특 집

공개키기반구조(PKI) 구축 및 활용

최 영 철, 박 성 준
(주)비씨큐어

I. 서 론

최근 많은 기업체와 공공기관 등에서 인터넷 기반의 인트라넷 시스템 구축, 전자입찰 시스템 구축, EIP(Enterprise Information Portal) 시스템 구축 등을 수행하고 있으며, 이러한 과정 중에 보안 인프라를 구축하는 작업은 상당히 중요한 작업들 중의 하나가 되고 있다. 과거 수 년 전만 하더라도 보안 시스템은 하나의 선택사항으로서 여겨지던 시절이 있었지만, 현재는 반드시 포함되어야 할 의무사항으로 인식되고 있다. 총체적 보안을 위해서는 네트워크 보안(Network Security), 시스템 보안(System Security), 트랜잭션(데이터) 보안(Transaction Security) 등이 모두 고려되어야 하지만, 그 중에서도 가장 채택하고 구축하기 어려운 부분이 바로 트랜잭션 보안이다.

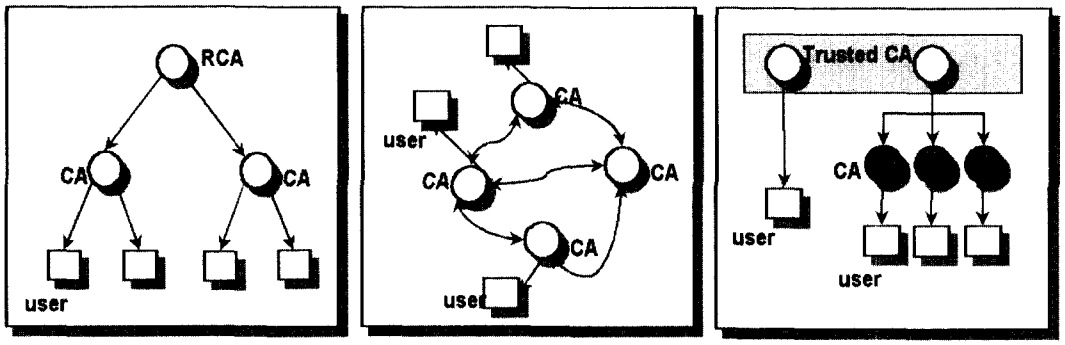
"트랜잭션 보안"이라 함은 네트워크로 송·수신 또는 저장되는 데이터나 이에 관계된 행위자들의 진정성을 보장해주는 부문의 보안을 말한다. 즉, 송신자의 신원을 보장하는 사용자 인증(Authentication), 데이터의 진정성을 보장하는 데이터 무결성(Intergrity), 데이터의 무단 노출을 방지하는 비밀성(Confidentiality), 사용자의 행위를 부인할 수 없게 하는 부인방지(Non-repudiation) 등이 트랜잭션 보안의 범주가 된다. 트랜잭션 보안은 주로 암호기술을 사용함으로써 해결하게 되는데, 그 중 공개키암호(Public Key Cryptography) 기술의 적용이 핵심이 된다. 결국 공개키암호 기술에 근간을 두는 전자서명 또는 암호화라는 작업을 통해서 트랜잭션 보안을 이룰 수 있는 것이다.

전체 시스템 구축 시 트랜잭션 보안 부분을 적절히 적용시키기 어려운 이유는 네트워크 보안이나 시스템 보안과는 달리 공개키기반구조(Public Key Infrastructure, 이하 PKI라 칭함)라는 보안 인프라가 필요하고, 적절한 적용 대상의 선별과 실제 기술 적용이 어렵기 때문이다. 본 고에서는 PKI에 대한 이해와 트랜잭션 보안에 대한 이해를 높임으로써 PKI를 도입하고 이를 활용하는 방식에 대해 소개하고자 한다.

II. PKI의 기본적 이해

인증(Certification) 서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 안전한 전자상거래 환경의 구축을 위해서는 서두에서도 언급한 바와 같이 인증, 무결성, 비밀성, 부인방지 등의 정보보호 서비스가 필요하게 되며, 인증, 무결성, 부인방지 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다. 현재 안전성을 일정 수준 정량화 시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증서비스가 필요하게 된다.

인증기관은 공개키 암호 시스템을 이용하고자 하는 사용자들에 대하여 공개키가 해당 사용자의 소유임을 증명하고 또한 해당 키가 위·변조되지 않았다는 사실을 증명하기 위하여 공개키 및 소



(a) 계층형 모델 (b) 네트워크형 모델 (c) 신뢰형 모델

〈그림 1〉 PKI 구성모델

유자 정보 등으로 구성된 데이터에 전자서명을 수행함으로써 인증서(Certificate)를 생성한다. 결과적으로 인증기관이라 함은 인증서 발급 서비스를 제공해 줌으로써 이윤을 창출하거나, 기업 내 안전한 전산망 구축을 담당하는 하나의 조직을 일컫는 것이며, 인증 서비스란 인증기관이 제공해주는 인증서 발급, 인증서 관리 등 일련의 인증 관련 서비스를 통칭하는 것이라고 말할 수 있다.

PKI는 인증기관(Certification Authority), 등록기관(Registration Authority), 저장소(Repository), 사용자(Client)와 같이 4개의 구성객체로 이루어진다. CA은 인증서를 발급해 주고 이를 관리해주는 신뢰기관이며, 등록기관은 사용자 신원확인 및 고객 데이터유지 등의 업무를 수행하는 기관이며, 저장소는 사용자와 CA의 인증서 및 인증서폐지목록(Certificate Revocation List, CRL)을 저장, 공고해주는 기관이다.

CA는 PKI 환경에 따라 조직적, 계층적 형태의 관계를 가질 수 있다. 이러한 CA의 관계에 따라 PKI는 계층형(Hierarchical) 모델, 네트워크형(Network) 모델, 신뢰형(Trust) 모델 등으로 나뉘어 진다. 계층형 모델은 국내 전자서명 인증관리체계가 채택하고 있는 형태로서 최상위 인증기관(Root CA)과 그 하부에 하위 인증기관(Sub CA)으로 구성되는 모델이다. 네트워크형 모델은 CA가 상하위 관계성을 갖는 것이 아니라, 하나의 CA가 독립적인 형태로서 다른 CA들과 동등한 입장에서 연결되는 형태의 모델이다. 실제로 응용이 다양하고 광범위한 경우 이러한 네트워크형 모델이 적합하게 된다. 그러나, 계층형 모델이나 네트워크형 모델들은 CA들간의 상호 유기적 연결을 전제로 하고 있기 때문에 실제 환경에 구축하는 경우 많은 어려움들에 직면하게 된다. 이러한 문제점을 회피하고자 등장한 것이 신뢰형 모델이다. 현재 웹 브라우저가 채택하고 있는 방식이 신뢰형 모델이며, 실제적으로 인터넷 환경에 가장 널리 퍼진 모델이라고 말할 수 있다. 〈그림 1〉은 PKI 구성모델을 도식화한 것이다.

III. 트랜잭션 보안의 이해

인터넷 환경에서 트랜잭션 보안 방식은 크게 2가지로 나뉘어진다. 첫 번째는 국제 표준화 단체나 또는 주요 업체에 의해 표준화되어 여러 제품들이 이를 동시에 지원하는 형태의 범용(Public) 트랜잭션 보안 방식이다. 트랜잭션 보안이 하나의 표준 네트워크 프로토콜로서 정의되어 활성화된 것은 1990년대 초 부터이지만, 실제로 인터넷 환경에서 가장 큰 영향을 미치게 된 시점은 1995년 넷스케이프(Netscape, 현 AOL)社가 SSL(Secure Socket Layer) 트랜잭션 보안 프로토콜을 개발하면서 부터이다. SSL 트랜잭션 보안

프로토콜의 개발을 계기로 웹 브라우저와 웹 서버 사이의 네트워크 프로토콜인 HTTP는 보다 안전한 프로토콜로 발전되었으며, 많은 웹 관련 개발 업체들이 SSL을 지원함으로써 SSL은 현재 HTTP 채널을 보호하기 위한 가장 손쉬운 방법으로 사용되고 있다. PKI 관점에서 SSL을 범용 트랜잭션 보안의 첫 계기로 보는 것은 SSL 프로토콜을 지원하는 웹 서버와 웹 브라우저가 시장에 등장함으로써 인증서가 본격적으로 사용되는 최초의 환경을 만들었으며, 실제로 이러한 배경을 통해 미국에서는 VeriSign社라는 최초의 인증기관 업체가 등장하였기 때문이다. 이후 SSL은 SSL v3.0 이후 TLS(Transport Layer Security)라는 프로토콜로 발전하였으며, 이외에도 전자메일 관련 트랜잭션 보안 프로토콜인 S/MIME(Secure Multipurpose Internet Mail Extensions), VPN(Virtual Private Network) 구성을 위한 IPSEC(IP Security) 등 다양한 네트워크 계층 상에서 범용 트랜잭션 보안 프로토콜들이 등장하였다.

두 번째는 범용 트랜잭션 보안 프로토콜과는 달리 응용계층에서 특정 도메인내에서 어떤 필요성에 의해 별도의 트랜잭션 보안을 정의함으로써, 독자적인 트랜잭션 보안 프로토콜을 구성하여 사용하는 전용(Private) 트랜잭션 보안 방식이다. 예를 들면, 인터넷 뱅킹 시스템을 구축하는 경우 은행이 사용자의 부인방지를 위하여 계좌이체 시 웹 폼(Form) 입력 데이터에 대하여 사용자 전자서명이 필요함을 결정했다고 가정하자. 이 경우 시스템 개발자는 이러한 요구사항을 만족하는 범용 트랜잭션 보안 프로토콜을 찾아야 할 것이다. 그러나, 상기에서 언급한 대부분의 트랜잭션 보안 프로토콜(SSL, IPSEC 등)들은 인증, 무결성, 비밀성 이라는 3대 정보보호서비스 기능만을 제공한다. 그러므로, 시스템 개발자 입장에서는 이러한 범용 트랜잭션 보안 프로토콜을 사용할 수 없게 되며, 이러한 문제를 해결하기 위해 서 별도의 전용 트랜잭션 보안 프로토콜을 설계·구현하게 된다. 이와 같은 배경으로 인해 전용 트랜잭션 보안 프로토콜들이 널리 사용되고 있으며, 특히 국내에는 이와 같은 형태를 제품화 시켜 솔루션으로 판매하는 보안 업체들이 많이 있다.

트랜잭션 보안을 고찰하는 이유는 트랜잭션 보안이 바로 PKI의 도입 이유이기 때문이다. 즉, 사용자의 관점에서 PKI를 도입하고자 하는 경우 사용자는 PKI의 궁극적인 도입 목적인 트랜잭션 보안을 타겟 구축 시스템에 어떤 이유(Why)로, 무슨 기능을(What), 어느 부분(Where)에, 어떻게(How) 적용할 것인지에 대한 이해가 있어야만 하며, 이를 통하여 PKI의 도입 여부 및 도입 방식을 올바르게 결정할 수 있게 된다.

Ⅳ. PKI 구축 방법론

본 절에서는 사용자 관점에서 PKI를 구축하는 방법론에 관하여 고찰하고자 한다. 앞 절에서도 언급한 바와 같이 사용자가 PKI를 구축하고자 하는 이유는 트랜잭션 보안을 구축 시스템에 적용하고자 하기 때문이다. 그러므로, PKI 구축 전 정확한 트랜잭션 보안의 도입 배경과 이에 대한 진단이 필요하게 된다. 즉, PKI 환경 구축에 있어 트랜잭션 보안 도입 분석이 우선적으로 이루어져야 하며 그 단계는 다음과 같다.

1단계) [Why] 트랜잭션 보안이 필요한 이유 분석 : 사용자는 우선적으로 트랜잭션 보안이 필요한 이유(Why)를 도출해야 할 것이다. 예를 들면, "인트라넷 환경을 웹 기반으로 구축하고자 함에 있어 HTTP 채널로 중요 데이터가 송·수신되기 때문에 이에 대한 보안대책이 필요하다." 라는 이유를 도출해야 한다는 것이다. 특히, 이 부분에서는 막연한 웹 트랜잭션 보안 대책보다는 보다 구체적인 사항들을 기술해야 한다. 이것은 곧 시스템 보안 요구사항 기술과 같게 될 것이며, 이를 바탕으로 어떠한(What) 정보보호서비스가 필요한지 도출하게 된다.

2단계) [What] 적용할 정보보호서비스 결

정 : [Why]가 도출된 후 사용자는 도출된 사항에 대응되는 구체적 정보보호서비스를 연결시켜야 한다. 예를 들면, 1단계) 도출 사항이 "사용자 로그인 이후 송·수신 되는 데이터는 당사자만이 보아야 한다."라는 것이라면 여기에는 4가지(인증, 무결성, 비밀성, 부인방지) 정보보호서비스 중 "비밀성" 서비스가 대응되어야 하며, [What]의 항목으로서 비밀성이 추가되는 것이다.

3단계) [Where] 1, 2단계)의 과정을 통하여 사용자는 트랜잭션 보안이 필요한 이유와 이에 대한 대책을 도출하였다. 이 과정 후 사용자는 해당 정보보호서비스를 구체적으로 적용해야 할 부분을 도출할 수 있게 된다. 예를 들어 상기 2단계) 예를 가정한다면, 사용자는 사용자 로그인 이후 웹 페이지 중 비밀성 서비스 적용이 필요한 폼 데이터 항목(예 : 계좌번호, 이체금액 등)을 구체적으로 도출할 수 있게 된다. 3단계)에서는 이러한 내용들을 구체적으로 정리하게 된다.

4단계) [How] 1, 2, 3단계)를 통해서 사용자는 타겟 시스템에서 필요한 정보보호서비스 항목을 도출하였고, 이를 적용할 구체적 부분도 도출하였다. 이후 사용자는 이러한 정보보호서비스를 제공하기 위한 마지막 방법론을 결정하게 된다. 예를 들어, 1, 2, 3단계) 분석 후 필요한 항목이 웹 채널의 단순한 비밀성 및 무결성 보장이라고 한다면, 사용자는 두 가지 방식을 선택할 수 있게 된다. 첫 번째는 범용 트랜잭션 보안 프로토콜인 SSL 프로토콜의 적용을 선택하는 것이고, 두 번째는 암호 SDK(System Development Kit)을 도입하여 별도의 전용 트랜잭션 보안 프로토콜을 적용하는 것이다. 전자의 경우는 SSL 프로토콜을 지원하는 웹 서버를 구축하고, 이에 대한 SSL 서버 인증서만 외부 인증기관으로부터 발급받으면 되기 때문에 아주 간단하게 시스템을 구축할 수있게 된다. 후자의 경우는 원하는 폼 데이터만 암호화할 수 있고, 원하는 암호 알고리즘을 선택적으로 사용할 수 있다는 장점이 있게 된다. 결국 사용자는 1, 2, 3단계)를 통하여 도출된 사항을 기반으로 어떠한 방식의 접근을 취할 것인가를 결정하게 된다.

상기의 트랜잭션 보안 도입 분석을 통하여 사용자는 PKI 도입 여부를 결정할 수 있게 된다. 사용자의 관점에서 PKI의 도입은 크게 PKI 인소싱(Insourcing) 방식과 PKI 아웃소싱(Outsourcing) 두 가지 방식으로 나누어진다. PKI 인소싱이라 함은 사용자가 외부 PKI 솔루션 개발업체로부터 PKI 솔루션(CA서버, RA서버, 디렉토리서버, 사용자S/W)을 구매하여 이를 자사에 구축하고, 이를 직접 운영함으로써 필요한 인증서들을 발급하는 방식을 말하는 것이다. 반면, PKI 아웃소싱이라 함은 사용자가 필요한 인증서들을 외부의 인증기관 서비스 업체로부터 발급받아 사용하는 방식을 말한다. 두 가지 방식은 각각 일장일단을 가지고 있기 때문에 사용자는 이에 대한 철저한 분석이 필요하게 된다. PKI를 인소싱할 것인가, 아웃소싱할 것인가에 대한 판단으로서 가장 중요한 요소는 범용 트랜잭션 보안을 사용할 것인가, 전용 트랜잭션 보안을 사용할 것인가의 판단이다. 일반적으로 범용 트랜잭션 보안을 위해서는 다음 〈표 1〉과 같은 인증서비스가 필요하게 된다.

범용 트랜잭션 보안을 위해서 〈표 1〉과 같은 인증서가 필요한 경우에는 주로 PKI 아웃소싱을 수행하게 되는데, 그 이유로서는 사용되어지는 인증서 수가 많지 않기 때문이다. 결론적으로 타겟 시스템 구축 시 필요한 인증서 수가 적은 경우(서버 측만 인증서가 필요하거나, 특수한 목적의 인증서 몇 개만 필요한 경우)는 거의 전적으로 PKI 아웃소싱 방식을 택하는 것이 효율적인 방법이 된다. 그러나, 때로는 클라이언트 인증서가 많이 필요한 경우도 발생할 수 있는데(예 : 5만명의 임직원을 가진 기업체가 안전한 전자우편의 사용을 위하여 S/MIME 인증서를 도입하고자 하는 경우) 그러한 경우에는 아웃소싱 경우의 「인증서 수×단가비용=전체비용」과 인소싱 경우의 「PKI솔루션도입비용+향후운영비용=전체비용」을 비교함과 동시에 기타 다른 판단 근거들을 종합하여 도입방식을 결정해야 한다.

반면 전용 트랜잭션 보안의 경우에는 PKI 인

〈표 1〉 인증 서비스 종류 및 내용

분 류	서비스 종류	내 용
범용서비스	Individual Certificate	안전한 전자우편 프로토콜인 S/MIME이나, 보안 프로토콜인 SSL에서 클라이언트 인증서로 사용되는 개인용 인증서 발급 서비스
	Server Digital Certificate · Secure Server Certificate · Global Server Certificate · OFX Server Certificate · EDI Server Certificate	보안 프로토콜인 SSL이나 OFX 또는 EDI 환경에서 안전한 트랜잭션을 위한 서버용 인증서 발급 서비스 · 40비트 암호화가 가능한 SSL용 인증서(Secure Server) · 128비트 암호화가 가능한 SSL용 인증서(Global Server) · 금융망 프로토콜인 OFX에서 사용되는 금융 서버용 인증서(OFX Server) · 전자데이터교환(EDI) 시스템에서 사용되는 서버용 인증서(EDI Server)
	Code Signing Certificate · Microsoft Authentication Code · Netscape Object Signing · Marimba Castanet	네트워크 상으로 S/W 모듈이나 데이터를 배포하는 경우 안전 신뢰성을 향상시키는데 사용되는 인증서 발급 서비스 · 네트워크를 통해 마이크로소프트사의 32-bit.exe(PE files), .cab, .ocx .class 파일등의 S/W 모듈을 배포하는 경우 사용되는 개발자용 인증서 · 네트워크를 통해 자바, 자바스크립트, Pulg-in 등의 S/W 모듈을 배포하는 경우 사용되는 개발자용 인증서 · 네트워크를 통해 마림바社의 Push기술을 통해 데이터가 배포되는 경우 사용되는 채널 서명용 인증서

※ SSL(Secure Socket Layer), S/MIME(Secure Multi-purpose Internet Mail Extension), OFX(Open Financial Exchange)

소싱이 보다 강한 접근 방식이 된다. 일반적으로 전용 트랜잭션 보안을 사용하는 경우는 클라이언트가 전자서명을 수행하거나, 또는 클라이언트가 자신의 인증서로 서버에 로그인하는 경우 주로 전용 트랜잭션 보안을 사용하게 된다. 그러므로, 이러한 경우에는 대부분 클라이언트 인증서가 필요하게 되고, 동시에 그러한 정보보호서비스를 제공하기 위해서 암호 SDK가 필요하기 때문에 사용자는 주로 PKI 솔루션을 도입함으로써 PKI 환경을 구축하게 된다. 그러나, 최근에는 인증서비스만을 제공하는 인증기관들이 암호 SDK도 사용자에게 공급해줌으로써 전용 트랜잭션 보안 부문에 진출하고 있다. 특히, 국내의 경우에는 인증서비스를 전문적으로 제공하는 공인인증기관들이 범용보다는 전용 트랜잭션 보안 부문에 집중함으로써 인소싱과 아웃소싱의 영역을 오버랩하고 있다. 그러나, 일반적으로 세계 유수의 컨설팅 보고서에 따르면 PKI 시장 전체를 보았을 때, 인소싱과 아웃소싱의 시장영역이 약 6 : 4 정도로 평가하고 있다.

V. PKI 활용과 발전

PKI 구축은 향후 네트워크 환경에서 시스템을 구축하는 경우 선택사항이 아닌 의무사항으로 발전되리라 판단된다. 그러나, 이러한 폭 넓은 확산을 위해서는 보다 많은 응용이 필요하다고 사료된다. 현재, 국내의 PKI 구축은 주로 웹 기반의 트랜잭션 보안에 초점이 맞추어져 있다. 예를 들어, 현재 가장 PKI 구축이 활성화되어 있는 금융 분야의 경우 모두가 인터넷 뱅킹이라는 웹 기반의 전자거래 시스템에서 클라이언트가 서버에

게 데이터를 전달함에 있어 비밀성을 보장하거나 부인방지를 제공하는 기능에 집중된 것이다. 기업체의 경우에 있어서도 웹 기반의 그룹웨어(Groupware), 워크플로우(Wokrflow), 지식관리(KM) 등을 도입하여 EIP(Enterprise Information Portal) 등을 구축함에 있어 PKI를 도입하는 이유는 클라이언트가 서버에 접속하는 경우 인증서를 이용한 사용자 인증과 비밀성 보장등에 주로 초점이 맞추어진다. 정리하면, 현재의 PKI 구축 목적은 대부분이 클라이언트/서버의 웹 환경에서 주로 클라이언트가 서버에 접속하는 환경에서의 트랜잭션 보안을 위한 것이다. 그러나, 보다 PKI가 폭 넓게 확산되기 위해서는 단순한 웹 환경의 클라이언트/서버 구조가 아닌 클라이언트/클라이언트, 서버/서버 등 다양한 환경으로 응용이 확산되어야 할 것이다. 예를 들면, A와 B라는 두 클라이언트가 전자계약을 함에 있어 전자서명을 사용한다고 하는 경우 상기에서 설명한 웹 기반의 클라이언트/서버 구조의 트랜잭션 보안으로는 해결책을 제시할 수가 없게 된다. 이것을 위해서는 많은 사용자들이 실생활에 직접 이용하는 응용 S/W나 기타 다른 응용 S/W의 개발들이 필요하게 되며, 동시에 보다 철저한 인증서 관리 메커니즘이 필요하게 된다. 국외에서는 PKI의 향후 발전 방향이 사용자들이 쉽게 사용할 수 있는 PKI 응용 S/W의 개발과 PKI 구축을 용이하게 만드는 PKI 미들웨어 개발에 집중되고 있다. 그러므로, 국내에서도 PKI 분야의 보다 많은 발전을 위해서는 PKI 응용과 활용에 대한 다양한 접근들이 이루어져야 될 것이다.

참 고 문 헌

〔1〕 최영철, 홍기융, 이홍섭 "전자서명법과 전자서명인증관리체계", 한국정보과학회 과학학회지, 2000. 1.

〔2〕 NIST, The 1994 Mitre PKI Study Final Report, http://csrc.ncsl.nist/pki/mitre.ps

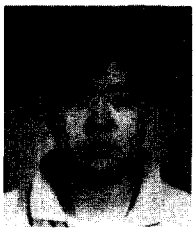
〔3〕 American Bar Association, "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce", August 1, 1996.

〔4〕 "SSL Protocol", http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

〔5〕 "Thawte Digital Certificate Services", http://www.thawte.com

〔6〕 "VeriSign", http://www.verisign.com

저 자 소 개



崔 榮 哲

1996년 : 성균관대학교 정보공학과 학사, 1998년 : 성균관대학교 전기 전자 컴퓨터공학부 석사, 1997년~2000년 : 한국정보보호센터 인증관리팀 연구원, 2000년 : 한국정보인증 시스템개발부, 2000년~현재 : (주)비씨큐어 시스템개발부장, 2001년 : 성균관대학교 전기 전자 컴퓨터공학부 박사수료, 〈주관심 분야 : 공개키기반구조, 전자상거래 보안, 암호이론〉

朴 性 俊

1985년~1994년 : 한국전자통신연구원(현 국가보안기술연구소) 부호기술부 선임연구원, 1996년~2000년 : 한국정보보호센터 기반기술팀장, 1997년~1998년 : 정보통신부 "전자서명법" 제정 실무위원, 1999년~현재 : 외교통상부 전자상거래 자문 그룹위원, 1999년~현재 : 성균관대학교 정보통신대학원 겸임교수, 1999년~현재 : 고려대학교 정보보호기술학과 연구교수, 2000년~현재 : (주)비씨큐어 대표이사, 성균관대학교 공학박사(암호학 전공), 〈주관심 분야 : 확률론적 공개키암호시스템, 공개키기반구조, 디지털저작권관리기술 등〉