오프라인상에서의 전자문서 위변조 방지 시스템 설계

이윤오°, 유황빈
광운대학교 정보통신학과
{y265n,ryou}@kw.ac.kr

Design of System for Prevent Forgery of Digital Document on Off-Line

Yun-o Lee°, Hwang-Bin Ryou
Department of Information communication, Kwangwoon University

요 약

현재 인터넷을 통한 상대방의 신뢰성을 보장해 주는 인증서 사용이 빈번해지고 있다. 그러나 오프라인상의 전자문서는 상대방의 신뢰성 보장과 전자문서의 위변조의 위험성이 많다. 또한 전자문서는 오프라인상의 이동성에 제약을 받게 된다. 본 논문에서는 이러한 문제를 해결하고, 사용자가 온라인과 오프라인에서도 사용하게 편리하도록 문서내용, 문서작성자의 인증서 그리고 전자서명값을 이차원 바코드로 변환하여 출력된 전자문서에서 상대방의 신뢰성과 문서의 무결성을 보장하도록 제안한다. 제안된 시스템에서는 문서내용, 문서작성자의 인증서, 전자서명값을 변환해 출력문서에 이차원 바코드를 첨부하게 된다. 출력된 문서에서 첨부된 이차원 바코드를 스캐닝 하고 문서내용, 문서작성자의 인증서 그리고 전자서명값을 얻어오고 검증을 통해 위변조 여부 판단하여 상대방의 신뢰성과 문서의 무결성을 확인 하도록 한다.

1. 서 론

모든 정보는 과거부터 사용해 오던 종이 문서의 교류에서 벗어나 전자문서로 그 주체가 변해가는 것이 하나의 특기 사항이다. 전자화된 문서의 교류가 늘어나고, 동시에 사용자들이 증가하면서 부정적인 면도 생기게 되었다. 이러한 부정적인 면을 해결하고 전자문서 교환에서 상대방의 신뢰성을 보장하기 위해 인증서비스가 필요하다. 인증서는 인증기관이 전자서명을 통하여 공개키와 이를 소유한 사람과의 귀속관계를 확인, 증명하는 전자적 정보를 말하는 것으로 상대방에게 이를 제시하여 자신의 신뢰성을 확인받는데 사용된다. 현재 인증기관이 발급한 인증서를 사용자가 보관하여 온라인상에서 전자문서를 보낼 경우 전자서명과 함께 상대방에게 제시하여 서로의 신뢰성을 확인한다. 온라인에서 가능한 신뢰성을 오프라인에서 적용할 수 없고 상대방의 신뢰성과 문서의 위변조의 문제 때문에 전자문서의 오프라인에서의 효력은 상실된다.

본 논문에서는 이런 문제점을 해결하기 위하여 공개키 기반 구조와 이차원 바코드 기술을 이용해 오프라인 상의 전자문서의 위변조를 방지하기 위한 방안을 제시한다. 인증서, 전자서명을 온라인에서와 같이 사용자 인증 및 데이터 무결성을 보장하고 공개키 기반구조 요소들에 대한 오프라인 상에서의 무결성의 보장을 이차원바코드를 이용한다. 기존에 일차원 바코드는 많은 데이터량을 갖지 못한 반면에 이차원 바코드는 많은 데이터량과 암호화 기능을 가지고 있다. 또한 휴대성과 이동성이 편리하고 높은 데이터 신뢰성을 가지고 있는 이차원 바코드로 변환한 인증서는 오프라인에서 상대방의 신뢰성과 문서의 무결성을 보장한다.

본 논문에서는 오프라인상에서도 전자문서의 효력이 발휘되도록 문서내용, 문서작성자의 인증서 그리고 전자서명값을 바코드로 변환한 후 출력문서에 첨부하여 문서교환에서의 상대방의 신뢰성과 문서의 무결성을 보장하는 방안을 제시한다.

2. 관 련 연 구

2.1. PDF417

1989년 미국 Symbol Technologies사에 의해 개발된 가변적인 길이와 높이를 가진 다층형바코드이다. 많은 데이터를 포함할 수 있어서 휴대형 데이터 파일로 적합하며, 다양한 스캐너로 판독 가능하고 개방 체계(Open system)이므로 어느 사용자라도 용이하고 편리하게 필요한 응용분야에 적용할 수 있는 장점이 있다.

한 바코드는 데이터 표현양식에 따라 최대(오류검출단계가 0인 경우) ASCII 1850문자(Character)나 1108byte, 또는 2710수치(Digit)을 표현한다.[1]

이차원 바코드의 특징으로는

1) 대용량 데이터 : 최소 수십 문자에서 수천 문자까지 데이터를 포함하고 여러 바코드들을 연결시켜 하나의 메시지처럼 읽혀지도록 하는 기능을 가지고 있다. 이런 특성의 장점은 호스트컴퓨터와 연결되지 않고서도 언제나 현장에서 데이터를 수집하거나 조회할 수 있다.

2) 고밀도의 데이터 : 고밀도 데이터를 표현할 수 있어 적은 면적을 차지 한다.

3) 데이터 암호화 기능 : 이차원 바코드는 데이터 암호화

기능을 가지고 있으므로 비밀 및 보안을 요하는 자료의 표현과 저장 또는 전달에 유용하게 이용될 수 있다. 이런 특징이 있으므로 자료의 위조나 변조 또는 오용을 방지할 수 있는 확률이 크게 향상된다.

2.2. 전자서명

전자서명은 Online에서 이루어지는 거래나 데이터의 송수신에 있어서 상대방의 신원을 확인할 수 없거나, 혹은 전자 메일을 사용하는데 있어서 메일을 송신한 사람이 불분명 하기 때문에 상대방의 신원을 확일 할 수 없다는 것의 약점을 보안하기 위해, 또는 데이터의 암호화를 위해 사용된다. 전자서명은 인증(Authentication), 무결성(Integrity), 부인봉쇄(Non-repudiation)를 보장하기 위한 공개키 메커니즘의 하나로 비밀 키(private key)와 공개키(public key)라는 2종류의 키를 사용하여 자신의 비밀키로 서명을 하면 통신 상대방은 발신자의 공개 키를 사용, 검증(verify)하므로 발신자가 서명한 후 메시지는 수정될 수 없다. 전자서명기술은 공개 키와 개인 키간 합치성(Correspondence)의 특성을 이용하여 전자문서를 수신한 상대방이 송신자의 신원확인, 전자문서의 위.변조 방지, 전자문서의 송신사실의 부인 방지를 기술이다. 공개키 암호기술에 기반을 둔 전자서명기술은 개인키(Private Key)와 공개키(Public Key)라는 두 개의 키를 이용하여 문서를 전자서명하고 이를 검증하는 기술로 공개키 암호기술에서 개인키는 사용자 자신만이 알고 있는 키를 말하며, 사용자는 이 키를 이용하여 문서에 전자서명을 한다.[2],[5]

전자 서명의 특징으로는

1) 위조 불가(Unforgeable) : 합법적인 서명자만이 전자서명을 생성할 수 있어야 한다.

2) 서명자 검증(User authentication) : 전자서명의 서명자를 불특정 다수가 검증할 수 있어야 한다.

3) 부인 봉쇄(Non-repudiation) : 서명자는 서명행위 이후에 서명한 사실을 부인할 수 없어야 한다.

4) 변경 불가(Unalterable) : 서명한 문서의 내용을 변경할 수 없어야 한다.

5) 재사용불가(Not reusable) : 전자문서의 서명을 다른 전자문서의 서명으로 사용할 수 없어야 한다.[3],[7]

2.3. 인증서

인증서(Certificate)는 인증기관(Certification Authority)이 가입자의 신분과 그의 공개키 정보를 보장하기 위해 발급하는 전자문서를 말한다. 전자거래 시 전자서명 및 공인인증서를 사용하면 신원확인, 문서의 위.변조, 거래사실의 부인방지 등의 효과를 얻는다. 공개키 기반의 전자서명 기술은 자신이 공개 키를 외부에 공개한 후, 이를 이용하여 자신을 상대방에게 인증시키는 기술 이지만, 공개키는 누구나 쉽게 획득할 수 있도록 공개된 장소에 등록되어 있기 때문에 항상 공개 키의 위 변조에 대한 문제가 존재하게 된다. 뿐만 아니라 자신이 획득하고자 하는 공개키가 누구의 공개 키인지 확인할 수 있는 수단이 별도로 존재해야만 한다. 따라서 사용자의 공개 키를 그 사용자의 개인정보와 함께, 믿을 수 있는 제3자가 보장해 주는 것을 검증이라 한다. 이러한 역할을 하는 것이 인증기관이며, 인증기관이 발급한 사용자의 공개 키에 대해 보장하는 전자문서를 인증서라고 한다. 인증기관은 자신이 개인키로 사용자의 공개키 인증서를 전자서명 함으로써, 사용자 인증서의 무결성 및 진실성을 보장한다.[4],[6]

3. 제안 시스템 처리 과정

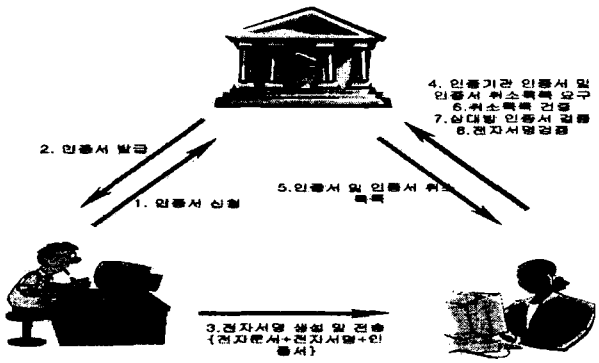

그림 1. 전자문서 생성과정

위 그림 1은 오프라인상에서의 전자문서 생성 전달을 보여준다. 인증기관을 통하여 인증서를 받아 전자서명을 하여 전자문서를 전달, 받은 전자문서를 인증기관에서 검증 한다.

3.1. 전자문서 인쇄시 처리 과정

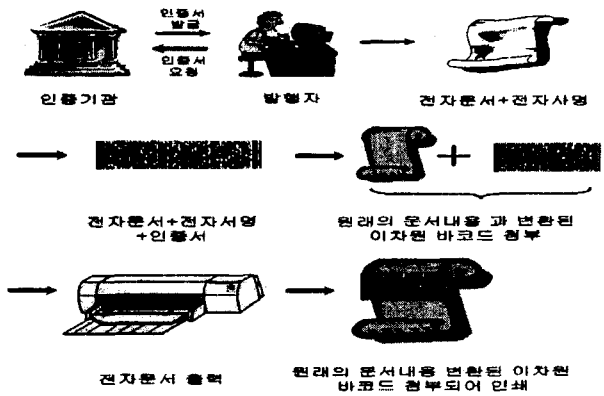

그림 2. 전자문서 출력 과정

위 그림 2의 처리과정은 다음과 같다.

1. 자신의 개인키를 이용해 전자문서에 대한 전자서명 생성.

2. 생성된 전자서명값과 인증서와 문서 내용을 이차원 바코드로 변환. 전자서명 값이 바코드로 변환되어 전자문서와 같이 출력.

3. 전자문서에 변환된 이차원 바코드 첨부.
4. 이차원 바코드가 첨부된 문서 인쇄.

3.2. 인쇄된 전자문서 검증과정

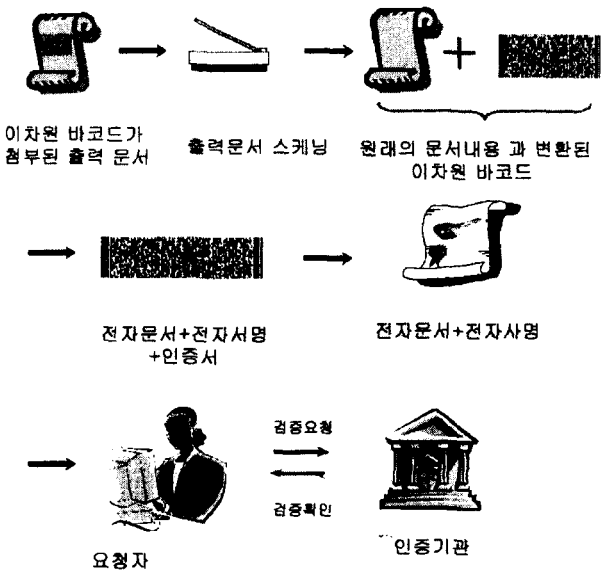

그림 3. 출력 문서 검증 과정

위 그림 3의 처리과정은 다음과 같다.
1. 이차원 바코드가 첨부 출력 문서 스케닝.
2. 이차원 바코드 문서 내용, 전자 서명, 인증서로 변환.
3. 인증기관에서 인증서와 전자서명 검증
4. 전자서명에서 해쉬값과 전자문서의 내용과 비교

3.4. 전체 구성도

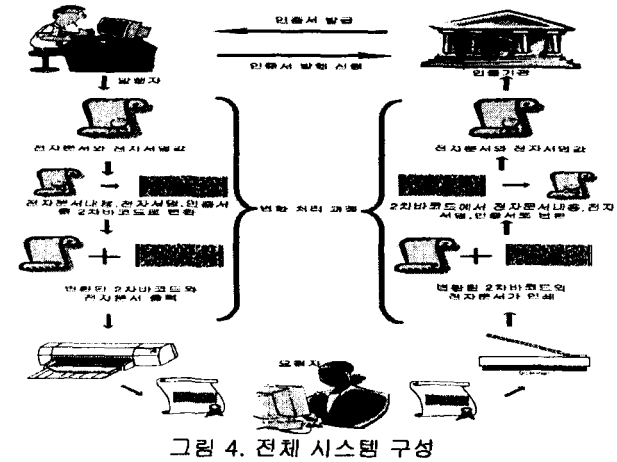

그림 4. 전체 시스템 구성

위 그림 4는 상호간의 처리과정을 전체 시스템을 보여준다. 문서를 발행인으로 요청을 하면 발행인은 인증기관으로부터 인증서를 발급받아 전자서명을 하여 전자문서를 발행한다. 전자문서는 문서의 내용과 문서작성자의 인증서, 전자서명을 이차원 바코드로 변환하여 문서에 첨부하여 출력된다. 출력 문서는 오프라인으로 요청자에게 전달된다. 출력문서를 받은 요청자는 문서 검증을 위하여 스케닝을 하고 이차원 바코드를 변환하여 나온 공개키를 인증기관에서 검증을 받고 전자서명에서 나온 해쉬값으로 원래 문서내용 비교 검증할 수 있다. 이로써, 전자문서의 위·변조 유·무를 확인할 수 있고 상호간의 안전하고 신뢰성 있는 문서교환이 오프라인에서도 가능하다.

4. 결 론

공개키 기반 구조는 사용자의 공개키를 안전하고 신뢰성 있게 공표하는 수단을 제공한다. 따라서 안전하고 신뢰성 있게 사용자의 공개키를 사용할 수 있게 해준다. 이런 구조는 인터넷에서 매우 중요한 역할을 수행하지만 이러한 공개키 기반구조의 장점을 오프라인상에서는 활용할 수 없다. 본 논문에서는 오프라인에서 전자문서를 출력하여 교환하였을 때 문서의 안전성과 신뢰성과 무결성을 보장하는 방안을 제안한다. 문서의 내용과 문서작성자의 인증서 및 전자서명을 이차원 바코드로 변환하여 출력시 문서에 첨부한다. 이렇게 변환된 이차원 바코드는 오프라인상으로 전달 되어 다시 문서 작성자의 공개키, 문서의 내용과 인증서 그리고 전자서명값으로 변환되어 검증 된다.

본 논문에서 사용자의 인증서와 전자서명을 통해 사용자의 신뢰성과 문서의 무결성을 보장한다. 이차원 바코드를 통해 오프라인상에서의 인증서와 전자서명에 대한 무결성을 보장한다.

5. 참고 문헌

[1] 오호근," 최신 바코드 기술 및 응용" , 성인당.
[2]강주성외6명," 현대 암호학" , ETRI부설 국가보안기술연구소.
[3] 정재원,류대걸," 보안과 암호학 모든 것" , 인포북.
[4] 이만영외6명," 전자상거래 보안 기술" 생능출판사 .
[5]W.Diffie and M.E.Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654,November 1976.
[6]F.Bauspiess and F.Damm. Requirements for cryptographic hash functions. Computers & security
[7]National Bureau of Standards. FIPS PUB 46 : Data Encryption Standard, January 1977.