主題

공공분야의 정보보호
- 공공분야의 공인인증서비스 -

한국전산원 윤병남, 반형식

차 례

1. 서론

정보통신 기술의 발전과 함께 사이버 뱅킹, 전자상거래, 기업간 전자거래 등 인터넷을 이용한 전자거래가 급속히 확산되고 있으며, 민간분야의 이러한 변화에 대하여 공공분야에서는 전자정부사업 추진을 통하여 행정의 편의성과 효율성을 제고하고 인터넷을 통한 편리한 대민서비스 제공을 위해 노력하고 있다.

그러나 인터넷과 같은 개방형 정보통신망에서 이루어지는 전자문서의 거래는 익명 또는 가명으로 이루어질 수 있고, 상대방에 대한 명확한 신원확인에 한계가 있으며 전자문서 송신자나 해커에 의한 문서내용의 위·변조 및 송·수신 행위에 대한 부인 등의 문제가 발생할 수 있다.

우리나라에서는 1999년 7월 1일 전자서명법이 본격 시행됨에 따라 인터넷을 통한 전자거래에서 문제가 되는 거래 상대방의 신원확인, 거래 내용의 위·변조 및 송수신 행위에 대한 부인 등의 문제를 법률적인 효력이 있는 공인인증서에 기초한 전자서명을 이용하여 해결하고 있으며, 전자정부 서비스 및 공공분야의 정보화사업으로 구축하는 정보시스템의 안전·신뢰성을 확보하기 위해 전자서명 기술을 적용하고 있다.

전자정부 서비스를 이용하기 위해서는 전자서명이 필수이고, 본인확인이 필요한 경우 민원인은 공인전자서명으로 본인확인을 받을 수 있어 서비스가 본격 제공되는 10월경에 전자서명 인용자수가 급속히 확산될 것으로 기대된다.

2. 전자서명 기술

비대면 방식의 전자적 거래 환경에서 요구되는 정보보안 요구사항은 비밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 부인방지(Non-repudiation) 등이 있으며 전자서명은 인증, 무결성, 부인방지에 대한 보안 기능을 제공한다.

ㅇ 비 밀 성 : 전송되는 정보의 비밀보장
ㅇ 인　　증 : 전송자의 신분을 증명
ㅇ 무 결 성 : 전송되는 정보가 변경되지 않음 을 보장
ㅇ 부인방지 : 사후 자신의 행위에 대한 부인 불가

전자서명은 70년대 개발된 공개키 암호 기술과 해쉬함수를 이용한다[1, 2, 3, 4].

ㅇ 공개키 암호 알고리즘
- 전자문서를 암호화 및 복호화 할 때 서로 다른 값을 갖는 공개키(Public key)와 개인키(Private key)를 사용하는 비대칭형 암호 알고리즘으로 전자문서를 자신만이 알고있는 개인키를 이용한 수학연산을 통해 암호화하고,
- 암호화된 내용은 대응하는 공개키를 이용한 수학연산을 통해서만 복호화된다.
- 공개키는 전자문서를 암호화 할 때 이용되며, 누구나 사용할 수 있도록 공개하고,
- 개인키는 전자문서를 복호화 할 때 이용되고, 소유자만이 사용할 수 있도록 자신이 안전하게 관리하여야 한다.
- 전자문서를 자신만이 알고있는 개인키로 암호화하는 순간 그 전자문서에 전자서명이 생성되는 것을 의미하고 암호화된 내용은 대응하는 공개키로 암호화해야만 복호화 될 수 있어 전자서명 사실에 대한 부인 방지 기능이 가능하다.

ㅇ 해쉬함수
- 전자문서를 항상 일정한 출력(해쉬값)을 갖도록 압축하는데 사용되며(보통 160 비트), 해쉬함수는 충돌저항성을 가져야 하는데 이는 전자문서가 변경된 경우 전혀 다른 출력 값을 생성하는 성질을 말한다.

ㅇ 전자서명
- 해쉬함수를 이용하여 전자문서를 압축하고 압축된 결과를 공개키 암호 알고리즘의 개인키를 이용하여 암호화하는 것은 전자서명을 의

$$E_{KP}(E_{KR}(M)) = E_{KR}(E_{KP}(M)) = M$$

M : 전자문서, E : 공개키 암호 알고리즘, KP : 공개키, KR : 개인키

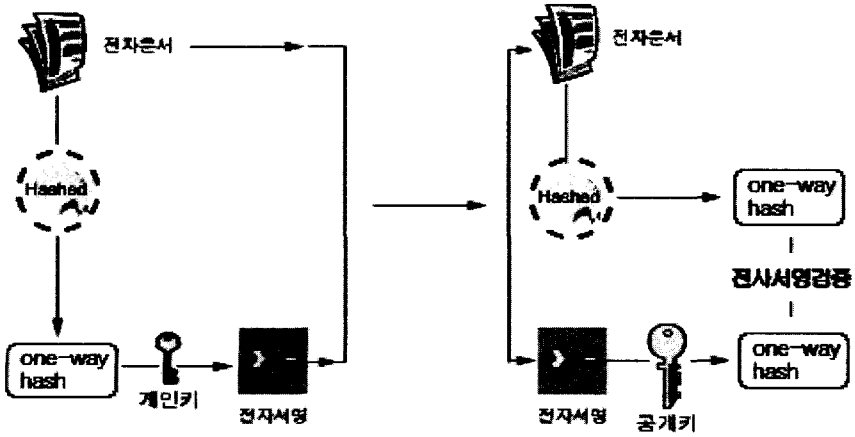


그림 1. 전자서명 생성 및 검증 절차

미하며 그 결과 값을 전자서명 값이라 한다.
- 한편 전자문서와 첨부된 전자서명 값을 받은 사람은 대응하는 공개키로 전자서명값을 복호화한 값과 자신이 해쉬함수로 만든 전자문서의 해쉬값을 비교하여 전자서명의 진위여부를 검증한다.

○ 전자서명의 기능
- 이러한 과정을 살펴보면, 해쉬함수의 충돌저항성은 무결성을 보장하고 공개키 암호 알고리즘의 개인키는 사용자 자신만 알고있기 때문에 인증과 부인방지 기능을 제공 할 수 있다.

공개키 암호 알고리즘 기반의 전자서명 기술은 자신이 공개키를 외부에 공개하고 이를 이용하여 자신을 상대방에게 인증 시키는 기술이다. 그러나 공개키는 누구나 쉽게 획득할 수 있도록 공개된 장소에 등록되어 있어 항상 공개키의 위·변조에 대한 문제가 존재하게 된다. 뿐만 아니라 자신이 획득하고자 하는 공개키가 누구의 공개키인지 확인할 수 있는 수단이 별도로 존재해야 한다. 이러한 기능을 제공하는 기반을 공개키기반구조(Public key infrastructure: PKI)라 한다.

3. 공개키기반구조(PKI)

공개키기반구조의 구성요소는 인증기관, 등록기관, 디렉토리시스템, 가입자 및 신뢰당사자 등으로 이루어진다.

○ 인증기관(Certification Authority)
- 공개키 암호 시스템 사용자의 개인키와 개인정보를 함께 믿을 수 있도록 보장해주는 제3자(TTP)의 역할 수행
- 인증기관은 사용자들의 인증서 발행 요청에 따라 인증서(Certificate)를 발행·폐지하고, 인증서 폐지목록(CRL)을 발행
- 인증서는 발행한 인증기관이 사용자의 개인키와 개인정보의 내용을 보증하는 전자문서로서 인증기관은 자신의 개인키로 사용자의 인증서를 전자서명 함으로써, 사용자 인증서의 무결성 및 진실성을 보장
- 인증서 폐지목록은 인증기관이 유효하지 않은 인증서의 목록을 보증하는 전자문서로서 인증기관은 자신의 개인키로 내용을 전자서명 함으로써, 인증서 폐지목록의 무결성 및 진실성을

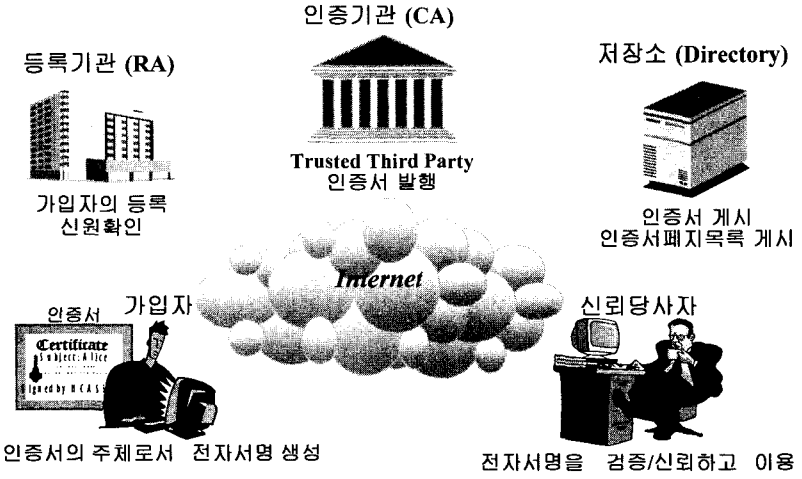


그림 2. PKI 구성요소

보장

○ 등록기관(Registration Authority)
- 인증기관으로부터 위임받은 등록업무 및 신청자의 신원확인 업무 수행

○ 디렉토리(Directory)
- 인증기관이 발행한 인증서 및 인증서 폐지목록 정보를 공지하고 관련 당사자들에게 배포하는 시스템

○ 가입자(Subscriber)
- 인증기관의 인증서비스에 가입하고 자신의 개인키를 인증받은 자를 말하며, 인증기관이 발행하는 인증서의 주체로서 인증받은 개인키를 이용하여 전자서명을 생성
- 가입자는 인증서 발행 및 폐지를 요청

○ 신뢰당사자(Relying Party)
- 인증기관의 인증서를 신뢰하고 이용하는 자로서 전자서명을 적용하고 있는 응용시스템들이 이에 해당 됨
- 전자서명된 메시지를 수신하는 경우 신뢰당사자는 전자서명값의 진위 및 정당성 여부를 확인해야 하며, 이를 위해 송신자의 인증서와 인증서 폐지 목록을 인증기관의 디렉토리 시스템으로부터 획득하여 해당 인증서의 유효성 여부를 검증

4. 전자서명 공인인증제도

전자서명 공인인증 제도는 공개키 암호 알고리즘을 이용한 정보보호 서비스인 전자서명에 법률적 효력을 인정하는 기술과 법이 결합하는 대표적인 사례이다. 우리나라에서는 1999년 7월 1일 전자서명법의 본격 시행으로 공개키기반구조(Public key infrastructure: PKI)가 구축되어 전자서명인증 적용이 활발히 추진되고 있다.

전자서명법에 의한 공인인증기관으로 지정 받기 위해서는 다음의 지정기준을 충족하여야 하고, 시스

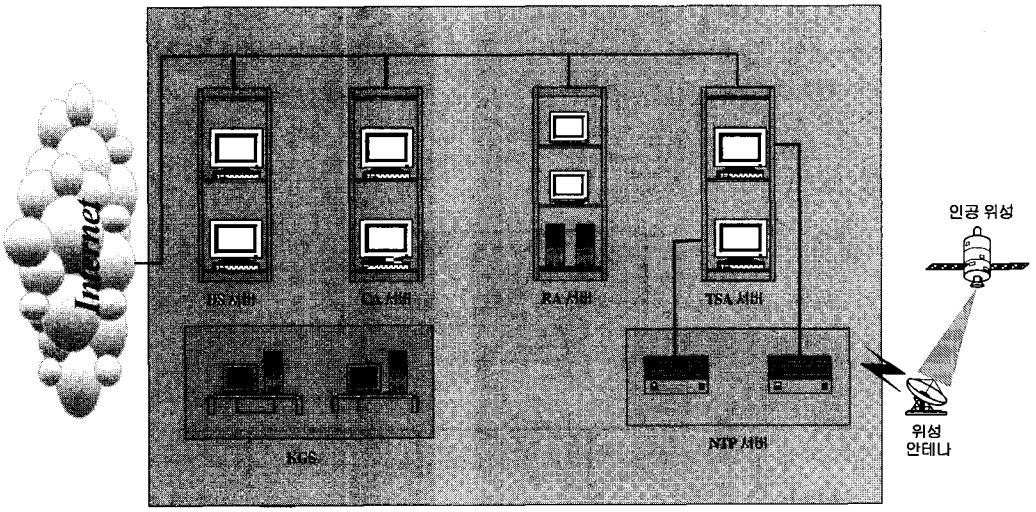


그림 3. 인증시스템 구성예

CA 서버 : 인증서 발급·관리 서버　　RA 서버 : 등록관리 서버
TSA 서버 : 시점확인 서버　　NTP 서버 : 네트워크 타임 서버
DS 서버 : 디렉토리 서버　　KGS : 키생성 시스템

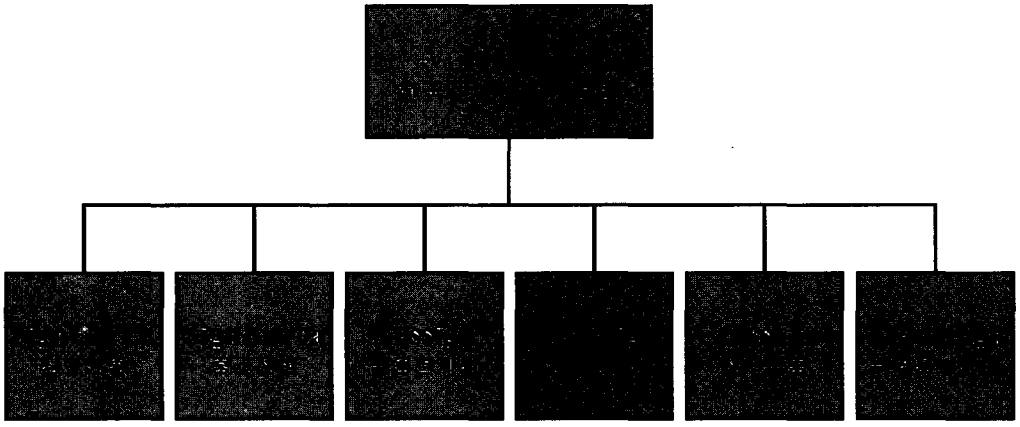
템 및 시설에 대한 철저한 실사를 거쳐 공인인증기관으로 지정된다.

○ 자본금 80억 이상의 재정능력
○ 기술능력의 요건을 갖춘 운영인력 12인 이상
- 국가기술자격증 소지 또는 이와 동등 이상의 자격
- 정보보호 또는 정보통신 분야의 2년 이상 실무경력
- 인증관리체계교육 이수
○ 인증업무에 관한 시설 및 장비(정통부장관이 고시)
- 인증업무의 원활한 수행을 위한 설비
- 인증업무의 안전성 및 신뢰성을 보장하기 위한 설비
- 시설 및 장비에 대한 관리·운영 내규

한국정보보호진흥원이 최상위인증기관으로 지정·운영 중에 있으며, 현재 한국전산원, 정보인증, 금융결제원, 증권전산, 전자인증, 무역정보통신 등 6개의 공인인증기관이 지정·운영 중에 있다. 정보인증과 전자인증은 전자상거래분야, 증권전산은 증권분야, 금융결제원은 금융 분야, 한국전산원은 공공분야, 무역정보통신은 무역분야를 주요 업무 영역으로 인증서비스를 제공하고 있다.

한편 공인인증기관은 전자서명 공인인증제도의 안전·신뢰성을 확보하기 인증업무 수행시 다음의 사항을 준수하여야 한다.

○ 전자서명 인증업무지침의 준수
○ 공인인증업무의 안전성 및 신뢰성 유지
- 인증업무 시설의 안전성 확보를 위한 보호조치
- 시설 및 장비의 안전운영 여부에 대한 정기적인 점검
- 시설 및 장비에 변경이 있을 경우 지체없이 신고
- 인증업무를 휴지 또는 폐지할 경우 다른 공인인증기관에 인계하여 인증업무의 지속성을 보장
- 개인정보보호
(정보통신망이용촉진및정보보호등에관한법률의 개인정보보호규정 준용)
○ 손해배상 책임
- 공인인증기관은 이용자에게 손해를 입힌 경우 그 손해를 배상하여야 함
- 공인인증기관이 과실 없음을 입증하면 면책
○ 상호연동 의무화
- 누구든지 특정 공인인증서 요구금지
- 위반시 1년이하의 징역 또는 일천만원이하의



※ 공인인증기관 지정순

벌금

5. 인증서 발급 절차

① 인증서비스를 받고자 할 경우에는 먼저 등록기관을 방문하여 인증서비스 가입신청서를 작성하여 제출

② 등록기관은 전자서명법령에서 정한 절차에 따라 신청자의 신원을 확인

③ 신원확인 절차후 등록기관은 On-line으로 신청등록을 인증기관에 요청

④ 인증기관은 정상적인 등록요청에 대하여 On-line으로 참조번호와 인가코드를 등록기관 전송

⑤ 등록기관은 전달받은 참조번호와 인가코드를 신청자에게 Off-line으로 전달

⑥ 신청자가 자신의 PC에서 인증기관에서 제공한 인증모듈을 이용하여 전자서명키(개인키와 공개키) 쌍을 생성

⑦ 인증기관에 On-line으로 인증서 발급 요청 (참조번호/인가코드와 신청자의 공개키를 인증기관에 제출)

⑧ 인증기관은 신청자의 제출정보에 대한 검증을 한후 해당 인증서를 생성

⑨ 인증기관은 생성한 인증서를 디렉토리 서버(저장소)에 게시

⑩ 인증기관은 가입자에게 해당 인증서를 발급

⑪ 가입자는 자신의 인증서를 하드디스크, 디스켓, 스마트카드, USB 키 등 원하는 저장매체 저장

6. PKI 관련 표준

PKI 관련 기술에 대한 국제 표준화 작업은 기관은 주로 ISO/IEC JTC 1 SC27, ITU-T, IETF 등에서 진행되고 있으며 국내에서의 표준화 작업은 TTA에서 진행하고 있다. 주요 적용기술 및 표준은 다음과 같다.

○ 암호 알고리즘 및 해쉬 알고리즘

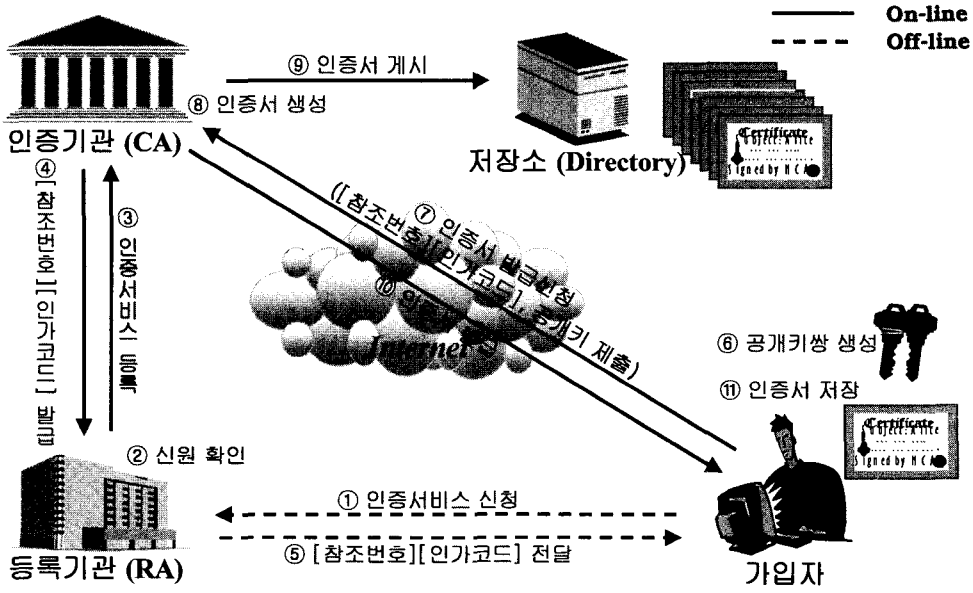


그림 4. 인증서 발급절차

대칭키 암호 알고리즘	국외	DES/3-DES, IDEA, RC2/4/5 SKIP JACK, Blowfish, CAST
	국내	SEED (TTA.KO-12.0004)
공개키 암호 알고리즘	국외	RSA, DSA, ElGamal
	국내	KCDSA (TTA.KO-12.0001)
해쉬 알고리즘	국외	MD2/4/5, SHA/SHA-1, RIPEMD-160
	국내	HAS-160 (TTA.IS-10118)

○ 인증서 규격

ISO/IEC와 ANSI에서는 X.509의 버전을 갱신하여 표준 단체나 사용자 조직에서 정의될 수 있는 확장영역을 부가한 X.509 버전 3(X.509v3)을 개발하였다. 현재 공인인증기관은 인증서 규격으로 X.509v3 규격을 준용하여 사용하고 있다 [5, 6].

version (0-v1, 1-v2, 2-v3) certificate serial number CA's signature algorithm ID issuer name (X.500 DN) validity (not before, not after) subject name (X.500 DN) subject public key information	v1
issuer unique identifier subject unique identifier	v2
extensions (확장 영역)	v3
CA's Signature	

X.509v3 인증서 규격

X.509v3 인증서 확장 영역의 확장 필드(Extension field)는 다음과 같이 분류된다.

- Key and Policy Information
- Certificate Subject and Issuer Attribute
- Certificate Path Constraints
- CRL(Certificate Revocation List) Identification

확장 필드가 critical=true이면 응용은 해당 정보를 무시할 수 없으며 해당 정보를 처리할 수 없는 응용은 인증서를 거부해야하며, critical=false이면 해당 정보를 무시할 수 있다.

○ 인증서 폐지목록(CRL) 규격

공인인증기관은 인증서 폐지목록으로 X.509v2 CRL 규격을 준용하여 사용하고 있다[5, 6].

CRL Version		
issuer's signature algorithm ID		
date and time of this update		
date and time of next update		
serial number	revocation time	CRL entry extension
. . .		
serial number	revocation time	CRL entry extension
CRL extension		
CA's signature		

X.509v2 인증서 폐지목록 규격

X.509v2 인증서 폐지목록 확장 영역의 확장 필드(Extension field)는 다음과 같다.

CRL extensions	• authority key identifier • issuer alternative name • CRL number • delta CRL indicator
CRL entry extensions	• reason code • hold instruction code • invalidity date • certificate issuer

인증서 폐지목록 확장필드

○ PKI 인증서 관리 프로토콜

IETF PKIX의 인증서 관리 프로토콜(CMP: Certificate Management Protocols, RFC2510)은 다음과 같은 내용에 대한 기준을 제시하고 있다[7].

○ 인터넷 PKI 구성 객체
- 인증기관(CA: Certification Authority)
- 등록기관 (RA: Registration Authority)
- 최종 객체(EE: End Entity)
- 저장소(Repository)

○ 인터넷 PKI 기능
- CA 구축(예: 키를 생성한 후, 공개키 공개)
- 최종객체 초기화(예: 루트 CA의 공개키를 적재)
- 인증(certification): 초기 등록, 키쌍 갱신, 인증서 갱신, CA 키쌍 갱신, 상호인증, 상호인증 갱신
- 공개: 인증서 공개, CRL 공개
- 복구: 키복구
- 취소: 취소 요구

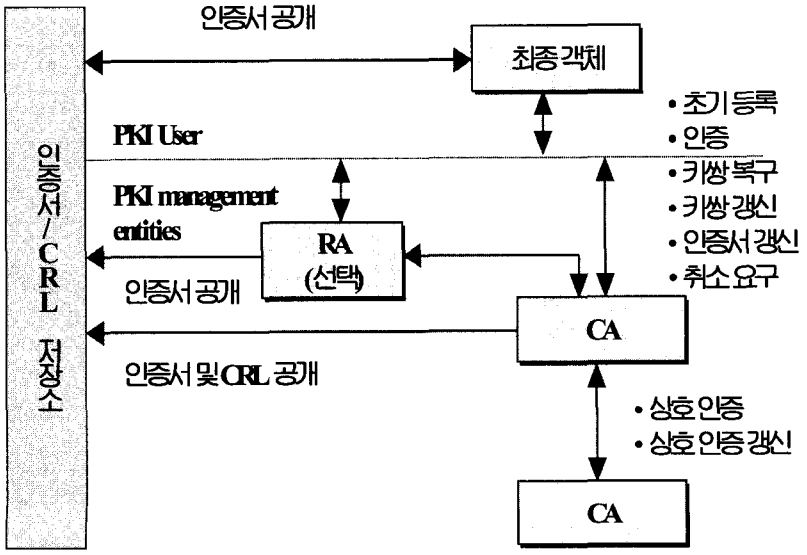
- LDAP, FTP, HTTP, OCSP

7. 공공분야 인증서비스

국내 공공분야의 인증서비스로는 처음으로 한국전산원이 1998년 1월에 조달EDI 이용기관을 대상으로 인증서비스(사설인증)를 제공하였고, 1999년 1월에 재정정보시스템 이용기관을 대상으로 인증서비스(사설인증)를 제공하였다[8, 9].

정부에서는 전자서명이 인터넷을 통한 전자거래시 상대방의 신원확인과 전자문서의 위·변조 방지 및 거래사실의 부인방지 기능을 제공하는 정보화시대의 핵심인프라로 자리잡고 안전한 전자거래 환경을 조성하기 위해 1999년 2월에 전자서명법을 제정하여 전자서명 인증제도를 도입하였다.

전자서명법이 발효되면서 한국전산원에서는 기존의 사설인증서비스를 공인인증체계로 전환하기 위해 한국전산원 용인 본원에 정보인증센터를 구축하여 2001년 3월에 공공분야의 공인인증기관으로 지정받아 2001년 4월부터 국방부 조달본부, 조달청, 조



인터넷 PKI 구성 객체 및 기능

달 수요기관을 대상으로 하는 공인인증서비스와 주택공사, 도로공사의 전자입찰 업무에 인증서비스를 제공하고 있다.

현재 추진되고 있는 전자정부 사업이 금년 10월중에는 완료되면 본격적으로 인터넷을 통한 전자정부서비스를 개시할 예정이며 전자정부서비스를 이용하기 위해서는 공인전자서명이 반드시 필요하다. 정부에서는 공인전자서명을 이용하여 언제 어디서나 간편하게 전자정부서비스를 이용할 수 있는 환경을 조성하고 이를 통하여 2002년 말까지 공인전자서명 이용자를 1,000만명을 확보할 예정이다.

공인인증서가 적용예정인 전자정부 서비스 다음과 같다.

- O 교육행정정보시스템 구축사업(교사, 학부모)
- O G4C, 시군구 행정 종합정보화 사업(민원인)
- O 종합국세서비스(세무대리인, 자영업자 등)
- O 전자조달 시스템 구축사업(조달수요기관, 입찰참여업체)
- O 4대 사회보험 정보연계사업(4대 사회보험 가입자)

한편 한국전산원에서는 2002년 8월부터 교육인적자원부의 교육행정정보시스템을 이용할 전국의 교직원 및 교육관련 공무원 43만명을 대상으로 인증서를 발급하여 교육행정정보시스템에 접속시 또는 중요 업무처리에 한국전산원의 인증서를 적용할 예정이다.

전자정부 서비스의 성공을 위해서는 민원서비스를 이용할 국민들이 얼마나 공인인증서를 발급 받느냐에 달려 있다. 전자정부 서비스도 국민들에게 제공되는 보편적인 민원서비스이므로 국민들이 쉽게 접근이 가능한 동사무소나 행정기관의 민원실 등을 통해 인증서를 발급 받을 수 있는 방안이 마련되어야 할 것으로 생각한다.

8. 향후 전망

현재 공공분야의 공인인증서 적용업무는 인터넷 국세신고, 전자조달·입찰 등이 있으나 전자정부서비스가 10월부터 제공될 예정 이여서 전자서명 이용이 확산될 것으로 예상된다.

한편, 공무원에 대한 인증서 발급도 활성화 될 것으로 기대된다. 전자정부법의 전자관인은 행정기관, 보조기관 또는 보좌기관으로 그 발급대상이 정해져 있었으나, 전자관인을 행정전자서명으로 용어 및 그 개념을 정비하고, 그에 따른 행정전자서명의 효력을 새롭게 규정하여 모든 공무원이 행정전자서명을 공·사무 용도로 사용 가능하도록 하는 개정안이 국회에 제출되어 있어 향후 공무원에 대한 인증서 발급업무는 행정자치부의 GCC와 한국전산원을 통하여 이루어 질 것으로 기대된다.

또한 향후 공공분야의 업무환경도 사무실에서 처리되는 업무뿐만 아니라 재택 및 이동근무환경에서 VPN 및 유무선 인터넷을 통한 업무처리가 도입 될 것으로 기대되며, 이 경우에도 접속자의 신원확인 및 유통되는 전자문서의 무결성을 확인할 수 있는 인증서를 이용한 전자서명으로 업무처리가 가능할 것으로 기대된다.

참고 문헌

[1] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

[2] RSA Laboratories, "The Public-Key Cryptography Standards(PKCS)", RSA Data Security Inc., Redwood City, California, November 1993 Release.

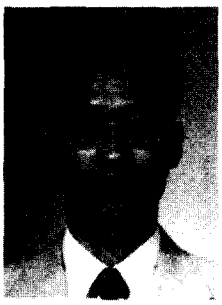
[3] 한국정보보호진흥원, 인증관리체계기술규격(Version 1.0), 2001. 7.

[4] Secure Hash Standard. FIPS Pub

180-1. National Institute of Standards and Technology. 17 April 1995.
[5] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
[6] Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile", RFC 2459, January 1999.
[7] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure, Certificate Management Protocols", RFC 2510, March 1999.
[8] 이영로 외, "1999년도 정보연계센터 운영사업 결과보고서", 한국전산원, 1999년 12월 31일
[9] 김기수, "공공부문 정보인증서비스 현황", NETSEC-KR2000, 한국정보보호센터, 2000년 6월

윤 병 남

1975년 한양대학교 전자공학과 (학사), 1989년 청주대학교 대학원 정보통신공학 (석사), 1997년 충남대학교 대학원 전산학 (박사), 1974. 5 - 1978. 8 스페리 유니벡, 컴퓨터 하드웨어 엔지니어, 1978. 8 - 1982. 11 삼성전자(주), M10CN전자교환시스템 시험과장, 1982. 11 - 1999. 8 한국전자통신연구소 (ETRI) 근무, 1999. 8 - 현재 한국전산원 근무, 현재 국가정보화센터 단장



반 형 식

1989년 2월 인하대학교 수학과(학사), 1991년 2월 포항공과대학교 대학원 수학과(석사), 1995년 2월 포항공과대학교 대학원 수학과(박사), 1996년 9월 - 1998년 8월 미국 University of Florida 수학과 KRF Post-Doc., 1998년 9월 - 1999년 12월 포항공과대학교 전산수학센터 연구원, 1999년 12월 - 현재 한국전산원 근무, 현재 국가정보화센터 선임연구원