



이재일

한국정보보호센터 사업부 인증관리팀 선임연구원

1. 서론

글로벌(Global)한 전자상거래 환경의 구축을 위하여 전 세계적으로 인증기술 및 이의 응용에 대한 표준 및 기술규격의 정립이 활발히 진행중에 있으며, 동시에 각각의 요소기술에 대한 표준화가 이루어지고 있다.

네트워크 레벨에서의 인증 관련기술은 SSL(Secure Socket Layer)에서 점차 IPSec(IP Security)과 TLS(Transport Layer Security)로 표준화가 진행중이며, 애플리케이션 레벨에서의 인증 관련기술은 X.509가 핵심으로 자리를 잡았

다. 보안 API로서는 GSS-API 및 CDSA가 표준 보안 API로 각광을 받고 있고, 인증기술의 응용분야에서는 S/MIME, PGP 및 SET이 점차 사실상의 표준으로 자리를 잡아가고 있다.

기반기술 레벨에서의 인증 관련기술 중에 전자서명 알고리즘은 RSA가 가장 널리 쓰이고 있으며, ECC(Elliptic Curve Cryptography)가 RSA의 향후 대안으로 각광을 받고 있다. 암호 알고리즘으로는 그동안 DES가 가장 널리 쓰여 왔지만, 현재 NIST에서 공모를 하고 있는 AES(Advanced Encryption Standard)로 대체될 것으로 전망되고 있다.

[표 1] 전자서명 인증관련 보안기술 표준화 추진현황

	~ 1998	1999 ~ 2001	2001 ~ 2003	2003 ~
네트워크 보안표준				
SSL	○			
SHTTP				
TLS				○
IPv6/IPSec			○	
애플리케이션 보안표준				
CAPI			○	
CDSA			○	

	~ 1998	1999 ~ 2001	2001 ~ 2003	2003 ~
GSSAPI		○		
X.509		○		
S/MIME		○		
PGP	○			
SET				○
기반기술 보안 표준				
RSA		○		
ECC		○		
DES	○			
3DES		○		
AES			○	

2. 국외 전자서명 인증기술 표준화 동향

현재, 전 세계적인 공개키 기반구조의 구축 및 상호인증을 위한 국제적인 노력의 일환으로 각종 인증관련 표준 및 기술규격이 개발중에 있으며, 대표적인 것이 ITU-T X.509, ISO/IEC JTC1/SC27, ETSI, ANSI, IETF PKIX, PKCS (Public Key Cryptography Standard) 및 FIPS (Federal Information Processing Standard) 시리즈가 있다. 이들은 보안 알고리즘 및 API (Application Protocol Interface), 인증서 및 인증서 폐지목록 규격, 인증서 운영·관리 프로토콜 등을 정의하고 있다.

2.1 ITU-T 표준화 동향

ITU-T(International Telecommunication Union-Telecommunication) X.509는 인증 서비스 제공을 위한 하부구조를 정의하고 있으며, 세부사항으로는 공개키 인증서 형식(프로파일은 정의하고 있지 않음)과 인증절차(authentication procedure)를 정의하고, PKI(Public Key Infrastructure) 구조를 제시하고 있다. ITU-T X.509에서 제시하는 주요 표준은 인증서 및 인증서 폐지목록(Certificate Revocation List) 규격

이며, 인증서는 버전 3(표준영역 및 확장영역을 정의), 인증서 폐지목록은 버전 2까지 발표된 상태이다.

[표 2] ITU-T X.509 프로파일 발전과정

1988	○ X.509 버전 1 발표
1993	○ X.509 버전 2 발표 ○ PEM에서 사용(RFC 1422)
1994	○ ISO/IEC와 ANSI9에서 X.509 v2에 대한 개선착수
1996. 6	○ 최종적인 X.509 버전 3을 위한 표준확장 개정

2.2 ISO/IEC 표준화 동향

ISO/IEC JTC1/SC27은 TTP(Trusted Third Party) 관련문서에서 전자서명에 필요한 TTP 서비스규격 및 인터페이스, 타임스탬프 모델과 서비스를 정의하고 있다.

ISO/IEC JTC/SC27에서 발표한 X.509와 관련한 표준 문서로는 “Guidelines on the use and management of Trusted Third Party services [ISO/IEC 14516, 1999.5]”와 “Specification of TTP services to support the Digital Signature [ISO/IEC 15945, 1998.11]”로 이들 문서는 X.509에 기반하고 있으며, 전자서명에 관련된 TTP의 관리, 역할 및 사양 등을 정의하고 있다.

[표 3] ISO/IEC JTC1/SC27의 TTP

<p>Requirements for the use and management of Trusted Third Party services (ISO/IEC 19878)</p> <ul style="list-style-type: none"> • TTP의 관리 • TTP의 구조적 특성 • TTP응용과 관련된 문제 	} X.509 기반
<p>Specification for TTP services to support the Digital Signature (ISO/IEC 19879)</p> <ul style="list-style-type: none"> • 디지털 서명의 응용에 필요한 TTP 서비스 규격 정의 • TTP 서비스에 연관된 구성요소 간의 상호운용을 가능하게 하는 인터페이스 및 프로토콜 정의 • TTP 서비스와 관련된 상업적 응용의 구현 지원 	
<p>TTP Support Protocols (ISO/IEC 19880)</p> <ul style="list-style-type: none"> • 타임 스탬프 서비스 포맷 정의 • 타임 스탬프 프로토콜 정의 	

2.3 ETSI 표준화 동향

ETSI(European Telecommunication Standard Institute)는 ISO/IEC 표준과 유사하며, 1997년 7월과 10월에 각각 “Requirements for TTP services”와 “Specification for TTP services”를 표준 문서로 발표하였다. Requirements for TTP services는 TTP의 기능 및 서비스에 대한 요구사항을 정의하고 있으며, TTP의 기능에 관용키 생성 및 분배도 포함하고 있다. Specification for TTP services에서는 TTP 구조 및 서비스규격을 정의하고 있는데, 이는 X.509를 기반으로 하고 있으며, TTP의 키관리 및 키복구 기능을 강조하고 있다.

2.4 ANSI 표준화 동향

ANSI(American National Standard Institute)는 공개키 알고리즘 관련 표준화를 추진하고 있으며, DSS, RSA 및 인증서 확장영역과 인증서 관리부분 등을 정의하고 있다.

ANSI의 공개키 관련표준은 일반적으로 X9 시리즈로 불리우며, 전자서명 알고리즘 표준(DSS 및 RSA는 표준화됨, Elliptic Curve 전자서명 표준화는 진행중 임)과 인증서 확장영역 및 관리부분에서 X.509의 표준을 준용하는 형태로 표준화가 진행중이며 특히, 인증서 관리부분은 IETF의 CMP(Certificate Management Protocol)를 준용하는 표준화(X9.77)를 진행중에 있다.

특히 ANSI X.509의 형태가 아닌 인증서의 활용부분(Non-X.509)에도 관심을 갖고 있으며, 이에 대한 표준화(X9.68)를 진행중이다.

2.5 IETF PKIX 표준화 동향

IETF(Internet Engineering Task Force) PKIX(Internet X.509 Public Key Infrastructure) 워킹그룹은 인터넷환경에서 PKI 기반구조를 구축·운영하기 위하여 1994년 구성된 인터넷표준 단체이며, 인터넷환경에서의 X.509 표준화를 진행중이다.

PKIX가 추진하는 표준은 크게 5개의 파트로

[표 4] ANSI 전자서명 인증기술 표준화 현황

X9.30	Digital Signature Standard - NIST DSS(1997년)
X9.31	RSA Signature(1998년)
X9.55	Certificate Extensions(X.509 기반)(1997년)
X9.57	Certificate Management(X.509 기반)(1997년)
X9.62	Elliptic Curve Digital Signature(진행중)
X9.68	Short Certificates for High Volume System(non-X.509)(진행중)
X9.77	public Key Infrastructure Management Protocol(IETF PKIX의 Certificate Management Protocol 수용)(진행중)

[표 5] IETF PKIX RFC 표준화 추진 현황

Part 1 (인증서 및 인증서 폐지목록 프로파일)	Internet X.509 Public Key Infrastructure Certificate and CRL Profile(RFC 2459)(1999. 1) Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates(RFC 2528)(1999. 3)
Part 2 (운영 프로토콜)	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2(RFC 2539)(1999. 4) Internet X.509 Public Key Infrastructure LDAPv2 Schema(RFC 2587)(1999. 6) Internet X.509 Public Key Infrastructure Operational Protocols- FTP and HTTP(RFC 2585)(1999. 5) X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP(RFC 2560)(1999. 6)
Part 3 (관리 프로토콜)	Internet X.509 Public Key Infrastructure Certificate Management Protocols(RFC 2510)(1999. 3) Internet X.509 Certificate Request Message Format(RFC 2511)(1999. 3)
Part 4 (인증 정책)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework(RFC 2527)(1999. 3)
Part 5 (타임 스탬프 및 이터 인증 서비스)	No RFCs

구성된다. 제1파트에서는 인증서 및 인증서 폐지목록 프로파일을 RFC 2459에서 정의하고 있으며, 제2파트에서는 신뢰 당사자가 인증서 또는 인증서 상태 정보를 알 수 있게 해주는 운영 프로토콜을 RFC 2259, RFC 2560, RFC 2585, RFC 2587에서 정의하고 있다.

제3파트에서는 PKI 관리를 위하여 필요한 정보를 주고받을 때 이용되는 관리 프로토콜을 RFC 2510에서 정의하고 있으며, 제4파트에서는 인터넷기반의 PKI에서 요구되는 인증서 정책 및 인증 업무준칙의 프레임워크를 RFC 2527에서 정의하고 있다.

최근에 PKIX에서는 제5파트를 표준에 추가하였고, 그 내용으로는 타임스탬프 및 데이터 인증서비스에 대하여 정의하고 있으며, 인터넷 드래프트 상태이다.

2.6 PKCS 표준화 동향

PKCS(Public-Key Cryptography Standard)는 RSA 알고리즘의 구현 방법론과 여러 가지 구분표현을 정의한 것이며 현재 전 세계적으로 가장 많이 이용되고 있는 표준으로 1991년 3월 NIST/OSI Implementor's Workshop에서 문서 SEC-SIG-91-16으로 발표된 이후, 1993년 11월 1일 많은 수정을 거친 후 일관성 있는 문서방식으로 개선되어 발표되었고, 이후 지속적으로 갱신중이다. 이 중에서 전자서명 인증기술과 관계가 있는 것은 PKCS #1, PKCS #7, PKCS #10 등이다.

2.7 FIPS 표준화 동향

FIPS는 NIST에서 주관하고 있는 미연방 자동정보처리 시스템에서의 표준으로서 전자서명

인증기술과 관련된 표준으로는 전자서명 알고리즘 및 표준을 정의하고 있는 FIPS 186-1(Digital Signature Standard)이며 이는 DSA와 RSA 전자서명 알고리즘을 정의하고 있다. 최근에는 Elliptic Curve 전자서명 알고리즘이 포함된 FIPS 186-2를 발표하였으며, 2000년 6월 27일부터 효력이 발생한다.

이외에도 FIPS 180-1(Secure Hash Standard)은 해쉬 알고리즘을 정의하고 있으며, FIPS 140-1(Security Requirements for Cryptographic Modules)는 전자서명 모듈의 안전성에 대한 표준을 정의하고 있으며, 다음장 [표 7]은 FIPS 140-1을 요약한 내용이다.

3. 국외 시점확인 기술 표준화 동향

시점확인 기술과 관련한 국제표준은 현재 없으나 IETF PKIX 및 ISO/IEC JTC1/SC27에서 표준화를 위하여 추진중이며 시점 확인 서비스 기술은 PKI, 공증, 전자상거래 등의 기반기술로서 지속적으로 발전할 것이다.

[표 6] PKCS 표준

구분	제목	버전	일시
PKCS # 1	RSA Encryption Standard	2.0	1998. 10
PKCS # 3	Diffie-Hellman Key-Agreement Standard	1.4	1993. 11
PKCS # 5	Password-Based Encryption Standard	2.0	1998. 10
PKCS # 6	Extended-Certificate Syntax Standard	1.5	1993. 11
PKCS # 7	Cryptographic Message Syntax Standard	1.5	1993. 11
PKCS # 8	Private-Key Information Syntax Standard	1.2	1993. 11
PKCS # 9	Selected Attribute Types	1.1	1993. 11
PKCS #10	Certification Request Syntax Standard	1.0	1993. 11
PKCS #11	Cryptographic Token Interface Standard	2.1	1997. 12
PKCS #12	Personal Information Exchange Syntax Standard	1.0	1997. 4
PKCS #13	Elliptic Curve Cryptography Standard	Project	진행중
PKCS #14	Pseudorandom Generator Standard	Project	진행중
PKCS #15	Cryptographic Token Information Format Standard	1.0	1999. 4

[표 7] FIPS표준화 동향

요구사항	보안등급 1	보안등급 2	보안등급 3	보안등급 4
암호 모듈	암호 모듈과 암호 경계 명세. 모든 하드웨어, 소프트웨어 및 펌웨어 요소를 포함하는 암호 모듈에 대한 설명. 모듈 보안정책에 대한 설명			
모듈 인터페이스	필수 및 선택적 인터페이스. 모든 인터페이스와 모든 내부 데이터 경로 명세		중요한 보안 매개변수용 데이터 포트를 다른 데이터 포트와 물리적으로 분리	
직무 및 서비스	필수 및 선택적 직무 및 서비스를 논리적으로 분리	직무기반 인증	ID기반 인증	
유한 상태 머신	유한상태 머신 모델 명세. 필수상태와 선택적 상태. 상태전이 도표와 상태전이 명세			
물리적 보안	기본 보안장비	(각 1호 선택) • 탭퍼 방지 코팅 • 탭퍼 방지 실링 • 기계적 락이 가능한 봉인	(각 1호 선택) • 탭퍼 방지 코팅 (등급 2보다 강한) • 제거 시 작동 불능	(각 1호 선택) • 제거가 어려운 코팅 • 탭퍼 감지 시 작동 불능
EFP/EFT	규정 없음			온도와 전압
소프트웨어 보안	소프트웨어 설계명세. 무한상태 머신모델에 대한 소프트웨어와 관련됨		고급언어 구현	공식모델. 사전상태 및 사후상태
운영체제 보안	실행 코드, 인증됨. 단일 사용자, 단일 프로세스	접근 통제 보호(C2 또는 그와 동등한 등급)	보안레이블을 이용한 보호(B1 또는 그와 동등한 등급). 안전한 통신 경로	계층 구조화된 보호(B2 또는 그와 동등한 등급)
키 관리	FIPS가 승인한 생성/분배 기법		암호화된 형태로 키를 들어감/나감, 또는 split knowledge 절차로 직접 들어감/나감	
암호 알고리즘	분류되지 않은 정보를 보호하기 위해 FIPS가 승인한 암호 알고리즘			
EML/EMC	FCC 파트 15, 하위 파트 J, 클래스 A(업무용). 적용 가능한 FCC 규정(음성용)		FCC 파트 15, 하위 파트 J, 클래스 B(가정용)	
자체 테스트	전원 공급 테스트 및 상태 테스트			

3.1 IETF PKIX 표준화 동향

- Internet X.509 Public Key Infrastructure Time Stamp Protocols
- C. Adams, P. Cain, D. Pinkas, R. Zuccherato가 제안
- 1997년 첫 번째 드래프트 제출 이후 1998년 PKIX 작업반에서 논의
- 현재 "draft-ietf-pkix-time-stamp-05"가 2000년 1월에 제출됨.

3.2 ISO/IEC JTC1/SC27 표준화 동향

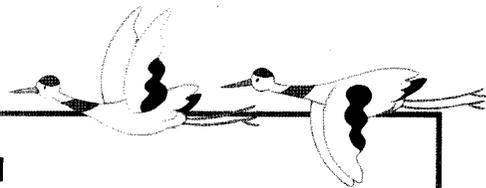
- Guidelines on the use and management of Time Stamping Services(GUMTSS)
- ISO/IEC JTC1/SC27 N2107
- Spain National Body(AENOR)가 1998년 10월에 제안
- ISO/IEC WD 18014, Information technology -Security techniques-Time stamping services
- 1998년 10월에 제안

- 2001년 11월에 IS로 추진중

4. 결론

국외 전자서명 인증기술 표준화 추진 분야 중 현재 가장 이슈가 되고있는 분야는 X.509기반의 인증서 관련 분야이다. ITU-T, ISO/IEC는 X.509 V3 인증서 및 인증서 폐지목록에 대한 표준을 정하였지만, IETF에서는 아직도 이에 대한 표준화가 진행중에 있다. 특히 X.509 V3 인증서 프로파일 중 인증서 경로 검증 부분은 계속적으로 정립이 필요한 분야이다. 이외에도 키 갱신과 같은 인증서 관리 프로토콜, 인증서 폐지목록 배포 및 검증 등의 인증서 운영 프로

토콜 부분은 끊임없이 새로운 개념이 나오고 있는 분야이기 때문에 우리나라도 이에 대한 국제표준화 추진현황을 지속적으로 파악해 나갈 필요가 있다. X.509 기반의 인증서 관련기술에 대한 새로운 표준이 계속 제안되고 있다는 것은 아직 이 분야에 대한 지배적인 기술이 나오지 않았다는 반증일 수도 있다. 국내 전자서명 인증기술은 외국과 비교해 볼 때 기술개발 능력에 있어서 별로 뒤쳐지지 않는 분야이다. 따라서 국내에서도 이에대한 관련기술을 개발하고 정립하여 국제표준으로 제안하고자 하는 노력을 아끼지 않아야 할 것이라고 생각한다. 또한 전자서명 인증기술 관련표준화 국제회의에도 적극적으로 참여하여 국제사회에서 우리의 입장을 대변할 수 있어야 할 것이다. TTA



미-EU, 전자상거래 개인정보 보호방안 합의

미국과 유럽연합(EU)이 전자상거래와 관련한 개인정보 보호에 합의했다.

「USA투데이」에 따르면 데이비드 아론 미상무부(<http://www.doc.gov>)차관과 존 모그 EU(<http://www.europa.eu.int>) 집행위원은 최근 이를 발표하고 새로운 보호방안이 오는 6월말부터 적용될 것이라고 밝혔다. 이에 따라 앞으로 유럽에서 활동하는 미 업체가 미국으로 보내는 고객들의 정보는 미국법에 의거해 그 안전성을 인정받게 된다. 또한 양지역의 전자상거래업체들은 자신들의 웹사이트를 개인정보 보호 감시기관에 등록시켜야 하며 고객들에게 개인정보가 보호되고 있음을 고지해야 한다. 새로운 법안은 일단 전자상거래업체를 대상으로 적용되며 온라인 금융기관에 대한 법안은 차후 추가로 마련될 예정이다. 양측은 또 EU의 「세이프하버(Safe Harbor)」 개념에 대해서도 합의했다. 세이프하버란 인터넷상의 정보가 제3국을 거쳐 전달될 때 경유지를 지칭하는 것으로서 EU는 중간 경유지가 최소한 EU수준의 개인정보 보호장치를 갖추도록 규정하고 있다.

개인정보 보호에 대해 기업의 역할을 중시하는 미국과 상대적으로 엄격한 법률을 시행하고 있는 유럽은 지금까지 많은 마찰을 빚어왔다. 특히 지난 '98년 EU가 유럽에 진출한 미국업체들이 고객들의 정보를 미국으로 보내는 것을 금지하는 법안을 승인하면서 이로 인한 갈등은 더욱 커져갔다.

하지만 미국과 EU의 이번 합의로 양지역간의 전자상거래는 앞으로 더욱 활기를 띠게 될 전망이다. 양측의 대표는 「개인정보 보호방안 합의가 기업에는 사업의 성공을, 시민들에게는 전자상거래에 대한 신뢰를 가져다 줄 것」이라고 말했다.