通信情報保護學會誌
第8卷 第3號, 1998. 9

전자공증 서비스 현황

Trend of Electronic Notary Service

김 지 홍*

요 약

공개키 기반구조에서는 인증서를 사용 함으로서 기본적으로 암호 및 인증기능을 제공한다. 이와 더불어 신뢰성 있는 부인방지기능을 제공하기 위하여 상위등급의 보안기능을 가진 인증기관 혹은 제3의 신뢰성 있는 공증기관을 별도로 둠으로서, 타임스탬프 기능과 공증기능을 부가하여 전자공증 서비스를 제공할 수 있다. 사용자의 요구에 따라 데이터 혹은 인증서에 대하여 타임스탬프를 발행하는 타임스탬프 발행당국(TSA)과 공증을 행하는 공증당국(NA)을 살펴보고, 현재까지 제안된 타임스탬프 및 공증 프로토콜에 대한 분석과 더불어 전자공증 서비스에 대한 국제동향을 검토, 분석한다.

1. 서 론

최근 일반가정에 개인용 컴퓨터의 보급이 급격히 늘고, 정보통신 기술의 발달로 인하여 전세계가 인터넷이라는 거대한 정보 네트워크 하에 움직이고 있다. 인터넷상에서 선진 외국의 최근 문서와 동향을 수집할 수 있을 뿐 아니라, 전자상거래와 같은 사이버 비즈니스가 급증하고 있다. 이러한 사이버 거래는 기본적으로 상호간의 신뢰가 바탕으로 이루어져야 한다. 따라서 이러한 요구를 수용하기 위하여 공개키 기반구조 및 각종 암호 및 인증알고리즘을 이용한 다양한 프로토콜이 제안되고 있다.

* 세명대학교 전자공학과

공개키 기반구조에서 사용되는 보안정책은 일반적으로 3개의 등급(하위, 중간, 상위보안등급)으로 나뉜다. 하위 보안등급 정책은 전자우편과 같이 기밀성이 낮은 데이터의 전송에 사용되며, 사용되는 키 비트수도 최하 768 비트 정도로 규정되어 있으며, 별도의 공증기능을 요구하지 않는다. 중간 보안등급 정책의 경우에는 사적인 공문서발송과 같이 중간등급의 기밀성을 요구하는 데이터전송에 사용되며, 키 비트수도 최하 896 비트 정도로 규정되어 있으며, 인증기관에서의 타임스탬프(time stamp) 기능 정도만을 요구한다. 상위 보안등급 정책의 경우에는 기밀을 요하는 전자상거래등과 같은 금융분야의 문서를 다루는데 사용되며, 키 비트수도 최소 1024 비트이상을 사용하도록 규정[4-2-1]되어 있으며, 인증기관에서의 공증

기능(notary service)을 요구한다.

일반적으로 문서에 대한 공증(notary) 기능을 공개키 기반구조에 적용할 경우에 기존의 인증기관(CA : Certification Authority)에 부가하는 경우와 별도의 제3의 신뢰기관(TTP : Trusted Third Party)으로 공증기관(NA : Notary Authority)을 이용하는 경우가 있다. 인증기관에 공증기능을 부가하는 경우에는 공증센터로서의 신뢰성이 문제가 될 수 있지만, 공개키 기반구조의 상위 인증기관을 통하여 인증을 받는 것으로 해결될 수 있다. 그러나 인증기관에 대한 부하가 커지고, 일반적인 공증센터로서의 개념보다는 소규모그룹에 대한 공증센터의 개념을 가지게 됨에 따라 공개키 기반구조에 별도로 공증기능만을 전담할 수 있는 제3의 신뢰성 있는 주체에 의해 구성되는 공증기관의 개념이 일반화되고 있다. 전자공증 기관의 요건으로는 신뢰성이 가장 중요하며, 안전성과 공증서비스와 관련된 기술력이 확보되어야 하며, 공개키 기반시스템과의 상호운용성이 보장되어야 한다. 그 외에도 사용자 측면에서는 공증기능이 편리하게 이루어져야 하며 가격이 적당하여야 한다. 또한 추후 분쟁이 발생되었을 때, 증거의 유효성을 제시하지 못함으로 인한 손해배상에 대한 책임을 져야 한다.

2. 전자공증 시스템 구성

전자공증 시스템의 구성은 PKI 구성에 준하며, 공개키/개인키에 대한 생성장소에 따라 두 가지로 구성될 수 있다. 공개키/개인키를 단말개체에서 생성할 수 있는 사용자 키 생성방식과 PKI 구성하에서 상위 보안등급이 보장되는 인증기관(CA) 혹은 제3의 신뢰기관(TTP)인 공증기관(NA)에서 생성하는 집중형 키 생성방식으로 분류할 수 있다. 먼저 공개키/개인키를 단말개체(end entity)에서 생성하는 경우에는 강력한 부인방지기능과 안전성이 높다는 장점을 가지고 있으며 그림 1과 같이 구성된다.

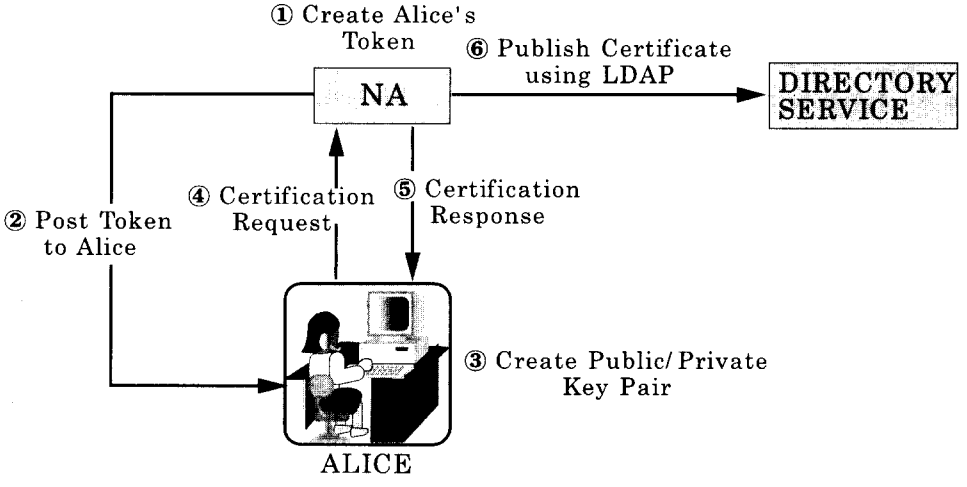


그림 1. 사용자 키 생성방식

① NA는 사용자(Alice)의 신원확인 과정을 거치고, 사용자에게 스마트카드 혹은 디스켓형태의 토큰을 발행한다. 이 토큰에는 사용자가 자신의 공개키/개인키 쌍을 생성할 수 있도록, 이에 부합된 키 자재(Key Material)가 포함된다.

② NA는 PIN이 할당된 토큰을 비밀채널을 통하여 사용자에게 보낸다 (크레디트카드 발급과정과 유사함).

③ 토큰과 PIN을 수신한 사용자는 자신의 공개키와 개인키를 생성한다.

④ 사용자는 자신의 공개키를 포함한 인증서 요구메시지를 NA에게 보낸다.

⑤ NA는 인증서 요구 메시지의 유효성을 확인하고, 인증서 요구에 대한 응답 메시지를 사용자에게 보낸다.

⑥ 동시에 NA는 발급한 인증서를 인증서 보관소(X.500 디렉토리 혹은 LDAP 서버)에 보낸다.

단말개체에서 공개키/개인키를 생성할 수 없는 경우에는 상위 인증기관(CA) 혹은 제3의 신뢰기관(TTP) 인 공증기관(NA)에 의해 생성될 수 있다. 이 방식은 키가 훼손된 경우에 키를 복구할 수 있는 기능을 가지고 있다는 장점이 있으며 그림 2와 같은 구조를 가진다.

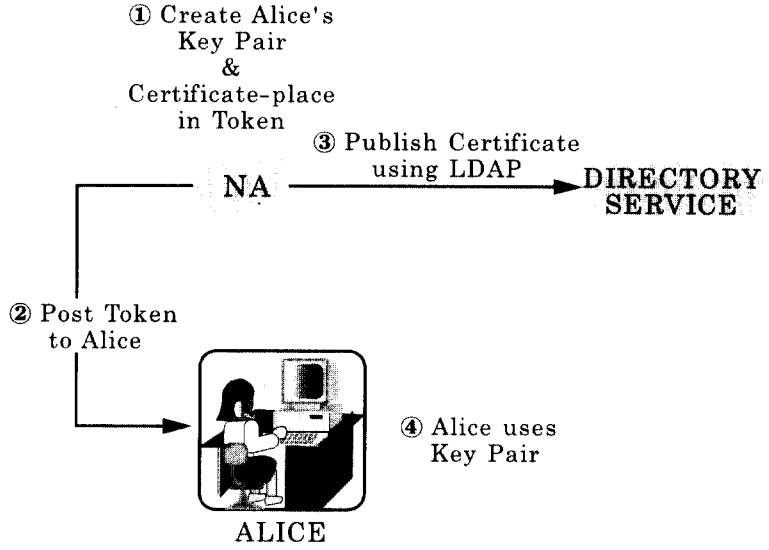


그림 2. 집중형 키 생성방식

① NA는 사용자(Alice)의 신원확인 과정을 거치고, 사용자에게 스마트카드 혹은 디스켓형태의 토큰을 발행하며, NA는 Alice에 대한 PIN을 할당한다. 이 때의 토큰에는 NA가 생성한 Alice의 공개키/개인키 쌍과 공개키 인증서가 포함된다.

② NA는 사용자에게 PIN이 할당된 토큰을 보낸다.

③ 동시에 NA는 인증서를 인증서 보관소(X.500 디렉토리 혹은 LDAP 서버)에 보낸다.

④ 사용자는 토큰을 수신한다.

3. 전자공증 시스템의 기능 및 프로토콜

3.1 전자공증 시스템의 기능

인터넷상에서 사용되는 전자공증 시스템의 기능은 일반적으로 상용되고 있는 공증의 기본서비스와 공개키 기반시스템과 관련된 인증서 공증 등의 추가서비스를 제공한다. 공증기관은 제시된 데이터(인증서, 서명문, 기타 메세지)에 대한 정확성, 유효성을 확인시켜 주는 TTP 로서, NA의 일반적인 기능은 다음과 같다.

- 서명문 공증요구인 경우에는 동봉된 디지털 서명이 정확한 지를 확인하고, 서명의 유효성을 입증하는 서명된 공증토큰을 생성한다.
- 인증서 공증요구인 경우에는 동봉된 인증서의 유효성과 인증서 폐지정보를 확인하고, 인증서의 폐지상태 정보와 유효성을 입증하는 서명된 공증토큰을 생성한다.
- 데이터 공증요구인 경우에는 동봉된 데이터의 정확성을 확인하고, 데이터의 유효성을 입증하는 공증토큰을 발행한다.
- 시간의 단조 증가값을 이용하며, 타임스탬프 토큰을 공증토큰내에 포함한다.
- 서명에 사용된 신뢰정책과 유효성 정책의 고유확인자를 서명된 각각의 공증토큰에 포함한다.
- 해당 공증토큰이 서명문 확인인지, 인증서 확인인지, 데이터 확인인지를 토큰내에 지정해 주어야 한다.
- 서명된 영수증을 의뢰인에게 발행한다.

3.2 공증 프로토콜과 타임스탬프 프로토콜

공증과 관련된 기본서비스에는 공증일자를 표시하는 타임스탬프 기능, 데이터의 무결성을 증명하는 내용증명, 착신부인방지를 위한 배달증명, 그리고 후일의 분쟁을 막기위한 전자 보존기능 등이 있다. 이러한 공증기능을 제공하기 위하여 공증 프로토콜과 타임스탬프 프로토콜이 사용되며, 본 장에서는 Entrust 사에서 제안한 "notary protocols 2.0"[4-3-2] 과 "time stamp protocols" [4-3-2]에 대하여 설명한다.

(1) 공증 프로토콜

공증서비스[4-3-1]에는 공증대상이 데이터인 경우와 인증서인 경우가 있다. 데이터를 공증하는 경우에는 공증기관(NA: Notary Authority)에서 데이터의 내용이 틀림이 없음을 확인하고 공증토큰을 발행한다. 이 경우에서 데이터의 정확성이란 데이터의 내용에 대한 정확성으로, 데이터와 함께 전송되는 서명문에 국한되는 것은 아니다. 예를 들면 데이터에는 한 개 이상의 서명문을 포함할 수도 있으며, 내용증명을 요구하는 일종의 주장을 포함할 수도 있으며, 또한 문서의 법적 유효성을 요구하는 계약서와 같은 내용도 될 수 있다. 따라서 이와 같이 내용에 대한 공증을 요구하는 경우에는 필연적으로 PKI 정책사항과 데이터 형식에 맞게 적용되어야 한다.

인증서를 공증하는 경우에, 공증기관은 해당 인증서가 유효한 인증서임을 확인하고, 일정기간동안 인증서를 보장하여야 한다. 즉, 인증서 서명자로부터 신뢰지점(trusted point)까지의 충분한 인증서 경로를 조사해야 한다. 또한 공증기관은 인증서 폐지목록을 참조하고, 현재 인증서의 상태정보를 보충할 수 있다. 따라서 이러한 정보를 포함하고, 공증으로 보장되는 일정기간동안 사용할 수 있는 공증 토큰을 생성하여야 한다. 생성된 공증토큰은 사용자의 인증서가 폐지된 상황이라 할지라도, 공증 토큰을 사용 함으로서 서명문의 수명이 연장될 수 있다. 다음은 공증서를 발행하는 과정[4-3-2]을 보인다.

① 공증 서비스 요구자는 NA에게 공증요구 메시지(표1)를 보낸다.

② NA는 공증요구 메시지의 유효성을 확인하고, 해당 요구와 관련된 공증서비스를

행하고, 공증토큰(표2)을 생성하고, 이를 공증 서비스 요구자에게 보낸다.

③ 공증 서비스 요구자는 NA로부터 공증 토큰을 수신하고, 해당 공증서비스의 유효성을 확인(시간, NA이름, 서비스 및 정책, 상태정보 등)한다.

이러한 확인절차가 끝나면, 공증 토큰은 데이터의 정확성과 소지를 인증하는 기준으로 사용될 수 있다.

표 1. 공증 요구데이터 형식

NotaryReqData	Service	서비스형태
	Requester	요구자 이름 - 선택영역
	signatureAlgorithm	사용된 서명문 알고리즘
	certs	인증서 체인
	reqPolicy	요구정책과 관련된 정보
	notary	공증기관 이름
	reqTime	요구시간 - 선택영역
	data	공증을 필요로 하는 데이터
Signature		서명문

표 2. 공증토큰의 형태

Notaryinfo	NotaryReqInfo	NotartyReqData와 동일
	MessageImprint	1. 순수 데이타 2. Hash algorithm을 경유한 데이타
	ReqSignature	요구된 공증 서비스의 종류
	Policy	공증정책과 관련된 정보
	Status	공증토큰의 상태정보
	Time	공증시간
	SignatureAlgorithm	서명문에 사용된 알고리즘
	CertID	NA의 공개키 확인 인증서
	ChainCerts	신뢰고리(trust chain)-선택영역
	Certs	인증서 체인 - 선택영역
	Crls	인증서 리스트 - 선택영역
Signature		서명문

(2) 타임스탬프 프로토콜

타임스탬프 프로토콜 [4-3-2]은 시각증명을 필요로 하는 사용자들을 위하여 제공되며, 공증기능을 담당하는 NA에 속할 수도 있으며, 또한 별도로 TSA(Time Stamp Authority)를 둘 수도 있다. 또한 이와 같이 TSA는 상당한

신뢰성을 요구하기 때문에 별도로 TDA(Time Data Authority)를 두어 타임스탬프 토큰에 포함된 시간을 확인해 주는 기능만을 행하는 별도의 기관을 구성할 수 있다. 타임스탬프 서비스요구 및 토큰 발생과정은 다음과 같다.

① 타임스탬프 서비스 요구자는 TSA에게 타임스탬프 요구메시지를 보낸다.

② TSA는 타임스탬프 요구 메세지(표3)를 확인하고, 해당 요구와 관련된 타임스탬프 토큰을 생성하고, 이를 타임스탬프 서비스 요구자에게 보낸다.

③ 타임스탬프 서비스 요구자는 TSA로부터 타임스탬프 토큰(표4)을 수신하고, 타임스탬프 토큰의 유효성을 확인한다. 또한 TSA의 서명문을 확인하고, 토큰에 기재된 타임 스탬프가 요구한 시간에 맞는지, TSA 이름 등의 각 영역별 내용이 정확한지를 확인한다.

이러한 확인절차가 끝나면, 타임스탬프 토큰은 신뢰성 있는 시간기준으로 설정되어 사용될 수 있다.

표 3. 타임스탬프 요구데이터 형식

TimestampReq	Requester	타임스탬프 서비스 요구자
	ReqPolicy	요구정책과 관련된 정보
	Tsa	TSA 이름
	Tdas	시황정보 확인을 위한 TDA
	MessageImprint - hash Algorithm - hashedMessage	타임스탬프 기능을 필요로 하는 데이터의 해쉬값

표 4. 타임스탬프 토큰 형태

TSTInfo	Policy	타임스탬프와 관련된 정책
	Status	PKIStatusInfo
	Requster	타임스탬프 요구자
	Tsa	TSA 이름
	SignatureAlgorithm	서명문에 사용된 알고리즘
	CertID	TSA의 인증서 ID
	Certs	단말개체인증에 필요한 인증서 계열
	GenTime	타임스탬프 토큰 생성시간
	TdaTokens	시황데이타(Tem poralData)토큰계열
	MessageImprint	타임스탬프 요구데이터와 동일
Signature		서명문

4. 전자공증 시스템의 연구동향

현재 전자공증서비스를 제공하는 업체는 Entegrity, Entrust, Verisign, Surety, NetDOX 등이 있으며, 본 장에서는 전자우편의 형식으로 사용되는 Entegrity 사의 Cashware 시스템을 설명하고, NETDOX 사의 공증방식에 대하여 구체적으로 설명한다. 마지막으로 기존의 공증서비스 제공업체와 연계하여 디지털 공증기록 인증서비스(Digital Notary Record Authentication)를 제공하는 Surety 사에 대하여 설명한다.

4.1 Entegrity

Entegrity사에서 제공되는 공증서비스[4-3-1] 구조는 기본적으로 PKI 구조를 따른다. Top-CA를 근원 CA로 두고, 하부의 각 CA는 계층구조로 구성되며, 상위계층의 CA는 하위계층의 CA에 대한 공증용 인증서를 발급한다. 각 CA는 상호인증 기능이 제공되며, 타 기반 시스템과의 상호인증기능도 제공된다. Entegrity 사에서 개발된 Cashware(그림 3)는 전자우편 방식을 이용하여 사용자와 서버간의 현금거래에 사용되며, 강력한 부인방지 기능을 제공한다.

Cashware를 이용하기 위해서는 사용자는 Cashware 응용모듈과 SDP(Security Development Platform)라는 보안모듈을 설치하여야 한다. 사용자는 NA로 부터 직접 인증서와 키 자재를 포함한 스마트 카드 혹은 디스켓을 수령하고, 이 후에는 스마트 카드를 이용하여 NA에 접속할 수 있으며, 또한 사용자와 서버간에는 SDP 기반하에 S/MIME 프로토콜에 의해 거래가 행하여 진다.

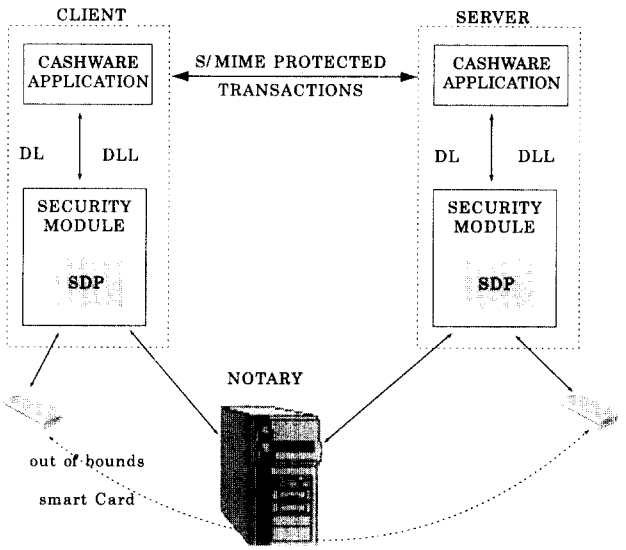


그림 3. Entegrity Cashware 구조[4-3-1]

일반적으로 PKI 구조에서는 상위등급의 보안정책으로 1024 비트이상의 RSA 키 비트를 권고하고 있지만, Entegrity사에서는 인증서를 발급하기 위해서는 2048 비트의 RSA 키를 사용한다. 인증서 형식은 X.509 V3.0을 사용하며, 인증서 폐지목록은 X.509 V2.0의 형식을 사용하고 있으며, 인증서 및 인증서 폐지목록을 획득하기 위한 전송계층의 프로토콜로는 WWW

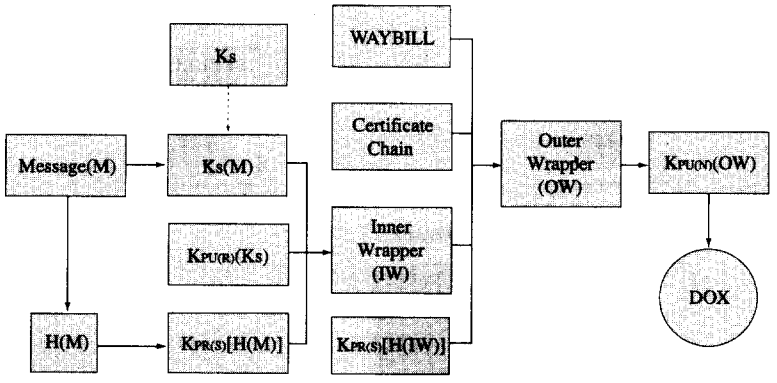
상에서 사용될 수 있는 HTTP 프로토콜을 사용하고 있으며, 인증서 보관소에 저장하기 위하여 LDAP 프로토콜을 사용한다.

4.2 NetDOX

NetDOX사에서는 중요 업무용정보를 안전하고 가장 효율적으로 전달할 수 있는 공증서비스로서 DOXIT 서비스를 제공한다. DOXIT 서비스[4-3-4]는 송신자, 수신자, NetDox 센터로 구성되며, 송신자 측에서는 다음과 같은 항목을 구비하여야 한다.

- 기밀성을 요하는 데이터
- 수신자의 디지털 인증서
- 송신자의 개인키/공개키 쌍
- Network에서 공유되는 암호화 알고리즘 및 해쉬함수
- NetDox 클라이언트 소프트웨어 패키지

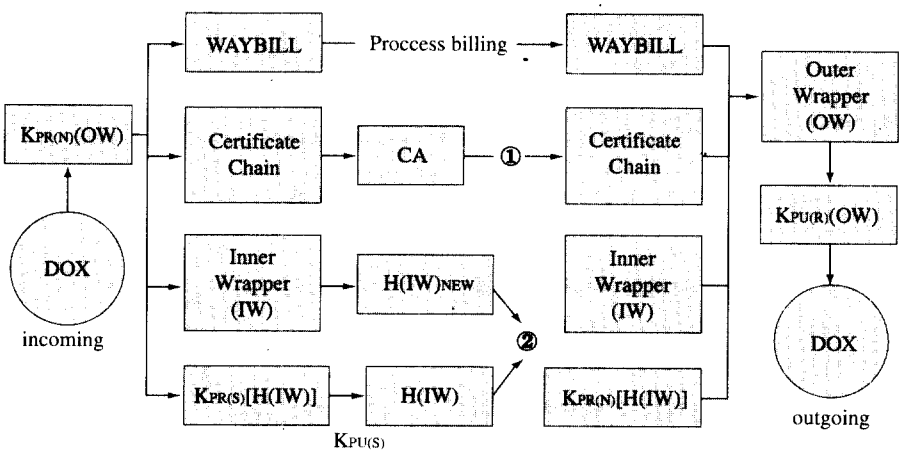
송신자는 메시지를 NetDox 소프트웨어 패키지에서 생성한 임의의 세션키로 암호화하고, 세션키는 수신자의 인증서로부터 획득한 수신자의 공개키를 이용하여 암호화된다. 또한 메시지는 NetDox 소프트웨어 패키지에서 제공되는 해쉬알고리즘을 이용하여 메시지 축약(Message Digest)을 생성하고, 이를 자신의 비밀키를 이용하여 서명문을 생성한다. 이러한 서명문은 후일 분쟁이 발생될 때 사용될 수 있도록 보관되어 진다. 결과적으로 위의 세가지 부분은 인터넷의 전자메일의 표준화 형식인 MIME 형식으로 만들어 지며, 이를 NetDox의 "Inner Wrapper(IW)"라 한다. 이러한 "IW" 에 다시 인증서 체인정보와 리스트정보가 첨부되고, "IW"를 다시 송신자의 비밀키로 암호화하여 서명문을 생성하고, 이를 다시 첨부하여 MIME 형식의 "Outer Wrapper (OW)"를 구성한다. 마지막으로 이러한 "OW" 파일은 다시 공증기관인 NetDox의 공개키로 암호화하여 표준 S/MIME 메시지 형식의 "DOX" 파일을 구성하여 인터넷을 통하여 NetDox로 전송된다.



Ks : Session Key
H : Hash Algorithm
KPR(S): Sender's Private Key, KPU(S): Sender's Public Key
KPR(R): Recipient's Private Key, KPU(R): Recipient's Public Key
KPR(N): NetDox's Private Key, KPU(N): NetDox's Public Key

그림 4. 송신자 측에서 하는 일

NetDox는 수신된 "DOX"에서 자신의 비밀키를 이용하여 리스트정보, 인증서 체인정보, "IW", 서명문을 분리한다. 인증서 체인으로부터 각각의 인증서의 유효성을 확인하기 위하여 해당 CA로부터 CRL 정보를 수신함으로서 이를 검증하고, "IW"를 해쉬 알고리즘을 통하여 만들어진 "IW"의 디지털 해쉬값과, "DOX"로부터 분리된 서명문을 송신자의 공개키로 복호한 값을 비교하여 동일하면, "DOX" 정보가 해당 송신자로부터 송신된 것임을 확인하게 된다. 확인된 경우에는 리스트정보, 인증서 체인, "IW", 서명문을 NetDox의 개인키로 서명문을 생성하고, 이를 다시 첨부하여 MIME형식의 "OW"를 구성한다. 마지막으로 이러한 "OW" 파일은 다시 수신자의 공개키로 암호화하여 표준 S/MIME 메시지 형식의 "Outgoing DOX" 파일을 구성하여 인터넷을 통하여 수신자에게 전송한다.



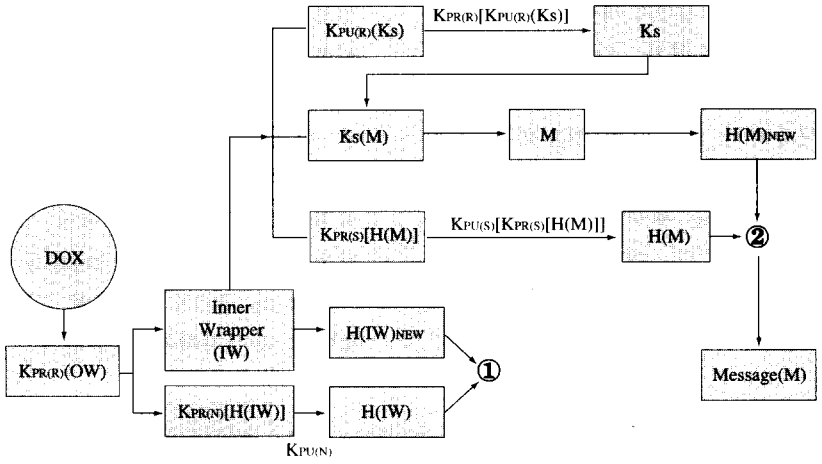
① Certificate is genuine and current
② Inner Wrapper(from sender) not altered or damaged

그림 5. NetDox 공증센터에서 하는 일

수신자는 수신된 "outgoing DOX" 파일에서, 자신의 비밀키를 이용하여 리스트정보, 인증서체인, "IW"와 NetDox의 서명문을 추출하고, NetDox의 서명문을 해독한 결과값과 해쉬 알고리즘을 통한 "IW"의 디지털 해쉬값을 비교하여, 이 값이 일치하면 내용이 변조되지 않았음을 확인하게 된다. 수신자의 개인키를 이용하여, "IW"에서 암호화된 세션키, 암호 메시지, 송신자가 서명한 디지털 서명문을 추출한다. 또한 수신자의 개인키를 이용하여, 암호화된 세션키에서 세션키를 추출하고, 이를 이용하여 암호 메시지를 해독한다. 해독된 메시지는 다시 디지털 해쉬값을 구성하고, 이 값과 송신자의 공개키를 이용하여 해독한 서명문의 디지털 해쉬값이 일치하는 지를 테스트한다. 이러한 과정이 성공하면, 송신자를 인정하게 되고 결국 수신자는 메시지에 이상이 없음을 확인할 수 있다.

4.3 Surety

마지막으로 기존의 공증서비스 제공업체와 연계하여 디지털 공증기록 인증서비스(Digital Notary Record Authentication) [4-3-5]를 제공하는 Surety 사에 대하여 설명한다. Surety 사



① Contents(from NetDox) not altered or damaged
② Original content(from sender) is not altered or damaged

그림 6. 수신자측에서 하는 일

의 디지털 공증기록 인증서비스는 매초 단위로 발생되는 여러 사용자들의 공증기록 데이터를 효과적으로 보관하기 위한 방법을 제공한다. 즉, 공증 기록 데이터를 보관하기 위해 해쉬 알고리즘을 사용하여, 각 문서에 대한 "Digital Fingerprints" 를 작성보관한다. 매초 단위의 기록보관 방법은 그림 7과 같이 구성되며, 각 level에서 하는 기능은 다음과 같다.

① level 2에서는 매초 단위로 발생되는 각 사용자들의 문서 A,B,C,D 를 각각 Hash Algorithm 을 이용하여 288 비트의 해쉬값 H(A), H(B), H(C), H(D) 를 생성한다.

② level 1에서는 각 문서의 해쉬값 H(A)와 H(B)를 연결하여 576 비트로 구성하고, 이를 다시 해쉬함수를 통하여 288 비트의 결합 해쉬값 H(E)를 생성하고, 마찬가지 방법으로 H(F)를 생성한다.

③ level 0에서는 level 1에서 생성된 해쉬값 H(E)와 H(F)를 연결하여 576 비트로 구성하고, 이를 다시 해쉬함수를 통하여 288 비트의 결합 해쉬값 H(S)를 생성한다.

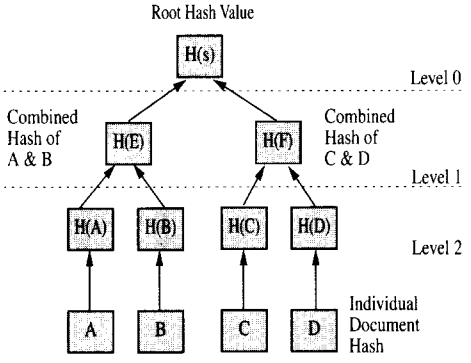


그림 7. 매초당 공증기록 보관용 RHV 생성방법

이와 같이 계층구조 방법으로 매 초당 1개의 288 비트의 근원 해쉬값(RHV : Root Hash Value)를 생성하고, 다시 1초 후에는 마찬가지로 1의 방법으로 이전에 생성된 근원 해쉬값과 현재시간에 생성된 근원 해쉬값을 연결하여 576 비트를 구성하고, 이를 다시 해쉬함수를 통하여 288 비트의 "SHV(Super Hash Value)"를 생성한다(그림 8 참조).

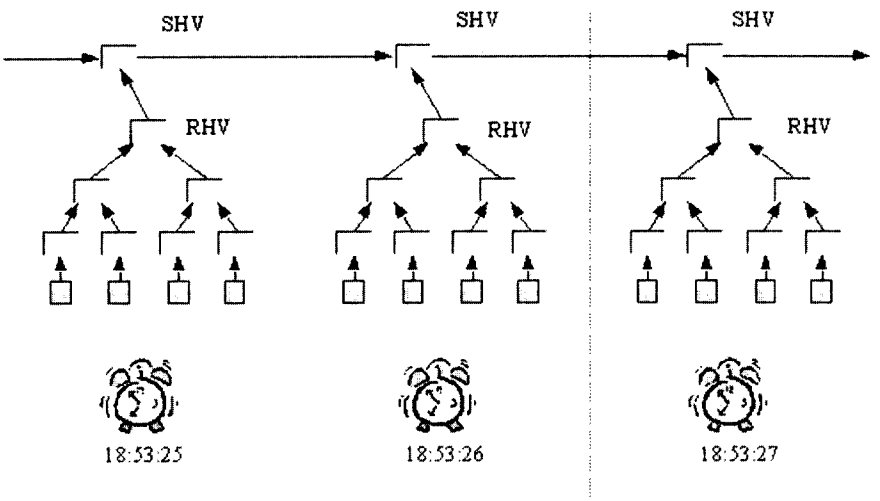


그림 8. 공증기록 보관용 SHV 생성방법

Surety사는 그림 8과 같은 방법으로 매 초당 288 비트씩 레지스트리에 보관하는 방식을 사용한다.

5. 결 론

본 논문에서는 공개키 기반구조에서의 신뢰성 있는 부인방지 서비스를 제공하기 위한 전자공증 서비스에 대하여 분석하였다. 인터넷의 급격한 보급으로 일반인들의 전자지불시스템 및 전자상거래 시스템에 대한 사용이 보편화 될 것으로 예측됨에 따라, 전자 상거래와 관련된 거래계약서, 금융관련 문서, 회사들간의 중요 공문서에 대한 암호 및 인증기능 뿐만 아니라 부인방지 서비스에 대한 수요도 급격히 늘고있다. 이러한 전자공증 서비스가 정착됨으로서 인터넷 사용자들이 안전하고 믿을 수 있는 거래장소로서 인터넷을 사용할 수 있을 것으로 기대된다. 아직까지 국내에서 전자공증 서비스와 관련된 분야는 초창기 단계에 머무르고 있지만, 차후 이에 대한 수요가 급증할 것으로 예상된다. 따라서 국내에서도 IETF의 보안분야의 PKIX WG에서 진행되고 있는 표준화 작업과 선진각국에서 진행중인 공증센터 구축사례에 대한 연구가 이루어 져야 하며, 또한 전자 공증센터에 대한 기능과 역할, 법적 책임성에 대한 연구도 이루어 져야 할 것이다.

참고 문헌

[1] B.Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, Wiley, 1994.

[2] M.Y.Rhee, Cryptography and Secure Communications, McGraw-Hill,1993.

[3] W.Stallings, Network and Internetwork Security, Prentice-Hall, 1995.

[4] 인터넷 자료

1) IETF Security Area의 X.509 (PKIX) Document : 1997 - 1998

(1) Part 1. Certificate and CRL Profile

(2) Part 2. Operational Protocols

(3) Part 3. Certificate Management Protocols

(4) Part 4. Certificate Policy and CPS Framework

2) 각국의 PKI Document :

(1). 미국 PKI Document : - "Federal PKI Study Final Report", MITRE, 1994

-"Federal PKI Technical Specifications", 1996.

-"Minimum Interoperability Specification for PKI Components(Ver1.0)", MISPC, NIST, 1997.

(2) 캐나다 PKI Document :

-"Government of Canada Pulic Key Infrastructure", White Paper,CSE, 1998.

(3) 호주 PKI Document :

-"Strategies for the implementation of a Public Key Authentication Framework (PKAF) in Australia", Standard Australia, 1996.

3) 각국의 Notary Document :

(1) Entegrity Document : "White Paper : Notary and PKI", 5, 1998.

(2) Entrust Document : "Notary Protocols Ver2.0", 11, 1997.

(3) NetDOX Document : "DOXIT Service Overview"

(4) Verisign Document : "Notarial Procedures for the Digital ID Requests"

(5) Surety Document : "Advanced Record Authentication for the Electronic Age"

□ 著者紹介

김 지 홍

1982년 2월 한양대학교 공과대학 전자공학과(공학사)
1984년 2월 한양대학교 대학원 전자통신공학과(공학석사)
1996년 2월 한양대학교 대학원 전자통신공학과(공학박사)
1984년 ~ 1991년 금성전선 연구소 근무
1991년 3월 ~ 현재 세명대학교 전자공학과 부교수