제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

전자 공증에 대한 고찰

유석환, 정종일, 차무홍, 신동일, 신동규
세종대학교
e-mail : {shwyu, jijeong, bidon, dshin, dkshin, }@gce.sejong.ac.kr

Survey of Electronic Notary

SeokHwan Yu, Jong-Il Jeong, Moo-Hong Cha, Dongil Shin, DongKyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

전자 상거래에서 보안과 신뢰성을 보장하는 것은 매우 중요하다. 공개키 기반 구조에서는 인증서를 사용 함으로서 암호 및 인증기능을 제공하나, 신뢰성 있는 부인 방지 기능을 제공하기 위해서는 상위 기관의 인증기관이나 타임 스탬프 기능과 공증 기능을 위한 제 3 의 신뢰성 있는 공증 기관이 필요하다. 본 논문에서는 전자공증의 기능과 필요성 및 동향에 대하여 소개한다.

1. 서론

네트워크상에서의 전자 상거래는 언제 어디서나 업무를 가능하게 하고 비용 절감, 거래의 기회증가에 효과를 주지만, 거래 당사자들이나 제 3 자로 인한 부인, 변조 등의 문제를 야기 시킬 수 있다. 이러한 위협이나 위험은 기술적인 부분에 의존 하게 될 것이다. 그러나 이러한 위험이나 위협을 단지 기술에 의존해서만 제거하기는 어려운 일이다. 그래서 문제를 예방하거나 해결하기 위한 포괄적인 계획, 기술적, 제도적 수단을 요구와 필요에 상응하는 처리모델의 흐름 분석을 통하여 고안 하는 것이 좋다.
전자공증(Electronic notary)은 전자 상거래를 위해 누구에 의해서 무엇이, 언제 전자교환이 이루어 졌는지의 잠재적 요소들을 고려하여 증거 방법으로 제시하는 수단이 된다.
구성 요소에는 전자 정보의 송신자 증명, 타임스탬프, 변조 탐지, 배달증명, 원문 증거 저장을 포함하며, 내부적으로는 승인방법, 접근 제어와 접근 기록에 중요할 것이고, 문제나 분쟁에서 증거물로서 유용 하다.
전자공증의 기능을 수행하기 위해서는 누구인지를 인증해줄 인증기관의 이용이 허락된다. 게다가 다른 조직과의 관계에 대해서 전자공증의 규칙과 정의는 변할 것이다 [1].

전자 공증의 요건으로는 신뢰성이 가장 중요 하며, 안전성과 공증 서비스와 관련된 기술력이 확보 되어야 하고, 공개키 기반 시스템과의 상호 운용성이 보장되어야 한다

2. 전자 공증의 기능

전자 공증에는 송신자임을 증명하기 위한 송신자의 신원 증명 기능, 전자 정보에 추가되는 날짜와 시간을 증명하는 타임 스탬프, 변조 검출, 수신자에게 정보가 전달 되었다는 것을 확인하기 위한 배달 증명 기능, 정보의 원본을 저장하는 전자 저장소, 승인 절차를 기록하는 승인기능, 데이터 베이스에 접근 제어와 기록을 위한 기능이 필요하다.
공증기관은 제시된 데이터(인증서, 서명문, 기타메시지)에 대한 정확성, 유효성 등을 확인시켜 주는 TTP(Trusted Third Party)이다. 공증 기관의 일반적인 기능은 다음과 같다.

1) 서명문 공증 요구인 경우, 동봉된 디지털 서명문이 정확한지를 확인하고, 서명의 유효성을 제 3자에게 입증하는 서명된 공증서를 발행한다.
2) 인증서 공증 요구인 경우에는 동봉된 인증서의 유효성과 인증서 취소 정보를 확인하고, 인증서의 취소 상태 정보와 유효성을 입증하는 서명된 공증서를 발행한다.
3) 데이터 공증 요구인 경우에는 동봉된 데이터의 정확성을 확인하고, 데이터의 유효성을 입증하는 공증서를 발행한다.
4) 시간의 단조증가 값을 이용하여, 타임스탬프 기록(또는 타임스탬프 토큰)을 공증서 내에 포함한다.
5) 서명에 사용된 신뢰성 정책과 유효성정책의 공유 확인자를 각각의 공증서에 포함한다.
6) 해당 공증토큰이 서명문 확인인지, 인증서 확인인

지, 데이터 확인인지를 공증서 내에 명시하여야 한다[2].

3. 전자 공증의 기본 서비스

전자 공증은 시간증명, 내용인증, 배달 증명, 데이터 보존 서비스를 제공한다.

1) 시간증명
저자문서가 적절한 시기에 특정 지점에 존재 했음을 확인하는 목적으로 타임스탬프 등을 첨부한다. 동시에, 타임스탬프와 암호화 키를 조합하여 구한 암호키로 문서를 암호화함으로써, 높은 신뢰성을 실현할 수 있다.

2) 내용 인증
정보의 내용과 누가 누구에게 언제 어떤 정보를 보냈는지를 인증하고, 문서를 허가 없이 변경하는 것을 방지하는 서비스이다. 전자 상거래에 있어서는 계약, 주문, 송장의 내용 등에 관해 분쟁이 발생했을 때, 이를 해결할 수 있는 증거가 될 수 있다.

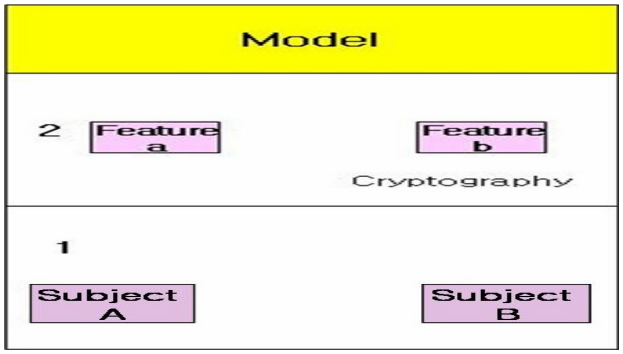
3) 배달 증명
송신자의 데이터가 수신인에게 정확히 배달되었는지를 확인해 주는 서비스이다. 송신자는 제 3 자를 거쳐 수신자에게 데이터를 전송하고, 송신자는 배달 증명센터에 접속해서 언제든지 배달 상태를 점검해 볼 수 있다.

4) 데이터의 전자 보존
나중에 증거로써 사용 가능한 저자 데이터를 보존하는 서비스이다. 기존 데이터에 입력, 삭제, 갱신, 내용 혼합 등이 불가능해야 하는 정체성(Authenticity), 접속 권한 제어기능이 요구되는 접근 가능성(Legibility), 보존 가능성(Preservability)을 요구한다 [1].

4. 전자 공증의 모델

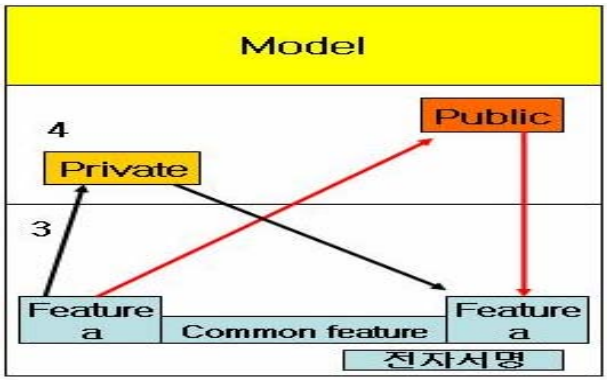
경제적 이점과 편의를 고려하여 필요한 공증 기능을 이행 해야 하고, 관리를 위한 비용을 추정해야 한다.

Model 1 은 상거래 당사자들 사이에는 보증과 안전성 부분을 보장하기 위한 특징은 없다



[그림 1] 전자 공증 model 1

model 2 에서, 상거래 당사자들의 고유한 전자적 특성은 내부적으로 완성 되었고, 보증과 안전성의 부분은 당사자들만이 사용할 수 있게 하는 방법에 의해 보장된다. 상업적 거래 정보가 교환된 상황하에서 당사자들간에 미리 합의된 것에 대한 형식이 암호화되어 명시된다



[그림 2] 전자 공증 Model 2

model 3 은 일반적으로 인지된 전자적 특성이 상거래를 하는 당사자들에 의해 내부적으로 공유된다. 예를 들면, 상업적 거래정보는 갖추어진 표준 보안 프로토콜에서 e-mail, EDI(Electronic Data Interchange)의 응용 등을 사용하여 교환 된다.

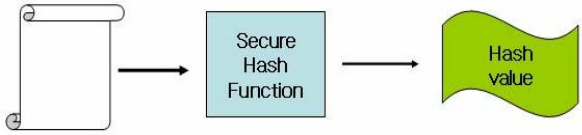
model 4 는 공공기관인 사설 기관이냐에 관계없이 일반적으로 인지된 제 3 의 기관에 의해 제공되고 승인 된다. 상업적 거래 정보는 부분적으로나 전체적으로 제 3 의 기관에 의해 제공되고 승인 된다. 상업적 거래 정보는 부분적으로나 전체적으로 제 3 의 기관에 의해 제공되고 승인 된다. 상업적 거래 정보는 부분적으로나 전체적으로 제 3 의 기관을 통해 교환 된다 [1].

5. 전자 공증 시스템과 해시 함수

전자 공증 시스템의 예로 Surety 사의 전자공증 시스템을 설명 한다.

전자공증 시스템은 암호학적으로 안전한 해시함수를 사용한다.

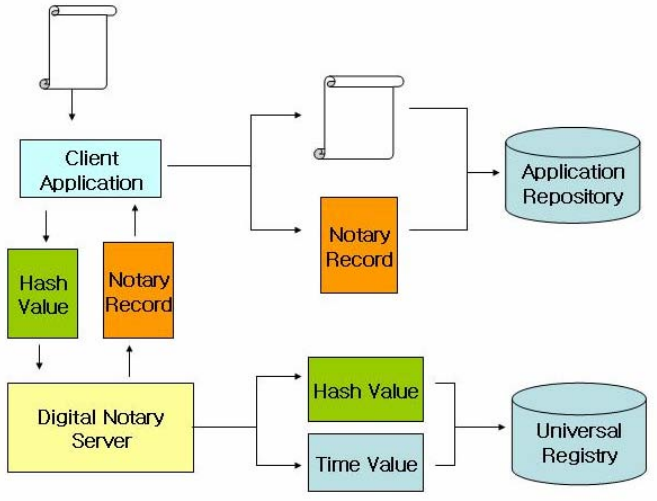
해시 함수(hash function)



[그림 3 hash]

입력되는 문서에서 한 비트만 바뀌어도 해시 값은 완전히 다른 값을 만들어 내기 때문에 다른 문서로 같은 해시 값을 만들어 내는 것은 계산 적으로 불가능 하다.

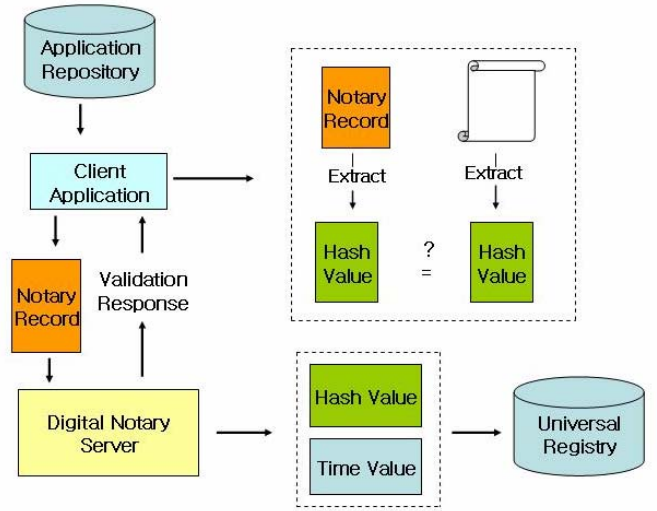
공증 생성(Notarization)



[그림 4 notarization process]

응용프로그램은 공증하기 위한 문서의 해시 값을 계산하여 공증요구(notarization request)를 통해 전자공증 서버(Digital Notary Server)에게 보내진다. 전자공증 서버는 해시 값과 타임스탬프를 Universal registry 라는 데이터 베이스에 저장하고, 해시문서와 타임스탬프를 포함하는 공증 기록(Notary Record)을 생성하여 응용프로그램에 반환한다. 이 문서가 미래의 어느 시점에선가 문서의 무결성을 증명하기 위해 사용되게 된다.

공증 평가(Validation)



[그림 5 Validation]

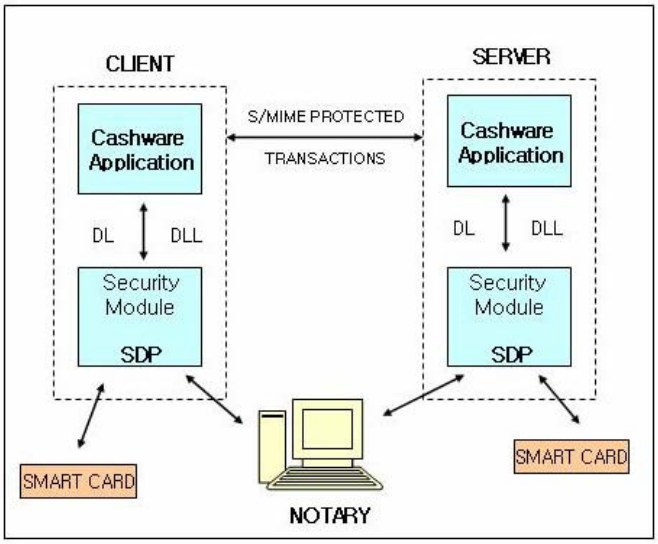
응용프로그램은 관련된 공증기록과 문서의 확인을 위해 회수하고, 문서의 해시를 계산하여 공증기록에 저장된 hash 와 비교를 한다. 전자공증 서버는 응용프로그램으로부터 받은 공증기록에 저장된 해시 값과 타임스탬프가 Universal Registry 에 저장된 값과 일치하는지를 평가한 후, 응용프로그램에게 공증기록이 유휴한지에 대한 결과를 평가 응답(Validation Response)을 통해 전달한다 [5][7].

6. 전자 공증의 동향

현재 전자공증 서비스를 제공하는 대표적인 업체로는 Cybernotary, Commerce-Net, Trust e, Surety Technologies, NetDOX, USPS, Verisign 등이 있다.

1) Entegrity

Entegrity 사에서 제공되는 공증 서비스 구조는 기본적으로 PKI(Public Key Infrastructure) 구조를 따른다. ROOT-CA 를 근원으로 하고, 하부의 각 CA(certificate authority)는 계층 구조로 구성되며, 상위 계층의 CA 는 하위 계층의 CA 에 대한 공증용 인증서를 발급한다. 각 CA 는 상호 인증 기능이 제공되며, 타 기반 시스템과의 상호 인증 기능도 제공된다. Entegrity 사에서 개발된 Cashwaree 는 전자 우편 방식을 이용하여 사용자와 서버간의 현금 거래에 사용되며, 강력한 부인 방지 기능을 제공한다 [3].



[그림 6 Cashware]

2) Cybernotary

무역 당사자들간의 신뢰 관계를 설립하는데 이것으로 서로 다른 법률과 협약, 어려움 하에서의 안전한 국제 무역을 제공하기 위해, 미국 International Business Conference 에 의해 국제 무역에서 안전성의 결여를 개선하기 위해 착수된 계획이다 [1].

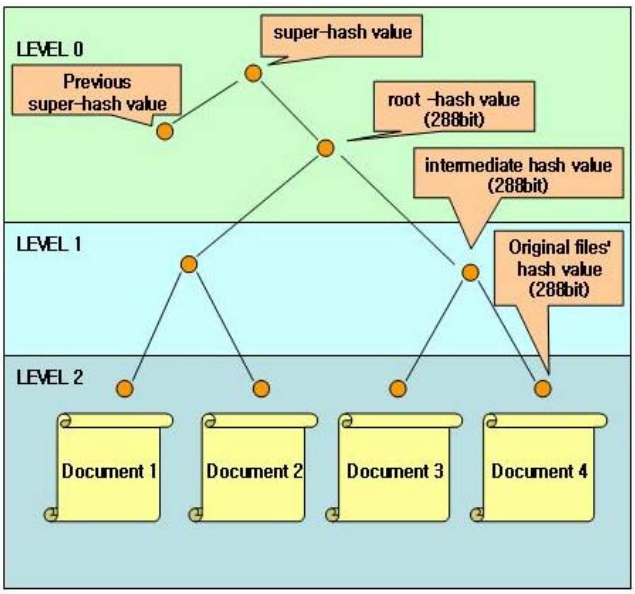
3) Trust e

Turst e 는 인터넷상의 교역에서 보안을 위한 “Trust Mark”를 승인하고, 신뢰할 수 있는 mark 를 만들거나 수용하는 단체이다. 현재는 거래나 추적에서 익명이 보장되는 사이트를 표시하는 No Exchange, 거래나 개인적 자료가 어떠한 제 3 자에게 폭로되지 안는 사이트를 표시하는 One-to-One Exchange, 거래나 개인적 자료가 제 3 의 기관에 알려지는 사이트를 표시하는 Third Party Exchange 를 사용 중 이다 [1].

4) Surety

Surety 사는 기존의 공증 서비스 제공업체와 연계하여 디지털 공증기록 인증서비스를 제공한다.

CORBASEC, HTTPS 와 같은 TCP/IP 에 기초한 통신으로 글로벌한 접근이 가능하며, 다양한 상호 접속 위치를 제공하고, 다양한 상호 접속 위치를 제공하고, 다양한 서버가 중복과 장애 극복을 제공하는 신뢰성, 안전성, 가변성을 갖추고 있는 것이 특징이다.[6]



[그림 7 SHV 생성]

매 초마다 각각의 문서를 연결하여 288 비트의 해쉬 값을 얻고, level 1 에서는 288 비트의 해쉬 값을 연결하여 다시 288 비트의 해쉬 값을 만들어 낸다. 이렇게 만들어 진 해쉬 값은 level 0 에서 288 비트의 RSH(root-hash value)가 생성되고, 이값과 1 초 전에 만들어진 SHV(super-hash value)과 결합하여 현재의 SHV 가 만들어진다. 이 SHV 는 1992 년부터 매초마다 생성되어져 왔고, 이값은 "NEW YORK TIMES"를 통해 발표 되어진다[6].

5) ReadNotify

ReadNotify 는 신뢰할수 있는 추적, 보증, 자동파괴, 보안, 인증, 광고메일과 바이러스를 방지하는 메일을 제공한다.

ReadNotify 는 모든 이메일 프로그램과 연동이 가능하지만 이메일외의 다른 종료의 문서에서는 사용할수 없다. Surity 와 같은 독자적인 시스템이 아닌 공개키 기반 구조에 의존하고있다[4].

결론

신뢰성 있는 부인 방지 서비스를 제공하기 위한 전자 공증 서비스에 대하여 조사 및 소개를 하였다. 인터넷의 급격한 보급과 전자 지불 시스템 및 전자상거래 시스템에 대한 사용이 보편화 됨 으로서 저자 상거래와 관련된 거래 계약서, 금융관련 문서, 회사들간의 중요 공문서에 대한 암호 및 인증기능뿐만 아니라 부인 방지 서비스에 대한 수요도 급격히 늘고 있다. 아직 국내에서는 전자 공증 서비스가 일부 외국계 회사를 통해 서비스 되고 있는 시작 단계에 있다. 그러나 수요가 급증할 것에 대비하여, 표준화 작업의 진행과 구축 사례연구가 이루어 져야 할 것 이며, 공증 센터에 대한 기능과 역할, 법적 책임성에 대한 연구도 이루어져야 할 것이다.

참고문헌

[1] Katsuhiko Oride, "Electronic Commerce Promotion Council of Japan"

[2]이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자 상거래 보안 기술", 생능출판사, 1999

[3]Entegrity document : http://www.entegrity.com/products/whitepaperall.shtml ," White paper : Notary and PKI", 1998

[4] ReadNotify document : http://www.readnotify.com

[5] Surety Document : http://www.surety.com, "Digital Notary Engin"

[6] Surety Document : http://www.surety.com, "TechnologyandArchitecture"

[7] Surety Document: http://www.surety.com, "AbsoluteProofWhitepaper"