

전자 상거래 인증 기술

하영국*, 임신영*, 강상승*, 함호상*, 박상봉*

Public Key Certification Technology for Electronic Commerce

Young-Guk Ha, Shin-Young Lim, Sang-Seung Kang, Ho-Sang Ham,
Sang-Bong Park

Abstract

Nowadays, major application of public key certification technology based on PKI(Public Key Infrastructure) is electronic commerce. Public key certification technology may include various sub-technologies such as key recovery, secret sharing, certificate/key management, and directory system technology. This thesis discusses PKI-based certification authority technology for electronic commerce on the Internet.

Key Word : *Public Key Infrastructure(PKI), Certification Authority(CA),
Key Recovery*

1. 서론

인터넷을 이용한 전자 상거래가 국내외에서 최대 관심사로 부각되고 있으며, 부분적으로 결과물이 도출되고 있는 상황이다. 인터넷이라는 불안정한 개방형 전산망에서 전자 상거래를 안전하게 실현하기 위해서는 개인정보 노출 또는 변조의 위험성을 최소화 하는 것이 중요하다[27], [28], [30].

인증 기술을 공개키 암호화 기반에서 사용할 때 인증 서비스의 확장성을 동시에 만족하며, 개인별 공개키를 인증해 주는 인증기관(Certification Authority)을 통하여 인증기관의 비밀키로 암호화된 인증서의 발급 과정과 인증기관의 공개키 확인 과정을 이용하여 양자간의 거래 시 송신측은 자신의 비밀키와 인증기관에서 획득한 상대방의 공개키로 전송 메시지를 암호화하여 자신의 인증서와 함께 상대방에 전송한다. 한편 수신측은 자신이 가지고 있는 비밀키와 상대방의 인증서 내에 있는 상대방 공개키를 인증기관의 공개키로 인증서를 복호화한 후 상대방의 공개키를 획득하여 암호화된 메시지를 해독한다. 이와 같이 거래 상대방의 신분확인과 거래 내역에 대한 내용 확인이 가능하게 된다.

인증기관과 인증서의 예로서 정부와 주민등록증을 들 수 있다. 우리나라 국민이면 일정한 나이가 되어 주민등록증을 발급받는데 이는 정부만이 발급할 수 있으며 위조와 변조가 용이하지 않기 때문에 주민등록증은 그 소유자의 신분을 확인할 수 있는 중요한 수단이다. 또한 인증서에 대한 실세계(Real World)의 예를 든다면 여권(passport)이 좋은 예가 될 수 있다. 여권은 외국으로 여행할 때 여권을

발행한 국가에서 그 나라 국민임을 보증해주기 위하여 여권에 날인한 외부부의 직인을 외국의 이민심사국 관리가 확인하고 여권 소지자의 신분(사진, 이름 및 생년월일 등)을 최종적으로 확인한 후 입국을 허용한다.

이와 같이 가상공간에서 전자 상거래 시 상대방의 신분을 확인할 방법, 거래 내역에 대한 쌍방의 부인 방지 대책 등이 커다란 문제가 되며 이러한 문제점에 대한 해결책은 현실적으로 암호/인증 기술에서 그 대책을 찾을 수 있으며, 현재 공개키 기반의 인증 기술을 활용하는 것이 권고되고 있다. 특히, 전자 상거래 시 안전한 전자 지불 방식 구현은 공개키 인증 기술이 필수적이다. 본 논문에서는 이러한 필요성에 따라 공개키 기반 하부구조에서 전자 상거래를 성공적으로 실현하기 위한 필수 요건인 공개키 기반 인증 기술 개요, 메카니즘 및 응용 예와 그 동향 등을 분석한다.

본 논문의 구성은 2장에서 인증기술과 공개키 기반 하부 구조에 대한 개요, 3장에서 공개키 기반 인증 메카니즘의 분석, 4장에서는 전자 상거래 인증 정보 흐름, 5장에서는 공개키 기반 인증기술의 동향을 논한다.

2. 인증 기술과 공개키 기반 하부구조

2.1 인증기술

인증 기술이란 전산망 환경에서 자신의 신분을 상대방에게 증명하는 기술 수단이다. 이는 가상 공간에서 상대방에게 자신의 신분을 증명하는 수단을 의미한다.

전산망에서 자신의 신분을 남에게 증명하기 위한 방법으로 전자 문서 형태의 인증서

(Certificate)를 사용하게 되었으며 인증서의 내용은 현실 세계에서 사용하는 신분 증명서 또는 인감 증명서와 동일하거나 그 이상의 내용을 담고 있다. 인증서 등록, 발급 및 조회 시 인증서의 유효성에 대한 관리를 총괄하는 시스템을 인증기관(Certification Authority)이라고 하며 인증기관의 기반은 확장성을 고려하여 공개키 하부 구조에 근간을 두고 있다.

안전한 공개키 사용을 위해 모든 호스트가 통신을 해야되는 공개키를 모두 오프 라인에서 확인한다면 인증 서비스에 많은 통신 비용이 요구되며, 이러한 문제점을 해결하기 위하여 공개키의 진위 여부를 확인하고 공개키에 인증기관의 디지털 서명을 함으로써 그 키를 사용한 사람의 신분을 증명해 주는 기관을 따로 둘 필요가 있는데 이것을 인증기관(Certification Authority, 줄여서 CA)이라고 한다.

근본적으로 인증기술은 공개키 기반 하부 구조를 지원하기 위한 기술이며, 공개키 기반 하부구조란 공개키 암호화 기술을 활용하여 개인의 공개키를 신뢰할 만한 기관에서 관리하는 기술 기반을 의미한다. 인증기술은 암호 기술, 분산 시스템 기술, 전산망 기술, 프로토콜 기술, 데이터베이스 기술과 관련성이 있으며, 인증 정책 수립에 따라 인증 시스템 구축이 가변적으로 조정된다[33].

2.2. 공개키 기반 하부 구조

공개키 기반 하부 구조란 사용자가 관리하는 키가 2가지로 하나는 공개키(어느 누구나 사용할 수 있는 키)와 다른 하나는 비밀키(사용자 개인만이 비밀로 관리하는 키)로 이루어진 하부 구조이다. 인증기관 형태는 사용자의

공개키를 관리하여 외부에서 원하면 알려주는 기능을 수행하는 인증기관 제반 업무를 공개키 기반 하부 구조하에서 수행한다. 물론 공개키 기반이 아닌 비밀키 기반의 인증 기술(Kerberos)도 있으나 확장성 측면과 관리 측면에서 문제가 되어 현재 고려 중인 인증기관은 공개키 기반을 전제로 하고 있다. 공개키 기반 인증 기술은 인증서 내용 중에 사용자의 공개키로 인증서를 작성하며 인증기관 자체의 비밀키로 암호화하여 제 3 자가 인증기관이 발행한 인증서를 임의로 변조하지 못하도록 변조 방지 기술을 적용하고 있다.

공개키 암호화 기술은 공개키를 안전하게 관리하기 위하여 개인별 공개키를 인증기관에서 인증서 형태로 관리하며 이러한 기반구조를 “공개키 기반 하부 구조(Public Key Infrastructure(PKI))”라 할 수 있다. 본 논문에서는 공개키 기반 하부구조를 다음과 같이 여러 관점에서 정의한다[7], [8].

- 사용자의 공개키를 인증해주는 인증기관간의 전산망 체제
- 익명의 사람과 비밀 통신을 가능하게 하는 암호학적 키와 인증서 배달 시스템
- 공개키 인증서를 이용해 공개키들을 자동적으로 관리해주는 기반 구조
- 공개키 인증서를 발행하고 그에 대한 접근을 제공하는 인증서 관리 기반 구조

본 논문에서는 공개키 기반 하부 구조를 분산 DB 기술, 인증 프로토콜 기술, 전산망 보안 기술, 정보 시스템 보안 기술, 전자 상거래 보안 응용 기술 등의 관련 기술 분야의 기술 집약을 통하여 인증서 기반의 공개키 사용

이 용이하도록 인증 기술 명세, 인증 정책, 관련 설비 등을 수립하여 관리하는 인증기관들 간의 유기적인 결합체라고 정의한다[26], [33].

공개키 기반 하부구조는 인증기관 사용자별 공개키, 인증서 및 인증서 취소 리스트를 관리하는 데이터베이스 시스템 기술이 필요하며, 인증 정책을 관리하는 상위기관(Policy Certification Authority(PCA), Policy Approving Authority(PAA))과의 계층구조를 유지하고 인증기관간의 상호 인증 정보를 공유하기 위한 분산 시스템 기술이 또한 필요하다. 인증기관 사용자와 인증기관간, 인증기관간, 인증기관과 상위기관간의 정보 처리를 안전하게 지원하는 인증 프로토콜 기술이 요구되며, 전산망에서 인증기관이 안전하게 인증 서비스를 수행하도록 전산망 기술이 요구된다.

인증기관을 매개로하여 상대방과 통신을 원하는 경우, 상대방의 공개키를 인증기관에 요청, 인증기관의 비밀키로 암호화된 인증서 형태로 발급받는다. 송신측은 암호화된 인증서를 인증기관의 공개키로 풀어 인증서내의 수신측 공개키를 획득한다. 송신측은 자신의 비밀키와 수신측의 공개키로 메시지를 이중 암호화하여 자신의 인증서와 함께 수신측에 보낸다. 수신측은 송신측의 인증서를 해당 인증기관의 공개키로 풀어 인증서내의 송신측 공개키를 획득하고 자신의 비밀키와 함께 이중으로 암호화된 메시지를 풀어 내용을 읽는다.

이 과정에서 인증기관 사용자는 등록된 인증서의 용도 변경, 사용자의 신분 변화 및 돌연한 사용 취소로 인한 인증서 등록 변경/취소를 할 수 있으며, 인증서의 유효성을 확인하기 위하여 인증서를 발급한 인증기관의 '인증서 등록 데이터베이스' 및 '인증서 취소 리스트

(Certificate Revocation List : CRL)'를 조회할 수 있다.

3. 공개키 기반 인증 메카니즘의 분석

3.1. 공개키 기반 인증 메카니즘의 개요

공개키 기반 구조를 이용한 사용자, 메시지 인증 및 디지털 서명과의 기술적인 차이점을 구분 설명하면 사용자 인증은 메시지를 보낸 사람이 바로 그 사람이라는 것을 증명하는 절차이며, 메시지 인증이란 수신된 메시지가 송신된 출처에서 보내졌고 그 내용이 변경되지 않았다는 것을 증명하는 절차이고, 메시지 인증은 순서 일치와 시간의 적합성에 대한 확인을 포함하여 인증할 수 있다[2], [13], [22], [23]. 한편 디지털 서명은 메시지 원문의 무결성(Integrity)과 송신측의 신분 확인(Authentication)을 포함하여 발신 또는 수신측에 의한 부인 봉쇄를 위한 인증 기법 중 하나라고 볼 수 있다.

전산망을 활용한 전자 상거래 서비스 시 정보 보호에 필수적인 인증기관 기술을 개발하는 것은 안전한 망 관리 및 전자 상거래 구현의 기반을 제공한다. 현재 이 기술은 X.509 기반의 공개키 하부구조에 대한 기술로 국제표준화가 진행 중이다. 인증 관련 신기술 동향과 국제 표준화 추진 동향에 대한 기본적인 검토와 사용자 공개키 인증 방식, 인증서 및 인증서 취소 리스트(Certificate Revocation List : CRL)를 배포할 공개키 디렉토리 서비스 구현을 위한 각각의 기술 사양과 기능/서비스에 대한 정의에 따라 국제적으로 인증 서비스가 연동될 때를 고려하여 국내에서 실질적

인 인증 메카니즘을 개발할 필요가 있다.

3.2. 공개키 기반 인증 메카니즘 관련 기술

공개키 기반의 인증 메카니즘을 구현하는 기술로서 다음과 같은 기술 분야가 있다.

- (1) 공개키 관리 기술 : 사용자 공개키 및 인증기관 개인키 관리 기술, 인증서 관리 기술, 인증서 취소 리스트(CRL) 관리 기술이 있다.
- (2) 사용자 등록 서비스 기술 : 인증서 및 CRL 생성 기술, 사용자 인증기관 등록 기술, 인증서 생성(키 생성) 및 분배 기술, 인증서 갱신 및 취소 기술이 있다.
- (3) 인증서 활용 기술 : 사용자 인증 프로토콜 기술, 인증서 및 CRL 조회 기술, 인증서 및 CRL 분배 서비스 기술이 있다.
- (4) 인증 기반 기술 : 디렉토리 서비스 기술 (X.509), 디렉토리 접근 프로토콜 기술, 디렉토리 관리 기술, 인증 경로 기술, 상호 인증 메카니즘 기술이 있다.

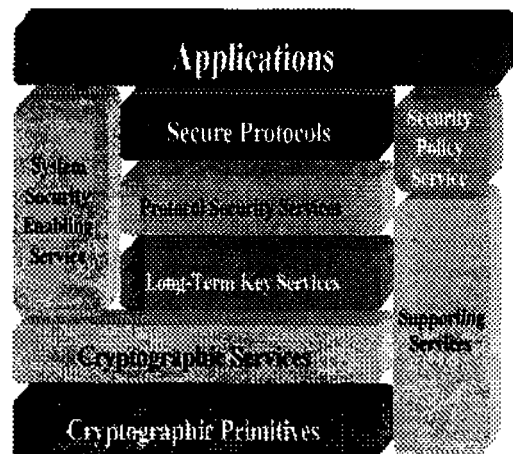
다음은 공개키 기반 인증 메카니즘을 기술하는 IETF(Internet Engineering Task Force)의 보안 분야(Security Area)내 PKIX(Public Key Infrastructure) Working Group에서 도출한 인터넷 RFC(Request For Comments) 초안 문서는 인터넷 기반의 인증기관 구현과 운영에 중요한 기준이 된다. 인터넷 기술 전문 집단인 IETF의 Security Area 내의 PKIX Working Group에서 현재 진행 중인 공개키 기반 인증 메카니즘의 세부 기술 사항에 대한 인터넷 초안 문서들은 늦어도 6개월마다 새로

운 인터넷 초안으로 개정되면서 업체 표준안으로 의견을 수렴 중에 있으며, 현재 본 기술에 대한 업체표준 사양이 완성단계에 있다 [29].

3.2.1. Architecture for Public-Key

Infrastructure(draft-ietf-pkix-apki-00.txt)

1996년 11월 작성된 문서로 B. Blakley (IBM)가 대표로 작성하였으며 이후 본 문서에 대한 개정이 없어서 현재 IETF 해당 working group 인터넷 초안 문서 목록에 삭제되어 있다. 주된 내용은 공개키 기반 하부구조 구성요소의 요구사항과 구조를 설명하고 어떠한 부분이 표준화되어야 하며, 표준 노력을 위한 기본 문서로 인터페이스 및 프로토콜 명세들에 대한 내용을 확인하는 문서이다. 다음 <그림 1>은 공개키 기반 하부구조에 대한 사항이다[1].



<그림 1> 공개키 기반 하부 구조

3.2.2. Internet Public Key Infrastructure

Part 1 : X.509 Certificate and CRL Profile (draft-ietf-ipki-part1-04.txt)

1997년 6월에 작성된 문서로 R.Housley (SPYRUS), W. Ford(VeriSign), W. Polk (NIST), D. Solo(BBN)이 작성하였다. 인터넷 공개키 기반 하부구조의 면세 설명을 위한 4개 문서 중 하나로 인터넷 PKIX에서 사용할 인증서 및 CRL 양식을 정의하였으며, 인증경

로 처리에 대하여 정의하였다.

암호화 규약은 일반적인 암호화 알고리즘을 적용할 경우에 대하여 설명하였으며, ASN.1으로 포괄적인 정리를 하였다. 여기에는 공개키 재료, 전자 서명의 확인과 암호화 절차를 명시하였다. 다음의 <표 1> 및 <표 2>는 인증서 양식과 인증서 취소 양식에 대한 요약된 내용이다[3], [4], [5], [9].

<표 1> X.509 인증서 양식

필드 이름	의 미
version(v3)	인증서 버전으로 최신 버전은 3임
serial number	인증서 발행시 부여하는 고유번호로 인증서를 식별하는 정보 중 하나임
signature algorithm id	인증서에 서명한 디지털 서명 알고리즘을 명시한 정보
issuer name	인증서를 발행한 주체를 밝히는 정보로 인증기관 이름을 사용함
validity(not before, not after)	인증서 유효 기간(시작-종료)
subject name	인증서 사용자 정보
subject public key info (algorithm id, subject public key)	인증서 사용자의 공개키에 관한 정보로 공개키에 서명한 알고리즘 식별자 및 공개키 내용을 정의함
issuer unique identifier	발행자의 고유 식별자
subject unique identifier	사용자의 고유 식별자
extensions (extn id, critical, extn value)	인증 정보의 확장 부분으로 확장 식별자, 필수 정보 부분, 옵션 정보 부분으로 구분
signature algorithm id	확장 정보에 서명한 디지털 서명 알고리즘 식별자
signature : by issuer CA	인증기관에 의하여 서명한 서명 내용(서명 자체)

<표 2> X.509 인증서 취소 리스트(CRL) 양식

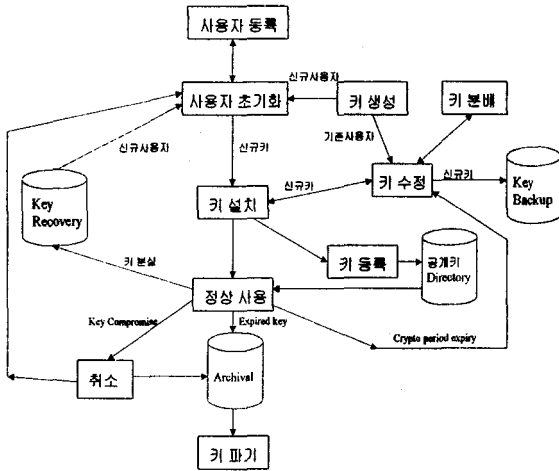
필드 이름	의 미
version(v2)	인증서 취소 리스트의 버전으로 최신 버전 번호는 2임
signature algorithm id	CRL에 서명한 디지털 서명 알고리즘 식별자
issuer name	발행자 이름(인증기관)
this update	발행시의 현재 시각
next update	다음번 발행시의 예상 시각
revoked certificates (certificate serial number, revocation date, CRL entry extensions)	취소된 인증서 정보 (인증서 일련번호, 취소 일자, CRL 입력 확장(취소 사유 등))
CRL extensions	CRL 확장자 유무 및 내용
signature algorithm id	확장 정보에 서명한 디지털 서명 알고리즘 식별자
signature : by issuer CA	인증기관에 의하여 서명한 서명 내용(서명 자체)

3.2.3. Internet Public Key Infrastructure Part II : Operational Protocols (draft-ietf-ipki2opp-00.txt)

1997년 3월 작성된 문서로 S. Boeyen (Entrust Technologies), R.Housley(SPYRUS), T. Howes(Netscape), M. Myers(VeriSign), P. Richard(Xcert)이 작성하였다. 여기서는 X.509v3 인증서와 X.509v2 CRL의 조화를 위한 경량화된 디렉토리 접근 프로토콜(Lightweight Directory Access Protocol : LDAP)와 X.509v3 인증서를 온라인으로 상태 확인을 하는 프로토콜(Online Certificate Status Protocol : OCSP) 등에 대하여 정의하였다[6], [10].

3.2.4. Internet Public Key Infrastructure Part III : Certificate Management Protocols (draft-ietf-ipki2cmp-02.txt)

1997년 6월에 작성된 문서로 S. Farrell (SSE), C. Adams(Nortel)이 작성하였다. 인증기관의 하부구조인 공개키 기반의 내용을 관리하는 정보를 주고받는 대상인 일반 사용자와 인증기관 그리고 인증기관과 인증기관간의 프로토콜을 정의하였다. 그리고 공개키 관리에 대한 키 복구(Key Recovery) 및 비밀 공유(Secret Sharing)의 구조와 키 관리 생명 주기(Key Mangement Life Cycle)에 대한 관리 프로토콜이 정의되어 있다. 다음 <그림 2>는 Part III에 근거한 키 관리 생명 주기를 도식적으로 요약하고 있다[11].



<그림 2> 키 관리 생명 주기

3.2.5. Internet Public Key Infrastructure
Part IV : Certificate Policy and
Certification Practices Framework
(draft-ietf-ipki-part4 -00.txt)

1997년 3월 25일 작성된 문서로 S. Chokhani(Cygnacom Solutions, Inc), W. Ford(VeriSign)이 작성하였다. 이 문서는 인증 정책 또는 인증 수행에 대한 정의를 작성 시 framework을 제공한다. 그리고 특히, 포괄적으로 인증 정책 정의와 인증 수행 내용에 대한 사항을 정리하였으며 향후 이 문서는 Informational RFC로 추진할 예정이다[12].

4. 전자 상거래 인증 정보 흐름

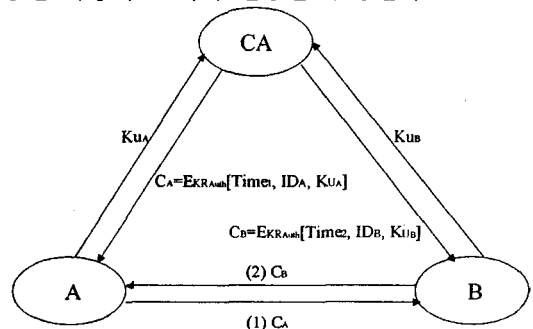
전자 상거래를 구성하는 기본 요소로 은행, 소비자 및 판매자를 들 수 있으며, 전자 상거래의 행위로 거래 문의, 거래 조건(가격) 협상, 거래 완료 및 지불이다. 행위 과정에서 현실 세계와는 달리 가상 공간에서의 상대방 신분

확인, 거래 성사 결과의 부인 방지, 지불의 안전한 처리에 대한 기술적인 해결 방법으로 인증 기술을 사용한다.

공개키 기반 하부 구조가 제공하는 서비스는 전자서명 서비스, UBS(Unclassified But Sensitive)수준의 암호화 키 관리 서비스 및 비밀 데이터의 복구 서비스로 구분된다. 이들 각각은 다음과 같은 세부 서비스를 제공한다.

- 전자 서명 서비스
 - * 인증(Authentication)
 - * 무결성(Integrity)
 - * 부인봉쇄(Non-Repudiation)
- UBS(Unclassified But Sensitive) 수준의 암호화 키 관리 서비스
 - * 암호통신용 세션키(Session Key for Secure Communication)
 - * 전자메일용 세션키(Session Key for E-Mail)
- 비밀데이터의 복구 서비스(Optional)
 - * 비밀키 복구 기능

다음 <그림 3>과 같이 공개키 기반(X.509)의 인증기관은 서비스 사용자에게 인증서를 통한 사용자 공개키 인증을 수행한다.



<그림 3> 공개키 기반 인증기관 인증 정보흐름

여기서 A와 B는 CA의 사용자이고 A와 B는 사전에 CA에게 자신의 공개키를 등록(K_{UA} , K_{UB})하여 CA로부터 각각 C_A , C_B 를 수신받아 자신의 시스템에 보관하다가 서로 통신을 하고자 할 때 각자의 인증서를 암호화 처리된 메시지와 함께 보낸다.

암호화 처리된 메시지는 서로의 공개키를 CA로부터 받아 암호화 처리과정에서 사용한다. CA가 A와 B에게 인증서를 보낼때 타임스탬프와 난수를 포함하여 송신하는데 이는 추후 A와 B가 서로 인증서내의 공개키를 확인하는 과정에서 인증서의 유효성 여부를 판단하는 기준이 되도록 하였다. A가 B에게 보낸 C_A 는 B가 이미 가지고 있는 CA의 공개키로 복호화하여 A의 공개키를 다음과 같이 확인한다[13], [33].

$$\begin{aligned} B : D_{K_{UA}}[C_A] \\ &= D_{K_{UA}}[E_{K_{CA}}[Time_1, ID_A, K_{UA}]] \\ &= [Time_1, ID_A, K_{UA}] \end{aligned}$$

전산망을 통한 전자 상거래 시 발생할 수 있는 제반 문제에 대하여 아래와 같은 시나리오 내에 인증 기술을 도입하여 해결하고자 한다. 물론 인증 기술만이 이 모든 문제를 해결할 수 없으며 인증 기술 외에 다른 몇 가지 기술이 복합적으로 사용함으로써 기술적으로 완벽한 정보화 역기능에 대한 대응 능력을 제공하게 될 것으로 보인다. 다음은 전자 상거래 과정에서 일반적인 구매 절차로서 인증서 사용 시나리오에 대하여 설명한다[31], [32].

(가) 소비자는 자신의 컴퓨터 단말기와 연결된 전산망을 통하여 인터넷 백화점(WWW 형태의 쇼핑 정보 서비스 제공)으로 들어가

서 자신이 원하는 상품 정보를 검색하고 상품 구매에 대한 일을 수행하려 한다.

- (나) 소비자는 이를 위하여 자신의 단말기와 연결된 전산망을 통하여 자신이 속한 전산망 영역(!Domain)내에서 인증 서비스를 제공하는 인증기관을 통해 인증서를 등록하여 발급 받고 자신의 시스템에 보관한다.
- (다) 소비자는 인터넷 백화점에 접속하기 위하여 인터넷 백화점의 인증서를 인증기관을 통하여 입수하여 인증기관의 공개키로 인증서 내의 인터넷 백화점의 공개키와 자신의 비밀키로 메시지(접속 요청 메시지)를 이중 암호화 한 후 자신의 인증서와 같이 웹 브라우저를 통하여 접속 요청을 한다.
- (라) 인터넷 백화점은 소비자의 인증서 진위 여부를 확인한 후, 소비자의 공개키와 자신의 비밀키로 이중 암호화된 메시지를 읽은 후 소비자의 접속 여부를 결정한다.
- (마) 소비자의 신분을 증명하는 인증서가 진본이면 인터넷 백화점에 접속이 가능하게 되고 소비자는 자신이 원하는 상품 정보를 검색하고 구매 조건을 흥정한다.
- (바) 소비자의 구매가 결정되면 소비자의 신용카드 또는 은행 계좌 이체를 통한 지불 절차를 수행한다.
- (사) 지불 과정에서도 인증서를 사용하게 되는데 인터넷 백화점은 소비자의 인증서가 첨부된 '지불 요청서'를 받아서 은행/카드 회사에 이를 신청하는 과정에 인터넷 백화점의 인증서를 추가로 첨부한다.
- (아) 은행/카드 회사는 지불 요청자(소비자)와 인터넷 백화점의 신분을 인증서를 통하여 확인하고 진본 인증서인 경우, 정상적인 처리를 한 후 이를 인터넷 백화점에 통보

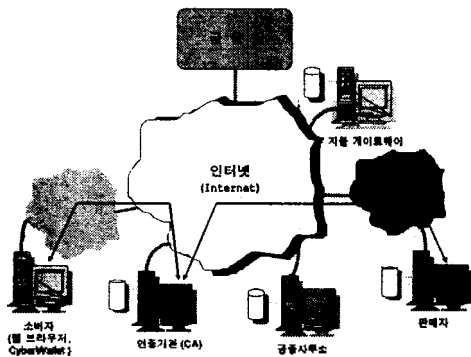
하여 준다. 만약 위조 인증서일 경우, 위조 내역과 지불 취소 메시지를 소비자 및 인터넷 백화점에 보낸다.

(자) 인터넷 백화점은 은행/카드 회사로부터 지불 처리 결과에 대한 통보를 받고 기업에게 판매 대금의 일부를 수수료로 제한 판매 대금을 전달하며, 동시에 택배회사로 하여금 소비자에게 상품 전달할 것을 요청한다.

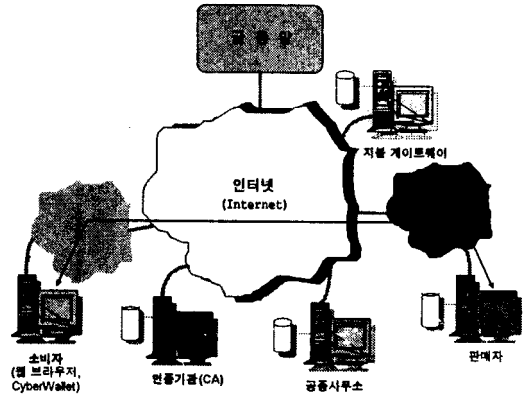
(차) 소비자는 택배 서비스를 통하여 상품을 배달받고 배달 확인(상품 인수증)을 한다.

이상과 같이 가상적인 시나리오를 설정하여 인증서가 전자 상거래에서 사용되는 정보의 흐름이 순차적으로 어떻게 사용되는 지를 예로 설명하였다.

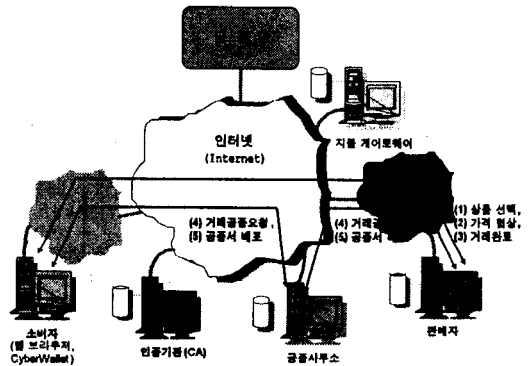
아래 <그림 4>에서 <그림 8>은 가상 시나리오에 설정된 전자 상거래 과정 중 인증 기술 적용을 중점적으로 표현한 것으로 전자 상거래 전반에 인증 기술이 적용됨을 알 수 있다.



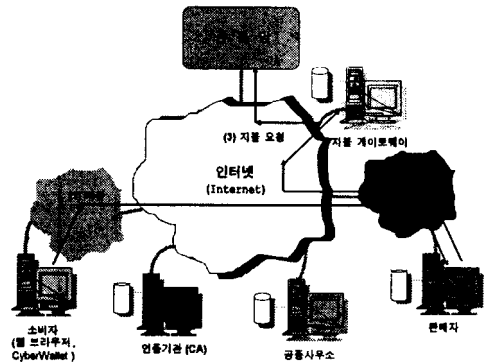
<그림 4> 개인별 공개키 등록 및 인증서 발급/보관



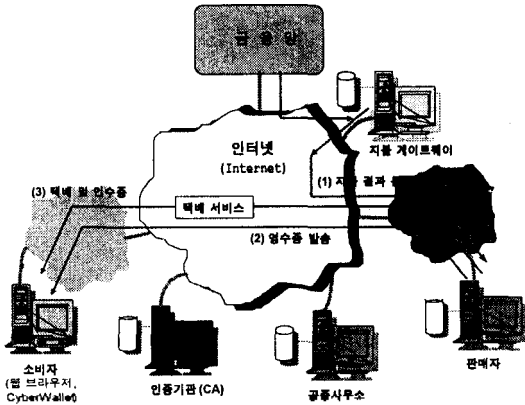
<그림 5> 소비자-판매자간 공개키인증 정보교환



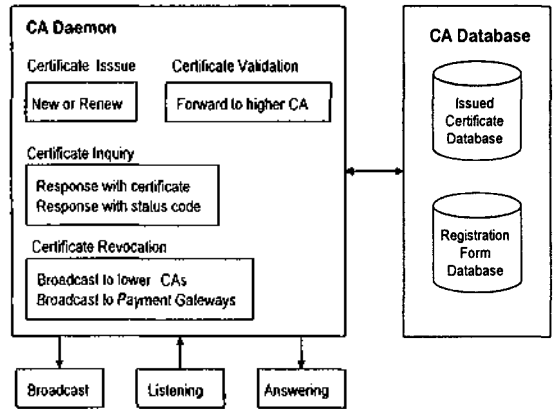
<그림 6> 구매작업, 거래 완료 및 거래내역 공증



<그림 7> 소비자 지불 및 지불 처리 요청



<그림 8> 지불 처리 완료 및 택배 서비스



<그림 9> SET에서의 인증 구조

5. 공개키 기반 인증 기술의 동향

본 장에서는 공개키 기반 인증 기술에 대하여 인증 기술을 활용한 사례를 검토하여 요소 기술과 서비스에 대하여 검토하였다.

5.1. SET 기반 인증 구조

SET은 모두 5개 부분으로 구성되어 있으며, 이들은 구매자(Cardholder), 판매자(Merchant), 인증기관(Certificate Authority), 지불 게이트웨이 (Payment Gateway) 및 다른 하나로 구성되어 있다. 이 중 SET에서의 인증 기관 구조는 위 <그림 9>와 같다[25].

인증서 발행 모듈은 새로운 인증서를 발행하는 부분과 기존 인증서에서 갱신을 처리하는 부분으로 구성되어 있다. 새로운 인증서를 발행하는 경우, 구매자(Cardholder)에게 이를 발급하는 루틴은 6개 단계로 구성되어 있으며, 판매자, 지불 게이트웨이, 인증기관에게 발급

하는 루틴은 4개 단계로 구성되어 있다. 등록양식 데이터베이스를 이용하여 인증서를 등록하고 발행된 인증서 데이터베이스에 등록한다. 그리고 갱신요청에 의하여 발행되는 인증서의 경우, 정상적인 인증서 유효기간 만료 또는 유효기간 동안에 취소한 인증서의 갱신을 처리하여 주며 발행된 인증서 데이터베이스를 update함으로써 갱신이 완료된다.

인증서 확인 모듈은 상위의 인증기관에 확인 요청하는 경우, 연속 확인(chain validation)으로 처리한다. 이때 요청하는 실체는 구매자, 판매자 및 지불 게이트웨이이다. 요청하는 내용으로는 상위 인증기관의 인증서에 대하여 확인하는 것이며, 인증 확인의 결과를 응답하는 것을 또한 처리하여 준다.

인증서 조회 모듈은 두가지 경우가 있는데 하나는 인증서로 응답하는 경우(이는 상대방과 통신하고자 상대방의 인증서(즉, 공개키)가 필요한 경우의 조회)와 다른 하나는 인증서 상태 코드로 응답하는 경우(이는 수신된 인증서

의 진위 여부를 묻는 경우의 조회)이다.

인증서로 응답하는 경우, 조회 시 인증서 발급이 완결되는 경우로 조회 요청자에게 인증서를 보내주며 발행된 인증서 데이터베이스에 등록한다. 인증서 상태 코드로 응답하는 경우, 조회 시 인증서 발급이 완결되지 않은 경우로 현재의 처리 상태를 인증서 상태 코드로 조회 요청자에게 전송한다.

인증서 취소 모듈은 취소 처리된 결과인 CRL(Certificate Revocation List)를 하위 인증기관에 알리는 경우와 지불 게이트웨이 및 구매자에 알리는 경우로 구분된다. 전자의 경우, 인증서 발행자 및 획득자를 제외한 인증기관에서 처리하며 자신의 하위 인증기관에게 CRL을 전송한다. 후자의 경우, 인증서 발행자 및 획득자가 구매자 및 지불 게이트웨이를 대상으로 CRL을 전송한다. 이 경우, 알리는 대상은 발행된 인증서 데이터베이스에 등록된 end entity이다.

5.2. VeriSign의 인증 구조

RSA Data Security의 관련 회사 VeriSign은 인증 서비스를 제공하는 회사로 탄생하였으며, 미국 대규모 전화회사인 GTE도 Cyber Trust라는 인증 서비스를 제공하고 있다.

1996년 12월, VeriSign에서 발표한 Digital ID라는 서비스는 웹을 통한 전자 상거래 시 거래 참여 양측을 인증서로 신분을 확인할 수 있는 3개 class를 가진 Digital ID를 판매하기 시작하였다.(참조 웹 사이트 : www.verisign.com) 인증을 전문으로 수행하는 제 3 자 기관(CA)가 부가된 인증 서비스를 통하여 상점의 진위 여부가 인증되며, 사용자의 진위 여부가

인증될 경우, 양측 모두 자신의 공개키에 대하여 등록하고 그것을 증명받는 서비스에 대한 요금을 지불한다[17].

VeriSign 및 GTE도 스스로 인증을 하는 CA와 기업 및 조직에서 내부 용도로 CA를 운영할 수 있는 구조의 구축을 지원하는 서비스 모두를 사업화 하고 있다.

특히, VeriSign이 수행하는 CA 서비스에서 발행되는 대상과 인증 수준에 따라 3가지의 인증 class가 있고 각각 개인용, 기업 및 단체용으로 나누어 진다.

제공하는 Digital ID는 Class1의 경우, 전자우편 및 일상적인 웹 검색에 사용하는 저급 신분확인 서비스를 제공하며 매년 6달러(미화)를 지불하면 전자 문서 형태로 인증서를 발급하여 준다.

Class2의 경우, 웹 검색과 고급 사용에 있어 상대방에게 신뢰와 보안을 제공할 수 있는 수준의 인증서를 발급하는 서비스로 매년 12달러(미화)를 지불하면 해당 인증서를 배포하여 준다. 그리고 Class3의 Digital ID는 회사내부에서 거래 시 고급 수준의 확인에 사용되는 인증 서비스를 제공하며 매년 24달러(미화)를 지불하면 서비스를 받을 수 있다.

Class1, 2의 경우는 웹의 온라인으로 배포 요청과 발급이 가능하지만 Class3의 경우, 웹의 온라인으로 신청하고 본인이 직접 자신의 인증서를 받으러 인증기관이 설치된 곳으로 출석하여야 한다. 이 3가지 등급의 인증서는 사용자 수준의 인증서이고 서버 수준의 인증서는 Class3에서 발급하며 첫해는 290달러(미화) 그리고 매년 75달러(미화)를 지불하면 서비스를 제공 받을 수 있다. 주된 기술 요소는 RSA 공개키 알고리즘을 기반으로한 공개키

<표 3> VeriSign에서의 인증 class

	개인용	기업 및 단체용
Class 1	사용자의 이름, 전자우편주소가 자신의 것임을 인증해 줌. VeriSign 자체의 CA 서비스에서는 이 class에 등록된 이용자의 운전면허와 같은 사항은 인증 범위에서 제외됨. 이 서비스는 VeriSign의 웹 사이트(www.verisign.com)에서 전세계 모든 사용자에게 제공됨.	없음
Class 2	공적인 정확도를 갖는 개인정보와 정합을 전제로 이용자의 이름, 주소 정보와 우편주소를 인증함. 전자 상거래 소비자 입장에서는 보통 수준의 인증임. 현재 미국 및 캐나다 거주자에 한하여 서비스가 제공됨.	없음
Class 3	인증 레벨을 높여 은행구좌 개설, 계약서 작성, 소속기업의 증명 등이 제공됨. 현재 구체적인 서비스 사양과 수혜 범위가 정해져 있지는 않음.	거래 상대로 신용할 수 있는 기업, 단체이고 그러한 조직에 의해 운영되고 있는 서비스임을 인증함. 기업 신용정보 기관 데이터베이스 등에 조회하여 기업 정보가 확인된 후 전자증명서가 발행됨.

관리(X.509), 인증서 암호처리 보관 기술, 인증서 생성 및 관리, 인증서 확인 및 취소 기술로 구성되어 있다.

<표 3>은 VeriSign이 발행하는 인증 class에 대한 세부 사항을 정리한 표이다.

개인 인증 class는 RSA 공개키 암호화가 기초인 SSL(Secure Socket Layer)가 탑재된 웹 브라우저에 맞추어 전자 증명서(인증서)가 발행된다. 일련의 신청 과정 중에서 브라우저가 비밀키, 공개키를 생성하여 공개키는 VeriSign에 등록되며 전자 증명서가 브라우저에 내장된다.

Class 2의 서비스 제공 범위를 미국과 캐나다로 국한한 것은 금융기관 이외라도 이용할 수 있는 개인 신용 정보기관이 존재하며

이러한 기관을 사용하여 미국 및 캐나다 거주자의 개인정보를 확인할 수 있기 때문이다.

VeriSign이 제공하고 있는 인증은 일종의 원형(primitive)으로, VISA, MasterCard, AmericanExpress와 JCB도 채용하고 있는 SET의 상거래 환경이 구체화되면 CA 역할은 각각의 카드 회사가 될 것이며 그 경우, 가맹점에 대하여는 class3을 발행하고, 카드 소유자에 대하여는 class2를 발행하게 될 것이다.

5.3. Xcert 인증 구조

미국의 Xcert Software Inc.라는 회사는 인터넷 상에서 인증기관간의 관련성이 없는 인증기관에 대한 교차 인증 기술을 최초로 실현

한 회사로 이러한 시연을 웹 상에서 확인 가능하다.(참조 웹 사이트 : www.xcert.com) 이러한 시연의 목적은 인증기관간의 통신이 보다 높은 보안성을 제공함을 보여주고 또한 인터넷 상에서 인트라넷 형태의 통신을 할 수 있는 가능성을 보여주기 위함이다.

즉, 기업간의 공중망(인터넷)을 활용한 가상 사설망(virtual private networks(VPNs)) 개념의 통신을 하기 위하여 VPN 상의 송수신자간의 신분 확인을 위한 기술적인 기반을 제공하기 위하여 Xcert라는 서비스를 제공한다. 이를 통하여 각 기관이 구축하여 운영하는 인증기관간의 교차 인증 기술을 사용하며, 이 과정에서 교차 인증이 완료되면 VPN을 통한 전용 통신을 안전하게 할 수 있다[18].

다음의 내용은 Xcert에서 제공하는 시연의 요약된 내용이다. 이 시연에서 다음을 확인할 수 있다.

1. 인증기관에게 인증서 요청을 하여 인증서를 받을 수 있다.
2. 사용자 인증(Client Authentication) 시연으로 동일한 인증서를 인증기관에서 관리하는 웹 사이트를 방문 시 사용할 수 있으며 동시에 교차 인증(Cross Authentication)의 시연으로 다른 인증기관에서 관리하는 웹 사이트를 방문 시에도 역사 같은 인증서를 사용하여 방문이 가능함을 확인할 수 있다. 시연 과정동안 인증기관은 다른 인증기관과 정보를 교환하며 사용자의 인증 정보를 상호 교환하게 된다.(인증서의 확인을 위한 과정에서 사용함)
3. 최종적으로 원래 시작하였던 사이트로 돌아와 신청하였던 인증서를 취소하면 그 즉시

이전에 접속 가능하였던 보안 웹 서버에 접근이 안되는 것을 확인할 수 있을 것이다. 만약 교차 인증을 시도한다면 취소한 인증서가 거부될 것이다.(문의처 : info@xcert.com)

이외에 인증 기술 응용 사례로 공중 서비스를 주 정부 차원에서 실시하는 미국 오레곤 주 정부의 경우, 오레곤 주 정부의 주도하에 공중 서비스 즉, Oregon Notary를 추진하여 현업에서 전자 상거래 시 전자 증빙 서류로 갈음이 가능하도록 제도권내의 준비를 하였으며 실 사회에서 전자 공중 서비스를 구체적으로 사용하고 있다. 이 기술의 지원은 미국 Intermarket 회사에서 CyberNotary 서비스를 통하여 인증 서비스로 인증서를 전산망 환경에서 전자 상거래 응용 서비스에서 사용 가능하도록 지원하고 있다 [20].

그외에 AmeriTech회사에서 CivicLink라는 서비스를 통하여 미국 정부의 인증 서비스를 대행하는 기능을 수행하고 있으며, 스웨덴에서는 COST라는 프로젝트를 통하여 인증 기술을 정착시키려고 노력 중이다. 그리고 유럽 연합국의 경우, EuroSign이라는 서비스를 제공하여 유럽 지역의 인증 서비스 및 기술을 제공하고 있으며, Sun에서는 Certificate Authorities라는 서비스를 특정 시스템에서 시험적으로 수행하고 있으며, 자사 내부에서 일부 시험적으로 사용 중에 있다[14], [15], [16], [19].

6. 결론

본 논문에서는 전자 상거래를 위해 암호 기술의 확장성 측면에서 우수한 공개키 기반 하부 구조에서의 공개키 인증 기술을 중심으로 분석하였다. 공개키 기반 인증 기술은 전자 상거래 서비스에서 필요한 신분 인증, 거래 내역 인증 및 지불 처리 인증에 사용하는 기반 기술이다. 이는 공개키를 보증하는 기반 기술과 인증서의 안전한 사용 기술 등이 필요하며, 전자 상거래를 실현하기 위한 필수적인 선결 사항이다. 인터넷이라는 불안정한 개방형 전산망 구조에서 안전한 전자 상거래를 제공하려면 향후 국제적인 인증 서비스와의 연동을 위한 표준화된 인증 기술의 적용이 중요하다. 본 논문의 2장에서는 공개키 기반 하부 구조에 대한 소개와 3장의 공개키 기반 인증 메커니즘의 분석 그리고 4장의 전자 상거래 인증 정보 흐름에 대하여 가상 시나리오를 중심으로

분석하였으며, 5장에서는 해외의 공개키 기반 인증 기술의 응용 사례에 대한 소개를 하였다. 국내에 공개키 기반 하부 구조가 구축하려면 국내 인증 체계의 정립이 우선되어야 하며 이를 위하여 관련 정책의 수립이 요구된다. 특히, 인터넷 기반의 전자 상거래 활성화는 이러한 공개키 기반 하부 구조의 구축이 필수적이며 국제적으로 구축되고 있는 전자 상거래 서비스를 통하여 국내 우수 상품이 효과적으로 판매되기 위하여 관련 연구 개발이 시급히 요청되는 바이며, 이러한 기술 사양에 대하여 IETF의 보안 분야 PKIX(Public Key Infrastructure) WG에서 업체 표준 사양을 추진 중이므로 이 부분에 대한 적절한 대응과 기술 분석 및 개발이 이루어진다면 선진 외국의 PKIX 관련 기술 수준을 용이하게 도달할 수 있는 방안이 될 것이라고 판단된다.

참고 문헌

- [1] Architecture for Public-Key Infrastructure(draft-ietf-pkix-apki-00.txt), 1996. 11.
- [2] Cryptography in Public Internetworks with Sun Screen, 1995.
- [3] Federal Public Key Infrastructure Technical Specification Part A : Requirements, NIST, 1996.1.31, <http://csrc.ncsl.nist.gov/pki/require5.ps>
- [4] Federal Public Key Infrastructure Technical Specification Part B : Technical Security Policy, NIST, 1996.1.24, <http://csrc.ncsl.nist.gov/pki/tspolicy.ps>
- [5] Federal Public Key Infrastructure Technical Specification Part C : Concept of Operations, NIST, 1996.2.12, <http://csrc.ncsl.nist.gov/pki/conops.ps>
- [6] Federal Public Key Infrastructure Technical Specification Part D : Interoperability Profile, NIST, 1995.9.27, <http://csrc.ncsl.nist.gov/pki/cross.ps>
- [7] GOC Public Key Infrastructure, <http://www.cse.dnd.ca/cse/english/gov.htm>
- [8] ICE-TEL, Architecture and General Specifications of the Public Key Infrastructure, 1996.9, <http://www.darmstadt.ut.de/ice-tel/deliverables/download/D1-Architecture.rtf>
- [9] Internet Public Key Infrastructure Part I : X.509 Certificate and CRL Profile (draft-ietf-ipki-partI-03.txt), 1997. 6.
- [10] Internet Public Key Infrastructure Part II : Operational Protocols (draft-ietf-ipki2opp-00.txt), 1997. 3.
- [11] Internet Public Key Infrastructure Part III : Certificate Management Protocols (draft-ietf-ipki2cmp-01.txt), 1996. 12.
- [12] Internet Public Key Infrastructure Part IV : Certificate Policy and Certification Practices Framework (draft-ietf-ipki-part4-00.txt), 1997. 3. 25.
- [13] Robin Whittle, Public Key Authentication Framework: Tutorial, 1996.6, <http://www.ozemail.com.au/~firstpr/crypto/pkaftute.htm>
- [14] Standards Australia, Strategies for the implementation of a Public Key Authentication Framework(PKAF) in Australia, SAA MP75-1996
- [15] The 1994 Mitre PKI Study Final Report, NIST, <http://csrc.ncsl.nist.gov/pki/mitre.ps>
- [16] Utah Digital Signature Act, 1996, <http://www.gvinfo.state.ut.us/ccjj/digsig/dsut-act.htm>
- [17] Verisign Web Home Page : www.verisign.com
- [18] Xcert Software Inc., www.xcert.com
- [19] 미국 전자서명법 관련 종합사이트, <http://www.abanet.org/scitech/isc/matrix10.html>
- [20] 미국 오레건주 정부 웹 홈페이지, www.sos.state.or.us/corporation/notary/nguide/toc.html
- [21] 박성준, 제 2회 정보보호 심포지움 발표 자료집, 1997.

-
- [22] 심영철, 제 1회 한국 전산망 보안기술(NETSEC-KR'95) 워크숍 발표자료집, 1995. 5.
 - [23] 임신영 외, 전자거래의 익명성과 확장성을 보장하는 보안 서비스 시스템 설계, 1996년 한국정보처리학회 춘계 학술발표논문집 제 3권 제 1호, 1996. 4.
 - [24] 임신영 외, 전자거래 사용자 보안 서비스 요구 사항 분석 및 설계, 1997년 한국정보처리학회 춘계 학술발표논문집 제 4권 제 1호, 1997. 4.
 - [25] 임신영 외, 인터넷 전자 상거래 구매자/거래처 인증을 위한 최적 지불 프로토콜 설계, 1997년 한국정보처리학회 춘계 학술발표논문집 제 4권 제 1호, 1997. 4.
 - [26] 임신영 외, 전자 상거래 보안 시스템 설계 및 암호화 기술의 적용, 1996년 제 8회 WISC 워크샵 논문집, 1996. 9.
 - [27] 임신영, 국내외 인터넷 보안 기술 연구 동향, KRNET'97 발표집, 1997. 7.
 - [28] 임신영, 차세대 인터넷 보안 기술, '97 International Conference on Industrial Survival Strategy for Next Generation Software Technology, 한국정보처리학회, 1997. 6.
 - [29] 임신영, 제 2회 한국 전산망 보안기술(NETSEC-KR'96) 워크숍 발표자료집, 1996. 5.
 - [30] 임신영, 제 3회 한국 전산망 보안기술(NETSEC-KR'97) 워크숍 발표자료집, 1997. 5.
 - [31] 임신영, 권도균, 전자 상거래 보안, pp. 45-52, 한국정보과학회지 제 15권 제 4호, 1997. 4.
 - [32] 임신영 외, 인터넷 기반 전자거래 전용망 보안 정책 수립 연구, 1997년 제 9회 WISC 워크샵 논문집, 1997. 9.
 - [33] 최용락 외, 통신망정보보호, 1996.2.

저자소개

하영국 (e-mail : ygha@econos.etri.re.kr)

- 1993 건국대학교 전산학과 학사
- 1995 건국대학교 대학원 전산학과 석사
- 1995~1998 한국전자통신연구원 부설 시스템공학연구소 연구원
- 1998~현재 한국전자통신연구원 전자상거래연구부 연구원

임신영 (e-mail : sylim@econos.etri.re.kr)

- 1983 건국대학교 공업화학과 학사
- 1985 건국대학교 화학공학과 석사
- 1992 건국대학교 전자계산학과 석사
- 1997 고려대학교 컴퓨터과학과 박사수료
- 1987~1998 한국전자통신연구원 부설 시스템공학연구소 선임연구원
- 1998~현재 한국전자통신연구원 전자상거래연구부 선임연구원

강상승 (e-mail : sskang@econos.etri.re.kr)

- 1997 경북대 전자공학과 학사
- 1999 경북대 전자공학과 석사
- 1999~현재 한국전자통신연구원 전자상거래연구부 연구원

함호상 (e-mail : hsham@etri.re.kr)

- 1977 고려대학교 산업공학과 학사
- 1983 고려대학교 산업공학과 석사
- 1995 고려대학교 산업공학과 박사
- 1979~1981 새한자동차(주)
- 1982~1998 한국전자통신연구원 부설 시스템공학연구소 전자거래연구팀 팀장
- 1998~현재 한국전자통신연구원 전자상거래연구부 전자거래연구팀 팀장

박상봉 (e-mail : hspark@etri.re.kr)

- 1974년 고려대 산업공학과 학사
- 1976년 고려대 경영학 석사
- 1975~1981 한국과학기술연구소 전자계산부
- 1982~1993 한국과학기술원 시스템공학센터
- 1993~1996 한국과학기술원 시스템공학연구소
- 1996~1998 한국전자통신연구소 부설 시스템공학연구소
- 1998~현재 한국전자통신연구원 전자상거래연구부 부장