通信情報保護學會誌
第9券 第3號, 1999. 09

전자상거래 인증서비스 체계

김 용준, 백 석철, 정 종윤, 박 정식, 김 재중

요 약

인터넷상에서 안전한 전자상거래를 영위하기 위하여 필수적인 전자서명용 인증서 발급 서비스 체계에 대하여 설명한다. 우선, 인증서 발급서비스를 하기 위하여 필요한 망 구조와 등록관리시스템, 전자서명생성키 생성 및 관리 시스템, 인증서 생성 및 관리 시스템, 디렉토리 시스템, 시점확인 시스템, 웹서비스 시스템 및 보안 설비들의 기능을 서술하고 이러한 시스템들을 이용한 인증서 발급 업무의 흐름을 세 가지 유형으로 분리 설명한다. 또한 인증서 갱신, 폐지, 정지 등에 대해서도 언급하며 끝으로 한국정보인증이 인증서비스를 바탕으로 향후에 제공할 서비스에 대해 소개한다.

I. 서 론

전자서명은 수학적인 해쉬 함수(hash function)를 이용한다. 다양한 길이의 메시지(예, 전자메일)를 해쉬 함수는 고정된 길이의 비트 스트링(message digest)으로 변환시킨다. 이 비트 스트링을 송신자의 개인키(private key)로 암호화시킨 후 원래 메시지에 부착하게 되면 전자서명이 완료되는 것이다. 전자서명된 메시지를 받은 수신자는 송신자의 공개키로 메시지에 부착되어있는 전자서명을 복호화한 내용을, 송신자와 같은 해쉬 함수로 메시지 본문을 해쉬한 결과와 비교하게 된다. 그 결과가 동일하면 공개키 주인인 송신자가 메시지를 보냈으며 그 내용이 중간에서 변조가 되지 않았음을 수신자가 확인할 수 있게 된다. 따라서 전자서명은 특정한 전자메시지에 작성자를 확인할 수 있게 함과 동시에 송신자가 작성한 전자문서가 전송되는 과정에서 변조되는 것을 방지할 수 있다. 즉, 데이터의 무결성을 보장할 수 있다.

이러한 전자서명은 실세계에서 신분을 확인하기 위하여 사용되는 여권이나 운전면허증처럼 인터넷상에서 사용자의 신분을 확인하기 위한 전자 인증서(이하 인증서로 표시)를 만드는 메커니즘으로 사용될 수 있다. 제3의 신뢰할 수 있는 기관(trusted third party)이 신분을 확인한 후 발급해 주는 인증서를 이용하면 전자문서에 개인이나 조직(기업, 기관, 단체 등)을 확실하게 결부시킬 수 있다. 이러한 TTP를 PKI 환경[3] 하에서는 인증기관(certificate authority)이라고 부른다. CA는 인증서에 서명함으로서 인증서 소유자의 신원을 보증한다. 인증서의 주 기능은 개인 또는 네트워크 디바이스의 공개키를 유효하게 하는 것이다. 인증서 내에는 이를 소유한 개체의 특권을 표시하는 정보도 포함시킬 수 있다. 따라서 인증서는 개체에 대한 접근제어 서비스에 널리 이용될 수 있다. 이러한 인증서 기능들은 HTTPS, S/MIME, IPSEC 등에 널리 응용되고 있다.

1999년 7월 1일 정보통신부에서 전자서명법을 제정 공포함에 따라 공인인증기관이 발급한 인증서를 이용한 전자서명이 법적인 의미를 갖게 되었다. 이러한 환경이 마련됨으로서 인터넷을 통한 전자거래가 급속도로 증가하게 될 것은 명백하다.

*한국정보인증 시스템개발실(jjkim@signgate.com)

Ⅱ장에서는 공인된 인증서를 발급하게 될 인증기관이 갖추어야 할 시스템들과 이들의 기능에 대하여 서술한다. Ⅲ장에서는 공인인증기관의 인증서 발급, 갱신, 폐지 절차에 관하여 기술한다. Ⅳ장에서는 공인인증기관이 향후에 제공할 서비스에 대한 간략한 설명과 인증서를 이용한 응용서비스들에 대한 전망을 하고자 한다.

Ⅱ. 인증 시스템 구성 및 기능

한국정보인증의 시스템 구성 및 각 시스템의 기능에 대한 설명과 인증서비스의 절차를 살펴보고자 한다.

1. 인증시스템 구조

한국정보인증의 인증시스템은 공인 인증기관(certificate authority)의 역할을 수행하기 위하여 한국정보보호센터(KISA)에서 제시한 기능들을 수행하는 시스템들과 고객에게 인증서 발급 서비스를 원활히 할 수 있게 하는 시스템들로 구성된다[1]. 이들 시스템들을 살펴보면 등록관리 시스템, 인증기관의 전자 서명키 생성 및 관리 시스템, 인증서 생성 및 관리 시스템, 디렉토리 서비스 시스템, 시점 확인 시스템, 고객들이 인증시스템과 접촉을 용이하게 하기 위한 웹서비스 시스템들로 구성된다. 물론, 이러한 시스템들을 네트워크 상에서 안전하게 보호할 수 있는 네트워크 및 서버 보안 시스템(방화벽, 실시간 침입탐지시스템 등)과 이들 설비를 안전하게 보호, 관리할 수 있게 해주는 물리적 보안 설비가 있어야 한다[2]. 이제부터 이들의 기능에 대하여 간단히 서술하기로 한다.

1.1 등록관리 시스템

- ㅇ 가입자의 전자서명 생성키에 대한 유일성 확인 기능
- ㅇ 가입자 식별을 위한 고유명칭(DN) 부여 기능
- ㅇ 가입자가 제출한 전자서명 검증키가 가입자의 전자서명 생성키에 합치하는지 확인, 검증하는 기능
- ㅇ 가입자 정보를 등록, 관리하는 기능
- ㅇ 권한 있는 직원만이 가입자 정보에 접근가능 하도록 하는 기능
- ㅇ 지역적으로 분리된 등록기관의 경우 가입자의 등록정보를 정보통신망을 통하여 공인인증기관에 안전하게 전달하는 기능
- ㅇ 가입자 등록정보 관리에 대한 감사기록, 보존 기능
- ㅇ 등록관리 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
- ㅇ 감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능

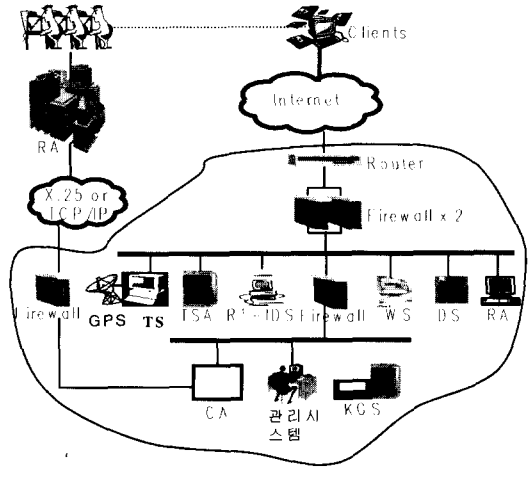


그림 1 공인인증기관 인증시스템 구조

1.2 전자서명 생성키 생성 및 관리 시스템

- ㅇ RSA의 1,024비트 이상의 안전성에 준하는 전자서명 키 생성기능
- ㅇ 내부 및 외부 정보통신망과 연결되지 않고 독립 운영되는 기능
- ㅇ 전자서명 생성키를 생성하여 전자서명 키 저장장치에 저장한 후 전자서명 생성키를 시스템에서 즉시 삭제하는 기능
- ㅇ 전자서명 생성키를 생성하여 가입자에게 교부용 장치에 저장한 후 전자서명 생성키를 시스템에서 즉시 삭제하는 기능
- ㅇ 전자서명 생성키를 암호화하여 전자서명 키 저장장치에 저장하는 기능

o 3인 이상의 권한 있는 직원이 공동으로 전자서명 생성키를 생성하는 기능
o 전자서명 키를 생성한 사실, 시각, 행위자 등 내역의 감사기록, 보존 기능
o등록관리 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
o공인인증기관의 전자서명 키를 유출, 복제하는 위협을 방지하는 기능
o감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능
o전자서명키 생성 시스템의 이중 설치 기능
o가입자의 전자서명 생성키를 스마트 카드에 저장하는 기능
o가입자의 전자서명 생성키를 암호화하여 디스켓에 저장하는 기능
o저장장치에 대한 봉인기능
o저장장치에 대한 접근권한 확인기능
o전자서명 생성키의 유출, 변경을 방지하는 기능
o전자서명 생성키의 유출 우려가 있는 경우 이를 자동 삭제하는 기능
o전자서명 생성키에 대한 접근내역을 기록, 유지하는 기능
oRSA, KCDSA 등 안전성을 검증 받은 국제, 국가, 단체 표준 알고리즘 지원 기능
oRSA 1,024비트 이상의 안전성에 준하는 키 크기를 지원하는 기능
oSHA-1, HAS-160 등 안전성을 검증 받은 국제, 국가, 단체 표준 알고리즘 지원 기능
o160비트 이상의 해쉬값 생성 기능

1.3 인증서 생성 및 관리 시스템

o X.509 V3 인증서 규격[4]을 준수하는 인증서 생성기능
o X.509 V3 인증서 규격을 준수하는 인증서 폐지 목록 생성기능
o 2인 이상의 권한 있는 직원이 공동으로 인증서를 생성, 발급, 갱신, 효력정지 또는 폐지하는 기능
o 인증서를 생성, 발급, 갱신, 효력정지 또는 폐지한 사실, 시각, 행위자 등의 내역을 감사기록, 보존 기능
o 인증서 생성, 관리 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
o 공인인증기관의 전자서명 생성키를 유출, 복제하는 위협을 방지하는 기능
o 감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능
o 인증서 생성, 관리 시스템의 이중 설치 기능

1.4 디렉토리 시스템

o 가입자의 인증서를 등록 관리하는 기능
o 가입자의 인증서 효력정지 및 폐지에 관한 기록을 등록, 관리하는 기능
o "가입자 인증서 등"(=가입자 인증서와 인증서 효력정지 및 폐지에 관한 기록)을 LDAP 또는 DAP을 통해 항상 검색할 수 있도록 하는 기능
o "가입자 인증서 등"을 등록, 관리한 사실, 시각, 행위자 등에 관한 내역을 감사기록 ,보존하는 기능
o 디렉토리 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
o 인증서 등을 삭제하는 위협을 방지하는 기능
o 감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능
o 디렉토리 시스템의 이중 설치 기능

1.5 시점 확인 시스템

o 초단위로 표현 가능한 정확한 표준시를 수신하는 기능
o 시점확인 시스템의 시간을 보정하는 기능
o 시점 확인용 전자서명 생성키를 이용하여 전자문서의 시점을 확인 할 수 있는 기능
o 전자문서를 시점 확인한 사실, 시각, 행위자 등에 관한 내역을 감사기록, 보존하는 기능
o 시점 확인 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
o 시점 확인 시스템의 시간을 변경하는 위협을 방지하는 기능
o 감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능
o 시점 확인 시스템의 이중 설치 기능

1.6 웹서비스 시스템

- ㅇ 이용자와의 안전한 통신을 보장해주는 기능(SSL 프로토콜 및 SEED 암호 알고리즘 지원)
- ㅇ 지속적인 웹서비스에 대한 위협을 방지하는 기능
- ㅇ 알려진 웹 서버에 대한 약점을 보완하는 기능
- ㅇ 웹서비스 시스템의 이중 설치 기능

1.7 보안 설비

- ㅇ "핵심인증시스템" 운영실
- ㅇ 다중 출입통제 장치
- ㅇ 침입감지, 경보 및 감시, 통제 장치
- ㅇ 물리적 잠금 장치
- ㅇ 네트워크 보안 설비(방화벽, 실시간 침입탐지 시스템 등)
- ㅇ 기타 보호 설비

2. 한국정보인증과 등록 기관

일반적으로 특정 인증기관(certification authority)의 등록 기관(registration authority)이라 함은 인증기관의 등록 관리 시스템의 기능을 사업적 또는 기술적인 목적에 의하여 지역적으로 분리하여 운영하는 기관이나 사업체를 의미한다. 등록 기관의 일반적인 역할은 공인인증기관 내에 있는 등록 관리 시스템이 하는 기능과 크게 다를 바 없지만 등록 기관이 사업 또는 기타 이유로 인증서 이용자들에 대한 독자적인 DB를 운용하기 원하는 경우도 있을 수 있다. 다시 말해서 등록 기관은 인증기관의 등록 관리 시스템에 대한 대행 역할을 하면서 RA자신의 사업 또는 업무를 위한 고객 또는 회원 확보 차원으로 등록 관리 기능을 할 수도 있다. 등록 기관은 등록 관리 시스템의 기능을 포함한 다음과 같은 역할을 수행한다.

- ㅇ 인증서 이용 신청자에 대한 신용 조회
- ㅇ 인증서 이용자들의 고유명칭(DN) 부여
- ㅇ 고유명칭을 이용한 인증서 사용자 DB 관리
- ㅇ 인증서 발급 신청서를 인증기관에게 안전하게 전달
- ㅇ 이용자들에게 인증서 전달 및 공지
- ㅇ 인증서의 재발행, 폐지, 갱신 신청 접수 및 수행

3. 시점확인(time stamping)서비스

3.1 시점확인 서비스 개요 및 필요성

네트워을 통한 전자상거래나 전자 문서 보존의 활성화를 위해서는 전자적 서명을 위한 인증서 발급 서비스뿐만 아니라 전자문서 시점확인 서비스가 필수적이다. 한 예로, 사용자간의 전자문서 서명 시점과 전자문서 제출 시점은 입찰이나 선착순 계약과 같은 전자거래에서 필수적인 요소가 될 것이 분명하다. 그러므로 이러한 전자거래에 서 시점확인 서비스는 필수적인 요소이다.

시점확인 서비스는 인터넷상에서 발생하는 행위의 시점(날짜, 시각 등)을 나타내는 토큰을 생성하며, 이 토큰을 생성한 사람 또는 디바이스의 신원을 확인해준다. 시점확인은 GMT와 UTC 시간을 사용하고 있으며, 시점확인이 필요한 것으로는 인증서, CRL 및 다른 취소 및 보류에 관련된 데이터베이스 요소, CPS 등이 있다.

시점확인 서비스 성격상 신뢰할 수 있는 기관만이(TSA: time stamping authority) 이 서비스를 하여야한다. 이 기관은 TDA(time data authority)를 두어 타임 스탬프 토큰에 포함된 시간을 확인해주는 기능을 수행할 수 있어야 한다. TSA는 다음과 같은 요구사항을 만족하여야 한다.

- ㅇ 신뢰할 수 있는 시간의 근원을 제공하여야 한다.
- ㅇ 시점확인 토큰 안에는 고객의 신원 정보를 포함시키지 말아야 한다.
- ㅇ 새로운 시점확인 토큰 발행 시 시각이 항상 증가되어야 한다.
- ㅇ 고객의 정당한 시점확인 서비스 요청이 있을 때만 토큰을 발행해야 한다.
- ㅇ 시점확인 토큰은 토큰 발행 시 적용된 보안정책을 나타내는 식별자를 포함하여야 한다.
- ㅇ 메시지의 해쉬 값에만 시점확인을 해야 한다.
- ㅇ 시점확인 목적으로만 생성된 키를 사

용하여 각 시점확인 토큰에 서명을 하여야 한다.

- 고객이 요구하면 시점확인 토큰에 보조적인 임시 정보를 포함시켜야 한다. 이것이 불가능하면 고객에게 에러 메시지를 반환해야 한다.

3.2 TSA 처리

TSA 처리는 시점확인 고객이 응용프로그램을 이용하여 시점확인 서버에 메시지를 보내 요청을 하면 여기에 대해 서버는 시점확인 토큰을 포함한 응답 메시지를 고객에게 전송한다. 고객은 서버로부터 토큰을 받으면 시점확인 토큰에 있는 서명이 유효한지 TSA의 시점확인용 인증서를 d이용하여 확인할 수 있다. 이러한 과정을 간단히 설명하면 다음과 같다.

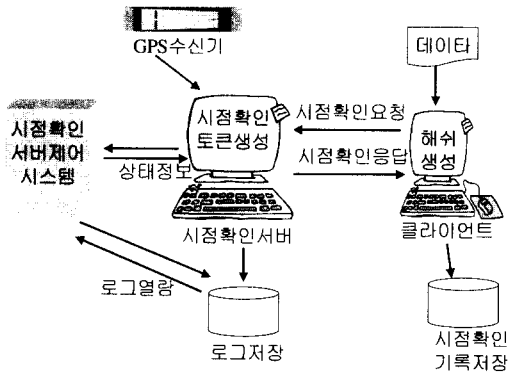


그림 2. 시점확인 시스템 구성도

1) 타임스탬프 서비스요구 및 토큰 발생과정

(1) 타임스탬프 클라이언트 고객은 타임스탬프 서버에게 시점확인 대상 메시지의 해쉬값을 생성하여 보낸다.

(2) 타임스탬핑 서버는 요구 메시지를 확인한 후 시점확인 토큰을 발생하여 클라이언트에게 보낸다.

(3) 클라이언트는 결과의 유효성을 검증한 후, 해당 파일을 기록 저장한다.

2) 타임 스탬프 전송 방법

아래에 제시된 항목들은 의무적인 전송 방법이 아니고 선택 사항들이다.

표 2 타임스탬프 요구 데이터 형식

TimeStampReq	
version	타임스탬프 버젼
reqPolicy	요구정책과 관련된 정보
MessageImprint - hash Algorithm - hashedMessage	타임스탬프에 기능을 필요로 하는 데이터의 해쉬값
tads	시황정보를 확인하기 위한 TDA

표 2 타임스탬프 응답 데이터 형식

TimeStampResp	
status	PKIStatusInfomation
timeStampToken	타임스탬프 토큰 정보

표 3 타임스탬프 토큰형태

TSTInfo	
version	타임스탬프 버전
policy	타임스탬프와 관련된 정책
tsa	TSA 이름
tstTime	토큰발행시간
messageImprint	타임스탬프에 기능을 필요로 하는 데이터의 해쉬 값
serialNumber	발급일련번호
tsaFreeData	TSA의 추가 정보
tdaTokens	TemporalDataToken

(1) File Based Protocol

시점확인 정보를 포함하는 파일은 하나의 시점확인 메시지에 대해 DER 인코딩만을 포함하며, 이러한 파일은 FTP를 사용하여 시점확인 메시지를 전송하는데 이용될 수 있다.

(2) Socket Based Protocol

시점확인 메시지를 위한 소켓 기반의 프로토콜은 318번 포트를 사용한다.

(3) Time Stamp Protocol Using E-mail

MIME 타입으로 송, 수신 될 수 있으며

시점확인 메시지를 위한 간단한 인터넷 메일 전송 기법을 제공된다.

Content-Type: application/timestamp
Content-Transfer-Encoding: base64
ASN.1 DER-encoded Time Stamp message, base64-encoded〉

(4) Time Stamp protocol via HTTP

Web상에서 일반적인 HTTP를 이용하여 송신/수신될 수 있으며 시점확인 메시지를 위한 간단한 브라우저와 서버간의 전송기법이 제공된다.

Content-Type: application/timestamp
〈ASN.1DER-encoded time stamp message〉

4) 보안 고려사항

TSA/TDA 서비스를 설계할 때 유효성 및 신뢰성 있는 시간을 제공해야 하므로 다음 몇 가지 사항을 고려해야 한다.

(1) TSA/TDA가 더 이상 신뢰될 수 없다고 판단할 수 있는 근거가 있으면, TSA의 인증서는 폐지되어야 한다

(2) TSA/TDA의 개인키가 공개되면 그 인증서는 폐지된다. 따라서 키의 공개 가능성을 줄이기 위해 TSA/TDA의 개인키는 적절한 보안과 제어로 보호되어야 한다.

(3) TSA/TDA 서명키는 오랜 생명주기를 허용하기 위해 충분히 길어야 한다. 비록 이 조건을 만족할 지라도 키는 한정된 생명주기를 갖게 된다.

(4) TSA/TDA 서비스를 이용하는 응용프로그램은 응답을 기다릴 수 있는 시간의 양에 대해 관심을 가져야 한다. 왜냐하면 메시지 가로채기 공격은 시간 지연을 일으킬 수 있기 때문이다.

3.3 활용 방안

전자적 시점확인 서비스는 전자문서에 시점 확인 토큰을 부착하여 법률적 효력을 부여할 수 있게 한다. 전자문서의 유통을 확대하고 인터넷을 통한 전자거래를 안전하게 함으로서 전자거래의 발전을 촉진할 수 있으며, 향후 전자공증 시스템에도 활용할 수 있다.

4. 디렉토리(directory) 서비스

4.1 디렉토리서비스의 개요 및 필요성

인터넷상에서는 다양한 데이터들을 디렉토리 형태로 관리하고 있다. 디렉토리 서비스는 인터넷에서 상호 신뢰성 있는 정보 교환을 가능하게 하기 위해 통신 서비스에 필요한 모든 자료를 효율적으로 저장 및 관리하기 위해 정의되었으며, 인터넷에 관련되는 모든 정보를 수집하여 데이터베이스화하여 효율적으로 제공하는 기능을 담당한다. 디렉토리 서비스는 X.500, Whois, Solo, LDAP(lightweight directory access protocol), CIP(common interface protocol) 등과 같은 프로토콜을 이용한다.

4.2 디렉토리 서비스 구성 요건

인증 업무와 관련하여 고객의 정보 및 인증서를 효율적으로 관리하고 향후 폭증할 것으로 예상되는 인증서 찾기 및 수신을 원활히 처리할 수 있는 요건을 갖추어야 한다. 또한 디렉토리 서버는 중단 없는 서비스를 제공할 수 있도록 안정성이 확보되어야 한다.

디렉토리 서버의 보안을 강화하기 위해서는 표준 기반의 암호화, 검증 기능, 네트워을 통해 이동하는 데이터 보호를 위하여 SSL 상에서 LDAP이 실행되도록 하여야 한다. SSL기반 위에 LDAP을 운용하는 것은 사용자들로 하여금 클라이언트와 서버간의 통신 채널 및 서버들 간의 통신을 보호하기 위함이다.

디렉토리 서버는 국제 표준인 LDAPv2, LDAPV3를 지원하여야 한다.

디렉토리 서버는 디렉토리 서버에 전체 디렉토리를 분할(referral) 배포할 수 있어야 하며, X.509v3 기반의 사용자 인증을 통한 암호화된 커뮤니케이션과 다국적 언어 지원 그리고 응용 프로그램이 서버를 중단시키지 않고도 LDAP 클라이언트를 사용하여 디렉토리 스키마를 확장할 수 있는 기능이 있어야 한다. 디렉토리 갱신이 발생한 즉시 응용프로그램이 디렉토리 갱신 사실을 검색할 수 있도록 해야 한다.

4.3 디렉토리 시스템의 기능

1) Structured by Attribute/Value

주어진 레코드가 Attribute/Value형식의 데이터들로 표현되며, 일반적 인 디렉토리서비스 시스템을 위해서는 표준 Attribute/Value 형식의 데이터 표현이 필요하다.

2) Distributed Model

관리의 용이성, 시스템 추가시의 신뢰성을 높이며 시스템의 부하를 경감시키기 위해서는 전세계적으로 디렉토리 시스템이 분산되어 있는 구조가 필요하다

3) Fast and Efficient Search

대용량 분산 디렉토리를 갖는 시스템에서는 효율적인 데이터 검색이 필요하다.

4) Flexible Database Structure

분산환경에서 데이터베이스 구조는 관리 및 수정을 용이하게 할 수 있도록 유연한 구조가 필요하다.

4.4 디렉토리 모델

디렉토리에 저장하는 정보의 집합을 DIB(directory information base)라 하며, 사용자는 DUA(directory user agent)라는 응용 프로세스 또는 프로그램을 통해 디렉토리에 접근한다. 디렉토리는 하나 이상의 DSA(directory system agent)로 구성되어져 있다. 즉, 각각의 DSA는 하나 이상의 접근 경로를 제공하며, 각각의 DSA는 다른 상대편 DSA와 이 접근 경로를 통해서 정보를 교환한다. 일반 사용자는 DSA에게 직접 서비스를 요청하지 않고 DUA를 통해서 DSA에 접근할 수 있다.
DUA와 DSA간의 통신 프로토콜은 DAP(directory access protocol)또는 LDAP(lightweight directory access protocol)을 사용하고 DSA끼리의 통신은 DSP(directory system protocol)를 사용한다.

1) 정보 모델(information model)

디렉토리 시스템이 가지는 정보의 집합을 DIB라고 하며 DIB는 오브젝트라고 부르는 정보의 대상들이 가지는 정보들을 엔트리(entry)들로 구성한다. DIB내의 모든 엔트리는 UNIX 파일 시스템과 유사하게 내부적으로는 계층적으로 배열된 트리 구조로서 이를 디렉토리 정보 트리 DIT(directory information tree)라고 한다.
DIT 내의 모든 엔트리는 특정한 속성들로 구성된 상대 고유 이름인 RDN(relative distinguished name)을 갖는다. RDN의 역할은 상위 엔트리(countries, organization)를 가진 하위 엔트리(people, application process)를 구분하기 위하여 사용된다.
DIT는 엔트리들 간에 상위(superior)와 하위(subordinate)의 계층적 개념을 부여하며 최상위에 루트(root)라는 엔트리가 존재하게 되며, root로부터 엔트리의 위치까지 연속된 RDN의 집합을 고유하게 구별하게 되는데, 이 RDN의 집합을 고유 이름 DN(distinguished name) 이라고 부른다.
RDN과 DN은 디렉토리 정보를 액세스하기 위하여 사용되는데 고유한 이름을 가져야 하며 동시에 디렉토리 사용자가 이해 및 기억하기가 쉬워야 한다

4.5 디렉토리 서비스 기능

사용자는 DUA를 통하여 DSA에 정보를 의뢰함에 따라 디렉토리가 제공하는 서비스를 받을 수 있다. 제공받는 서비스는 기능별로 분류되고 각 분류별로 세분화된 서비스를 제공받는다.

서비스 제어는 사용자로 하여금 서비스 완료 요구 시간, 질의 결과의 양, 질의 범위, 질의의 우선 순위 등을 조절할 수 있게 한다.

1) Read:엔트리 속성의 전부 또는 일부 값을 디렉토리에서 읽기 위한 서비스 동작

2) Compare:이것은 명시된 엔트리의 어떤 속성 유형에 대한 값을 사용자가 원하는 값과 비교하는 동작

3) Search: 이것은 지정된 객체에서부터 하위 엔트리들에 대하여 제시된 조건에 맞는 엔트리들을 찾아서 선택된 정보를 출력해주는 동작

4) List:지정된 객체의 모든 하위 엔트리들을 찾아서 출력해 주는 동작

5) Add Entry:DIT에 새로운 엔트리인 Object Entry / Alias Entry를 추가하는 동작

6) Remove Entry:DIT에 지정된 엔트리를 삭제하는 동작

7) Modify Entry:현재 DIT에 존재하는 하나의 엔트리를 대상으로 새로운 속성 유형을 추가 또는 지정된 속성을 삭제하거나, 새로운 속성 값을 추가 또는 지정된 속성 값을 수정, 삭제하는 동작

8) Modify RDN:현재 DIT에 존재하는 Object Entry / Alias Entry를 대상으로 RDN을 변경시켜 주는 동작

4.6 디렉토리 서비스의 향후 전망

인터넷이 발달함에 따라 정보의 원활한 교환을 위해 디렉토리 서비스는 중요한 수단으로 부각되고 있으며 향후 디렉토리 서비스는 인트라넷, 그룹웨어 등에 널리 사용될 것이다.

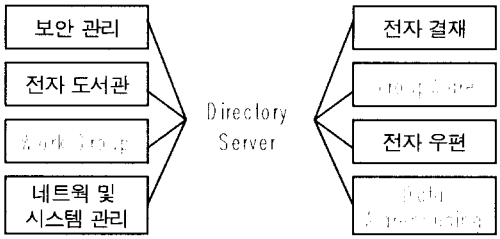


그림 3 디렉토리 서비스 전망

Ⅲ. 인증 서비스 절차

인증서의 생성, 갱신, 폐기, 정지의 주기에 따른 상호 연동과 흐름을 살펴보고자 한다.

1. 인증서 생성(certificate issue)

공인인증기관의 인증 센터를 이용하여 인증서를 발행하는 절차에 관한 여러가지 시나리오를 설명하고자 한다.

1.1 첫 번째 시나리오

RA는 등록을 대행하고 CA는 인증서를 발행하는 역할을 수행하는 것으로 사용자가 서명키를 생성하는 시나리오

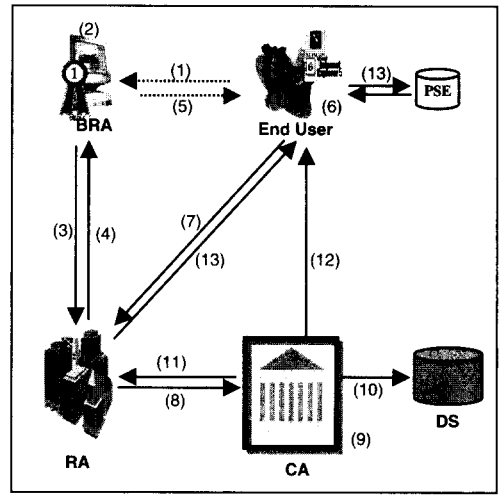


그림 4. 사용자가 RA를 통해서 먼저 사용자의 신원을 확인하고 사용자가 서명키를 생성하고 CA에 인증서를 발급하는 시나리오

이다.

(1) 사용자가 인증서를 대면(off-line)으로 신청

(2) 사용자가 제출한 서류를 통해 신분을 확인하고 신용에 대한 확인이 필요하면 신용평가의 정보를 이용하여 확인하고 필요한 사용자 정보를 입력

(3) 인증서 생성에 필요한 정보와 RA가 필요한 정보를 함께 신뢰성 있는 망을 통해서 RA에게 전달

(4) RA는 필요한 정보를 저장하고 고객에게 고유한 등록번호를 부여하여 BRA에게 보냄

(5) BRA는 고객에게 등록번호와 사용자 S/W를 사용자에게 배포

(6) 사용자는 사용자 S/W를 이용하여 자신의 서명용 키 쌍을 생성하여 전자서명 생성키는 암호화하여 저장소에 보관

(7) 사용자는 등록번호, 필요한 정보, 자신의 전자서명용 검증키를 인증서 요청 형식을 만들어 RA에게 신청

(8) RA는 등록번호를 확인하고 인증서 요청 형식을 즉시 또는 RA 관리자에 의해 CA에게 요청함

(9) CA는 해당 RA를 확인하고 인증서

신청 형식을 검증한 후 자신의 전자서명 생성키를 이용하여 인증서를 발급하고 필요시 키 관리용 키를 생성하고 사인하여 저장

(10) CA는 고객의 요구에 따라 발급된 인증서를 디렉토리 서버에 게시

(11) 발급된 인증서를 RA에게 전송

(12) CA는 인증서 발급을 메일로 통보

(13) 인증서를 사용자가 RA에서 Download를 받아서 자신의 안전한 저장소에 저장

1.2 두 번째 시나리오

RA에서 신원확인을 하고 인증서의 발행은 CA와의 신뢰성 있는 프로토콜을 이용하여 상호연동 함으로써 CA의 모습을 숨기는 시나리오이다.

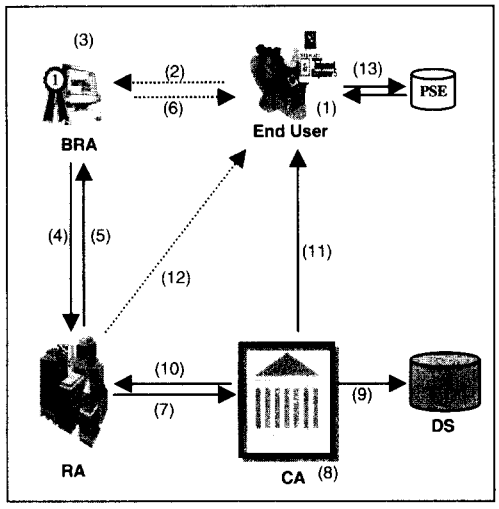


그림 5. 사용자가 서명키를 생성하고 RA를 통해 신원/신용을 확인하고 CA에게 인증서 발급요청을 하여 인증서를 발급하는 시나리오.

(1) 사용자는 사용자 S/W를 이용하여 자신의 전자 서명용 키 쌍을 생성하고 자신의 전자서명 생성키는 안전한 저장소에 보관

(2) 사용자가 공개키와 인증서 생성에 필요한 정보를 가지고 인증서 신청형식(PKCS#10)을 작성하고 비밀키를 이용하여 서명하여 대면(off-line)으로 신청

(3) 사용자가 제출한 신분증 및 기타 서류를 이용하여 신분을 확인하고 비밀키 보유여부를 확인하고 필요한 정보를 입력하고 인증서 요청형식을 저장

(4) 인증서 요청형식과 RA가 필요한 정보를 RA에게 신뢰성 있는 망을 통해 전달

(5) RA는 필요한 정보를 저장하고 고객에게 유일한 등록번호를 부여하여 BRA에게 통보

(6) BRA는 고객등록번호 및 사용설명을 사용자에게 통보

(7) RA는 인증서 요청 형식을 즉시 또는 RA 관리자에 의해 CA에게 안전하게 전달

(8) CA는 RA에 정보를 확인하고 사용자 관련정보에 저장하고 새로운 엔트리를 생성하고 CA는 사용자의 공개키를 자신의 전자서명 생성키로 서명하여 인증서를 생성

(9) CA는 고객의 요구에 따라 발급된 인증서를 디렉토리 서버에 게시

(10) 발급된 인증서를 RA에게 전송

(11) CA는 인증서 발급을 메일로 통보

(12) RA는 사용자의 인증서를 Disk나 Smart Card를 이용하여 off-line으로 전달

(13) 사용자는 인증서를 받아서 안전한 저장소에 저장

1.3 세 번째 시나리오

사용자와 RA간의 On-line으로 인증서를 신청하고 RA가 신원정보를 확인하고 CA에게 인증서를 신청하고 CA는 인증서를 발급하는 시나리오이다.

(1) 사용자는 사용자 S/W를 이용하여 전자 서명용 키 쌍을 생성

(2) 사용자가 전자서명 검증키와 인증서의 생성에 필요한 정보를 가지고 인증서의 요청형식(PKCS#10)을 작성하여 RA에게 신청

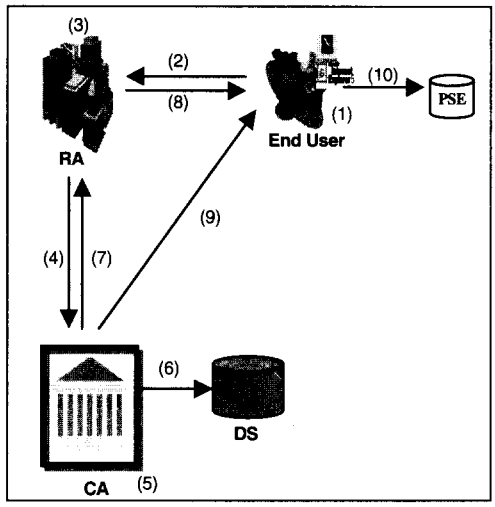


그림 6. 사용자에게 인증서를 on-line으로 발급을 위한 것으로 RA는 신원을 확인하고 CA에게 발급을 요청하여 인증서를 발급 받는 시나리오.

(3) 사용자가 제출한 정보를 이용하여 신원정보 및 신용정보를 확인하여 발행 가능 여부를 판단하여 적절치 못한 경우는 사용자에게 통보하고 이상이 없을 시에 RA에 사용자 정보를 저장

(4) 인증서 요청형식과 CA가 필요한 정보를 함께 CA에게 신뢰성 있는 망을 통해 전달

(5) CA는 RA에 정보를 확인하고 사용자 관련정보에 저장하고 새로운 엔트리를 생성하고 CA는 사용자의 공개키를 자신의 비밀키로 서명하여 인증서를 생성

(6) 발행된 인증서를 디렉토리 서버에 게시

(7) 생성된 인증서와 CA에 관한 정보를 RA에게 전달

(8) RA는 사용자에게 인증서를 전달 (HTTP/FTP/LDAP)

(9) CA는 사용자에게 인증서 발급을 메일로 통지

(10) 전송된 인증서를 자신의 안전한 저장소에 저장

2. 인증서 갱신(certificate renewal)

인증서의 유효기간이 지나기 전에 CA에게 사용자는 소유를 증명할 수 있는 새로운 공개키와 인증서 발급 시 입력한 암호를 이용하여 갱신하고 갱신절차는 인증서 발급에 준하여 실행한다.

3. 인증서 폐지(certificate revocation)

사용자가 자신의 키가 노출되었거나 분실되었을 경우 RA를 통해 인증서 폐지를 신청하고 CA는 인증서를 폐지하여 인증서 폐지 목록(CRL)에 추가하여 디렉토리서버나 사용자에게 배포한다.

4. 인증서 정지(certificate suspension)

사용자가 인증서의 사용을 일정기간 정지를 요구하거나 특정 사유에 의해 정지가 필요한 경우에 정지를 하고 인증서 정지 목록(CSL)을 통해 정지된 인증서 목록을 정기적으로 배포한다.

Ⅳ. 결 론

공개키 알고리즘을 이용한 전자서명에 법적인 효력이 부여됨에 따라 인증서를 기반으로 한 각종 서비스들이 더욱 많이 제공될 것으로 보인다. 이를 지원하기 위한 공인인증서 발급기관인 한국정보인증(주)이 갖추어야 할 각종 시스템들과 이들이 갖추어야 할 기능들에 대하여 간략히 기술했다. 또한, 고객이 인증기관으로부터 인증서를 발급 받는 과정뿐만 아니라 갱신 및 폐지하는 절차에 대해서도 언급했다.

공인인증기관을 통하여 발급되는 인증서는 인터넷상에 존재하는 전자 쇼핑몰 서버가 자신의 존재를 공인인증기관으로부터 공식적으로 인정받게 됨으로서 이 쇼핑몰의 고객도 좀 더 안심하고 인터넷 쇼핑을 즐길 수 있게 될 것이다. 한편, S/MIME을 이용한 전자메일의 경우, 공인인증기관이 발급한 인증서를 이용하여 메일 본문에 전자서명을 하게 되면 문서로서 법적인 효력을 갖게 됨으로서 개인 또는 기업간의 공식적인 문서교환에 S/MIME 전자메일 프로토

콜이 널리 이용될 것으로 보인다.

공인인증기관이 제공할 시점 확인 서비스(time stamping service)는 문서 발생 시점을 공인해줌으로서 기존 인터넷상에서 작성, 유통되는 전자문서의 생성 시점 불명확으로 인한 많은 문제들을 해결할 수 있을 것이며 향후 전자문서 내용 증명, 공증 등과 같은 서비스에 활용될 것이다.

참 고 문 헌

[1] 한국정보보호센터 "공인인증기관 세부지정기준(안)", 전자서명 인증관리센터 개원 자료집, pp. 49-61, July 7, 1999.

[2] 한국정보보호센터 "전자서명 인증관리센터 구축, 운영을 위한 시스템 규격", 전자서명 인증관리센터 개원 자료집, pp. 63-68, July 7, 1999.

[3] Arsenault, A., Turner, S., "Internet X.509 Public Key Infrastructure PKIX Roadmap," Draft-ietf-pkix-roadmap-02.txt, June 23, 1999.

[4] Housley, R., Ford, W., Polk, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC2459, January 1999.

著者紹介----------

김 용 준(Yong-June Kim)

1971년 2월 : 서강대 물리학과 졸업(학사)
1974~1978년 : KIST 전산개발실 연구원
1978~1998년 12월 : 전자통신연구원 부설 정보통신진흥원 서울 사무소장
1999년 현재 : 한국정보인증(주) 시스템개발실 실장
<관심분야> 정보처리, 정보보호

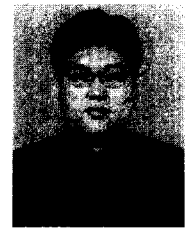
백 석 철(Seok-Chul Baek)

1982년 2월 : 서울대학교 물리교육학과 졸업(학사)
1983~1985년 2월 : KAIST 물리학과 석사과정 졸업(석사)
1985~1991년 2월 : 한국통신 연구개발본부 전임연구원
1991~1995년 8월: KAIST 물리학과 박사과정 졸업(박사)
1995~1998년 7월: 한국통신 멀티미디어연구소 인터넷 보안연구실장
1998~1999년 5월: 시큐어소프트 보안연구소 소장
1999년 현재: 한국정보인증(주) 시스템개발1부 부장
<관심분야> 정보보호(PKI, Firewall, IDS), 정보처리

정 종 윤(Jong-Yoon Jung)

1994~1996년 2월 : 국민대학교 정보통신학과 석사과정 졸업(석사)
1992~1999년 7월: 한국통신 멀티미디어연구소 인터넷보안연구실 연구원
1999년 현재 : 한국정보인증(주) 시스템개발1부 응용서비스 개발과장(선임연구원)
<관심분야> 정보보호, 정보처리

박 정 식(Jung-Sik Park)



1992~1994년 2월 : 연세대학교 수학과 석사과정 졸업(석사)
1995~1999년 8월: 한국통신 멀티미디어연구소 인터넷연구실 전임연구원
1999년 현재 : 한국정보인증(주) 시스템관리부 관리과장(선임연구원)
<관심분야> 정보보호, 암호학, PKI, 고속 연산 알고리즘

김 재 중(Jae-Jung Kim)

1990~1997년 2월 : 충남대학교 퓨터과학과 학사과정 졸업
1996~1999년 7월: LG-EDS 시스템 인터넷사업팀 연구원
1999년 현재 : 한국정보인증(주) 시스템개발1부 연구원
<관심분야> 정보보호, PKI