PKI(Public Key Infrastructure)에 대한 연구가 많이 진행되고 있다. PKI는 공개키 암호 시스템과 공개키에 대한 인증서, 인증기관 등으로 구성되어 전자 거래의 안전성을 제공하는 기반구조로서 많은 응용 분야에서 활용되고 있으며 그 성장 가능성이 매우 크다. 본 고에서는 공개키 기반구조에 대한 개념과 국내외 연구 동향, 그리고 한국전자통신연구원에서 개발한 공개키 기반구조인 ETRI CMS(Certificate Management System)를 설명한다.

1. 서 론

최근 통신기술의 발달과 전세계적인 규모의 통신기반인 인터넷은 전자상거래(Electronic Commerce)라는 새로운 경제 패러다임을 창출하고 있다. 전자상거래는 기존 상거래의 시간적 공간적 제약을 극복하며 유통, 물류 비용등의 상거래 비용을 절감하고 탄력성있는 기업/경제활동이 가능하도록 하여 사이버 기업(Cyber Company), 사이버 마켓(Cyber Market), 사이버 거래사회(Cyber Trading Community) 등과 같은 신종 기업/비즈니스 문화를 탄생시키고 있다. 전자상거래는 인터

넷 뱅킹, 사이버 증권거래, 전자결재 등과 같이 다양하게 기존 상거래를 대체하고 있으며 최근 급속하게 확장하고 있다[1,2].

전자 상거래는 기존 상거래와는 달리 통신망을 통한 사이버 공간에서 수행되기 때문에 위조된 거래자의 거래, 거래 내용의 노출, 거래 내용의 변조, 거래 사실의 부인 등과 같은 다양한 위협에 노출될 수 밖에 없다. 따라서 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 거래자의 신원확인(Authentication), 거래 내용의 무결성(Integrity)과 기밀성(Confidentiality) 확보, 그리고 거래자가 거래사실을 부인하는 것을 방지하는 부인봉쇄(Non-Repudiation) 기능을 제공하는 보안 메커니즘이 필요하다[1,3].

이와 같이 인터넷 상의 전자상거래에 보안 메커니즘을 제공하기 위해 최근 공캐키 암호 시스템(Publick Key Cryptography System)과 공개키(Public Key)에 대한 인증서를 기반으로한 보안 메커니즘을 제공하는 기반 구조인 PKI에 관한 많은 연구가 진행되고 있다. 현재 PKI에 대한 연구와 개발 제품의 성능은 매우 미약하지만 IDC 사에 의하면 1998년 1.2억$에서 2003년에는 13억$ 정도로 시장이 확장될 것으로 예측하고 있을 정도로 그 시장 규모가 급격히 팽창하고 있으며 향후 전자상거래 보안 메커니즘의 핵심이 될 것으로 전망되고 있다 [4]. 그러나 PKI에 대한 중요성과 시장 잠재력에 비해 국내에서는 아직까지 PKI에 대한 연구가 미흡하고 전반적인 기능을 지원하는 시스템에 대한 개발이 전무한 실정이다.

본 고에서는 이와 같이 전자상거래의 핵심 보안 메커니즘이며 향후 그 성장 가능성이 매우 큰 PKI에 대한 개념을 설명하고 PKI에 대한 전반적인 기능을 지원하도록 개발된 ETRI CMS(Certificate Management System) 에 대하여 기술한다.

본 고의 구성은 다음과 같다. 2장에서는 PKI의 출현 배경 및 개념을 간단히 설명하고 3장에서는 PKI에 대한 국내외 연구동향을 살펴본다. 4장에서는 한국전자통신연구원에서 개발한 PKI인 ETRI CMS에 대하여 설명하고 5장에서 결론을 맺는다.

2. PKI

2.1 암호 시스템(Cryptography System)

전통적으로 정보보호를 위해서 가장 많이 사용되는 방식은 키를 이용하여 송수신되는 데이터를 암호화하고 복호화하여 보안을 제공하는 암호시스템이다. 암호시스템은 비밀키 암호 시스템(Secret-Key Cryptosystem)과 공개키 암호 시스템(Public-Key Cryptosystem)으로 분류할 수 있다[5].

비밀키 암호 방식은 암호화와 복호화에 사용되는 키가 서로 동일한 대칭키 암호 시스템(Symmetric Cipher System)으로 암호화할 데이터의 송수신자가 서로 동일한 키를 공유하여 암·복호를 수행한다. 비밀키 암호 방식은 구현이 쉽고 암·복호화 속도가 빠르다는 장점을 가지고 있다. 그러나 비밀키 암호 방식은 암호 통신을 수행하려는 사용자들 사이에 키를 공유하여야 하기 때문에 키를 안전하게 분배하여야 하는 문제가 발생한다. 특히 인터넷과 같은 공개된 네트워크에서는 암호 통신을 수행하고자 하는 사용자들 사이에 안전한 키 분배가 매우 어렵다는 단점이 있다. 또한 전자 상거래를 수행하기 위해서는 거래에 대한 서명 기능이 제공되어야 하지만 비밀키 암호 시스템으로는 서명 기능을 제공하지 못한다는 단점이 있다. 현재 비밀키 암호 알고리즘으로는 DES, IDEA, RC5, RC6, AES, SEED 등

이 있다[5,6].

공개키 암호 시스템은 비밀키 암호 시스템과 달리 키 쌍을 이용하여 암·복호를 수행하는 암호 시스템으로 암호에 사용되는 키와 복호에 사용되는 키가 서로 다른 비대칭 암호 시스템(Asymmetric Cipher System)이다. 키 쌍은 누구든지 사용할 수 있도록 공개하는 공개키(Public Key)와 자신만이 비밀스럽게 보관하는 개인키(Private Key)로 구성된다. 공개키로 암호화한 데이터는 비밀키를 가진 사용자만이 복호할 수 있으며 비밀키를 이용하여 암호화한 데이터는 공개키로 복호화할 수 있다. 따라서 사용자가 자신의 비밀키로 데이터에 대한 암호뿐만 아니라 사용자 자신에 대한 유일성을 증명하여 서명기능도 제공하게 된다. 이러한 특성으로 공개키 암호 시스템은 전자상거래에서 중요한 거래에 대한 서명 기능을 제공할 수 있다. 키쌍 중에서 공개키는 일반에게 공개하는 것이기 때문에 비밀키 암호 시스템의 키 분배 문제가 해결된다. 또한 키 관리가 쉽다는 장점이 있다. 즉 n명이 서로 암호화 통신을 하기 위해서는 비밀키 암호 시스템의 경우 n(n-1)/2 개의 키가 필요한 반면에 공개키 암호 시스템의 경우에는 n개의 키만 필요하다는 장점을 가지고 있다. 그러나 비밀키 암호 시스템에 비해 구현이 어렵고 속도가 느리다는 단점이 있다. 현재 공개키 암호 시스템에는 RSA, DSA, KCDSA 등이 있다[5,6].

따라서 일반적으로 데이터를 암호화할 때는 속도가 빠른 비밀키 암호시스템을 이용하고 데이터를 암호화하는데 사용된 키를 암호화하거나 거래에 대한 서명을 생성할 때는 공개키 암호시스템을 이용하여 송수신 데이터의 보안을 유지한다.

2.2 PKI 개념

공개키를 이용하여 정보보호를 수행하기 위해서는 공개키의 소유주가 합법적인 사용자이며 공개키에 대응되는 개인키를 가졌다는 것을 입증하는 것이 필요하다. 이것은 공개키 시스템을 이용하여 전자거래의 안전성과 신뢰성을 얻을 수 있는 근거가 된다. 이러한 공개키와 공개키 소유주의 정당성에 대한 인증은 신뢰할 만한 제 3자(Trusted Third Party)인 인증기관(Certification Authority)에서 수행한다. 인증기관은 사용자의 공개키에 대한 인증서를 발급하여 사용자가 공개키에 대한 정당한 소유주이며 공개키에 대응되는 비밀키를 소유하는 것을 입증하고 이를 인증서 형식으로 표현한다. 일반적으로 인증서는 X.509[7] 형식을 따른다.

PKI는 이와 같이 공개키의 인증문제를 해결하여 정보의 기밀성, 접근제어, 무결성, 인증, 부인봉쇄를 제공하는 기반구조이다. PKI는 공개키에 대한 인증서를 발급하는 인증기관과 사용자에게 인증서 발급 요청을 등록하고 신원 확인 기능을 수행하는 등록기관 그리고 인터넷 상의 다양한 사용자와 응용이 인증기관에서 발급한 인증서를 쉽게 검색할 수 있도록 인증서를 저장 관리하는 디렉토리 서버로 구성된다. 다양한 응용에서 공개키를 이용하여 서명을 생성하고 검증하며 데이터에 대한 암·복호를 수행할 수 있는 보안 툴킷을 제공한다. 또한 인증서 발급 정책과 관리 정책 등을 포함하고 각각의 시스템 컴포넌트간의 통신 프로토콜을 정의한다.

다음 (그림 1)은 PKI가 다양한 전자상거래에서 사용되는 환경을 보인다.

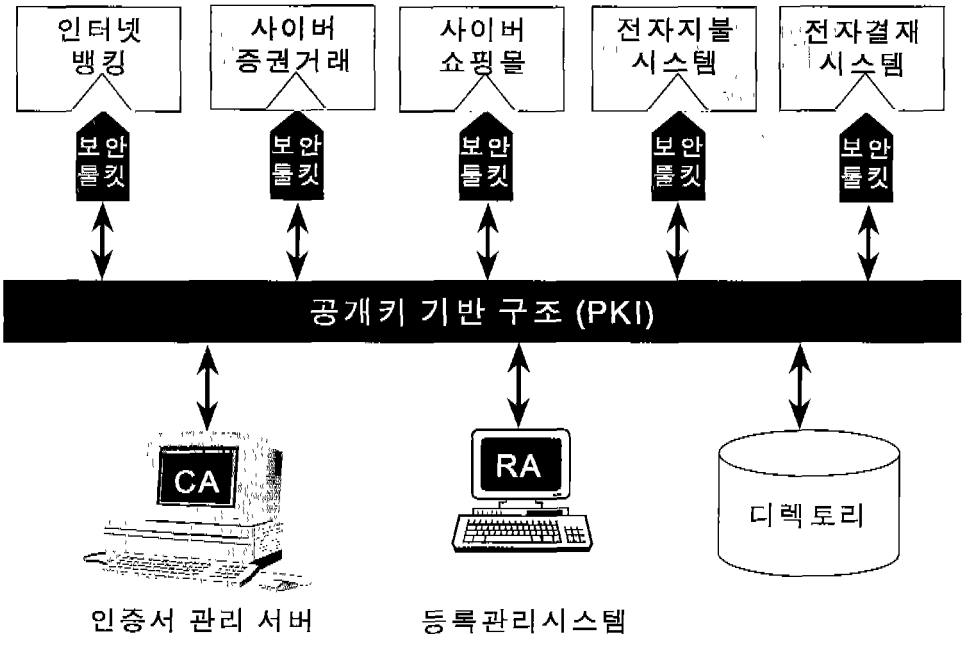

그림 1. PKI를 이용한 전자상거래 정보보호 환경

3. PKI 연구 개발 현황

국내의 PKI에 대한 연구는 최근에서야 진행되어 아직 초보적인 단계로 일부 업체에서 인증기관을 운용할 수 있는 인증서버 위주의 제품을 출시하고 있다. 이들 제품은 인터넷 쇼핑몰, 인터넷 뱅킹, 사이버 증권 등에서 사용되고 있다. 그러나 다양한 PKI 컴포넌트와 프로토콜의 지원이 미약해 아직까지 전반적인 PKI로서의 기능 제공이 미흡한 실정이다.

국외의 경우 PKI는 정부차원에서 연구개발이 시작되었으며 일부 업체에서 PKI 제품군을 출시하고 있다. 미국의 경우 정부차원에서 PKI인 FPKI (Federal PKI)를 구축하고 있다. FPKI는 NIST(National Institute of Standards and Technology)에서 주도적으로 개발하고 있다. 캐나다의 경우 GOC PKI를 구축하고 있으며 연방 정부 각 부처들로 구성된 PKI 추진팀을 주축으로 하고 있다. 유럽에서는 유럽전체를 하나의 공개키 기반시스템으로 묶기 위한 시도로 ICE-TEL PKI를 구축하고 있다[6]. 일반 업체로는 Entrust [8]와 CyberTrust[9]에서 PKI 제품군을 개발하고 있으며 Verisign[9]사의 경우에는 인증기관업무를 대행해주고 있다.

또한 PKI에 대한 필요성이 증대됨에 따라 IETF에서는 PKIX(Public Key Infrastructure X.509) Working Group을 운용하며 PKI 각 컴포넌트의 기본 기능과 통신 프로토콜에 대한 표준을 제정하고 있다.

4. ETRI CMS

4.1 시스템 구성

ETRI CMS는 공개키를 기반으로 정보보호를 제공하는 PKI 시스템이다. ETRI CMS은 다음

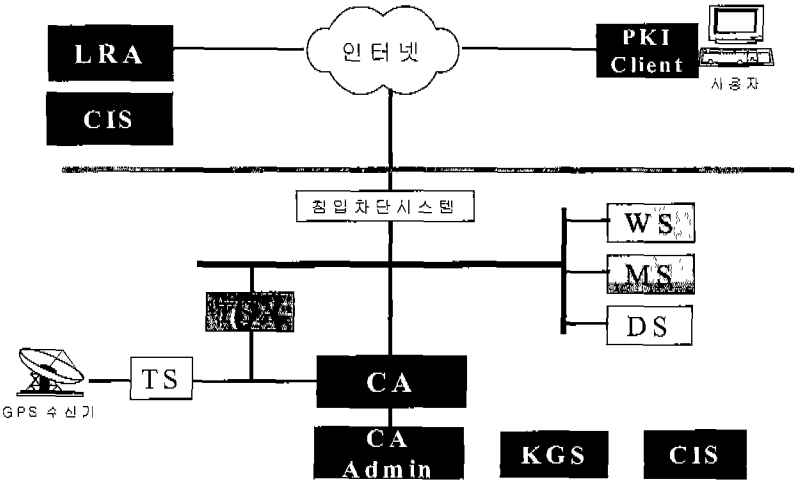

그림 2. ETRI CMS

(그림 2)와 같은 시스템 컴포넌트로 구성된다.

CIS(Card Issuing System)는 인증서의 저장 매체인 IC Card 발급기능을 수행하는 시스템이며 KGS(Key Generation System)는 ETRI CMS를 구성하는 CA와 운영자의 키 쌍을 생성하는 키 생성시스템이다. 인증기관은 CA와 CA Admin으로 구성된다. CA(Certification Authority)는 인증서 발급, 갱신, 정지, 폐지 등과 같은 인증서 라이프 싸이클을 관리하고 인증기관, 등록기관, 사용자에 대한 정보를 관리한다. CA Admin은 CA에 대한 관리 기능을 수행한다. LRA(Local Registration Administrator)는 사용자의 인증서 발급 요청 접수를 대행하며 사용자의 신원확인을 수행하는 등록관리 시스템이다. PKI Client는 사용자가 자신의 공개키쌍을 생성하고 인증서 발급을 CA에 요청하고 발급된 인증서를 관리하는 기능을 제공한다. WS는 웹을 통해 CA에 접근할 수 있도록 하는 웹 서버이며 MS는 메일 관리를 수행한다. DS(Directory Server)는 인증기관에서 발급한 인증서와 인증서 폐지목록을 게시하여 인터넷 상에서 사용자와 응용들이 이를 접근할 수 있도록 한다. TSA(Time Stamping Authority)는 인증서로 보호되는 트랜잭션에 Time Stamping을 제공하는 시스템이다. TS(Time Server)는 GPS를 통해 국제 표준시를 제공하는 시스템이다.

4.2 시스템 구성 요소

■ CIS

ETRI CMS는 인증서와 개인키의 저장 매체로 IC Card를 지원하며 시스템의 접근제어용 키의 저장매체로 IC Card를 사용한다. 이는 IC Card가 기존의 플로피 디스크 장치에 비해 매체 접근시 패스워드를 통한 인증 기능을 제공하는 등 향상된 보안기능을 제공하기 때문이다. CIS는 IC Card의 EPROM 세그먼트를 적절히 할당하여 초기화하는 기능을 제공한다. 또한 시스템 접근에 대한 감사기록 및 조회 기능을 제공한다.

■ KGS

KGS는 인증기관, 인증기관 관리자, 등록기관 관리자에 대한 키를 생성하는 시스템이다. 인증기관의

경우 접근제어 기능이 매우 중요하다. 이를 위해 KGS는 secret sharing 알고리즘을 통한 접근제어를 제공한다. 즉 m out n key splitting으로 인증기관 접근제어 키를 생성하였다면 이것은 n개의 키를 생성하여 각각 n개의 IC Card에 저장하고 이 중 m개 이상의 키가 모였을 경우에만 시스템의 접근을 허용하는 기능이다. KGS는 공개키쌍 생성 기능과 생성된 키의 무결성을 보장하는 기능을 제공한다. 또한 시스템 자체에 대한 위변조 및 삭제 감시 기능을 제공하며 인증기관, 등록기관 운영자에 대한 시스템 접근제어용 키 쌍을 생성 기능을 제공한다. 또한 감사기록 및 보존기능을 제공한다.

■ CA

CA는 PKI의 핵심 구성요소로 인증서의 발급, 갱신, 정지, 폐지 등의 인증서 라이프 싸이클 관리 기능을 제공하고 인증기관, 등록기관, 사용자에 대한 정보를 관리한다. CA는 인증서의 형식 및 관리에 있어 IETF RFC 2459 Certificate and CRL Profile[11]을 준용한다. 또한 인증서 발급 요청 양식은 IETF RFC 2511 Certificate Request Message Format[12]과 PKCS#10 Certification Request Syntax Standard[13]을 지원한다.

CA에서 제공하는 주요 기능은 다음과 같다.

- X.509 버전3 인증서 생성 기능
- X.509 버전2 인증서 폐지목록 생성 기능
- 인증서 정책 등록 및 관리 기능
- LDAP을 이용한 디렉토리 서버 접근 기능
- 전자서명 검증키에 대한 전자서명 생성키 소유 확인 기능
- 감사기록 및 보존 기능
- 역할기반 운영자 접근제어 기능
- 소프트웨어 위·변조 감지 기능

■ CA Admin

CA Admin은 CA에 대한 운영자 인터페이스를 제공한다. CA 운영자는 CA Admin을 통해 CA를 관리한다. CA Admin은 인증기관의 정책관리, 디렉토리 서버 운영관리, 패스워드 정책 등을 관리한다. 또한 CA, LRA 운영자와 사용자를 관리하며 CA의 감사기록을 관리한다. 인증서 폐지목록관리 기능도 지원한다. 인증서 관리 시스템의 구성은 (그림 3)과 같다.

■ LRA

LRA는 사용자의 신원확인을 통해 사용자 정보를 등록하고 인증서 발급인가를 CA에 요청하는 시스템이다. 발급 요청이 인가되었을 경우에는 사용자에게 참조번호(Reference Number)와 인가 코드(Authentication Code) 형식의 패스워드를 제공하여 향후 사용자가 CA에서 인증서를 발급받을 때 사용자 자신을 인증할 수 있도록 한다. LRA는 CA의 등록 기능을 대행하여 CA의 부하를 줄여 전체 시스템의 효율을 높일 수 있으며 사용자가 CA와 지역적으로 멀리 떨어져 CA에 직접 등록할 수 없는 경우에 사용될 수 있는 시스템이다.

LRA의 주요기능은 다음과 같다.

- 사용자 등록 기능
- 사용자 인증서 발급 요청 기능
- 사용자 인증서 효력정지, 회복, 폐기 기능
- 사용자 등록 정보 변경 기능
- 조회 및 통계 보고서 생성 기능
- 소프트웨어 위·변조 감지 기능

■ PKI Client

PKI Client는 등록기관을 통해 인증서 발급 요청을 인가받은 사용자가 CA에 인증서 발급을 요청하여 인증서를 발급받을 수 있는 기능을 제공한다. 또한 인증서의 갱신과 인증서의 일시 정지 그리고

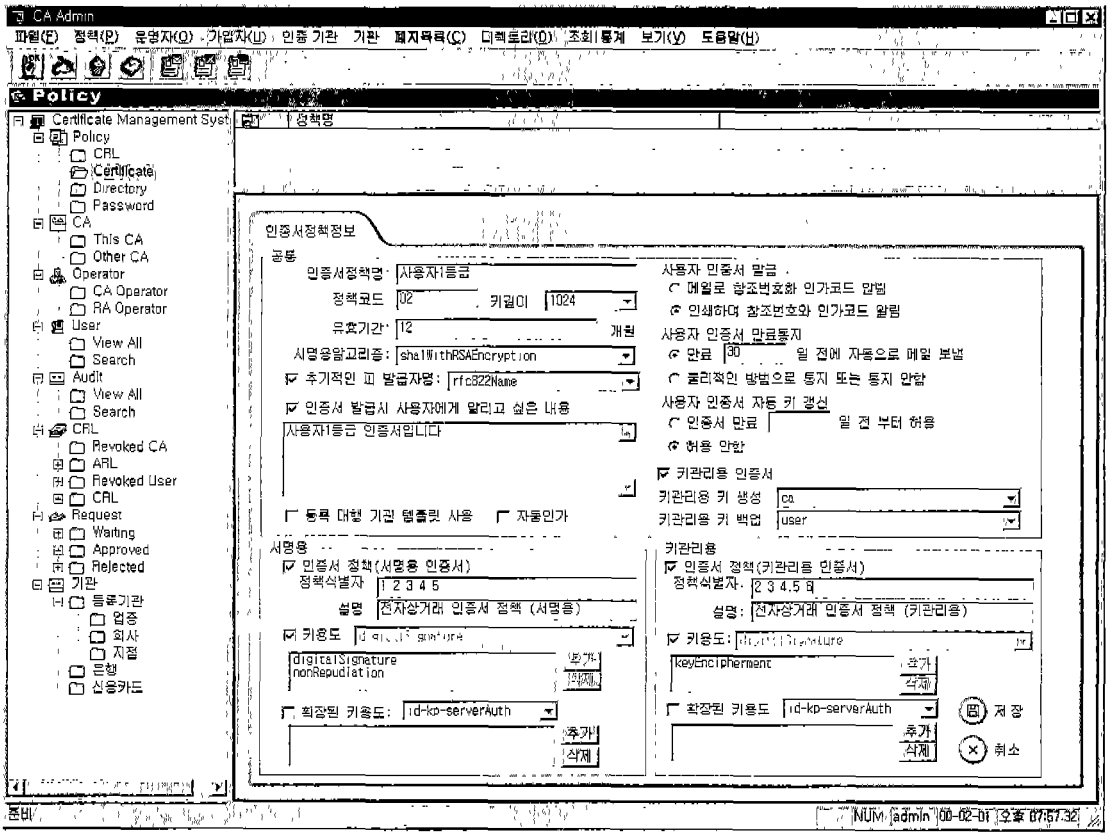

그림 3. CA Admin

인증서 폐지를 CA에 요청할 수 있는 기능을 제공한다. PKI Client와 CA간의 메시지 전송 프로토콜은 IETF RFC 2510 CMP(Certificate Management Protocol)[14]을 준용한다.

PKI Client가 제공하는 주요 기능은 다음과 같다.

- 인증서 발급, 갱신, 폐지 및 효력 정지
- IC Card를 사용한 사용자 전자 서명키 및 인증서 관리
- 인증서 백업 기능
- 전자 서명 및 암호 서비스 제공

■ DS

인증기관에서 발급한 인증서는 인터넷 상에서 불특정 다수의 사용자와 응용에게 공개되는 정보이다. DS는 인증기관의 인증서, 인증서 폐지목록, 사용자의 인증서, 인증서 폐지목록을 게시하여 일반 응용과 사용자가 접근할 수 있도록 한다. DS는 LDAP (Lightweight Directory Access Protocol)을 이용하여 접근할 수 있다.

■ 그외 시스템 컴포넌트

Mail Server는 사용자에게 인증기관의 공지사항을 전달하거나 인증서 만료를 알려 사용자가 인증서 갱신을 요청할 수 있도록 메일을 전달하는 기능을 수행한다. Web Server는 사용자가 웹을 통해 PKI Client를 다운받을 수 있도록 한다. 또한 웹 브라우저를 통해 CA에게 직접 인증서 발급 요청을

등록하고 인증서를 발급받을 수 있는 기능을 제공한다. TSA는 인터넷 트랜잭션에서 인증서를 사용할 경우 트랜잭션의 발생 시간을 공증해 주는 TTP (Trust Third Party) 기능을 수행하는 시스템이다.

보안 툴킷은 인증서를 이용하여 다양한 응용들이 보안업무를 수행할 수 있는 기능을 제공한다. 보안 툴킷은 암호 알고리즘으로 구성된 Crypto API와 인증서에 관련된 기능을 수행하는 Certificate API로 구성된다. Crypto API는 서명, 해쉬, 키분배 등과 같은 공개키 관련 암호 알고리즘과 비밀키 암호 알고리즘을 구현한 툴킷이다. Crypto API는 TOG(Tho Open Group)의 CDSA(Common Data Security Architecture)[15] 2.0을 준용하는 API를 구성하여 이식성을 높였다. Certificate API는 응용에서 서명, 검증, 암호, 복호를 수행할 수 있도록 제공된 라이브러리로 암·복호, 서명 검증에 사용되는 메시지 형식은 PKCS #7 Cryptographic Message Syntax[16]을 지원한다. 또한 인증서의 검증은 RFC 2459의 경로검증 알고리즘을 따른다.

4.3 ETRI CMS 지원 표준

ETRI CMS는 다양한 표준을 준용하여 구현한 PKI 시스템이다. 또한 다양한 암호 알고리즘을 지원하여 여러 응용 환경에서 활용될 수 있는 시스템

표 1. ETRI CMS 준용 표준 및 기술 비교

구 분		Federal PKI	Canada PKI	Entrust	CyberTrust	ETRI
Crypto Library	서명 알고리즘	RSA DSA El Gamal	RSA DSA	RSA DSA	RSA DSA	RSA DSA KCDSA
	해쉬 함수	MD5 SHA SHA-1	MD2 MD5 SHA-1	MD5 SHA-1	MD2 MD5 SHA-1	MD2/4/5 SHA/SHA-1 RIPEMD-160 HAS-160
	키 분배 알고리즘	Diffie Hellman KEA RSA	Diffie Hellman RSA	Diffie Hellman RSA	RSA	Diffie Hellman RSA
	암호 알고리즘	DES SKIPJACK IDEA 3-DES RC4/5	DES CAST 3-DES RC2	DES CAST 3-DES RC2	?	DES 3-DES IDEA RC2/4/5 Blowfish SEED
Crypto API		GSS-API GSS-IDUP	GSS-API GSS-IDUP	GSS-API GSS-IDUP PKCS#11	?	CSP/CDSA
Directory API		LDAP DAP	LDAP DAP	LDAP DAP	LDAP	LDAP (RFC2559)
Certificate API		CSSM/CDSA PKIX-Profile (RFC2459)	PKIX-Profile (RFC2459)	CMS-API PKIX-Profile (RFC2459)	PKIX-Profile (RFC2459)	CSSM/CDSA PKIX-Profile (RFC2459)
Data Formatting		ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690
Certificate & CRL Format		PKIX-Profile (RFC2459) ITU-T X.509	PKIX-Profile (RFC2459)	PKIX-Profile (RFC2459) ITU-T X.509	PKIX-Profile (RFC2459) SET 1.0	PKIX-Profile (RFC2459)
Certificate Transfer		PKIX-CMP (RFC2510) MISPC	PKIX-CMP (RFC2510) MISPC	PKIX-CMP (RFC2510)	PKIX-CMP (RFC2510)	PKIX-CMP (RFC2510)

이다. 다음 〈표 1〉은 ETRI CMS에서 준용하는 표준과 지원하는 기술을 국외의 PKI와 비교한 것이다.

4.4 ETRI CMS 활용 현황

국내에서는 전자상거래가 활성화되면서 이를 뒷받침하기 위해 1999년 7월에 전자서명법이 공표되었고 인증서를 이용한 전자상거래의 법적인 보호를 위해 공인인증기관을 지정하고 있다. 국내에서 공인인증기관의 루트는 한국정보보호센터에서 맡고 있으며 정보인증, 금결원, 증권전산이 공인인증기관을 신청한 상태이다. 2000년 2월 현재 이들 중 정보인증주식회사와 증권전산은 공인인증기관으로 지정받았으며 금결원은 현재 실사가 진행중이다. ETRI CMS는 이들 중 금결원 CA, 증권전산 CA 시스템으로 구축되어 있다. 또한 ETRI CMS는 시큐어소프트㈜, 소프트포럼㈜, 이니텍 등 인증 기관 서버 개발 관련 국내 7개 업체에 기술 전수를 통해 국내 인증시스템의 기술표준 및 상호연동 기술을 지원하고 있다.

5. 결 론

인터넷의 급격한 확장에 따른 전자상거래는 기존의 전통적인 상거래의 많은 부분을 대체해 나갈 것이다. 현재 사용되고 있는 인터넷 쇼핑몰, 사이버뱅킹, 사이버 증권 등의 전자상거래는 향후 그 영역을 더욱 확장해 나갈 것이다. 이러한 전자상거래가 안전성과 신뢰성을 확보하기 위한 핵심 보안 기술인 PKI는 앞으로 전자정부 및 전자상거래 전반의 응용환경에서 정보보호의 기반구조로서 그 활용의 폭을 더욱 넓혀갈 것이다. 또한 현재 유선 인터넷 환경을 기반으로 구성되어진 PKI는 향후 무선 인터넷 환경의 정보보호 기반구조로 그 영역을 더욱 확장해 나갈 것이다.

※ 참고문헌

[1] W. Ford, M. S. Baum, Secure Electronic Commerce, Prentice Hall, 1997

[2] 권용진, 김정선, 전자상거래의 보안, 한국통신학회지, Vol. 16 No. 11, pp.2945, 1999

[3] J. Feghhi, P. Williams, J. Feghhi , Digital Certificate : Applied Internet Security, Addison-Wesley , 1998

[4] Abner H. Germanow, PKI: Nothing But Pilots?, International Data Corporation, December 1999

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 1998

[6] 이만영, 김지홍, 류재철, 송유진, 영홍열, 이임영, 전자성거래 보안 기술, 생능 출판사, 1999

[7] ITU-T Recommandation X.509(1997) ISO/IEC 9594-8:1997, Information Technology Open System Interconnection The Directory : Authentication Framework, 1997

[8] Entrust, http://www.entrust.com, 2000

[9] Cybertrust, http://www.gte.com, 2000

[10] Verisign, http://www.verisign.com, 2000

[11] RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF PKIX Working Group, January, 1999

[12] RFC 2511, Internet X.509 Certificate Request Message Format, IETF PKIX Working Group, March 1999

[13] PKCS#10, Certificate Request Syntax Standard, RSA, 1993

[14] RFC 2510, Internet X.509 Public Key

Infrastructure Certificate Management Protocols, IETF PKIX Working Group, March 1999
[15] CDSA 2.0, Common Security: CDSA and CSSM , The Open Group, 1999
[16] PKCS#7, Cryptographic Message Syntax Standard, RSA, 1993

조 영 섭

1993 인하대학교 전자계산공학과 학사
1995 인하대학교 전자계산공학과 석사
1999 인하대학교 전자계산공학과 박사
1998~ 현재 한국전자통신연구원 정보보호기술연구본부

윤 이 중

1988 인하대학교 전산과 학사
1990 인하대학교 전산과 석사
1997~현재 충남대학교 컴퓨터괴학과 박사과정
1990~1999 한국전자통신연구원 부호기술연구부
1999~2000 한국전자통신연구원 정보보호기술연구본부 인증기반팀장
2000~현재 한국전자통신연구원 정보보호기술연구본부 정보보호시스템연구부장

진 승 헌

1993 숭실대학교 전자계산학과 학사
1995 숭실대학교 전자계산학과 석사
1994~1996 대우통신 종합연구소
1996~1999 삼성전자 통신연구소
1999~현재 한국전자통신연구원 정보보호기술연구본부

조 현 숙

1979년 전남대학교 수학교육과(학사)
1991년 충북대학교 대학원 전산학과(석사)
1999년 충북대학교 대학원 전산학과(박사과정수료)
1992년 충북대학교 전산학과 시간강사
1982년~현재 한국전자통신연구원 책임연구원 정보보호기술연구본부장