The Journal of Korean
Institute of CALS/EC
Vol 6, No. 3, Dec. 2001

인터넷 환경 하에서의 Secure-ReXpis 시스템 설계 및 구현

안경림*, 박상필*, 백혜경*, 임병찬*, 박준홍**, 고대식***

The Design and Implementation of Secure-ReXpis System with Internet Environment

K.R. Ahn, S.P. Park, H.K. Paik, B.C. Yim, J.H. Park, D.S. Koh

Abstract

Security is very important in EC(Electronic Commerce) environment because exchanged information(that is transaction details, private data, charges data(card-no, accounts), etc) is various and is very sensitive. So, In this paper, we propose Secure-ReXpis(Reliable & excellent XML Processing InfraStructure) System that transfer message and support Message Level Security(Encryption/Decryption and Digital Signature). And we implement Message Confidentiality Service, User Authentication & Message Integrity Service and Non-Repudiation Service among the various Security Services. This system support XML message format and EDI message, WEB Data and Private Format Data, etc.

KeyWord : EDI, XML, Security, Digital Signature, Certificate

* 한국물류정보통신㈜
** 한국통신 엔트로플렉스 사내기업장
*** 목원대 전자 및 컴퓨터공학과 정교수

1. 서론

국지적으로 행해지던 전자상거래가 사업 영역 확대와 네트워크의 발달로 인해 점차 국제적 환경으로 확대되고 있다. 이렇듯 전자상거래가 도입되면서 종이로 처리되던 업무를 점차 전자적으로 전송하면서 메시지 표준화에 대한 요구사항이 도출되었다. 예를 들면, UN/EDIFACT(UN/EDI for Administration, Commerce and Trade), ANSI(American National Standards Institute Accredited Standards Communittee) X12, 등의 EDI (Electronic Data Interchange)나 전자 거래 분야의 ebXML(Electronic Business XML), 화학 분야의 CML(Chemical Markup Language), 웹 서비스의 WIDL(Web Interface Definition Language) 등의 XML (extensible Markup Language)이 정의되어 사용되고 있다[5][6][7][8][9]. 거래되는 업무가 증가함에 따라 거래 내용, 개인 정보, 비용(계좌번호, 카드 번호 등) 정보, 비밀번호 등 교환되는 메시지의 종류도 다양해 기밀성이 요구된다. 더욱이 인터넷을 기본으로 하는 환경으로 변화함에 따라 네트워크 상의 보안도 중요시 되고 있다. 각 기업이나 조직 내에서는 방화벽(Firewall)이나 VPN (Virtual Private Network)을 설치하거나, 또는 웹을 사용하는 경우 SSL(Secure Socket Layer), 웹 인증서를 사용하기도 한다. 그러나 이것만으로는 인터넷을 기반으로 하는 전자상거래 환경에 존재하는 보안 위협요소에 대해 방어할 수 없으므로, 암호화나 전자서명 등의 메시지 레벨의 응용 보안이 요구된다. 이를 위해 본 논문에서 제안한 안전한 메시징 시스템인 Secure-ReXpis (Reliable & excellent XML Processing InfraStructure) 시스템은 인터넷 환경 하에서 안전하게 메시지를 전송하기 위해 설계되었으며, 여러 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스 그리고 부인불능 서비스를 선정하여 구현하였다.

본 논문의 구성을 살펴보면 먼저 제 2장에서는 전자상거래 환경 하에 존재하는 보안 위협요소와 이에 대응하기 위한 보안서비스에 대해 살펴보고, 제 3장에서는 보안 서비스를 구현하기 위해 사용될 수 있는 보안 기술과 현재 국내에서 시행되고 있는 사례에 대해 설명하겠다. 제4장에서는 Secure-ReXpis 시스템 설계와 이 시스템이 제공할 수 있는 서비스 중 몇 가지를 선정하여 구현한 예와 더불어 인증서 발급 절차에 대해 설명하겠으며, 마지막으로 제 5장에서는 결론과 향후 해결해야 할 문제에 대해서 언급하겠다.

2. 보안 위협 요소 및 보안 서비스

요즘 활발히 시행되고 있는 전자상거래는 수 백만, 수 천만의 시스템이 상호 연결되어 있는 인터넷을 기반으로 함으로써, 인터넷의 기본적인 취약성으로 인하여 거래 내용, 자기 정보, 비용(계좌번호, 카드 번호 등) 정보, 비밀번호 등의 정보가 쉽게 노출될 수 있다. 기존에는 단순 정보 전송이나 정보 조회에 불과하였으나, 현재 전자상거래 환경은 국가간, 조직간, 개인간 거래를 위해 연결되어 있을 뿐 아니라 사용자의 인

적 사항과 거래에 따른 지불 정보가 전송되고 있어 더욱 위협에 노출되어 있다. 또한 웹 기술의 발달에 따라 전문가 뿐만 아니라 일반 사용자들도 이러한 정보들에 손쉽게 접근할 수 있어 보안 문제는 더욱 중요한 과제로 부각되고 있으며 보다 강력한 보안 서비스가 요구된다. 전자상거래에서 발생하는 보안상의 위협 요소와 이에 대응하는 보안 서비스 요소를 살펴보면 다음과 같다[1][2][3].

2.1 보안 위협 요소

(1) 도청(Eavesdropping)

네트워크를 도청하여 전송되는 메시지를 복제(Counterfeit , Replication)한다.

(2) 위장(Masquerade)

침입자가 합법적인 사용자인 것처럼 시스템에 접근하여 임의의 사용자로 위장하여 메시지의 수신에 대해 정당한 수신자인 것처럼 거짓 응답을 할 수 있고, 거짓요청을 하여 임의의 메시지가 제출되게 할 수도 있다.

(3) 메시지 변조

의도된 수신자에 대한 정보, 라우팅 정보, 또는 그 외 데이터가 감지되지 못한 채 분실 또는 변경될 수 있으며, 도청한 메시지의 내용을 변경하여 재사용하거나 수신된 메시지를 변경하여 저장할 수 있다.

(4) 공격(Attack)

시스템과 시스템 내에 저장된 정보를 불법적으로 접근하거나 그 기능을 마비시키기 위한 행위로서 시스템을 파괴하거나 정보를 삭제 또는 그 시스템을 경유하기도 한다.

(5) 논리적 폭탄(Logic Bomb)

특정 조건이 만족되면 임의의 형태로 공격하는 것으로서, 바이러스와 달리 논리 폭탄은 단순 정보를 가로채는 것 이외에 정보를 훼손, 변조하는 능동적 위협(Active Threat)이 존재한다.

2.2 보안 서비스

(1) 메시지 비밀보장

내용 비밀보장을 위해, 발신자는 메시지 내용을 암호 알고리즘과 키를 사용하여 암호화한다. 암호 알고리즘과 키는 상호 협의하여 사용할 수 있다.

(2) 메시지 무결성 및 사용자 인증

사용자 인증 및 메시지 무결성은 전자서명과 암호화를 통해 제공되며, 암호/서명키(즉, 미리 설정되고, 공유된 대칭키, 발신자 개인키, 임의로 생성된 대칭키)가 정의된다.

(3) 부인불능 서비스

"송신자가 의도된 수신자로의 메시지 전송을 요구하였다"는 것이나 "수신자가 메시지 수신하였다"는 부인할 수 없는 증명을 제공하는 것으로, 이러한 서비스를 제공하기 위해 인증 및 무결성에 사용된 전자서명과 암호화를 사용하며, 신뢰할 수 있는 제3자가 전자서명과 암호문을 저장하여 분쟁 발생시 증거자료로 사용된다.

(4) 네트워크 보안

인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스 및 네크워크 상의 정보를 보호하는 것으로 네트워크의 중요 기능이 정확히 수행되는지, 위험이 있는

지, 정보가 정확한 지를 보증하기 위한 방법이다.

3. 보안 기술 및 정책

3.1 보안 기술(보안 알고리즘)

(1) 대칭키 알고리즘

대칭키 알고리즘은 동일한 대칭키를 사용하여 암호화 및 복호화를 수행하며, 변환 방법에 따라 블록 암호 알고리즘과 스트림 암호 알고리즘으로 구분된다. 이 때 사용되는 키 크기는 비대칭키 알고리즘보다 상대적으로 작아 암호화시 효율적이나 당사자간 동일한 키를 공유해야 함으로 인해 거래 상대방이 늘어날수록 키 관리에 어려움이 있다[2][3].

블록 암호 알고리즘은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변경하는 방식으로 암호화 및 복호화 과정을 수행한다. 대표적인 알고리즘으로는 미국의 DES(Data Encryption Standard), Triple-DES, Skipjack, 유럽의 IDEA (International Data Encryption Algorithm), 일본의 FEAL(Fast Data Encipherment Algorithm), MISTY 등이 있다.

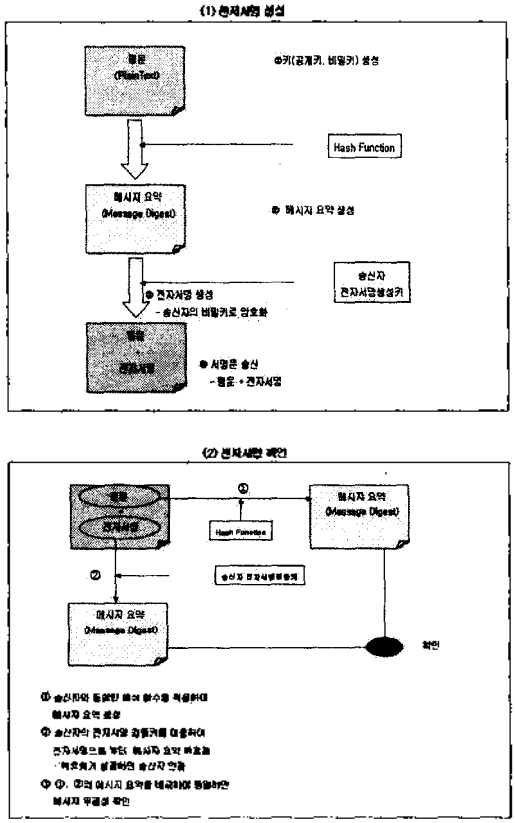
1970년 대부터 유럽을 중심으로 발달한 스트림 암호 알고리즘은 이진화된(Binary) 평문과 키 이진수열을 배타적 논리합(Exclusive-OR)이라는 비트 단위(Bit by Bit) 이진 연산으로 결합하여 암호문을 생성한다. 스트림 암호 시스템은 어떠한 키 이진 수열을 발생하여 평문과 결합시키느냐가 암호 시스템의 안전도에 직접적인 영향을 미치므로, 키 이진 수열의 특성과 발생 방법이 이 암호 시스템의 핵심이다. 스트림 암호 시스템은 군사 및 외교용으로 널리 사용되고 있으며, 일부 상용으로도 활발히 사용되고 있다. 또한 이동 통신 환경에서 구현이 용이하고, 안전성을 수학적으로 엄밀하게 분석할 수 있는 장점 등으로 인하여 이동 통신 등의 무선 통신 데이터 보호에 적합하다.

(2) 비대칭키 알고리즘

비대칭키 알고리즘은 암호화와 복호화시 사용되는 키가 서로 다르며, 공개키 알고리즘으로 불리운다. 사용되는 키는 키 생성 알고리즘에 의해 두 개의 키가 생성되는데 하나는 비밀키로서 자신이 보관하며, 다른 하나는 공개키로서 외부에 공개한다. 송신자는 메시지를 암호화 하여 전송하기 위해 수신자의 공개키로 암호화하여 전송하고, 수신자는 자신의 비밀키로 복호화한다. 그러므로 사용자들은 자신의 비밀키만 보관하면 되므로 대칭키 알고리즘보다 키 관리가 용이하다. 그러나 상대적으로 키 크기가 커서 암호화시 처리 시간 및 부하가 걸리게 된다. 그래서 전체 메시지를 암호화하기 보다는 전자서명시 사용된다. 지금까지 발표된 것으로는 인수 분해를 이용한 RSA (Rivest, Shamir, Adleman) 알고리즘, Knapsack 문제를 이용한 Merkle-Hellman Knapsack 알고리즘, Graham-Shamir 알고리즘, McElieced 암호화 방식, 최근에 가장 큰 관심을 모으고 있는 타원 곡선 암호 시스템(ECC : Elliptic Curve Cryptography) 등이 있다[2][3].

3.2 보안 정책

정보사회에서 활성화되고 있는 전자문서는 일반 문서에 비해 쉽게 변형될 수 있으며, 특히 수기 서명 방식을 전자 문서에 적용하는 것은 불가능하다. 따라서 전자문서에 작성자의 신원 확인 및 무결성을 보장할 수 있는 새로운 서명 방식이 필요하게 되었다. 이에 1999년 2월 5일 법률 제 5792호에 따라 전자서명법이 제정되었으며, 이 법은 전자 문서의 안전성과 신뢰성을 확보하고 국가 정보화와 국민 편익 증진을 목적으로 한다. 여기서 전자서명이라 함은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화 방식을 이용하여 전자서명 생성키로 생성한 정보를 의미한다. 전자서명법 제 3조에 의해 공인인증기관이 발급한 인증서에 포함된 전자 서명 생성키로 생성한 전자서명은 법령이 정한 서명 또는 기명 날인으로 인정된다. 전자서명은 전자문서에 일방향 해쉬 함수(One-Way Hash Function)를 적용시켜 메시지 요약(Message Digest)을 만든 후 공개키 알고리즘과 송신자의 전자 서명 생성키를 이용하여 서명한다. 송신자의 전자 서명 검증키를 가지고 있는 수신자는 서명 검증을 통해 송신자 인증 및 전자문서 무결성을 보장할 수 있다. 다음 <그림 1>은 전자서명의 절차와 확인 과정을 나타내고 있다.



<그림 1> 전자서명 생성 및 확인 절차

2000년 이후 B2B(Business to Business) 전자상거래가 본격적으로 발전하기 시작하면서 계산서 교부나 보관 등 세금계산서 관련 업무의 효율화를 위해 국세청에서는 관련 규정을 정비하여, 2001년 1월부터 전자세금계산서를 인터넷을 통해 수수할 수 있도록 하였다. 이 때, 공인인증기관(금융결제원, 한국정보인증, 한국증권전산 등)의 인증을 거치거나, 이에 준하는 기술을 사용하는 사설인증기관이나 자체 인증시스템 등을 통해 가능하며, B2B, e-Marketplace 등을 운영하는 사업자가 전자상거래를 중개하는 경우에는 실제 사업자를 대신하여 전자세금계산서의 교부 및 보관을 대행할 수 있다. 이렇게 전자세금계산서를 도입, 활성화하여 기업의 경상비용을 절감함은 물론 전자상거래의 거래증빙으로서의

기능도 할 수 있을 것이며 전산자료형식을 표준화하여 세금계산서 관리의 체계화를 위한 기반을 확립하게 된다.

여기서 공인 인증 기관(CA : Certificate authority)이라 함은 인증 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 지정하며, 국가기관.지방자치단체 또는 법인에 한한다. 공인인증기관으로 지정받고자 하는 자는 대통령령이 정하는 기술능력, 재정능력, 시설 및 장비 기타 필요한 사항을 갖추어야 하며, 이 기준은 전자서명법 제 4조 제 3항의 규정에 따른다. 이러한 사항에 따라 국내에서 지정된 공인 인증 기관은 전자민원서비스, B2B, B2C 분야의 "한국정보인증", 금융 분야의 "한국증권전산과 금융결제원", 공공 분야의 인증서비스를 제공 중인 "한국 전산원"이 있다.

4. 시스템 설계 및 구현

2장에서 언급한 바와 같이 현재의 전자상거래 시스템은 대부분 웹과 인터넷을 기반으로 하고 있기 때문에 도청, 위장, 메시지 변조 등과 같은 보안 위협에 노출되어 있다. 교환되는 데이터 중에는 자기 정보, 지불 정보, 거래 내역 등과 같은 개인과 기업의 중요 데이터는 더욱 보안이 요구된다. 그러므로 본 논문에서는 B2C, B2G, B2B 시스템이나 e-Marketplace 등 전자상거래 시스템에서 안전하게 메시지를 전송하기 위해 Secure-ReXpis(Reliable & Excellent XML Processing Infrastructure) 시스템을 설계하였으며, 제공될 수 있는 보안 서비스로 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스 그라고 신뢰할 수 있는 제 3자(CA 또는 중계사업자)와 함께 부인불능 서비스를 우선 선정하여 구현하였다. 이 서비스들은 암호 알고리즘과 전자서명을 통하여 구현되었으며, 사용된 키(인증서)는 공인인증기관으로부터 발급받아 사용하였다. 또한 사용자 환경에 따라 보안 모듈을 설치할 수도 있고 중계사업자가 보안 서비스를 대행할 수 있도록 하였다.[4]

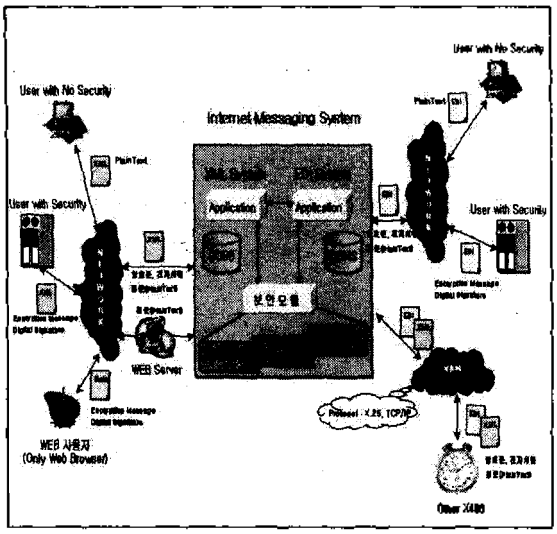
4.1 시스템 구조 및 메시지 흐름도

안전한 메시징 시스템인 Secure-ReXpis 시스템은 인터넷을 기반으로 하여 설계된 시스템으로서 교환되는 메시지는 XML을 기본으로 하나, Legacy EDI나 웹을 통해서 전송된 메시지도 처리가능토록 설계되었다. 보안 서비스로는 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스, 부인 불능 서비스를 구현하였으며, 각각 Component 개념으로 구현되었다. 이 때 사용되는 키는 사용자별로 구분되어 관리되며, 부인불능 서비스를 위해 전자서명은 정부에서 고시한 기간동안 시스템 내에 보관된다. 다음 <그림 2>는 Secure-ReXpis 시스템 구조와 교환되는 메시지의 흐름을 보여주고 있다.

4.2 구현 보안 서비스

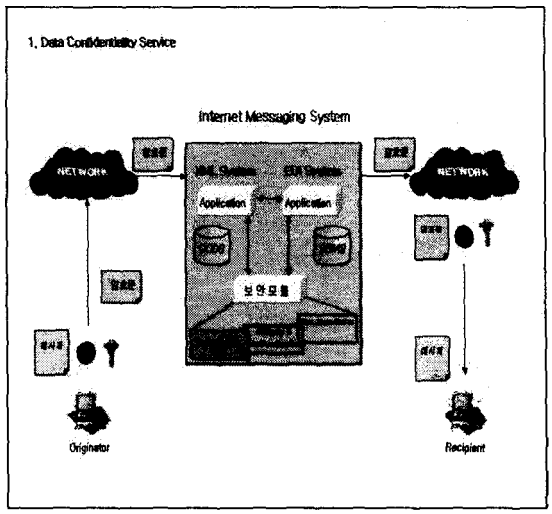
4.2.1 메시지 비밀보장 서비스(Data Confidentiality)

메시지 비밀보장 서비스는 불법 노출로부터 데이터를 보호하기 위한 것으로서 일반



<그림 2> Secure-ReXpis 시스템 구조 및 메시지 흐름

적으로 대칭키 암호화 알고리즘을 사용하지만, 키 관리 문제와 보다 강력한 보안 기능을 위해 본 논문에서는 국내 비대칭키 표준 알고리즘인 SEED-CBC 128 비트 블록 암호 알고리즘을 사용하였다. 다음 <그림 3>은 비밀보장 서비스의 처리절차를 보여주고 있다. 먼저 송신자는 전송하고자 하는 메시지(M)에 암호화 키(수신자의 공개키, Rp)를 적용하여 암호화(E=Rp(M)) 를 수행한 후, 암호문을 수신자에게 전송한다. 수신자는 복호화 키(수신자의 비밀키, Rs)를 사용하여 암호문을 복호화(M=Rs(E))한다. 이 때 암호화때 사용된 키는 공인인증기관(CA)으로 발급받은 인증서를 통해 정의된다. 여기서 사용된 공개키는 두 가지 방법으로 얻을 수가 있는데, 첫번째로 암호화시마다 CA에 LDAP을 통해 접속하여 상대방의 공개키를 가져다 사용한다. 이 방법은 거래 상대방에 대한 공개키를 관리할 필요가 없지만 암호화시마다 접속을 해야 함으로 통신 부하나 처리 속도가 늦어질 수 있다. 다른 방법은 거래 상대방의 공개키를 CA로부터 전송받아 자신의 Local System에 저장하여 사용하는 것이다. 이렇게 하면 부하나 처리 속도는 빨라지나 주기적으로 CA에 접속하여 CA 공개키와 저장된 공개키의 Consistency를 유지해야 하는 단점이 있다.

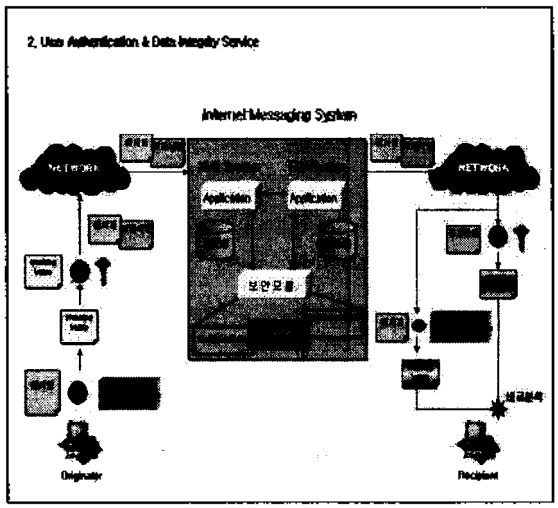


<그림 3> 메시지 비밀보장 서비스

4.2.2 사용자 인증(User Authentication)과 데이터 무결성(Data Integrity) 서비스

사용자 인증 서비스는 메시지가 발신자로부터 보내진다는 것을 보장할 수 있는 서비스로서 송신자는 자신의 비밀키로 암호화하여 전송하고, 수신자는 송신자의 공개키로 복호화한다. 메시지 무결성 서비스는 송신자가 전송한 메시지가 수신자가 수신하기 전에 불법 변경이나 수정이 없었다는 것을 보장하는 서비스이다. 이 두 서비스는 X.509

의 디지털 서명 메커니즘으로 구현되며, 비대칭 암호화 알고리즘을 사용하기 때문에 메시지의 크기가 클수록 처리시간이 많이 소요된다. 그러므로 암호화 전에 메시지를 블록 단위의 길이로 나누어 해쉬 함수를 수행한다. X.509 에서는 Square-Modular 방식을 제시하고 있으나, 본 논문에서는 SHA (Secure Hash Algorithm)을 보완하여 1995년에 발표한 160 bit, 4 round SHA1(현재 미국 연방 정부의 표준 해쉬 알고리즘으로 공인되었음)을 사용하였으며, 암호화 알고리즘으로는 RSA 를 사용하였다. 다음 <그림 4>는 사용자 인증 서비스와 메시지 무결성 서비스 처리 절차를 나타내고 있다.



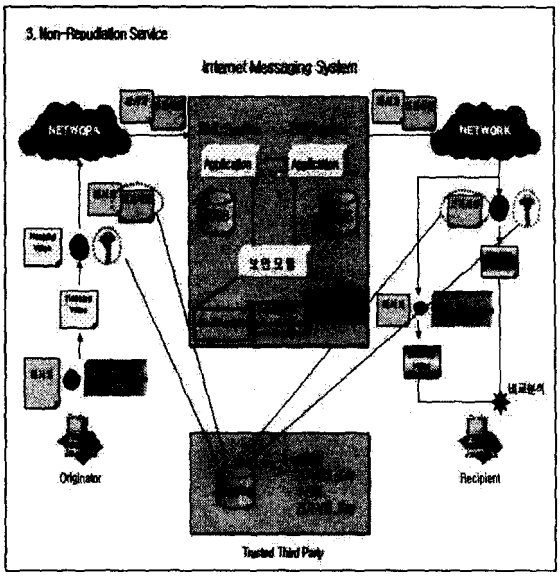
<그림 4> 사용자 인증 및 메시지 무결성 서비스

먼저 송신자(O)는 메시지(M)에 해쉬 함수를 적용하여 나온 메시지 요약 (Message Digest)에 자신의 비밀키(Os)로 암호화하여 전자서명(DS=Os(MD))을 얻는다. 원문에 전자서명을 포함하여 수신자에게 전송하면, 수신자(R)는 송신자의 공개키(Op)로 전자서명을 복호화한다. 이때 복호화된 값(메시지 요약 : Message Digest)과 원문을 송신측과 동일한 해쉬 함수를 적용하여 나온 값(메시지 요약)을 비교한다. 이 두 값이 동일하면 정당한 메시지 발신자로부터 전송되었다는 것과 전송된 메시지가 전송도중 변경 없이 전송되었다는 것을 보장할 수 있다.

4.2.3 부인불능(Non-repudiation) 서비스

일반적인 전자상거래시 거래 상대방들의 부인에 따른 위협요소가 있는데, 수신자가 수신 사실을 부인하고 미수신 Claim을 제기하거나 수신자가 수신받은 메시지 내용이 송신된 내용과 다르다거나 송신 사실을 부인하는 시도로부터 보호하기 위해서 제공되는 서비스이다. 이 서비스를 통해 송신내용 부인불능과 수신내용 부인불능을 지원할 수 있으며, 근거자료 보관 방법은 각자의 시스템에 전자서명을 보관하거나 또는 신뢰할 수 있는 제 3자에게 저장할 수 있다. 본 논문에서는 디지털 메커니즘을 사용하는 사용자 인증 및 메시지 무결성 서비스에다가 전자서명 및 키를 신뢰할 수 있는 제 3자가 보관하는 방식으로 구현하였다. 다음 <그림 5>는 부인불능 서비스 절차를 보여주고 있다. 전자서명 메커니즘에 의해 먼저 송신자(O)는 메시지에 해쉬 함수를 적용하여 나온 메시지 요약(Message Digest)에 자신의 비밀키(Os)로 암호화하여 전자서명(DS=Os(MD))을 얻는다. 원문에 전자서명을 포함하여 수신자에게 전송하면, 수신자(R)는 송신자의 공개키(Op)로 전자서명을 복호화한다. 이

때 복호화된 값(메시지 요약 : Message Digest)과 원문을 송신측과 동일한 해쉬 함수를 적용하여 나온 값(메시지 요약)을 비교한다. 이 두 값이 동일하면 정당한 메시지 발신자로부터 전송되었다는 것과 전송된 메시지가 전송도중 변경없이 전송되었다는 것을 보장할 수 있다. 또한 송신자는 메시지를 송신하기 전에 생성된 전자서명을 제3자에게 제출하고, 수신자 또한 수신한 전자서명을 제출한다. 저장된 전자 서명은 분쟁 발생시 증거자료로서 사용된다.

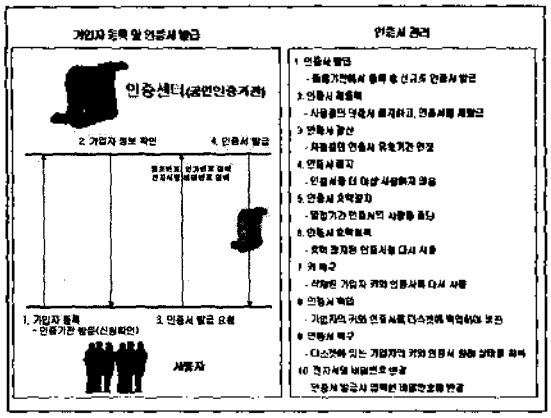


<그림 5> 부인불능 서비스

4.3 사용자 유형별 서비스 적용

4.3.1 인증서 발급

일반 개인이나 법인 사용자가 보안 서비스를 시행하기 위해서 공인 인증 기관(한국정보인증, 금융결제원, 한국증권전산, 한국전산원)이나 사설 인증 기관(한국 전자 인증 등)으로부터 인증서를 먼저 발급받아야 한다. 일반적으로 사용자는 웹이나 응용 프로그램을 통해 등록신청을 하지만, 인증서를 발급받기 위해서는 공인인증기관을 방문하여 얼굴 대면을 통해 신원 확인을 한다. 신원 확인이 끝난 후 사용자는 웹을 통해 인증서 등록 신청을 하고 인증서를 발급받아 시스템에 설치하여 사용한다. 인증서는 CA(Certificate Authority)나 RA(Registration Authority)에 의해서 관리되며, 발급, 재발급, 폐기, 정보 변경 등의 절차가 있다. 다음 <그림 6>은 인증서 발급 절차와 관리 기능에 대해 보여주고 있다.

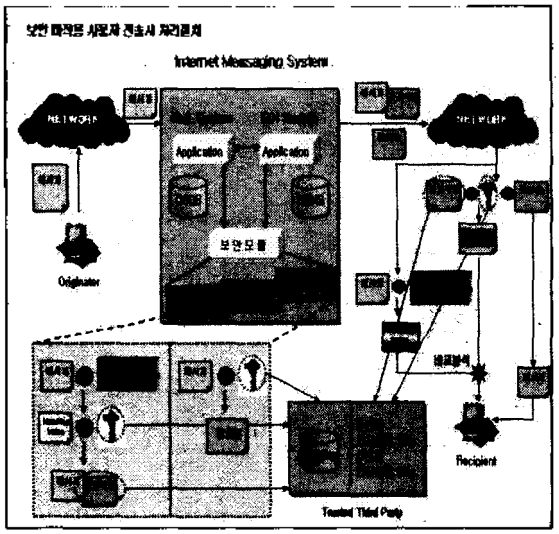


<그림 6> 인증서 발급 절차와 기능

4.3.2 보안 미적용 사용자

사용자 환경에 따라(거래량이 적거나 자체 시스템을 보유하지 못한 사용자들) 중계 사업자는 보안 대행 서비스를 제공할 수 있다. <그림 7>은 보안 미적용 사용자들의 보안 대행 서비스 절차를 보여주고 있다. 사용자는 웹 브라우저나 응용 프로그램을

통해 평문(EDI, XML 등)을 중계 사업자(VAN : Value Added Network)에게 전송하면, 중계 사업자는 요구된 보안 서비스에 따라 보안 서비스를 적용한다. 즉, 메시지 비밀보장 서비스 요구시, 송신자(O)는 암호화 키(수신자 공개키, Rp)로 평문을 암호화하여 수신자에게 전송한다. 사용자 인증 및 메시지 무결성 서비스는 전자서명을 생성하여 평문과 함께 수신자에게 전송한다.



<그림 7> 보안 미적용 사용자 처리 절차

특히 부인불능 서비스 요구시 생성된 전자서명은 별도의 저장소에 보관하며, 수신자에게 수신된 전자서명을 전송토록 요구한다. 또한 중계 사업자는 수신자의 환경에 따라 보안 시스템을 구축하지 못한 사용자일 경우, 복호화 및 전자서명 검증을 거친 후 정상적인 메시지만 전송한다. 보안 대행 서비스를 대행하는 중계 사업자는 보안 서비스시 사용되는 암호화 키나 전자서명 키는 사용자별로 별도로 구분하여 관리하여야 하며, 키 유출 등의 위협에 각별히 대처하여야 한다. 그리고 부인불능 서비스를 위하여 전송된 문서에 대한 전자서명도 저장하여야 한다. 또한 웹 브라우저를 통해 데이터를 전송하는 사용자를 위해 사용자(Client)와 WEB Server 사이의 보안을 위해 SSL이나 VPN을 설치하거나 별도의 보안 정책을 수립하여야 한다.

4.3.3 보안 적용 사용자

사용자 시스템 내에 보안 시스템을 구축한 경우, 메시징 서버에 전송되기 전에 암호화 및 전자서명이 적용되어 전송된다. 이 때 메시징 서버(중계 사업자)는 전송된 암호문과 전자서명을 변조나 수정없이 수신자나 다른 중계사업자(VAN)에게 전송한다. 단 수신자가 보안 시스템을 구축하지 못한 사용자(즉, 보안 미적용 사용자)일 경우에는 복호화나 전자서명 검증 후 사용자에게 전송한다. 부인 불능 서비스가 적용된 문서일 경우에는 전자서명을 저장소에 저장한다.

5. 결론

통신 환경과 인터넷의 발달로 인해 소규모로 시행되던 전자상거래가 점차 광범위하게 시행되어 발전 속도를 예측할 수 없게 되었다. 예전의 단순 메시지 전송이나 정보 조회에 불과하던 기능도 점차 off-line으로 행해지는 상거래의 기능까지 포함하게 되었다. 이렇듯 전자상거래가 도입되면서 종이로 처리되던 업무를 점차 전자적으로 전송하면서 표준화된 메시지 형태에 대한 요구

사항이 도출되어, EDI(Electronic Data Interchange)나 XML(extensible Markup Language) 등이 정의되어 사용되고 있다. 업무가 증가함에 따라 거래 내용, 개인 정보, 비용(계좌번호, 카드 번호 등) 정보 등 메시지 종류도 다양해지면서 보안에 대한 필요성이 중요시되고 있다. 그러나 물리적 보안(방화벽)이나 단순 인증(Simple Authentication)만으로는 인터넷을 기반으로 하는 전자상거래 시스템 내에 존재하는 위협요소에 대해 방어할 수 없으므로, 메시지 암호화나 전자서명 등의 메시지 레벨의 응용 보안이 요구된다. 이를 위해 본 논문에서 제안한 메시징 시스템은 인터넷 환경하에서 안전하게 메시지를 전송하기 위해 설계되었으며, 여러 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스 그리고 부인불능 서비스를 선정하여 구현하였다.

향후 연구과제로는 현재 시스템은 트랜잭션(Transaction) 단위로 처리되는 메시징 처리 시스템(Messaging Processing System)이나, 전자 지불과 전자 카탈로그(Catalog) 등 다양한 상거래 분야와 접목할 수 있도록 확장하겠다. 또한 유선 네트워크를 환경만을 고려하여 설계되었으나, 무선(Wireless) 통신까지 지원할 수 있도록 하겠다.

참고 문헌

1. [성균관대, 1993] 한국통신 최종 연구 보고서, 성균관대, "EDI 시스템 시큐리티 선행기술 연구", 1993.
2. [안경림, 1994] "OSI 환경을 위한 EDI 보안서비스요소의 설계 및 구현", 논문, 1994.
3. [한국전산원, 1999] "전자상거래를 위한 보안 기술 체계 및 요소 기술에 대한 이해", 1999, 6
4. [안경림, 박상필, 안정희, 2001] "인터넷을 기반으로 하는 메시징 시스템(XML/EDI System) 설계 및 구현", 한국전자거래(CALS/EC)학회지 제 5 권 제 2 호, 2001. 3, pp.101-112
5. [이영교, 안경림, 안정희, 2001] "Java를 기반으로 하는 Internet Messaging System(XML/EDI System) 설계 및 구현", 한국OA학회논문지 제 6 권 제 2 호, 2001. 6. pp.78-83
6. [안경림, 백혜경, 임병찬, 이영교, 2001] "Java를 이용한 Xconverter 시스템 설계 및 구현", 한국전자거래(CALS/EC)학회지 제 6 권 제 2 호, 2001. 8., pp.1-12
7. [Dan Chang&Dan Harkey, 1998] Dan Chang, Dan Harkey : Client/Server Data access with Java and XML, Wiley & Sons Inc., Canada, 1998
8. [Sean McGrath, 2000] Sean McGrath:XML Processing with Python, Prentice-Hall Inc. Upper saddle River, NJ
9. [David Webber, 1998] David Webber: XML/EDI Perspectives, Japan.
10. http://www.xmledi-group.org/xmledigroup/guide.htm - "Guidelines for using XML for Electronic Data Interchange"
11. http://www.w3.org/TR/REC-xml - Extensible Markup Language (XML) 1.0 Specification 10 Feb 1998, Tim Bray, Jean Paoli, C. M. Sperberg-McQueen

저자 소개

안경림

충북대학교 컴퓨터공학과 학사
성균관대학교 정보공학과 석사
현재 한국물류정보통신㈜ 연구소
관심분야 : 메시징 시스템(X400), 전자상거래, E-Maketplace, 무선통신, 보안 등

박상필

동국대학교 전자계산학과 학사
현재 한국물류정보통신㈜ 연구소
관심분야 : 전자상거래, E-Maketplace, C-Commerce, 보안 등

백혜경

숭실대학교 전자계산학과 학사
현재 한국물류정보통신㈜ 연구소
관심분야 : 전자상거래, E-Maketplace, C-Commerce, 보안 등

임병찬

한양대학교 전자.전자통신.전파공학과군 학사
현재 한국물류정보통신㈜ 연구소
관심분야 : 전자상거래, E-Maketplace, C-Commerce, 보안

박준홍

경희대학교 전자공학과 학사
경희대학교 전자공학과 석사
목원대 전자 및 컴퓨터공학과 박사과정
현재 한국통신 엔트로플렉스 사내기업장
관심분야 : 통신, 망관리, 전자상거래 등

고대식

경희대학교 전자공학과 학사
경희대학교 전자공학과 석사
경희대학교 전자공학과 박사
현재 목원대 전자 및 컴퓨터공학과 정교수
관심분야 : 통신, 망관리, 전자상거래 등