通信情報保護學會誌
第8卷 第3號, 1998. 9

인증실무준칙 분석

이 종 후* 김 지 선** 류 재 철*

요 약

인증 서비스는 인터넷을 통한 전자상거래에서의 안전성 및 신뢰성을 확보하기 위해 반드시 필요한 요소이다. CPS는 인증 서비스를 제공하는 CA에 의해 제공되는 인증 업무에 대해 세부적으로 기술한 문서로써, 인증서 사용자들이 인증기관의 신뢰도를 측정하는데 있어서 기준이 되는 역할을 한다. 본 고에서는 현재 인증 기술 부분의 연구에 있어서 주도적 역할을 하고 있는 IETF pkix 워킹 그룹의 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework의 분석을 통해, CPS의 역할 및 기능을 분석하였다.

1. 서 론

인터넷의 급격한 성장과 함께 인터넷을 이용한 전자상거래는 이미 우리의 생활에 깊숙히 파고들고 있다. 그러나 전자상거래의 보다 빠른 확산과 성공을 위해서는 인터넷 상에서 일어날 수 있는 여러 가지 보안 문제의 해결이 필수적이다. 즉 전송되는 내용의 기밀성 보장 및 변경 방지, 네트웍에서의 상대방 인증 등 보안 서비스 제공은 전자상거래의 성공을 위해서 반드시 해결해야 할 중요한 과제이며, 이의 해결에는 암호 기술의 이용이 중요한 역할을 담당하고 있다. 특히 공개키와 비밀키 쌍을 이용한 공개키 암호 방식은 향후 전자상거래 실현을 위해서는 필수불가결한 요소로 취급되고 있다. 이러한 공개키 암호 방식에서는 제 3자가 본인의 공개키를 생성, 공개, 악용하는 것을 방지하기 위하여 그 공개키가 본인의 것임을 확인하는 '인증(certification)' 기능이 필요하게 된다.

인증은 소비자가 인터넷상의 전자상점에서 쇼핑할 때, 소비자나 전자상점이 진짜 당사자인지를 네트웍 상에서 확인하는 기능으로, 전자상거래의 모든 상황에서 이용되고 있으며, 장기적으로는 기업 네트웍(Intranet 등) 내에서의 이용도 고려된다. 이와 같이 공개키 암호 방식에서의 인증 시스템은 네트웍 거래의 안전성 및 신뢰성 확보를 위해 반드시 필요한 요소이며, 인증기관(CA : Certification authority)은 그 기본적인 기능을 수행하는데 있어서 중요한 역할을 담당한다.

인증기관이 인증 업무를 수행함에 있어서 갖추어야 할 몇 가지 요소중의 하나로 인증실무준칙(CPS: Certification Practice Statement)이 있다. CPS는 인증기관에 의해 제공되는, 인증 업무를 세부적으로 기술한 문서로 인증기

* 충남대학교 컴퓨터 과학과
** 한국전자통신 연구원

관의 인증 서비스 제공에 있어서 매우 중요한 역할을 하고 있다. 본고에서는 현재 인증 기술 부분의 연구에 있어서 주도적 역할을 하고 있는 IETF(Internet Engineering Task Force) pkix 워킹그룹에서 draft로 제출된 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework'의 분석을 통해, CPS의 역할 및 기능에 대해 보다 자세히 살펴보고자 한다.

2. 인증 실무 준칙

인증 정책이란 용어는 X.509 표준으로부터 나온 용어이다. 이 X.509에 의하면 인증 정책은 어떤 특정한 목적에 어떤 인증서를 사용하는 것이 적합한가를 인증서 사용자에게 안내하기 위한 방법을 뜻하는 것으로, "특정 집단 혹은 일반적으로 보안을 요구하는 응용 모듈에서의 적절한 인증서를 발급하기 위해 적용되는 일련의 규정"으로 정의하고있다[1]. 인증 정책은 인증서 발급자와 인증서 사용자 모두에 의해서 인지되어야 하며, 개개의 인증서는 보편적으로 하나의 인증 정책과 관계를 가진다. 미국 변호사 협회(ABA: American Bar Association)의 전자서명 안내서(Digital Signature Guidelines)에 의하면, CPS는 "인증기관이 인증서를 발급하기 위해 사용한 실무 절차에 관한 세부 규정"으로 정의하고있다[2]. 즉 CPS는 인증서 소유자를 비롯한 인증서를 신뢰하여 사용하는 사용자의 인증 업무에 대한 이해를 돕기 위해 인증기관에 의해서 발행되는 인증 업무에 대한 세부적인 기술 문서이며, 인증 정책에 비하면 좀 더 구체적인 내용을 포함한다.

CPS는 인증기관의 인증 서비스 제공에 요구되는 전반적인 사항을 규정하고 있다. 또한 CPS는 인증기관이 인증서를 발급하기 위해 적용하는 공공 법규에 해당하며, 조직 내에서 사용하기 위한 사적인 계약서에 해당하는 것이다. 일반적으로 인증서 사용자들이 인증기관의 신뢰도를 측정하는데 있어서 척도가 되는 인증 정책, 사용자 인증 절차, 비밀키 관리 절차 등은 모두 CPS의 내용에 포함되며, 인증기관은 이 CPS의 규정에 의해서 모든 업무를 수행해야 한다[3][4]. 따라서 인증서 사용자들은 CPS에 의해서 인증기관의 신뢰도를 측정할 수 있다.

또한 CPS는 인증서의 발급/ 취소/ 보류/ 재발급 등 인증서 발급과 관련된 인증기관의 인증 서비스에 대해 법적인 근거를 제시하는 역할을 한다. 따라서 인증기관은 반드시 CPS를 작성하여 이를 공개하여야 하고, 인증 서비스를 제공하는데 있어서 반드시 CPS의 규정을 준수해야 한다. CPS는 〈그림 1〉과 같이 크게 9개의 구성요소로 이루어지는데, 본 장에서는 이 들 각각에 대해서 살펴보고자 한다.

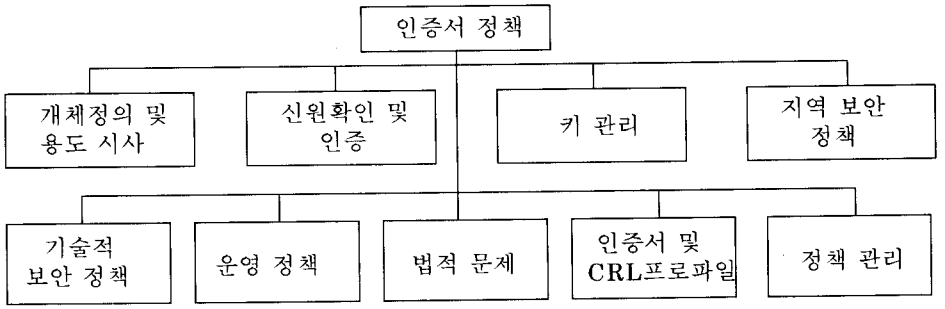


그림 1. CPS의 구조

2.1 개체 정의 및 용도 명시(community and applicability)

개체 정의 및 용도 명시에서는 인증 서비스를 구성하고 있는 요소들에 대해 설명하며, 인증서의 사용 용도와 인증기관이 인증 서비스를 위해 사용하는 여러 가지 표준들에 대해 명시한다. 즉 인증기관, 등록기관 및 최종 사용자에 대해 정의하고, 인증서의 종류를 기술하며, 발급된 인증서가 적용되는 예와 발급된 인증서의 사용에 관한 규정을 설명한다. 예를 들어 현재 가장 활발하게 상용 인증 서비스를 제공하고 있는 미국의 VeriSign에서는 〈표 1〉과 같이 인증서를 3개의 클래스로 구분하고, 각 클래스별로 인증서가 어떠한 분야에 적용될 수 있는지를 기술하고 있다[3].

표 1. VeriSign의 인증서 클래스 및 속성

속성 / 클래스	ID 확인	IA의 비밀키 보호	신청인의 비밀키 보호	인증서의 사용
클래스 1	자동화된 신청인의 이름 확인과 전자우편 주소 확인	PCA:신뢰할수 있는 하드웨어 CA:신뢰할 수 있는 소프트웨어 또는 하드웨어	암호화 소프트웨어	웹 브라우징, 전자우편
클래스 2	클래스 1에 거주지 주소 확인 추가	PCA, CA:신뢰할 수 있는 하드웨어	반드시 암호화 소프트 웨어 사용	전자우편, 온라인 가입패스워드 교체, 소프트 웨어 인증
클래스 3	클래스 2에 개인의 출석 및 서류제출 추가, 사업체의 인증 서류 제출 추가	PCA, CA :신뢰할 수 있는 하드웨어	반드시 암호화 소프트 웨어 사용 하드웨어 토큰사용 (선택사항)	E-banking, 전자상거래 서버, 소프트웨어 인증등

또한 개체 정의 및 용도 명시 부분에서는 다음과 같은 인증 서비스를 위해 사용되는 기술들에 대한 표준 사용 여부를 설명한다.

- 통신 프로토콜
- 응용 프로토콜
- 인증서와 인증서 취소 목록(CRL : Certificate Revocation List) 표준
- 비밀키 토큰
- 암호 알고리즘
- 기타

2.2 신원 확인 및 인증 정책(Identification and Authentication policy)

신원 확인 및 인증 정책은 특정 공개키가 정당한 소유주에게 속해 있음을 보장하는데 있어서 기본이 되는 요소이다. 즉 인증서 발급 신청이나 인증서 취소 요청과 같이 신원 확인 및 인증이 필요한 경우에 신청인이 이를 위해 제출해야 하는 여러 가지 정보를 정의하고, 이에 대한 확인 절차를 기술한다. 이는 대상이 인증기관인가 아니면 등록기관인가, 혹은 사용자인가에 따라 동일하게 적용될 수도 있고, 다르게 적용될 수도 있으며, 인증 서비스 각 구성요소의 최초 등록(인증서 발급 신청), 또는 만기나 취소에 의한 인증서 재발행 신청 및 취소 신청 등에 적용된다. 신원 확인 및 인증 정책이 필요한 경우는 〈표 2〉와 같다.

표 2. 신원 확인 및 인증 정책

구 분	내 용
최초등록	각각의 구성요소가 최초 등록하기 위해 필요한 절차 명시
정기적인 재발행	인증서 만기에 의한 인증서 재발행 절차 명시
취소에 의한 재발행	키 손상을 제외한 다른 이유에 의해서 인증서가 취소되었을 경우의 인증서 재발행 절차 명시(예 : 더 이상 서비스를 원하지 않을 경우)
키 손상에 의한 재발행	키 손상에 의해서 인증서가 취소되었을 경우의 인증서 재발행 절차 명시
취소 공지	인증서 취소 공지 절차 명시
키 손상 공지	키 손상 공지 절차 명시

구성요소의 최초 등록시에 고려해야 할 사항으로는 다음과 같은 것들이 있다.

- 개체에 부여되는 이름의 종류(X.500 distinguished name, RFC 822 Internet name, URL 등)
- 의미있는 이름인가의 여부
- 이름의 유일성 여부
- 이름이 중복될 경우 해결 방법
- 등록상표(trademark)의 인식 여부 및 인증 방법
- 등록된 공개키에 대응하는 비밀키의 소유주임을 증명하는 방법
- 필요한 신분증의 갯수
- 개인의 출석 여부

CA는 위의 사항들에 근거하여 인증서의 종류 및 각각의 인증서의 발급 신청에 필요한 정보와 이에 대한 심사 절차에 대하여 명시하여야 한다. 일반적으로 전자우편이나 웹 브라우징에 사용되는 인증서에 비해서 전자상거래 등에서 사용되는 인증서 발급을 위해 제출되는 정보가 좀 더 자세하고 심사 절차도 까다롭게 적용된다. 〈표 3〉은 VeriSign의 클래스 1과 클래스 2 인증서 발급 신청에 필요한 정보 및 신청서 제출 방법이다[3].

최초 인증서 발급 신청에 필요한 정보뿐만 아니라 인증서의 갱신 및 재발행 신청에 필요한 정보와 인증서 전달 방법 또한 신원 확인 및 인증 정책에서 기술되어야 하는 내용이며, 인증서의 갱신이나 재발행 신청에 필요한 정보는 인증기관의 정책과 인증서의 종류에 따라 최초 발급 신청 때와 동일하게 적용할 수도 있고, 그렇지 않을 수도 있다.

2.3 키 관리 정책(Key management policy)

키 관리 정책에서는 인증기관, 등록기관 또는 최종 사용자에서 자신의 암호키나 중요 보안 파라미터(critical security parameter)를 보호하기 위한 수단을 정의한다. (중요 보안 파라미터의 대표적인 예로는 PIN(Personal Identification Number)나 passphrase 등을 들 수 있다.) 키 관리의 범위는 키 생성에서부터 저장, 사용, 보관 및 파괴에 이르기까지 모든 과정을 포함한다.

표 3. VeriSign의 인증서 신청서 제출 방법 및 신청 정보

인증서 클래스	인증서 신청에 필요한 정보
클래스 1	개인 : 필수 정보 l 이름 (또는 별명) l 공개키 l 전자우편 주소 l 신용카드 정보 (신용카드 정보를 요구하는 것은 인증서 발행에 대한 요금의 지불을 위해서이다.) l 도전 문장(Challenge Phrase) l 기타 IA(Issuing Authority) 또는 VeriSign에서 요구하는 정보 선택 정보 l 통계 정보(Demographic data) 신청서 제출 방법: IA는 인증서 시작품과 계약서를 인증서 신청자에게 전달한다. 이 때 전달은 안전한 웹 채널(예 : SSL)을 통해 온라인으로 이루어지며, 전달이 끝나면 신청자는 다음 사항을 확인한다. l 인증서 신청 정보의 정확성 여부 l 계약서의 내용의 이해 및 동의 여부 IA에 의해서 신청서의 유효성 검사가 끝나면, IA는 신청서에 기입된 전자우편 주소로 전자우편을 발송한다. 이 때 이 전자우편에는 인증서 신청자가 IA로부터 인증서를 획득할 때 필요한 PIN(Personal Identification Number)을 함께 보낸다.
클래스 2	개인 : 필수 정보 l 이름 (법적인 이름) l 유일 이름(RDN: Relative Distinguished Name) l 거주지 주소 l 전화번호 l 전자우편 주소 l 공개키 l 신용카드 정보 l 배우자 성명 l 주민등록번호 l 생년월일 l 고용주 l 도전 문장(Challenge Phrase) l 거주지 前주소 (2년 안에 변화가 있다면) l 운전면허 정보 l 소프트웨어 출판 보증 l 기타 IA(Issuing Authority) 또는 VeriSign에서 요구하는 정보 선택 정보 l 통계 정보(Demographic data) 신청서 제출 방법 : 클래스 1과 동일

구성요소 별로 조금씩 다르기는 하지만, 일반적으로 공개키쌍의 관리와 관련하여 키 관리 정책에서 언급되어야 사항들은 다음과 같다.

- 키 생성 주체
- 사용자가 인증기관에 공개키를 전달하는 방법
- 인증기관의 공개키를 사용자에게 전달하는 방법
- 키 크기
- 공개키 파라미터 생성 주체
- 키 생성 중에 공개키 파라미터에 대한 검사 여부
- 키 생성 방법(하드웨어적 또는 소프트웨어적 방법)
- 키 사용 목적(X.509 version3 key usage flags)
- 키 생성 모듈의 표준 준수 여부(예 : 미국의 FIPS 140-1)
- 비밀키의 분리 여부(secret sharing)
- 비밀키 위탁 여부, 비밀키 위탁이 이루어진다면 비밀키 위탁기관 및 비밀키 위탁 방법
- 비밀키의 백업 여부, 백업이 이루어진다면 백업 장소 및 방법
- 비밀키 기록 보관 여부, 기록 보관이 이루어진다면 장소 및 방법
- 공개키 기록 보관 여부, 기록 보관이 이루어진다면 장소 및 방법
- 비밀키 관리자
- 공개키쌍의 유효기간
- 비밀키 파괴 절차

이와 같은 사항은 공개키쌍 뿐만 아니라 중요 보안 파라미터에도 유사하게 적용된다. 중요 보안 파라미터 관리와 관련하여 일반적으로 언급되는 사항은 다음과 같다.

- 중요 보안 파라미터의 생성 주체
- 중요 보안 파라미터의 크기
- 중요 보안 파라미터의 관리(복수에 의한 관리)
- 중요 보안 파라미터의 위탁 여부, 중요 보안 파라미터의 위탁이 이루어진다면 위탁기관 및 위탁 방법
- 중요 보안 파라미터의 백업 여부, 백업이 이루어진다면 백업 장소 및 방법
- 중요 보안 파라미터의 기록 보관 여부, 기록 보관이 이루어진다면 장소 및 방법
- 중요 보안 파라미터의 관리자

CA의 키는 보안상 매우 중요한 위치에 있기 때문에 키 생성 및 저장, 사용 등에 있어서 주의 깊은 관리가 필요하다. 따라서 CPS를 작성하는 CA는 위에서 언급한 사항들에 근거하여 다음의 예와 같이 자신의 키 관리 절차에 대하여 기술함으로써, CA의 인증서를 사용하는 사용자들에게 신뢰성을 주는 것이 필요하다. 그러나 보안상 자세한 절차의 기술이 오히려 위험한 것으로 판단되는 경우에는 기술하는 내용을 조절하는 것이 필요할 것이다.

- **CA 공개키 쌍의 생성**: 복수의 직원에 의해서 FIPS PUB 140-1 Level 2를 따르는 신뢰할 수 있는 암호키 생성 시스템을 사용하여 생성한다.
- **CA 비밀키의 저장**: CA의 비밀키는 3개 이상으로 분리되어 각각 128비트 DES로 암호화되어 스마트카드에 저장되며, 각각의 스마트카드는 각기 다른 직원에 의해 관리된다.
- **CA 비밀키의 백업**: CA의 비밀키와 비밀키 저장에 사용되는 암호키는 CA 운영 시스템과 분리된 시스템에 백업된다.
- **CA 비밀키의 보관**: CA의 비밀키와 비밀키 저장에 사용되는 암호키는 인증서의 유효기간이 지난 후에도 필요한 경우를 대비하여 보관된다. 보관기간은 3년이며

보관되는 비밀키와 암호키는 복수의 직원에 의해 관리된다.

- **CA 비밀키의 파괴**: 유효기간과 보관기간이 지난 CA의 비밀키는 파괴되는 것을 원칙으로 하며, 이 때 이와 관계된 정보는 비공개로 유지한다.
- **키 손상 또는 재해로부터의 복구** : CA의 비밀키가 손상 또는 누출된 것으로 확인된 경우, CA의 인증서는 즉시 취소되며, 이 사실을 모든 사용자에게 공지한다.

이와 같이 CA의 비밀키 관리 외에도 사용자의 키 관리 및 비밀키 위탁 등에 관한 기술도 키 관리 정책에서 이루어진다.

2.4 내부 보안 정책(Local security policy)

내부 보안 정책에서는 인증기관의 기능을 안전하게 수행하기 위해서 사용되는 비기술적인 보안 규제에 대해서 정의한다. 비기술적인 보안 규제는 물리적 관리, 직원 관리, 업무 절차 관리 등 크게 3가지로 구분할 수 있다. 자세한 내용은 다음과 같다.

- **물리적 관리** : 인증 업무와 관련된 시설 및 장치 등에 관한 관리 규정, 즉 CA 운영 시스템이 위치한 건물에 대한 출입 관리 및 화재, 지진, 수재, 전자기적 영향 등에 대한 방어 대책과 CA 운영 시스템이 위치한 전산실에 대한 관리 대책을 기술한다. 또한 정전에 대비한 발전시설과 고온 및 저온에 대비한 냉난방 시설에 대한 관리 상태를 기술한다.
- **직원 관리** : 인증 서비스의 중요성을 감안할 때, 인증 업무를 수행하는 직원들에 대한 강도 높은 직원 관리가 필요하다. 따라서 직원 채용 규정 및 직원 연수 규정, 직무 순환, 처벌 규정 등의 관리에 대해서 기술함으로써 사용자에 대한 신뢰성을 확보하여야 한다.
- **절차 관리** : 인증 업무와 관련된 직원들의 역할 및 책임에 관한 규정을 기술한다.

2.5 기술적 보안 정책(Technical security policy)

기술적 보안 정책에서는 인증기관의 기능을 안전하게 수행하기 위해서 사용되는 기술적인 보안 관리에 대해서 정의한다. 기술적 보안 정책은 컴퓨터 보안 관리, 생명주기 보안 관리, 네트워 보안 관리, 암호 모듈 관리 등 크게 4가지로 구분할 수 있으며, 이 밖에 컴퓨터 보안 보증, 생명주기 보안 보증이 포함될 수도 있다.

일반적으로 기술적 보안 정책은 CA가 채택하고 있는 컴퓨터 시스템, 네트워 시스템, 암호 모듈 관리, 시스템 관리 등이 어떠한 평가기준을 준수하고 있는가를 기술하는 것으로 이루어지고 있다.

2.5.1 컴퓨터 보안 관리

컴퓨터 보안 관리에서는 다음과 같은 사항들에 대하여 CA가 어떻게 관리하고 유지하는가를 기술한다.

- 사용자 인증 및 접근 제어
- 레이블(Labels)
- 객체 재사용(Object Reuse)
- 감사
- 보안 테스트/ 보안 침투 시험

2.5.2 생명 주기 관리

생명 주기 관리는 시스템 개발 관리와 보안 관리 제어로 나뉘며 그 내용은 〈표 4〉과 같다.

표 4. 생명 주기관리

구분	내 용
시스템 개발 관리	개발 환경 보안
	개발자 보안
	구성 관리
	개발 시설에 대한 보안
	소프트웨어 공학 실무(practice)
	소프트웨어 개발 방법론
	모듈화(modularity)
	계층화(Layering)
	내고장 설계(Fail-safe design)
	내고장 구현(Fail-safe implementation)
보안 관리 제어	보안 절차(procedures)
	보안 도구(tools)
	소프트웨어 무결성
	펌웨어 무결성
	하드웨어 무결성

2.5.3 네트웍 보안 관리

네트웍 보안을 위해서 사용되는 시스템에 대해 기술하는 부분으로 사용하고 있는 침입차단 시스템(Firewall)과 네트웍 보안 정책, 침입차단 시스템의 등급에 대해서 기술한다.

2.5.4 암호 모듈 관리

인증 업무를 위해 사용되는 암호 모듈과 관련하여 다음 사항들을 어떻게 유지하고 있는가를 기술한다.

- 암호 모듈의 입/출력
- 암호 모듈의 역할 및 제공 서비스
- 유한 상태 머신(finite state machine)
- 암호 모듈에 대한 물리적 보안
- 암호 모듈에 대한 소프트웨어적인 보안
- 운영체제 보안
- 키 관리
- 자체 테스트

2.5.5 보증

CA는 위에서 언급한 보안 요소들은 각 구성요소별로 적절한 평가 기준에 의해서 평가한 후 CPS를 통해 그 등급을 기술한다. 각 보안 요소에 대한 평가 기준들은 〈표 5〉와 같다.

2.6 운영 정책(Operations policy)

운영 정책에서는 인증서 취소, 감사, 기록 보관, 키 변경, 키 복구 등과 관련된 정책을 규정한다. 자세한 내용은 다음과 같다.

- **키 변경**: 인증서의 유효기간 및 인증서 발급에 소요되는 시간에 대해서 기술한다.
- **비공개 정책**: 사용자에게 발급된 인증서는 CA의 데이터베이스 및 저장소에 등록되며, CA는 인증서를 사용자에게 공개해야 할 의무가 있다. 따라서 CA는 인증서

표 5. 보안 평가 기준

컴퓨터 보안 보증	• TCSEC : Trusted Computer System Evaluation Criteria • Canadian Trusted Products Evaluation Criteria • European Information Technology Security Evaluation Criteria • CC : Common Criteria
생명주기 보안 보증	• TSDM : Trusted Software Development Methodology • SEI-CMM : Software Engineering Institute's Capability Maturity Model
암호 모듈 보증	• US FIPS 140-1

공개와 관련된 정보를 CPS를 통해 공개해야 한다. 그러나 인증 업무를 위해 CA가 얻게된 사용자의 개인 정보는 노출되지 않도록 해야한다. 또한 CA는 사용자들로부터 신뢰도를 높이기 위해서 CA의 행정 정보, 기술적 정보, 재정 정보 등을 공개해야 한다. CPS에서는 이러한 정보를 얻을 수 있는 방법을 기술한다.

- **감사 정책**: CA는 신뢰성 있는 업무의 유지를 위해 정기적 또는 비정기적인 감사를 실시하여야 하며, 이에 대한 감사 기록의 저장 절차, 감사자 선책 방법, 정기 감사의 주기, 비정기적인 감사가 실행되는 요건, 감사 기록의 공개 및 감사에 대한 조치, 감사 정보와 감사 결과의 보관 등을 기술하여야 한다.
- **기록 보관**: CA는 인증서 신청과 인증서의 생성, 발행, 사용, 보류, 취소 등에 필요한 정보와 관련된 문서를 안전성 있는 방법으로 보관하여야 하며, CA는 CPS를 통해 이와 관련된 정보를 공개한다.
- **재해 복구 절차**: 자연재해로부터 시스템, 인증서, 비밀키 등의 복구 대책을 기술한다.
- **인증서 취소 및 키 손상 보고**: 인증서의 취소가 이루어지기 위한 요건, 취소 요청의 절차, 키 손상 보고 절차, CRL 발행 주기 및 공표 방법 등에 대해서 기술한다.

표 6. 법적 문제

내 용	구 분
요 금	인증서 발행/ CRL 접근 등에 대한 요금
	환불 정책
법/ 규정	인증 서비스와 관련된 법/ 규정
재정적 기반	인증기관의 재정 상태 공개
의 무	각 구성요소의 의무 사항 규정 • CPS 준수의 의무 • 정확한 정보 공개 • 비밀키 보호 • 키 손상/ 인증서 취소에 대한 공지 등
책임 한도	책임 한도

2.7 법적 문제(Legal poivision)

인증기관을 통해 제공되는 인증 서비스의 신뢰도를 높이기 위해서는 인증 서비스와 관련된 여러가지 법적 문제들에 대한 기술이 반드시 필요하다. 즉 인증기관, 등록기관, 최종 사용자의 의무 및 책임 한도에 대한 명확한 규정이 필요하며, 또한 인증기관의 재정 상태와 인증 서비스와 관련된 법 규정, 서비스 요금 등에 대한 명시가 있어야 할 것이다. 법적인 문제에 포함되는 내용은 〈표 6〉과 같다.

CA는 〈표 6〉과 같이 인증서 종류별 사용 요금 및 환불 정책을 CPS에서 기술하여야 하며, 제공하는 인증 서비스와 관련된 법/규정에 대해서 기술하여야 한다. 국내에서는 전자상거래기본법, 전자서명법 및 기존의 상거래 관련법, 전산망보호법, 개인 정보 보호법 등에 의해 인증서 사용자가 보호받을 수 있음을 명시하여야 할 것이다.

2.8 인증서 및 CRL 프로파일(Certificate and CRL profile)

인증서 및 CRL 프로파일에서는 인증서와 CRL의 버전과 인증기관에서 지원하는 확장 필드에 대해서 정의한다. 자세한 내용은 다음과 같다.

- 인증서 버전
- 정책(policy) OID
- 인증기관, 등록기관, 최종 사용자에서 사용되는 이름의 형식
- 인증기관, 등록기관, 최종 사용자에서 사용되는 이름의 형식의 제한
- 사용되는 인증서 확장 필드
- CRL 버전
- 사용되는 CRL 확장 필드

2.9 정책 관리(Policy administration)

정책의 수립, 유지, 해석 등을 책임지는 기관을 정의하는데 사용되는 항목으로 크게 계약 정보, 정책 변경 절차, 정책의 공개의 세 부분으로 나누어진다. 각각의 내용은 〈표 7〉과 같다.

계약 정보에서는 인증 서비스에 대해 문의할 수 있는 담당 부서 및 담당자의 연락처를 기술하고, 정책 변경에서는 CA의 인증 정책이 변경되는 경우 이에 대한 공지 절차를 기술한다. 정책 공개에서는 CA 및 RA가 더 이상 업무를 수행하지 않을 때 취하는 절차 및 CA의

표 7. 정책 관리

내 용	구 분
계약 정보	담당 부서
	담당자
정책 변경	공지가 필요 없는 정책 변경
	공지가 필요한 정책 변경
	새로운 OID가 필요한 정책 변경
정책 공개	정보에 대한 접근 관리
	CA 업무 종료 정책
	RA 업무 종료 정책

정보에 대한 접근 관리 대책 등을 기술한다.

3. 결 론

전자상거래와 함께 인증 서비스가 미래의 정보통신 산업에 중요한 부분이 될 것으로 전망되는 가운데, 미국을 중심으로 한 세계 여러 나라에서는 이미 인증 서비스가 실험 단계를 거쳐 상용화의 단계에 이르고 있다. 또한 우리나라 정부에서도 전자상거래 기본법, 전자서명법 등의 법률을 준비하고 있으며, 본격적인 전자상거래 및 인증 서비스를 위한 환경이 성숙되어가고 있다. 현재 국내에서는 여러 기관에서 인증 서비스를 제공하거나 준비중에 있지만 아직까지는 초보적이고 시험적인 단계라고 할 수 있다.

본 고에서는 인증 서비스에 있어서 매우 중요한 역할을 하는 CPS의 분석을 통해 인증 서비스를 이루고 있는 구성요소들 간의 관계를 정립하고, 이들의 기능을 정의하며, 인증 서비스를 위한 인증 구조 및 절차를 살펴보았다. 이는 안전하고 신뢰성 있는 인증 서비스 제공에 근간이 되는 역할을 할 것으로 기대된다.

인터넷의 급속한 성장과 통신 기술의 발전에 따라 전자상거래의 추진, 전자정부의 구현 등 사회 전 분야의 디지털화가 지속적으로 나타날 것이다. 이에 따라 전자상거래 뿐만 아니라 인터넷의 모든 응용 서비스에서 활용이 기대되는 인증 시스템의 역할이 점차 강조되고 있으며, 안전하고 신뢰성 있는 인증 시스템의 구축이 필수적인 요소로 떠오르고 있어 이에 대한 보다 많은 연구가 필요하다. 이는 안전하고 신뢰할 수 있는 전자상거래 환경의 구축뿐만 아니라 국가안보, 경제 질서, 개인 사생활 등에서 위협이 되는 요인을 제거하는 역할을 할 것이다.

참 고 문 헌

[1] ITU-T Recommendation X.509, The Directory: Authentication Framework, 1993

[2] Digital Signature Guidelines, American Bar Association, 1996

[3] VeriSign CPS, VeriSign, 1997

[4] IETF Internet Draft, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 1998

□ 著者紹介

이 종 후

1997년 충남대학교 컴퓨터과학과 졸업
1997년 ~ 현재 충남대학교 대학원 컴퓨터과학과 석사과정

※ 주관심분야: 컴퓨터 및 통신보안체제, 전자상거래

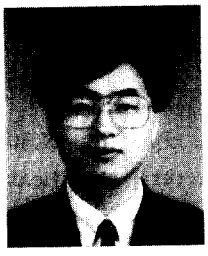
□ 著者紹介

김 지 선

1983년 경북대학교 전자공학과 졸업
1985년 경북대학교 대학원 전자공학과 (공학석사)
1987년 ~ 현재 전자통신 연구원 선임연구원

※ 주관심분야: 전자상거래, 통신망 프로토콜

류 재 철



1985년 한양대학교 산업공학과 졸업
1988년 Iowa State University(전산학 석사)
1990년 Northwestern University (전산학 박사)
1991년 ~ 현재 충남대학교 컴퓨터과학과 부교수

※ 주관심분야: 컴퓨터 및 통신 보안체제, 전자상거래