전자상거래를 위한 공개키 기반 하부구조의 인증 기술

유창열, 임신영, 송유진*, 함호상

시스템공학연구소, 동국대학교*

Authentication Technology of Public Key Infrastructure for Electronic Commerce

Chang-Yeol Yoo, Shin-Young Lim, You-Jin Song*, Ho-Sang Ham

Systems Engineering Research Institute

Dongguk University*

Abstract

암호화 기술의 확장성과 비도 측면에서 우수한 공개키 기반 하부구조(Public Key Infrastructure)는 공개키를 보증하는 기반 기술과 인증서의 안전한 사용 기술로 구성되어있으며, 전자상거래의 기본 기술중 하나이다. 이러한 기본 기술 중에는 키 복구(Key Recovery) 및 비밀 분산(Secret Sharing) 기술등이 포함되며, 인증기관(Certificate Authority : CA)을 통한 키 관리 효율성 및 인증 기관과 사용자 간 안전한 정보 교환 기술이 요구된다. 본 논문에서는 인터넷 기반의 전자 상거래 시 사용되는 공개키 기반 하부구조에 대하여 검토 분석한다.

1. 서론

인터넷을 이용한 전자 상거래가 국내외에서 최대 관심사로 부각되고 있으나 인터넷이라는 불완전한 개방형 전산망에서 전자 상거래를 안전하게 실현하기 위해서는 개인정보 노출 또는 변조의 위험성을 최소화 하는 것이 중요하다. [27], [28]

인증 기술을 공개키 암호화 기반에서 사용할때 인증 서비스의 확장성과 비도를 동시에 만족하며, 개인별 공개키를 인증해주는 인증기관(Certificate Authority)을 통하여 인증기관의 비밀키로 암호화 처리된 인증서의 발급 과정과 인증기관의 공개키로 확인 과정을 이용하여 양자 간의 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 확득하여 암호화된 메시지를 해독한다. 이렇게 함으로써 거래 상대방의 신분확인과 거래 내역에 대한 내용 확인이 가능하게 된다.

이와 같이 가상공간에서 전자 상거래 시 상대방의 신분을 확인할 방법, 거래 내역에 대한 쌍방의 부인 방지 방안 등이 커다란 문제가 되며 이러한 문제점에 대한 해결책은 현실적으로 암호/인증 기술에서 그 방안을 찾을 수 있으며, 현재 공개키 기반의 인증 기술을 활용하는 것이 최선의 대책으로 간주되고 있다. 특히, 안전한 전자 지불 방식의 구현을 위해서 인증 기술이 필수적이다. 본 논문에서는 이러한 필요성에 따라 공개키 기반 하부구조에서 전자 상거래를 성공적으로 실현하기 위한 필수 요건인 인증 기술의 개요, 공개키 기반 인증 메카니즘 등을 분석한다.

본 논문의 구성은 2장에서 인증기술과 공개키 기반 하부구조에 대한 개요, 3장에서 공개키 기반 인증 메카니즘의 분석, 4장에는 전자 상거래 인증 정보 흐름, 5장에서는 인증기술 응용에 관한 동향을 논한다.

2. 인증 기술과 공개키 기반 하부 구조

2.1 인증기술

인증 기술이란 전산망 환경에서 자신의 신분을 타인에게 증명하는 증명서와 같은 역할을 수행하며, 이는 사이버스페이스에서 상대측에게 자신의 신분을 증명하는 수단을 의미한다.

공개키 암호화 방식을 사용할 경우에는 '주어진 공개키가 진짜로 그 사람것인가?' 를 일일이 확인 해야 하는 '공개키 문제' 가 있다. 침입자가 임의로 열쇠 쌍을 생성하고, 공개키를 사칭하는 호스트의 이름으로 전송한다 하더라도 그것을 확인할 수 없기 때문이다. 따라서, 공개키의 확인은 전산망에서가 아닌 off-line에서 사람이 개입되어 확인하는 것이 보통이다. 그러나 안전한 공개키 사용을 위해 모든 호스트가 통신을 해야되는 대상(공개키)을 모두 off-line에서 확인한다면 인증 서비스에 많은 비용이 요구되며, 이러한 문제점을 해결하기 위하여 공개키의 사실 여부를 확인하고 공개키에 디지털 서명을 함으로써 그 열쇠를 사용한 사람의 신분을 증명해 주는 기관을 따로 둘 필요가 있는데 이것을 인증기관(Certification Authority, 줄여서 CA)이라고 한다.[32]

근본적으로 인증기술은 공개키 기반 하부구조를 지원하기 위한 기술이며, 공개키 기반 하부구조란 공개키 암호화 기술이 실현되도록 개인의 공개키를 신뢰할 만한 기관에서 관리하는 기술 기반을 의미한다. 인증기술은 암호화 기술, 분산 시스템 기술, 전산망 기술, 프로토콜 기술, 데이터베이스 기술과 관련성이 있으며, 인증 정책 수립에 따라 인증 기술 구축이 가변적으로 조정된다.

2.2. 공개키 기반 구조

공개키 기반이란 사용자가 관리할 키가 2가지로 하나는 공개키(이는 어느 누구나 사용할 수 있는 키를 의미함)와 다른 하나는 비밀키(이는 사용자 개인만이 관리하는 키로 비밀키 개념임)로 이루어진 기반이다. 인증기관 형태는 사용자의 공개키를 관리하여 외부에서 원하면 알려주는 기능을

수행하는 인증기관 제반 업무를 공개키 기반 하부 구조하에서 수행한다고 가정한다. 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 암호화 처리를 하여 외부의 제 3 자가 인증기관이 발행한 인증서를 임의로 변조하지 못하도록 변조 방지 기술을 적용하고 있다.

공개키 암호화 기술은 공개키를 안전하게 관리하기 위하여 개인별 공개키를 신뢰성있는 기관(인증기관 : Certificate Authority(CA))에서 인증서(Certificate) 형태로 관리하며 이러한 기반구조를 "공개키 기반 하부구조(Public Key Infrastructure(PKI))"라 할 수 있다. 본 논문에서는 공개키 기반 하부구조를 다음과 같이 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

즉, 공개키 기반 하부구조는 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 사용이 용이하도록 인증 기술 명세, 인증 정책, 관련 설비 등을 수립하여 관리하는 인증기관들간의 유기적인 결합체이다.[26], [32]

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(Certificate) 형태로 발급받는다. 송신측은 암호화된 인증서를 인증기관의 공개키로 풀어 인증서내의 수신측 공개키를 획득한다. 송신측은 자신의 비밀키와 수신측의 공개키(인증기관에서 받은 상대방 인증서내에 있는 공개키)로 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 등록한 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. 인증 메카니즘의 개요

공개키 기반 구조를 이용한 인증(사용자 및 메시지 인증)과 디지털 서명과의 기술적인 차이점을 명확히 구분하여 설명한다면 사용자 인증은 메시지를 보낸 사람이 바로 그 사람이라는 것을 증명하는 절차라고 정의 할 수 있으며, 메시지 인증이란 수신된 메시지가 송신된 출처에서 보내졌고 그 내용이 변경되지 않았다는 것을 증명하는 절차라고 정의할 수 있으며, 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. 인증 기법에는 크게 비밀키 기반 인증과 공개키 기반 인증 기법으로 구분하며 대표적인 예로는 전자의 경우, Kerberos를 후자의 경우, PKIX(X.509기반)가 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 국제 표준화가 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 실질적인 인증 기술을 개발할 필요가 있다.

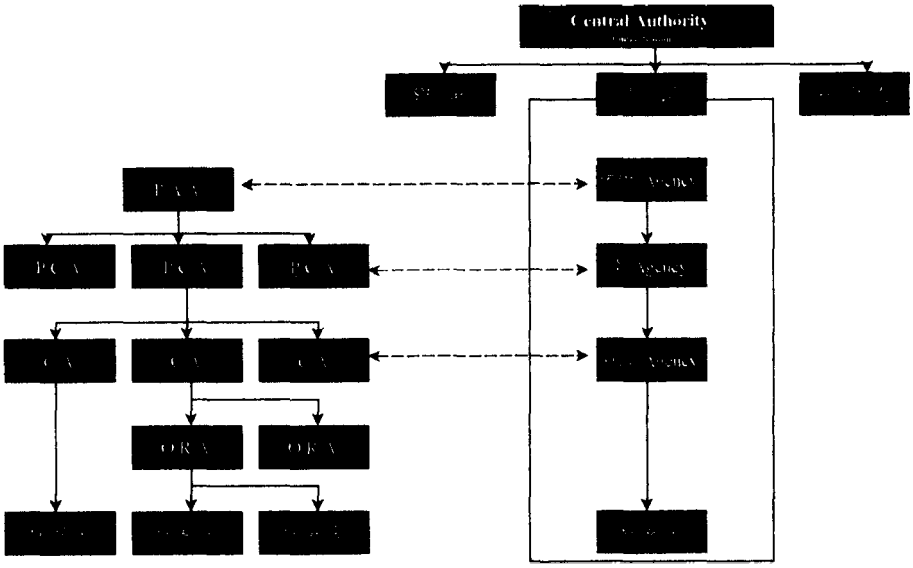
3.2. 공개키 기반 하부 구조 모델의 구조

일반적으로 공개키 기반 구조는 인증기관 등의 역할 및 기능에 의하여 계층적으로 구성된다.

- PAA(Policy Aproving Authority)
  - 전체 PKI에 대한 전반적인 가이드라인을 수립
  - PCA의 공개키를 확인
- PCA(Policy Certification Authority)
  - 도메인내의 모든 CA와 사용자들의 정책을 수립
  - CA의 공개키를 확인

- CA(Certification Authority)
  - PCA와 PAA의 정책에 따라 사용자의 공개키를 확인
- ORA(Organizational Registration Authority)
  - CA와 사용자 사이의 Agency 역할

다음 [그림 1]은 위의 계층적 인증 구조에 대한 하나의 예를 나타내고 있다.



[그림 1] 계층적 공개키 기반 하부구조의 인증체계

3.3. 공개키 기반 인증 메카니즘 관련 기술

공개키 기반의 인증 메카니즘을 구현하는 구체적인 기술로서는 다음과 같다.

(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.

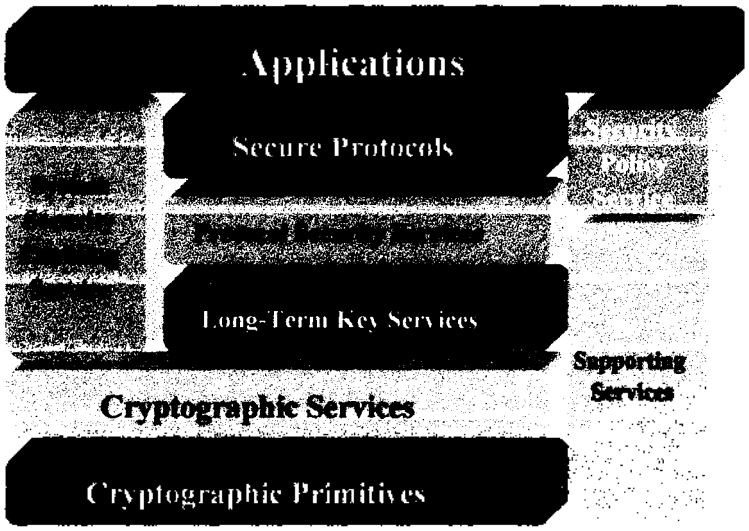
(3) 인증서 활용 기술 : 사용자 인증 프로토콜 기술, 인증서 및 CRL 조회 기술, 인증서 및 CRL 분배 서비스 기술이 있다.

(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 IETF의 보안 분야(Security Area)내 PKIX(Public Key Infrastructure) Working Group에서 도출한 인터넷 RFC(Request For Comments) 초안 문서의 개요에 대하여 설명한다. 인터넷 기술 전문 집단인 IETF의 Security Area내의 PKIX Working Group에서 현재 진행 중인 공개키 기반 인증 메카니즘의 세부 기술 사

항에 대한 인터넷 초안은 1997년 11월 시점에 다음과 같이 8가지이며 이들 문서들은 6개월마다 새로운 인터넷 초안으로 개정되면서 업체 표준을 목표로 의견을 수렴 중에 있으며, 현재 본 기술에 대한 업체표준 사양이 완성단계에 있다.

다음 [그림 2]는 공개키 기반 하부구조에 대한 사항이다.[1] 이는 1996년 11월 작성된 문서로 B. Blakley(IBM)가 대표로 작성하였으며 이후 본 문서에 대한 개정이 없어서 현재 IETF 해당 Working Group 인터넷 초안 문서 목록에서 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 확인한 문서이다.



[그림 2] 공개키 기반 하부 구조

3.3.1 Internet Public Key Infrastructure X.509 Certificate and CRL Profile (draft-ietf-ipki-part1-04.txt)

1997년 10월 15일에 작성된 문서로 R.Housley(SPYRUS), W. Ford(VeriSign), T. Polk(NIST), D. Solo(BBN)이 작성하였다. 이 문서는 인터넷 공개키 기반 하부구조 X.509 인증서와 CRL 프로파일의 6번째 문서이다. 이 문서에 새롭게 정의된 ISO 인증서 확장, 확장된 키 사용 그리고 각 필드별 의미의 정의를 추가하였다. 또한 확장된 키 사용 인증서 확장을 사용하기 위하여 객체 식별자(OID : Object Identifier)를 정의하였다. 인터넷 공개키 기반 하부구조의 설명을 위한 8개 문서 중 하나로 인터넷 PKIX에서 사용할 인증서 및 CRL 양식을 정의하였으며, 인증경로 처리에 대하여 정의하였다. 또한 X.509 기술을 사용하여 X.509 인증서 버전 3를 인터넷 응용에 필요한 프로파일과 관련 구조로 개발하였다. 그리고 사용상의 문제 해결을 위한 인증서 관리 시스템의 개발, 응용 도구의 개발, 정책에 의해 결정된 상호 운영성을 향상시킨 프로파일을 정의 하였다. 암호화 규약은 일반적인 암호화 알고리듬을 적용할 경우에 대하여 설명하였으며, ASN.1으로 포괄적인 정리를 하였다. 여기에는 공개키 구성요소, 전자 서명의 확인과 암호화 절차를 명시하였

다.

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 알고리듬을 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 알고리듬 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 알고리듬 식별자
signature : by issuer CA	인증기관에 의하여 서명한 서명 내용(서명 자체)

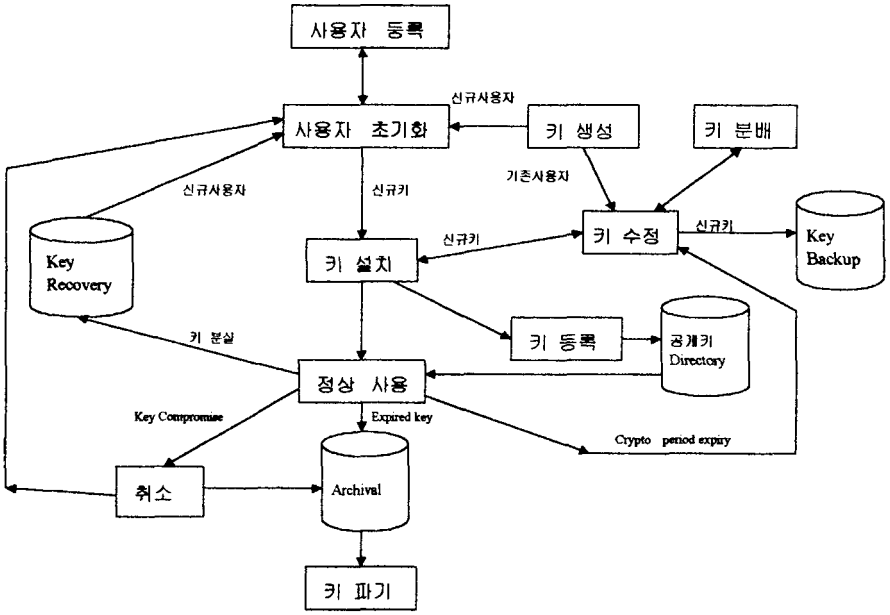
[표 2] X.509 인증서 취소 리스트(CRL) 양식

필드 이름	의 미
version(v2)	인증서 취소 리스트의 버전으로 최신 버전 번호는 2임
signature algorithm id	CRL에 서명한 디지틀 서명 알고리듬 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 알고리듬 식별자
signature : by issuer CA	인증기관에 의하여 서명한 서명 내용(서명 자체)

3.3.2. Internet Public Key Infrastructure Certificate Management Protocols

(draft-ietf-ipki2cmp-02.txt)

1997년 10월 15일에 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 프로토콜 메시지들은 인증서 생성과 관리에 대한 모든면을 정의하였다. 또한 공개키 관리에 대한 키 복구(Key Recovery) 및 비밀공유(Secret Sharing)의 구조와 키 관리 생명 주기(Key Mangement Life Cycle)에 대한 관리 프로토콜이 정의되어 있다. 다음 [그림 3]은 키 관리 생명 주기를 도식적으로 요약하고 있다.[11]



[그림 3] 키 관리 생명 주기

3.3.3. Internet Public Key Infrastructure Operational Protocols - LDAP

(draft-ietf-ipki2opp-00.txt)

1997년 9월 17일 작성된 문서로 S. Boeyen(Entrust Technologies), R.Housley(SPYRUS), T. Howes(Netscape), M. Myers(VeriSign), P. Richard(Xcert)이 작성하였다. 이 문서에 설명된 프로토콜은 인터넷 공개키 기반 하부구조(IPKI)내에서 몇가지 운영 요구사항들을 만족시키기 위하여 설계되었다. 특히 이 문서는 공개키 기반 하부구조 정보의 검색, 공개키 관련 정보를 관리하기위한 공개키 기반 하부구조 정보의 저장에 관한 요구사항을 설명하였다. 이문서에 설명된 메카니즘은 경량화된 디렉토리 접근 프로토콜(Lightweight Directory Access Protocol : LDAP) 버전2를 기반으로한다. 그리고 IPKI내에서 사용하기 위하여 RFC 1777에 정의되었으며, 프로토콜의 프로파일을 정의한다. PKIX 운영 요구사항들의 부가적인 메카니즘들은 본 문서와 별도로 설명하였다. X.509v3 인증서와 X.509v2 CRL의 조회를 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. 즉, 이문서는 인터넷에 대

한 공개키 하부구조의 개발에 대한 멀티 파트 표준의 Part 2 이다. 문서의 주된 내용은 인증서와 정보 저장소로부터 CRLs의 검색을 제공하기 위하여 요구되는 사항들에 대하여 논하였으며, 두 개의 프로토콜 프로화일들이 이러한 요구 조건을 만족시키기 위하여 제공하는 기능에 대하여 정의 하였다. 하나는 Lightweight Directory Access Protocol(LDAP)에 기초하고 있고, 다른 하나는 File Transfer Protocol(FTP)에 기초하고 있다. 부가적으로 온라인으로 인증에 대한 상태를 CA로부터 직접적으로 확인하기 위하여 필요로하는 요구 조건을 다루고 있다. 그리고 지원하는 프로토콜을 자세히 설명하였다.[6], [10]

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

1997년 10월 7일 작성된 문서로 S. Chokhani(CygnaCom Solutions, Inc), W. Ford(VeriSign)이 작성하였다. 이 문서는 인증정책 또는 인증 수행의 정의에 대한 framework을 제공한다. 그리고 특히, 포괄적으로 인증 정책 정의와 인증 수행 내용에 대한 사항을 정리하였으며 향후 이 문서는 Informational RFC로 추진할 예정이다.[12]

3.3.5. Internet Public Key Infrastructure Part V: Time Stamp Protocols (draft-ietf-pkix-ipki5tsp-00.txt)

1997년 7월 30일 작성된 문서로 C. Adams, D. Pinkas, Patrick Cain, Robert Zuccherato이 작성하였다. 이 문서는 Time Stamp Authority와 Time Stamp로 통신할 때 사용되는 프로토콜들에 의하여 작성된 데이터의 포맷을 설명하였다. Time stamping 서비스는 부인 봉쇄 서비스를 구축하기 위한 하나의 구성요소로서 사용될 수 있는 Trusted Third Party(TTP)에서 제공한다. CRLs을 적절히 확인할 수 있는 것과 특정한 시기에 특별한 포인트에 서명을 어떻게 할 것인지를 예로서 설명하였다.

3.3.6. Internet Public Key Infrastructure Part VI: Notary Protocols (draft-ietf-pkix-ipki6np-00.txt)

1997년 7월 30일 작성된 문서로 C. Adams, Robert Zuccherato이 작성하였다. 이 문서는 일반적인 공증인 서비스와 공증인 서비스로 통신할 때 사용되는 프로토콜에 대하여 설명하였다. 공증기관(Notary Authority)은 부인하지 않는 서비스를 구축하기 위한 하나의 구성요소로서 사용될 수 있는 Trusted Third Party(TTP)이다. 키 만료 기간 혹은 취소 이외의 서명 기간을 확장하기 위하여 공증인을 어떻게 사용하는지에 대한 예를 설명하였다.

3.3.7. Internet Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet Public Key Infrastructure Certificates (draft-ietf-pkix-ipki-kea-00.txt)

1997년 10월 15일 작성된 문서로 Russ Housley, William Polk이 작성하였다. 이 문서는 인터넷

공개키 기반 하부구조 X.509 인증서에서 Key Exchang Algorithm(KEA)에서 사용하는 키들의 설명에 대한 최초의 문서이다.

3.3.8. Internet Public Key Infrastructure Operational Protocols: FTP and HTTP
(draft-ietf-ipki2opp-00.txt)

1997년 10월 22일 작성된 문서로 Russ Housley이 작성하였다. 이 문서에 설명된 프로토콜은 인터넷 공개키 기반 하부구조(PKI)의 몇가지 운영 요구사항들을 만족하도록 정의하였다. 이 문서는 FTP를 사용하기 위하여 설명되었으며, PKI 저장소로부터 인증서와 인증서 취소 목록(CRLs)을 얻기 위하여 HTTP 사용 절차에 대한 설명을 하였다. PKIX 운영 요구사항들의 부가적인 메카니즘들은 본 문서와 별개로 설명하였다.

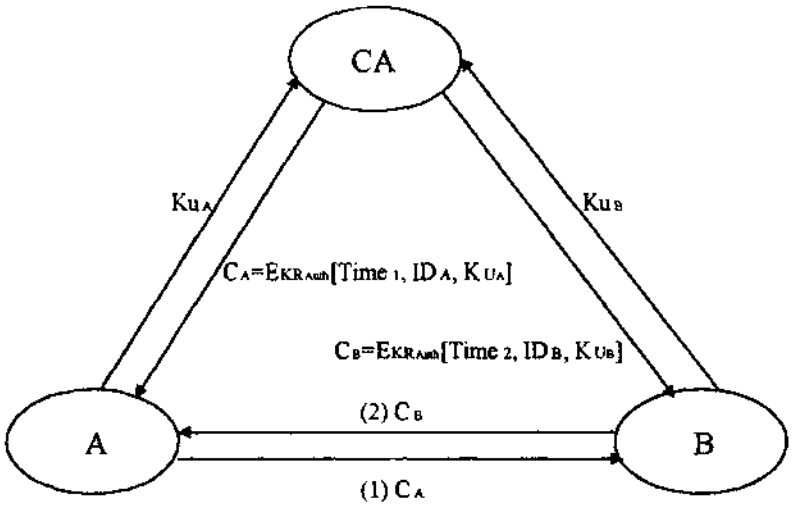
4. 전자 상거래 인증 정보 흐름

전자 상거래를 구성하는 기본 요소로 은행, 구매자 및 판매자를 들 수 있으며, 전자 상거래의 단위행위로 거래 문의, 거래 조건 협상, 거래 성사 및 지불이다. 이러한 행위 과정에서 현실 세계와는 달리 가시거리에 없는 즉, 사이버스페이스에서의 상대방 신분 확인, 거래 성사 결과의 부인 방지, 지불의 안전한 처리에 대한 기술적인 해결 방법으로 인증 기술을 사용한다.

공개키 기반 구조가 제공하는 서비스는 전자서명 서비스, UBS(Unclassified But Sensitive)수준의 암호화 키 관리 서비스 및 비밀데이타의 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)
- 비밀데이타의 복구 서비스(Option)
  - 비밀키 복구 기능

아래 [그림 4]과 같이 공개키 기반(X.509)의 인증기관은 서비스 사용자에게 인증서를 통한 사용자 공개키 인증을 수행한다.

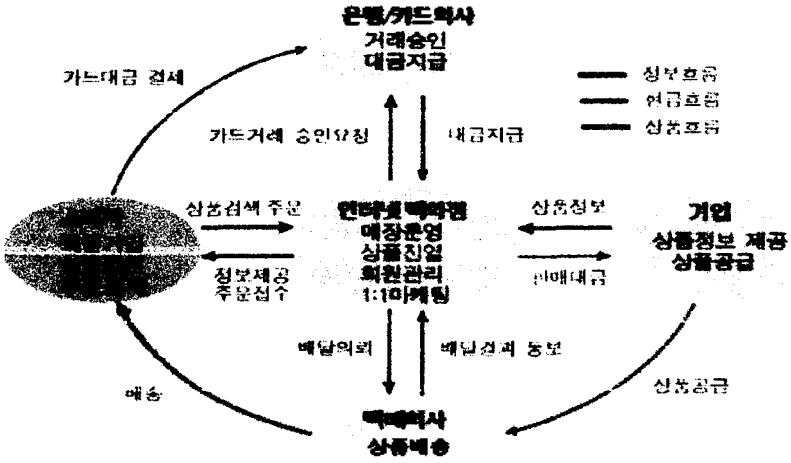


[그림 4] 공개키 기반 인증기관 인증 정보 흐름

여기서 A와 B는 CA의 사용자이고 A와 B는 사전에 CA에게 자신의 공개키를 등록(Ku_A, Ku_B)하여 CA로부터 각각 C_A, C_B를 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 타임스템프와 난수를 포함하여 송신하는데 이는 추후 A와 B가 서로 인증서내의 공개키를 확인하는 과정에서 인증서의 유효성 여부를 판단하는 기준이 되도록 하였다. A가 B에게 보낸 C_A는 B가 이미 가지고 있는 CA의 공개키로 복호화하여 A의 공개키를 다음과 같이 확인한다.[13], [32]

$$B : D_{KUAuth}[C_A] = D_{KUAuth}[E_{KRAuth}[Time_1, ID_A, K_{UA}]$$
$$= [Time_1, ID_A, K_{UA}]$$

아래 [그림 5]은 전자 상거래에 대한 전형적인 정보 흐름을 보나타내며, 사용자(소비자)가 인터넷 백화점을 사용할 시점부터 소비자와 백화점간에 상호 신분 확인이 필요하게 된다. 특히, 백화점 입장에서 소비자에 대한 신분 확인을 요구하게 되며, 동시에 소비자는 자신이 접속하여 전자 거래 서비스를 사용하고자하는 백화점의 인증서를 인증기관에서 입수해야한다. 즉, 소비자 역시 자신이 접속하고자 하는 백화점이 자신이 원하는 바로 그 백화점인지 확인하고자 인증서를 요구해야한다. 이 과정에서 사용자와 백화점간에 인증서 교환이 성립되고 이러한 인증서 교환은 이미 사전에 인증기관을 통하여 인증서 신청(공개키 등록) 결과로 각자 배포 받은 인증서를 사용함으로써 가능하게 된다.



[그림 5] 전자 상거래의 정보 흐름도

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 인증서 사용 시나리오에 대하여 설명한다.[30], [31]

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

(바) 소비자의 구매가 결정되면 소비자의 신용 카드 또는 은행 계좌 이체를 통한 지불 절차를 수행한다.

(사) 지불 과정에서도 인증서를 사용하게 되는데 인터넷 백화점은 소비자의 인증서가 첨부된 '지

불 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 통보하여 준다. 만약 위조 인증서일 경우, 위조 내역과 지불 취소 메시지를 소비자 및 인터넷 백화점에게 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.

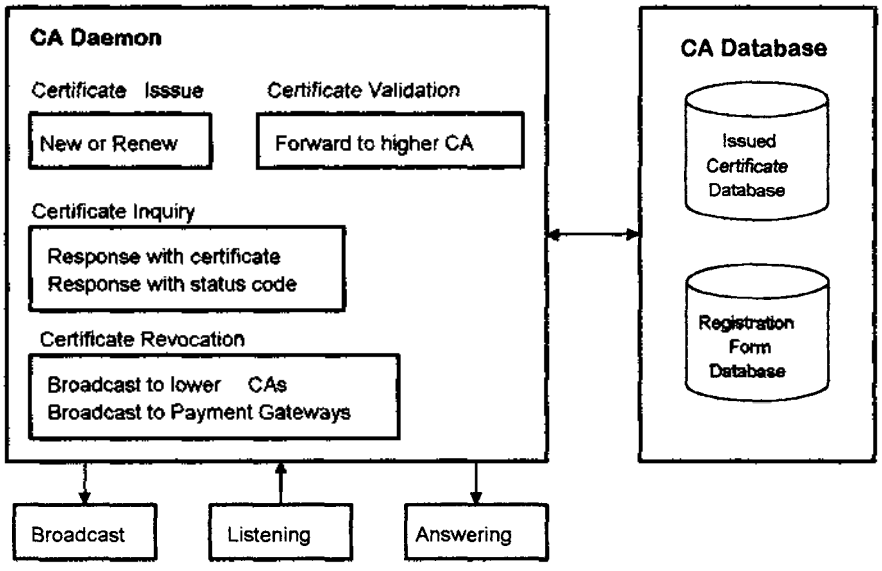
이상과 같이 가상적인 환경을 설정하여 인증서가 전자 상거래에서 어떠한 방식으로 사용되는 지를 예로 설명하였다.

5. 공개키 기반 인증 기술의 동향

본 장에서는 공개키 기반 인증 기술에 대하여 인증 기술을 활용한 사례를 검토하여 요소 기술과 서비스 내용에 대하여 분석하였다.

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 인증기관 구조는 아래의 [그림 6]와 같다.[25]



[그림 6] SET에서의 인증 구조

인증서 발행 모듈은 새로운 인증서를 발행하는 부분과 기존 인증서에서 갱신을 처리하는 부분으

로 구성되어 있다. 새로운 인증서를 발행하는 경우, 구매자(Cardholder)에게 이를 발급하는 루틴은 6개 단계로 구성되어 있으며, 판매자, 지불 게이트웨이, 인증기관에게 발급하는 루틴은 4개 단계로 구성되어 있다. 등록 양식 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.

5.2. VeriSign의 인증 구조

RSA Data Security의 관련 회사 VeriSign은 인증 서비스를 제공하는 회사로 탄생하였으며, 미국 대규모 전화회사인 GTE도 CyberTrust라는 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]

다음의 [표 3]은 VeriSign이 발행하는 인증 Class에 대한 세부 사항을 정리한 표이다.

[표 3] VeriSign에서의 인증 Class

	개인용	기업 및 단체용
Class 1	사용자의 이름, 전자우편주소가 자신의 것임을 인증해 줌. VeriSign 자체의 CA 서비스에서는 이 class에 등록한 이용자의 운전면허와 같은 사항은 인증 범위에서 제외됨. 이 서비스는 VeriSign의 웹 사이트(www.verisign.com)에서 전세계 모든 사용자에게 제공됨.	없 음
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.	없 음
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.

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 키드 회사가 될것이며 그 경우, 가맹점에 대하여는 class3을 발행하고, 카드 소유자에 대하여는 class2를 발행하게 될것이다.

5.3. Xcert 인증 구조

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

인증 기술 응용 사례 : 미국 오레곤 주 정부의 경우, 오레곤 주 정부의 주도하에 공증 서비스 즉, Oregon Notary를 추진하여 현업에서 전자 상거래 시 전자 증빙 서류로 갈음이 가능하도록 제도권내의 정비를 하였으며 실 사회에서 전자 공증 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](참조 웹 사이트 : http://www.sos.state.or.us/corporation/notary/nguide/toc.html)

그외에 완전한 분석은 정보의 부족으로 수행되지는 않았으나 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 위한 인증 기술로 암호화 기술의 확장성과 비도 측면에서 우수한 공개키 기반 하부구조(Public Key Infrastructure) 인증 기술을 중심으로 논하였다. 인증 기술은 전자 상거래 서비스에서 필요한 상호 신분 인증, 거래 내역 인증 및 지불 처리 인증에 사용하는 기반 기술이며, 이는 공개키를 보증하는 기반 기술과 인증서의 안전한 사용 기술로 구성된다. 이러한 기술은 공개키 기반 전자상거래 인증의 기본 기술이며, 전자 상거래를 실현하기 위한 필수적으로 선결해야할 기술 사항이다. 특히, 인터넷이라는 불완전한 개방형 전산망 구조에서 안전한 전자 상거래를 제공하려면 국제적인 인증 서비스와의 연동을 위하여 국제적으로 표준화된 인증 기술의 적용이 중요하며 이러한 기술 사양에 대하여 IETF의 보안 분야 PKIX(Public Key Infrastructure) WG에서 업체 표준화를 추진 중이며 본 논문에서 표준 대상이되는 기술 문서를 인증 메카니즘 분석에 포함하여 분석하였다.

참고문헌

[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-part1-03.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.gvnfo.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 정보호호 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,권도균, 전자 상거래 보안, pp. 45-52, 한국정보과학회지 제 15권 제 4호, 1997. 4.

[31] 임신영 외, 인터넷 기반 전자거래 전용망 보안 정책 수립 연구, 1997년 제 9회 WISC 워크샵 논문집, 1997. 9.

[32] 최용락 외, 통신망정보보호, 1996.2.