□특집□

전자상거래 인증서비스 기술

김 석 우† 서 창 호††

◈ 목 차 ◈

1. 전자상거래 동향

컴퓨터와 인터넷의 발달과 더불어 21세기 사회는 시간과 공간의 제한을 극복하고, 국경의 한계를 초월한 사이버 공간 사회로 변화되었다. 인터넷 PC나 네트워크 컴퓨터를 사용하여 사이버 공간 사회로 접속하는 전 세계 인터넷 이용자의 수도 1997년 8,600만명에서 2000년도에는 25,640만명으로 다시 2003년에는 50,240만명으로 예측하며, 전자상거래 규모도 각각 154억, 2,178억, 1조 3,173억 달러 평균 92% 성장이 예측된다.

국내 인터넷 및 전자상거래 현황 역시 1998년도 인터넷 사용자수 175만에서 2003년 923만으로 평균 25.3% 성장을 하고 전자상거래 규모는 1998년도 5,650만에서 2000년 9,133만, 2003년에 102억 9천만 달러로 평균 136.6%로 증가되리라 예측된다.

정보통신분야 시장전문 조사기관인 IDC(International Data Corporation)의 이와 같은 예측은 21세기 상거래의 상당부분이 사이버 공간에서 이루어지게 되며, 실 생활에서 발생되는 거의 모든 행위와 사

〈표 1〉 전세계 인터넷 이용자수 및 전자상거래 규모와 전망(1997~2003년)

구분 \ 연도	1997	1998	1999	2000	2001	2002	2003	성장률 (%)
인터넷 이용자수(백만)	86.8	144.2	196.1	256.4	327.3	398.6	502.4	29
전자상거래이용자수(백만)	15.0	30.8	48.0	71.5	99.7	133.9	182.6	43
전자상거래규모(10억달러)	15.45	50.43	111.36	217.81	398.12	733.63	1,317.3	92
1인당전자상거래액(달러)	1,029	1,635	2,321	3,046	3,994	5,479	7,216	35

〈표 2〉 국내 전자상거래 관련 규모와 전망 (1998~2004년)

구분 \ 연도	1998	1999	2000	2001	2002	2003	2004	성장률 (%)
인터넷이용자수(백만)	1.75	3.31	5.03	7.02	8.1	9.23	10.21	25.3
전자상거래이용자수(백만)	0.17	0.58	1.39	2.36	3.16	3.39	4.86	52.9
전자상거래이용자의비율(%)	9.7	17.5	27.6	33.6	38.8	43.0	47.6	-
전자상거래 규모(백만달러)	56.5	244.0	913 3	2,495.0	5,184,7	10,290.0	18.094.7	35

† 종신회원 : 한세대학교 정보통신학과 교수
†† 정 회 원 : 공주대학교 응용수학과 교수

건이 사이버 세상으로 옮겨 가게 됨을 의미한다. 특히 컴퓨터와 네트워크에 의하여 기업, 정부, 소비자가 서로 만나지 않고 상거래가 이루어지는 순기능의 역할과 동시에 보이지 않는 적으로 부터 동시 다발적으로 발생되는 역기능 침해를 고려하여야 만 할 것이다.

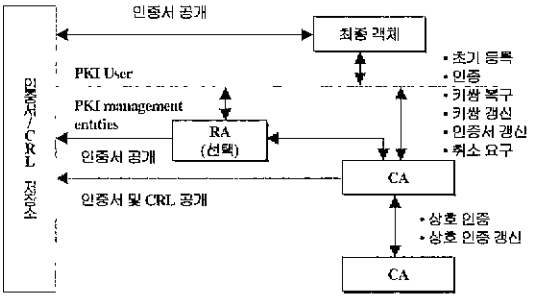
2. 전자상거래 인증서비스

2.1 인증서비스

전자상거래에 있어서 소비자가 가상상점에서 물건을 주문할 때, 소비자와 상점은 인터넷을 통하여 비대면으로 통신하게 된다. 이 때 상점과 소비자는 서로 간의 신분을 확인하거나 메시지의 변경이 없다는 메시지 무결성(Integrity)을 보장하는 인증(Authentication)서비스에 의존하게 된다. 공개키 암호 방식에서는 공개 키의 무결성을 보장하는 의미의 인증 (Certification)을 사용하는데, 이는 전자상거래에서 전자서명(Digital signature)에 의해 서비스되고 있다. 전자서명은 신뢰할 수 있는 제 3자가 (TTP:Trusted Third Party) 서명한 인증서로써 거래당사자의 신뢰를 제공하는데 이러한 제 3자의 역할을 하는 기관이 인증기관(Certification Authority)이다.

2.2 인증서비스 흐름

인터넷을 이용한 전자상거래에서 인증서비스는 필수적이다. 일반적으로 전자상거래를 구성하고 있는 주체로 고객, 쇼핑몰(판매자), 지급정보중계기관(Payment Gateway), 은행의 4 객체로 볼 수 있다. 전자상거래를 통하여 물품을 구매.지불하는 과정 중에 1) 고객이 판매자와 PG의 인증서를 수신하여 검증, 2) 판매자가 고객의 인증서를 수신 및 검증, 3) PG가 고객과 판매자의 인증서를 확인하는 단계에서 인증서비스가 사용된다. 이때에 사용되는 인증서는 국가적으로 인정된 공인인증센터가 서명하였음을 전제로 한다. 전자상거래에 참여하는 고객, 판매자, PG는 자신이 속한 인증센터가 서명한 인증서를 지니고 있어야 하며, 인증서를 검증하려는 상대방에게 제시한다. 제시된 인증서에 의해 검증작업을 거쳐 송신자의 공개 키(전자서명 검증키)를 얻게 된다.



(그림 1) 인증서 흐름

1.1.1 인증서 발급

일반적으로 인증서 발급은 지역적으로 분산된 등록기관(Registration Authority)에서 수행한다. RA는 CA를 대신하여 사용자 인증, 토큰 분배, 키 생성, 취소 보고, 키쌍 보관 등의 임무를 수행한다. 전자상거래의 인증서비스 활동에 참여하는 객체들은 등록기관에 신원을 확인할 수 있는 증명서를 제출하여 신원 확인을 득한다. 신원이 확인된 객체는 등록기관으로부터 전자서명용 키 생성 SW를 인수한다. 객체는 자신이 서명에 사용하는 전자서명생성키(Private Key)와 자신이 서명을 검증하는데 사용하는 전자서명검증키(Private Key)를 생성한다. 객체는 전자서명 검증키와 개인 정보를 담은 인증서 요청 형식(PKCS #10)을 작성하여 RA에게 발급 요청한다. RA의 요청은 CA에게 전해지고 CA가 자신의 전자서명 생성키로 요청자의 전자서명검증키에 대하여 서명함으로써 인증서를 생성한다.

객체와 등록기관 사이에 on/off-line, 전자서명키쌍(생성용 및 검증용)을 생성하는 방법에 따라

흐름 절차가 조금 다르지만, 아래에 on-line 상황에서 사용자가 키생성S/W를 이용하여 인증서를 발급 요청 및 디렉토리 저장소에 공개하는 절차를 보인다.

← 객체는 사용자 S/W를 이용, 전자 서명용 키쌍을 생성

↑ 객체가 개인정보와 전자서명 검증용 키를 인증서 요청형식(PKCS #10)을 작성하여 RA에게 전달

→ RA는 신청자인 객체의 신원 및 신용정보를 확인하여 적합한 경우 CA에게 전달

↓ CA는 신청자의 정보를 확인한 후 신청자의 전자서명 검증용 키를 서명한 인증서를 발급한다.

◦ 발급된 인증서를 디렉토리 서버에 공표하여, 차후 갱신 등에 사용. 또한, 인증서와 CA에 관한 정보를 RA에게 전달, 신청자인 객체에게 인증서 발급을 알림.

± RA는 신청자인 객체에게 인증서를 전달

〃 CA가 서명한 (전자서명 검증용 키를 담은) 인증서를 자신의 안전한 저장소에 저장

2.2.2 인증서 갱신/폐지/재발급 등

가. 인증서 갱신

인증서의 유효기간이 만료되기 전에 새로운 인증서를 발급한다. 만료된 인증서는 효력이 상실되어, 디렉토리로부터 인증서가 삭제된다. 인증서 갱신 발급 요청에 의해 신규인증서가 발급되는데, 신규 요청절차와 동일하다.

나. 인증서 폐지

CA가 발급한 인증서는 다음 사유가 발생된 경우 폐지된다. 폐지란 디렉토리로부터 인증서가 삭제되고, CRL에 등재되어 폐지가 공표된 경우이다.

← 당해 객체가 인증서 폐지를 요청하거나

↑ 부당한 방법으로 인증서를 획득하였거나

→ 당해 객체의 존재가 없어지거나 (사망 또는 파산 등)

↓ 전자서명 생성키가 안전하지 않다고 인정되는 경우

다. 재발급 등

서비스	설명
인증서 발급	전자서명 검증키에 대하여 CA가 서명하여 인증서를 생성
인증서 폐지	인증서의 효력이 취소되고, 디렉토리로부터 인증서를 삭제한 후 해당 인증서를 등재함
인증서 갱신	인증서의 유효기간이 만료되어 유효기간을 연장한 새로운 인증서를 발급, 만료된 인증서는 폐지함
인증서 재발급	유효기간이 만료되지 않은 상태에서 새로운 인증서가 발급됨. 재발급되는 인증서는 나머지 유효기간만이 부여됨.
인증서 효력 정지/회복	인증서의 사용을 일정기간 정지시킬 때, 디렉코리에서 삭제하고 인증서 정지목록(CSL)에 등재함.

3. 인증시스템

3.1 표준규격

인증서비스를 제공하기 위하여서는 공개키 기반구조의 표준에 따른 인증서가 발급되고 검증되

〈표 3〉 인증서비스 적용표준

분 야	적용표준
전자서명 알고리즘	KCDSA, RSA(PKCS#1)
인증서 규격	X.509v3
인증서 폐지목록규격 (CRL)	X.509v2
인증서 효력정지 목록 규격(CSL)	X.509v2활용
인증서신청 요구규격	PKCS #10
디렉토리 규격	LDAP V2
인증기관과 사용자 프로그램 사이의 통신	RFC 2510(CMP)
해쉬 알고리즘	SHA-1(PKCS#1), HAS-160

어야 한다. IETF의 PKIX(Public Key Infrastructure X.509)그룹에서 99년 1월에 채택한 X509 V.3와 V.2[1-3], 디렉토리 서버와의 통신 프로토콜 RFC 2559[4] RSA의 PKCS(Public Key Cryptography Standard)[5] RSA및 KCDSA의 전자서명 알고리즘이 표준으로 적용된다. <표 3>에 인증서비스에 적용되는 표준들을 보인다.

3.2 인증시스템 구성요소

인증서비스를 제공하는 인증시스템은 크게 등록관리 시스템, 키 생성 시스템, 인증서 생성 시스템, 디렉토리 시스템, 시점확인 시스템, 웹 서비스 시스템, 사용자 SW의 7가지로 나눌수 있다.[ ]

아래 <표 4>에 국내 공인 인증기관의 인증시스템들의 구성요소를 요약 정리한다.[6-8]

4. 결 론

인터넷의 발전과 더불어 전자상거래에 의한 구매가 급속히 증가되고 있다. 국내의 경우에도 1999년 2월 전자서명법이 공표되고, 이에 근거하여 전자서명 인증관리센터, 한국정보인증, 금융결제원, 한국증권전산이 공인인증기관으로 인정되었다. 현재까지의 전자상거래 인증서비스기술의 핵심은 전술한 공인인증기관구축에 치중되어 왔으며, 2000년도에 들어서서 공인인증기관의 인증시스템이 실용화 시험을 거쳐 본격적인 상거래 인증 서비스를 실시하기 위해서는 소비자, 판매자, PG, 은행과의 연동이 보다 활성화되어야 한다. 향후 전개되리라 예측되는 국내 전자상거래 시장에서 필수 불가결한 핵심요소로써 역할 하여야 하는 인증서비스의 기술 발전을 위하여서는 다음의 3가지 추가적인 연구.개발 방향을 제안하고저 한다.

첫째, 공인인증기관이외에 인트라 및 익스트라넷 등에서 사용될 수 있는 RA의 활성화가 필요하다. - ISO/JTC1 SC27/WGI의 경우, CA의 표준화는 어느정도 정착되고 이제 RA에 의한 부가 서

구성요소	기능	세부기능
키생성시스템	CA공개키/키관리 쌍 생성 키관리 백업/복구 개인보안 저장소, 관리 비밀분산기능 감사기록관리	RSA 1024비트이상 스마트카드
인증서 생성·관리 시스템	인증서 생성/폐지/취소/정지게시기능 CRL/CSL생성 및 기능 신청자 키쌍 생성/갱신 기능	X.509v3 X.509v2
등록관리 시스템	신청자로부터 등록 요청/폐지 수신기 CA에게 인증서 발급요청 신청자 등록정보관리	
디렉토리시스템	인증서 저장 및 검색 CRL/CSL저장 및 검색	LDAP v2
시점확인 시스템	시점확인 서비스 제공 인증서 생성시점 확인 전자문서 제출시점 확인	
웹 시스템	홈페이지, WWW, SW다운로드등 서비스	
사용자 SW	사용자 PC에 상주 키생성, 검증, 암복호화기능 수행 인증서, 시점확인등 client 기능수행	

비스 기술에 대한 새로운 프로젝트가 진행 중이다. 국내의 경우 공인인증기관이외의 인증서비스 기술 개발이 보다 필요하다고 판단된다.

둘째, 스마트카드와의 연동기술 개발이 보다 요구된다. - 마이크로소프트사 윈도우2000에서는 스마트카드 인터페이스가 표준으로 부착되었다. 향후 개인정보저장장소(PSE)로서 단말 사용자가 스마트카드를 사용하는 것이 보다 보편화될 것이다.

셋째, 인증기술의 적용분야 확장 필요하다. - 전자상거래는 SET, EDI, VPN등과 연동확장하여 적용될 수 있다. PKI기반의 인증서는 향후 인터넷을 바탕으로 하는 경제활동에서 피할 수 없는 중요한 기술 매체가 될 것이다.

참고문헌

[1] R.Housley, W. Ford and D. Solo, RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile. IETF X.509 PKI (PKIX) Working Group., January, 1999.

[2] C. Adams, S. Farrell, RFC 2510 : Internet X.509 Public Key Infrastructure Certificate Management Protocols, IETE X.509 PKI (PKIX) Working Group., March, 1999.

[3] M. Myers, C. Adams, D. Solo, D. Kemp, RFC 2511 : Internet X.509 Certificate Request Message Format, IETF X.509 PKI (PKIX) Working Group., March, 1999.

[4] S.Boeyen, T. Howes, P. Richard, D Kemp, RFC 2559 : Internet X.509 Public Key Infrastructure Operational Protocols LDAP v2, IETF X.509 PKI (PKIX) Working Group., April, 1999.

[5] NIST. MISPC : Minimum Interoperability Specification for PKI Components v.1 , NIST, July, 1998.

[6] 홍가윤, 인증관리센터 구축 및 운영 계획, 제4회 정보보호 심포지움(SIS 99), 1999. 4. 15 ~ 16.

[7] 김상래, 금융분야의 인증시스템 구축 및 서비스 계획, 한국 통신보호학회지 제 9권, 제3호, 1999.9.

[8] 김용준 외 4인, 전자상거래 인증 서비스 체계, 한국 통신보호학회지 제 9권, 제3호, 1999. 9.

김 석 우

1979년 한국항공대학교 통신정보공학과 학사
1989년 NEW JERSEY 공대 전산학 석사
1995년 아주대학교 컴퓨터공학과 박사
1979년-1980년 삼성 HP 근무
1980년-1997년 ETRI 부호5실장
1987년-1989년 AT & T Bell Lab. 방문연구원
1997년-현재 한세대학교 정보통신학과 교수, 군포창업보육센터 소장, 한국 통신정보보호학회 상임이사, 개방형 보안구조연구회 위원장, 한국 정보통신기술협회 정보보호기술위원회 부위원장.
관심분야 : 컴퓨터, 네트워크 보안, 정보보호시스템 평가, 전자상거래 보안, 스마트 카드

서 창 호

1986년-1990년 고려대학교 자연과학대학 수학과 졸업
1990년-1992년 고려대학교 대학원 수학과 졸업
1993년-1996년 고려대학교 대학원 수학과 졸업
1996년 국방과학연구소 선임연구원
1996년-2000년 한국전자통신연구원 선임연구원, 팀장
2000년-현재 공주대학교 응용수학과 조교수 재직 중
관심 분야 : 암호학, 응용대수학, 정보보호 관련 분야