□사례발표□

전자상거래 안전성과 인증 서비스

신 홍 식†

◈ 목 차 ◈

1. 안전한 전자상거래의 구현 방안 - 인터넷 안전성 문제와 인증 서비스

인터넷 상의 전자상거래 시장은 지난 96년 10억불 미만에서 이후 2년마다 10배씩 성장해 2000년에는 1000억불을 넘어서고 2003년이면 1조불을 상회할 것으로 전망된다. 이렇게 되면 지구 상의 모든 상거래의 약 15% 이상이 인터넷을 통해서 거래되는 놀라운 변화가 일어나는 것이다. 이러한 급속한 성장에 따라 인터넷 상거래의 안전성 문제는 심각한 문제로 발전되어 가고 있다. 본래 인터넷은 학교와 연구 기관을 중심으로 한 연구를 목적으로 정보의 공유를 주로 하여 발전하였기 때문에 정보의 보안 문제는 일반인들에게는 그다지 관심거리가 아니었다. 그러나 인터넷이 1995년 경부터 비즈니스 용도로 쓰이게 되면서 인터넷 사기도 급격하게 증가되게 되었다.

〈표 1〉 인터넷의 4대 위험 요소와 보안 대책

	위험 요소	보안 대책
1	신원 확인 (Authentication)	전자 서명
2	무결성 (Integrity)	암호화/전자서명
3	기밀성 (Confidentiality)	암호화
4	부인 방지 (Non-repudiation)	전자서명

† 정회원 : 한국전자인증(주) 대표이사

인터넷 상에서 정보가 교환될 때 발생할 수 있는 위험은 <표 1>에서와 같이 네 가지가 있다.

첫째, 신원 확인 (Authentication)이란 인터넷 상에서 정보를 주고 받는 당사자들 간의 신원을 확인하는 문제를 말한다. 남을 사칭하는 경우 여러 범죄가 발생할 수 있다.

둘째, 무결성 (Integrity)은 정보가 깨지거나 훼손되지 않도록 하는 것을 말한다.

셋째, 기밀성 (Confidentiality)은 남의 사적 정보를 불법으로 액세스하지 못하도록 기밀을 유지하는 것을 말한다.

넷째, 부인 방지 (Non-repudiation)란 자기가 해 놓고 안 했다고 잡아 떼는 행위를 방지하는 것을 말한다.

전자상거래가 안전하게 이루어지려면 이러한 네 가지 위험에 대비한 해결책이 요구된다.

첫째, 신원 확인을 제대로 해주기 위해서 전자서명 기술이 이용된다. 즉, 보내는 사람이 자기의 메시지나 문서에 전자적인 방법으로 서명을 하여 보내고 받는 사람 또한 전자적인 방법으로 이를 확인하는 방식을 말한다.

둘째, 무결성을 유지하기 위하여는 정보를 암호화하거나 전자서명을 한다. 정보를 암호화해서 보내면 암호문이 깨졌을 경우 훼손 여부를 확인할 수 있다. 그리고 전자 서명을 한 경우 해쉬 값을 대조함으로써 메시지의 변조 여부를 확인할 수 있다.

셋째, 외부로 노출돼서는 안되는 정보의 기밀성 유지를 위해서 암호화를 한다.

넷째, 메시지를 작성한 사람이 전자 서명을 한 경우 메시지에 대한 사실의 부인이 불가능하다.

이러한 전자서명과 암호화를 모두 해결하여 주는 서비스가 바로 인증이다.

2. 인증 기술 개요

정보를 암호화하는 보안 기술은 인류의 역사가 시작된 이래 오래 전부터 사용된 것으로 전해진다. 한 사례로 고대의 전쟁터에서 전령을 통하여 암호화한 메시지를 전달할 때도 사용되었다. 그러나 현대적인 암호화 기술은 1980년대 들어 공개키 암호화 기술이 상용화되면서 널리 사용되게 되었다. 공개키 암호 기술 (Public-Key Cryptography)은 암호화하는 키와 암호를 푸는 키가 다른 한 쌍의 키로 구성된다. 이는 수천년 동안 사용되었던 기존의 암호 방식 즉 암호화를 하는 키와 푸는 키가 같은 소위 대칭키 암호화 방식 (Symmetric Key Cryptography)과는 매우 다른 방식으로 복잡하지만 정교한 강점이 있다. 이러한 공개키 암호화 기술은 인증 서비스에서 사용하는 전자 서명과 암호화에 핵심적 수단이 되고 있다.

전자 서명은 다음과 같이 된다.

보내는 사람이 자신 만이 가지고 있는 전자 서명용 비밀 키 (Private Key)로 서명을 하여 메시지를 보낸다; 받는 사람은 전자서명을 확인할 수 있는 공개 키 (Public Key)를 상대방으로부터 전달 받아 상대방의 전자 서명을 확인한다.

공개키 기반의 암호화는 다음과 같이 이루어진다.

보내는 사람이 받는 사람의 공개 키 (Public Key)를 전달 받아 이를 사용하여 메시지를 암호화하여 보낸다; 받는 사람은 자기만의 비밀 키 (Private Key)로 상대방이 보낸 암호문을 풀어 본다. 여기서 공개키 (Public Key)라는 이름은 개인용 비밀키 (Private Key)와 달리 인증 기관에 의해 공개되어 있는 디렉토리 (Public Directory)를 통해서 일반에게 공개된 암호키를 말한다.

위 과정은 일반 인터넷 사용자들이 손 쉽게 사용하기에는 복잡하게 여겨질 수 있다. 실제 인터넷 거래에서는 인증 기관이 발급한 디지털 인증서를 다운로드 받아서 웹 브라우저에 설치하여 사용한다.

3. 국내외 인증 업계 동향

세계 정보 보안 시장은 그 규모가 정보 산업 시장 전체의 약 5% 가까이로 추정되고 있고 이 중 세계 인증 시장은 현재 인터넷 시장 전체의 1-2% 정도로 추정된다. 세계 인증 시장은 1995년 Verisign이 세계 최초의 인증 기관으로 출범하면서 형성되기 시작하였다. VeriSign은 작년 9천만불 가까운 매출로 2000년 2월 현재 회사 주식 가치가 200억불을 상회하고 있다. VeriSign은 인증 서비스의 세계적 호환성을 보장하기 위해 현재 세계 20여개의 주요 인증 기관과 제휴하고 있다.

국내 인증 시장은 작년 7월 전자거래기본법과 전자서명법이 발효되면서 형성되는 초기 단계에 있다. 전자 서명법에 의하면 인증기관 중 일정 자격을 갖추면 공인 기관을 신청할 수 있게 되어 있다. 그리고 공인 인증 기관이 인증한 전자 서명은 전자 서명법 상 그 문서명의인이 작성한 것으로 추정되는 효력이 있다. 그러나 그것이 민간 인증 기관의 인증서가 법적으로 무효이다라는 뜻은

아니다. 민간 인증 기관의 경우는 전문가의 증언에 의해 법원에서도 그 인증서의 효력을 인정 받게 될 것으로 전망된다.

국내 최초의 인증 기관으로 작년 3월 한국전자인증주식회사가 출범하고 이어 한국정보인증주식회사가 7월 설립되었다. 금융결제원과 한국증권전산도 금융 시장을 목표로 인증 기관을 설립하였다. 현재 우리나라에서 공인인증기관이 되려면 자본금 80억원 이상 등 일정 요건을 갖추어야 하고 정보통신부 산하 기구인 정보보호센터의 인증관리센터를 최상위 인증기관 (Root CA)으로 하여야 한다. 그러나 국내 인증 기관에서 발행한 인증서의 국제적 호환성 확보 문제 여부가 주요 관심사가 되고 있다. 한편 한국전자인증주식회사는 최근 미국의 VeriSign과 전략 제휴 협정을 체결하여 자사가 발행한 인증서(CrossCert)와 VeriSign의 인증서비스를 연계하여 국제적인 호환성을 확보하고 금년 1월부터 본격 서비스에 들어갔다.

4. 안전한 전자 상거래 시장 (Secure Electronic Commerce)의 실현

일본 노무라 연구소가 지난 해 소비자를 대상으로 한 조사에서 밝혀진 바로는 전자상거래 시장의 활성화에 최대의 걸림돌은 안전성과 신뢰 문제라고 하였다. 1998년 10월 개최된 OECD 회의에서는 인터넷을 신뢰의 네트웍 (Trust Network)으로 만들어 글로벌한 전자상거래 (Global Electronic Commerce)를 안전하게 실현하자는 세계적인 주제를 내걸었다. 미국, 유럽, 일본 등 세계는 지금 안전한 전자 거래 시장을 위해서 활발하게 국제 표준화 추세에 대응하고 있다. 전자상거래 시장의 안전성 확보는 모든 산업 분야에서 추진되고 있다. 통신 산업 분야에서는 미국의 AT&T, 영국의 British Telecom, 프랑스의 France Telecom등을 비롯한 세계적인 통신 사업자들이 가입자들에게 안전한 통신 서비스를 제공하기 위한 인증 서비스를 도입하고 있다. 금융 시장에선 세계의 유수한 은행, 증권, 카드, 보험 회사들이 고객들에게 안전한 인터넷 금융 서비스를 제공하기 위하여 인증 기술을 도입해 나가고 있다. 또한 공공, 제조, 유통, 무역, 교육 분야 등 여타의 산업 분야에서도 인터넷을 통한 전자 인증 서비스를 도입해 나가고 있다.

위에서 살펴본 대로 안전한 인증 서비스를 제공하기 위하여 세계 각국에서 국제 표준 공개키 기반의 인증 기술을 토대로 한 소위 중립적 인증기관 (Trusted Third Party)이 등장하고 있다. 인증기관은 일반 인터넷 사용자나 기업을 대상으로 인증서를 발급한다. 사용자는 웹 브라우저에 디지털 인증서를 설치하고 사용하게 되는데 인증서는 인터넷 상에서 메시지를 주고 받는 당사자 간에 암호 키를 주고 받아야 하기 때문에 호환성 있는 인증서의 사용이 필수적으로 요구된다. 특히 국제간 상거래나 무역 거래가 이루어 질 때 국제 표준에 의거한 상호 호환 가능한 인증 서비스의 채택이 쌍방 간에 필요하다. 인증 서비스 기술은 전자상거래의 신뢰를 확보하는 수단으로 세계적으로 확산되고 있다. 향후 전자상거래 시장은 이러한 신뢰와 안전성을 기반으로 크게 발전해 나가리라고 본다.

5. 인증과 인증 기관의 개념

인터넷이라는 가상공간에서 전자상거래를 수행할 때, 상대방의 신원을 확인하는 방법과 거래 내역에 대한 쌍방의 부인 방지 대책 등은 중요한 문제이며, 이러한 문제점은 암호 및 인증기술을 이용함으로써 해결할 수 있다. 인증기술이란 네트웍 환경에서 자신의 신분을 상대방에게 증명하는 기술을 의미하며, 전자문서 형태인 인증서(Certificate)를 사용하게 된다. 인증서는 현실 세계의 신분 증

명서와 같은 역할을 수행하게 되며, 이러한 인증서를 등록, 발급 및 조회와 같은 일련의 관리를 총괄하는 조직을 인증기관(Certificate Authority)이라고한다.

6. 인증 기술 활용 분야

인증서의 활용 대표 사례: 인터넷 거래를 하는 모든 산업에 적용

1) 금융 거래시: 인터넷으로 주식 거래시 주문 정보를 전자 서명 및 암호화하면 거래 당사자는 주문 사실이 확인되고 주문 정보도 보호된다.
2) 인터넷으로 기업간 거래 또는 무역 거래시: 당사자간 계약을 전자 서명하여 거래를 확인하고 기밀 보호를 함
3) 쇼핑몰 기업의 실체를 확인해 주고 주요 거래 정보를 보호함.

6.1 인터넷 쇼핑몰

인터넷 쇼핑몰을 통한 상품 구매시, 대금 결제는 신용카드를 기반으로 하는 방식이 보편화되고 있다. 인터넷을 통한 신용카드 결제시 문제점은 고객의 신용카드 정보가 보호되지 못한다는 점이다. 공개키 인증기술을 기반으로 하는 SSL 프로토콜을 사용할 경우, 인터넷을 통해 중요한 정보가 암호화되어 전송되므로 제3자에 의한 보안 사고를 사전에 방지할 수 있다.

6.2 인터넷 뱅킹

고객이 인터넷으로 고액의 현금을 자동 이체할 때 안전 관련 사고를 방지하기 위해 인증을 받아야 할 수 있다.

6.3 인터넷 증권거래

인터넷을 통한 증권거래시, 고객과 증권사 간에 발생할 수 있는 분쟁을 해결하는데 공개키 인증기술이 사용될 수 있다. 어떤 고객이 1000주의 주식을 사기 위해 신청서를 작성하고 전자서명을 붙여 증권사측에 보냈다고 가정할 경우, 추후에 신청서 내용에 대한 부인이나 신청서 발송 사실을 부정할 수 없게 된다. 예를 들어, 100주의 주식을 신청했다거나 혹은 그런 신청을 한 사실이 없다거나 하는 속임수를 쓸 수 없다. 반대로, 증권사 측에서도 신청서 접수 후 확인서에 전자서명을 하여 고객에게 보내면, 추후 신청서 내용이나 접수 사실에 대한 부인을 할 수 없다. 따라서, 거래시 발생할 수 있는 분쟁의 소지가 없어지게 된다.

6.4 인터넷 보험

보험 청약이 이루어지려면, 청약서에 청약자의 자필 서명이 필수적으로 요구된다. 인터넷을 통한 보험 청약의 경우에는 전자서명을 통해 문제를 해결할 수 있다. 먼저, 고객은 인터넷 보험 싸이트에 접속하여 자신에게 맞는 보험 상품을 선택하고, 청약서를 작성한 후 자신의 전자서명을 붙여서 보내면 고객과 보험사 간의 계약이 효력을 얻게 된다.

7. 인증 서비스의 종류

인증기관에서 제공하게 되는 인증서비스는 각 인증기관의 인증정책에 따라 다르지만, 일반적으로 인증서 사용 용도, 목적, 및 신뢰도 등에 따라 몇 개의 클래스로 구분하여 차별적인 서비스를 제공하게 된다.

Class 1 인증서는 개인에게만 발급된다. Class 1 인증서는 사용자의 이름과 email 주소가 명확하기 기재되어 있는지 만을 검사한 후 발급된다. Class 1은 온라인으로 발급되며 웹브라우징과 전자우편에 보안을 강화하기 위해서 사용된다.

개인용 인증서

인증 서비스	발급 대상	발급과정	용도
Class 1	개인	E-mail 주소 확인 과정을 통한 온라인 발급	개인간 E-mail 교환
Class 2	개인	전화로 신원확인 후 온라인 발급	일반상거래, 기업내, 기업간 E-mail 교환, 소프트웨어 검증, 회원제 온라인 서비스
Class 3	개인	인증기관이나 인증기관의 인증을 받은 등록기관에 직접 가서 신원확인과정을 거친 후 발급	고가의 전자상거래, 전자계약문서, 인터넷 뱅킹, 온라인 청약, 기업 DB 접근, SSL, 소프트웨어 검증, 등록기관 인증, 공공서비스

기관용 인증서

인증 서비스	발급 대상	발급과정	용도
Class 3	기관	인증기관이나 인증기관의 인증을 받은 등록기관에 직접 가서 신원확인과정을 거친 후 발급	고가의 전자상거래, 전자계약문서, 인터넷 뱅킹, 온라인 청약, 기업 DB 접근, SSL, 소프트웨어 검증, 등록기관 인증, 공공서비스
웹서버용 인증서	웹서버	검증은 회사 또는 기관의 이름과 도메인 등록, 담당자 이름 검사	SSL 보안

Class 2 인증서는 개인에게만 발급된다. Class 2 인증서는 신청자의 신청서를 제 3의 고객 데이터베이스의 정보와 비교함으로써 검증을 한다. 일반적으로 신용평가회사의 데이터베이스를 사용한다. Class 2 인증서는 일반상거래, 기업 내, 기업간 E-mail 교환, 소프트웨어 검증, 회원제 온라인 서비스 등에 사용된다.

Class 3 인증서는 개인과 기관에 발급된다. Class 3 인증서는 신청자가 직접 찾아와서 신분증을 통해 신원을 확인한 후 발급된다. Class 3 인증서는 고가의 전자상거래, 전자계약문서, 인터넷 뱅킹, 온라인 청약, 기업 DB 접근, SSL, 소프트웨어 검증, 등록기관 인증, 공공서비스 등에 사용된다.

웹서버용 인증서를 통해 웹서버는 현재 웹 기반 통신에서 가장 널리 사용되고 있는 SSL 프로토콜을 구현할 수 있다. 웹서버 인증서에 대한 검증은 회사 또는 기관의 이름과 도메인 등록, 담당자 이름 등을 검사하는 것이 일반적이다.

8. 인증서의 가격

개인용 인증서는 현재 개인용의 경우 Class 1의 서비스만 제공되고 있으며, 연 2만원에 무제한 사용 할 수 있다.

쇼핑몰 같은 전자 상거래용 웹사이트 인증서는 연 60만원 (40bits용); 120만원 (128bits용)이며, 기업용 인증서는 사이트 사용자 수에 따라 다르다. 5천명에서 1만명인 경우 연 2-3 억원 수준이다.

9. 인증서 발급 절차

인증서 발급 절차는 인증서 보안 등급에 따라 온라인 발급(Class 1, 2)과 오프라인 발급(Class 3)로 나뉘어진다. 온라인 발급이란 인증서 신청에서부터 인증서 발급에 이르는 전과정이 인터넷을 통해 이루어지는 것을 말하고, 오프라인 발급이란 인증서 사용자의 신원확인을 확실히 하기 위해 사용자가 직접 인증기관 또는 등록기관 등에 가서 인증서를 발급받는 것을 말한다.

온라인 발급(Class 1, 2의 경우)

일반적인 웹 브라우징이나 전자우편 보안에 사용되는 낮은 등급의 인증서 발급을 말하며, 절차는 다음과 같다.

1. 사용자가 인증기관의 홈페이지를 통해 인증 신청양식을 작성하여 보낸다.
2. 인증기관은 사용자의 공개키에 인증기관 자신의 서명을 붙인다.
3. 인증기관은 발급한 인증서를 사용자가 받아

갈 수 있도록 접근코드를 사용자의 전자우편 계정으로 발송한다.

4. 사용자는 전자우편을 통해 받은 자신의 접근코드를 사용하여 인증기관에 접속, 자신의 인증서를 온라인으로 받아온다.

오프라인 발급(Class 3)

인터넷 쇼핑이나 인터넷 뱅킹, 홈트레이딩, 무역 거래 및 계약과 같이 철저한 보안이 요구되는 분야에 사용되는 인증서 발급 방식으로써, 확실한 신원 확인을 위해 오프라인으로 발급한다.

1. 사용자는 인증기관(또는 등록기관)에 직접 방문하여 신청서를 작성하고, 자신의 신원을 증명할 수 있는 서류를 제출한다.
2. 인증기관(또는 등록기관)은 사용자가 제출한 정보를 이용하여 사용자의 신원을 확인한다.
3. 신원 확인 절차가 끝나면, 인증서를 발급하고 안전한 저장매체(예, 스마트카드 등)에 저장하여 사용자에게 건네준다.

10. 인증 보안 사고 사례

아래에 소개된 보안 사고들은 공개키 인증기술을 이용한 전자서명, 암호화, 웹 사이트 인증 등을 통해 충분히 사전에 방지할 수 있는 해킹 사례들이다.

1. Pairgain사 해커 체포

FBI는 99년 4월 19일, 북부 캐롤라이나, 롤리(Carolina, Raleigh) 출신의 25세 Gary Dale Hoke에 대한 조사에 착수했다. Hoke이 주식 시세 관련 웹사이트인 "Bloomberg"사 홈페이지를 가짜로 만들어 지난 수요일 PairGain 주식 시세를 치솟게 하기 시작했을 때, 캘리포니아 기반의 PairGain사는 이를 일컬어 가상공간 거짓정보의 걸작(cyber-hoax masterpiece)라고 칭했다. 로스앤젤레스의 국선 변호사는 『이 사건은 한 개인이 신기술의 힘을 이용하여, 거짓 정보를 수백만 투자가에게 급속도로 퍼뜨린 최초의 사건』이라고 말했다. Hoke은 현재 벌금 없이 집행유예 중이나 만일 Hoke이 유죄를 선고받게 된다면 백만 달러의 벌금과 10년 형에 처해질 것이라고 알려졌다.(CNET NEWS)

2. 소년도 할 수 있는 인터넷 사기

99년 3월 18일, 뉴질랜드의 몇몇 최대 기업에 불법 침입했던 22세의 웹 디자이너 Craig Ian Henderson은 인터넷 신용카드 범죄는 매우 간단하여 10세 소년도 문제없이 할 수 있다고 밝혔다. 그는 지난 5개월간, 인터넷 해킹 사이트에서 내려받은 프로그램으로 만든 가짜 신용 카드를 이용하여 통신사, 렌트카 회사 등에 미화 60,000 달러 이상을 불법 거래한 사기 혐의로 5년형을 선고받았다. 은행 등 금융기관에 따르면 인터넷과 전화 전산망을 이용한 무기명 신용카드 거래는 막기 힘든 허점을 지니고 있다고 한다. 이 사건은 뉴질랜드에서 알려진 최초의 인터넷 신용카드 사기 사건으로 전해졌다. (Infowar.com, 3/18/99)

3. 불가리아 통신회사 인터넷 침입

불가리아 전화국 (Bulgarian Telecommunication Conpany(BTC)) 이사회는 BTC가 해커들의 공격을 받고 있다고 2월 16일 발표했다. 6시간에서 7시간에 걸친 2개의 세션으로 이루어진 이 공격은 1월 26일에 최초로 시작되었으며 이 세션동안 침입자들은 미국 서버를 통해 바이러스가 감염된 메일을 수천 명의 WWW 사용자에게 보냈다. 이와 유사한 전자우편이 미국의 유명 대학에 보내졌으며 곧이어 BTC Email 서버에도 공격을 가했다. 그 이후 2월 12일, 해커들은 우편 통신 위원회(Committee of Posts and Telecommunications)의 인터넷 서버에 대한 공격을 시작했다. BTC 관계자는 이

러한 공격이 사용자들에게 직접적인 해는 없으나 인터넷 수행 능력에 장애를 줄 수 있다고 말하고, BTC는 정보통신망을 항상 감시하며 악의의 행위에 대한 기록을 하고 있다고 밝혔다. (Infowar.com, 2/26/99)

4. 14세 이스라엘 소년 이라크 정부 사이트 침투 (Israeli Boy, 14 Hacks Saddam Off The Internet)

이라크 정부의 인터넷 사이트를 침입한 이스라엘 소년이 국민적 영웅으로 떠올랐다. 14살 짜리 NIR ZIGDAN이란 이름의 이 소년은 E-메일을 통하여 바이러스를 이라크 정부 사이트에 침투시키는 방법으로 이러한 작업을 해왔다. 현재 이스라엘은 컴퓨터 산업이 가장 발전한 나라 중 하나이며, NIR는 어릴때부터 이미 컴퓨터를 정통하고 이미 한 기업에서 관련 업무를 맡고 있다. (Infowar.com, 2/8/99)

5. 중국, 은행 절도 해커범 중형 선고 (China Sentences Hackers To Death For Bank Theft)

98년 11월 15일, CENTERCOUNTY 지역법원은 PSU의 학생회 임원 당선자의 한 명인 JASON COVENER에게 다른 학생회 임원의 E-MAIL을 해킹한 혐의로 재판을 받도록 명했다. 이는 2년형에 처해질 수도 있는 범죄이다. 이로서 최종학기를 남기고 법률 대학원 진학을 계획하고 있던 COVENER는 전과 기록은 물론 학교에서 퇴학 당할 수도 있는 상황에 처하게 되었다. 대학 관계자는 이번 사건을 대학 역사상 가장 심각한 컴퓨터 범죄로 평했다. (Infowar.Com, November 22, 1998)

6. 기타

국내에서도 최근 인터넷 상에서의 불법 감청 및 전자 메일 불법 접근 등이 문제가 되고 있다. 인증은 전자 메일을 암호화하고 전자 서명함으로써 개인의 정보와 기밀을 보호함으로써 인증 서비스 사용자 이외의 사람에 의한 접근을 방지하는 효과를 가지고 있다.

11. 한국전자인증과 VeriSign의 Global Trust Network 제휴에 따른 향후 전망

한국전자인증주식회사는 국내 최초의 인증 기관으로 자사가 개발한 인증 기술을 기반으로 1999년 4월부터 인증 서비스를 시작했다. 그리고 인터넷 전자 상거래에서 인증서의 세계적 호환성 확보를 위해 1999년 9월 세계 제일의 인증 기관인 VeriSign과 제휴하면서 세계 20여개국의 주요 인증 기관이 협력하는 Global Trust Networt의 국제적 파트너사가 되었다. 이 글로벌 인증 네트웍(Global Trust Network)을 통하여 한국전자인증은 VeriSign의 인증 서비스를 자사가 발행한 인증서(CrossCert)와 연계하여 세계적으로 호환되는 인증 서비스를 시작하게 되었다.

한국전자인증은 기업용, 쇼핑몰 등과 같은 전자상거래 사이트용 및 개인용 인증서 발급 서비스를 제공한다. 인증을 원하는 기업이나 개인은 한국전자인증의 웹 사이트(www.crosscert.com)를 통해 신청하면 소정의 인증절차 (Validation Process)를 거쳐 신용 평가 및 제반 조사를 실시한 후 해당 웹 사이트에 인증서를 On-line 상으로 발급하게 된다. 이때 거래 상대방은 브라우저에서 제공하는 보안 기능을 통해 인증서 및 거래 상대방을 확인할 수 있어 안전한 전자상거래가 이루어 진다. 이로써 한국전자인증은 21세기 안전한 전자상거래 시대를 실현하는 신뢰 받는 기업의 대명사가 될 것이다.

신 홍 식

1984년-1989년 Georgia Institute of Technology 컴퓨터과학 (박사)
1981년-1983년 Pennsylvania 주립대학 컴퓨터과학 (석사)
1970-1974 서울대학교 공과대학 응용수학(학사)
1996년-1997년 동부정보시스템(동부그룹) 대표이사
1993년-1996년 동양 SHL(동양그룹) 상무이사
1991년-1993년 한국통신기술(Korea Telecom International) 책임연구원
1989년-1991년 GTE Labs(미국 Boston 소재) Senior MTS
1978년-1979년 Bell Telephone Mfg. Co.(현재 Alcatel) 파견 근무
1974년-1977년 해군사관학교 교수부 컴퓨터 교관 (해군중위)
1999년-현재 한국전자인증주식회사 대표이사
1997-현재 (주)신테크 대표이사

제 1회 한국정보처리학회 EC/ERP연구회 SIG 모임 안내

안녕하십니까?

본 연구회에서는 산학연의 협력을 통하여 21세기에 가장 이슈가 되는 전자상거래를 정립하기 위하여 EC/ERP연구회 관련기업 및 회원을 모집하고 있습니다. 본 연구회에서는 EC/ERP(B2B, B2C)표준모델에 대하여 연구하고자 정기적으로 격월 모임을 산학연으로 SIG모임을 갖고자 합니다. 관심이 있으신 교수님들께서는 반드시 참여하셔서 개발담당자와의 심도 있는 의견 및 토론·발표에 좋은 의견을 교환하여 주시면 감사 하겠습니다.

안 내

- 일 시 : 2000년 4월 29일(토요일) 11:00 - 13:00
- 장 소 : 한국기업전산원(전화번호 : 02-6248-7800(734))
  (서울 역삼동 르네상스호텔 건너편 삼정개발B/D 8층 세미나실)
- 참가자격 : 전국대학 컴퓨터·정보 관련학과, 산업공학 관련학과, 경영정보 관련학과 교수 및 관심있으신 정보처리학회 회원
- 참가 연락처 : EC/ERP사무국 김 태호국장 (TEL : 02-6248-7800(734)
  최 성 교수 (TEL : 0417-580-2000, 016-390-2062)
- 기타사항 : SIG자료제공 및 세미나 끝난 후에 중식예정(SIG주최측 제공)

EC/ERP연구회 회장 **김 길웅**