主題

전자서명 인증기술 동향

한국정보보호센터 이석래, 이재일, 고승철

차 례

요 약

글로벌 정보통신망을 통하여 전자문서 교환 및 전자상거래의 안전·신뢰성을 보장하기 위해서 공개키 기반의 인증서비스가 필요하다. 세계 각국은 자국의 통신 인프라에 대한 안전·신뢰성 보장을 위하여 공개키 기반구조를 구축하고 있다. 글로벌 정보통신망에서 인증기관간의 호환성 유지를 위하여 가장 중요한 기술요소는 인증서 혹은 거래문서에 대한 전자서명을 위한 암호알고리즘, 인증서 및 인증서 폐지목록의 프로파일 규격, 인증서 발급 및 관리를 위한 프로토콜, 인증서의 유효성을 확인할 수 있는 인증서 경로 검증 방법 등이다.

본 논문에서는 IETF PKIX 작업반의 내용을 중심으로 PKI 구현을 위하여 필수적 기술 요소인 인증서 및 CRL 프로파일 규격, 인증서 신청·발급 및 관리에 필요한 프로토콜, 인증서 유효성 검증을 위하여 필요한 기술 등을 우선적으로 다루고 국내외 인증 제품 개발 및 인증서비스 업체의 현황에 대하여 설명하고자 한다.

Ⅰ. 서 론

글로벌 정보통신망을 통하여 전자문서 교환 및 전자상거래의 안전·신뢰성을 보장하기 위해서 공개키기반의 인증서비스가 필요하다. 세계 각국은 자국의 통신 인프라에 대한 안전·신뢰성 보장을 위하여 공개키기반구조를 구축하고 있다.

특히 미국, 캐나다, 호주 등은 컨소시엄 형태로 공개키기반구조(PKI)에 대한 연구 및 구축을 진행하고 있다. 미국은 1994년 공개키 및 공개키 인증서 관리방안에 따라서 NIST(National Institute of Standards and Technology) 주도로 연방 정부의 정보화 자원의 안전한 사용과 국가 정보 인프라의 지원을 위하여 FPKI(Federal PKI)를 구축하고 있다[16]. 캐나다는 Entrust 사의 PKI 제품을 이용하여 GOC-PKI(Government Of Canadian PKI)를 구축 중이고 GOC-PKI와의 상호인증을 위한 방법 및 기준에 대한 논의를 진행하고 있다[18]. 호주는 안전한 전자상거래를 위한 공개키 프레임워크 구현 및 클라이언트들이 하나

의 인증서로 정부와 모든 거래가 가능한 서비스 제공을 목적으로 호주표준기관에서 PKAF TF (Public Key Authentication Framework Task Force)를 구성하여 관련 기술표준을 추진하고 있다[17].

또한 VeriSign, Thawte, Bolero.net, GlobalSign 등은 세계적인 다국적 기업으로 인증서비스를 제공하고 있다. VeriSign과 Thawte는 전자상거래에서 보안, 프라이버시 및 인증 등을 보장하기 위한 디지틀 인증서 제품 및 서비스를 제공하는 세계적인 업체이다. 두 회사는 SSL, S/MIME, VPN 등 크고 작은 비즈니스를 위한 인터넷 신뢰 서비스의 가장 넓은 범위를 제공하고 있다. VeriSign은 미국, 영국, 일본 프랑스, 한국 등 세계 16개국에 18개의 재휴업체를 두고 있는 세계 최대의 인증서비스 업체이다[20, 21]. Bolero.net는 세계 무역망을 인터넷 상으로 옮겨 국제 무역에서 모든 당사자들 사이의 서류 및 정보 교환을 웹 기반으로 지원한다[19]. GlobalSign 은 영국, 독일, 프랑스 등 유럽의 16개국에서 운영되는 국제 인증 네트워크 및 인증서비스를 제공한다[22].

글로벌 환경에서 각 국이 구축한 공개키기반구조를 이용하여 국제 거래 또는 서로다른 도메인간의 인증서비스를 수행하기 위해서는 인증기관간의 상호호환을 위한 상호연동 및 상호인증이 선결되어야 한다. 이러한 문제를 해결하기 위해서는 인증기관간의 기술규격 및 표준을 만들고 그를 준용함으로써 가능하다. 국제 표준화 기구인 ITU-T, 인터넷에 적합한 표준을 개발하는 IETF(Internet Engineering Task Force), 산업체 표준을 추진하는 PKCS(Public-Key Cryptography Standards) 등에서는 공개키기반구조의 상호호환성 유지를 위한 기술규격 및 표준 제정을 위하여 노력하고 있다.

인증서의 상호연동 및 상호인증을 위하여 가장 중요한 기술요소는 인증서 혹은 거래문서에 대한 전자서명을 위한 암호알고리즘, 인증서 및 인증서 폐지목록의 프로파일 규격, 인증서 발급 및 관리를 위한 프로토콜, 인증서의 유효성을 확인할 수 있는 인증서 경로 검증 방법 등이다.

본 논문에서는 IETF PKIX 작업반의 내용을 중심으로 PKI 구현을 위한 필수적인 기술 요소인 인증서 및 CRL(Certificate Revocation List) 프로파일 규격, 인증서 신청·발급 및 관리에 필요한 프로토콜, 인증서 유효성 검증을 위하여 필요한 기술 등을 우선적으로 다루고 국내외 인증 제품 개발 및 인증서비스 업체의 현황에 대하여 설명하고자 한다.

Ⅱ. 전자서명 인증기술 동향

1. 공개키 인증서 규격 표준화 동향

공개키 인증서는 인증서를 사용하고자하는 사용자 정보와 공개키 사이의 관계를 신뢰할 수 있는 인증기관이 디지털로 서명한 것이다. 이 공개키 인증서 규격의 표준화는 ITU-T에서 수행되고 있으며 x.509 권고로 발표되고 있다. 은행, 증권, 보험, 전자상거래 등 인증서의 활용분야가 넓어지고 서로 다른 인증기관에서 발행된 인증서를 검증해야 하는 필요성이 대두되면서 인증서의 규격은 네 번의 변화를 거쳤으며 그 내용은 표 1과 같다.

1988년의 인증서 규격을 버전 1이라 하고 "Signature" 영역을 제외한 나머지 영역을 기본영역이라 한다. 1993년 인증서 규격을 버전 2라고 일컫고 인증서의 기본영역에 발급자(Issuer)와 소유자(Subject)의 UID(Unique Identifier)가 추가되었다. 이 두 영역은 디렉토리 접근 제어를 지원하기 위하여 사용될 수 있다. 그러나 오늘날 디렉토리 접근을 위해서 DN(Distinguished Name) 및 확장영역의 Key Identifier를 사용하기 때문에

표 1. 인증서 규격의 비교

ITU-T X.509(1988)	ITU-T X.509(1993)	ITU-T X.509(1997)	ITU-T X.509(2000)
Version Serial Number Signature Algorithm Issuer Name Validity Subject Name Subject Public Key Info	Version Serial Number Signature Algorithm Issuer Name Validity Subject Name Subject Public Key Info	Version Serial Number Signature Algorithm Issuer Name Validity Subject Name Subject Public Key Info	Version Serial Number Signature Algorithm Issuer Name Validity Subject Name Subject Public Key Info
Signature	Issuer Unique Identifier Subject Unique Identifier	Issuer Unique Identifier Subject Unique Identifier	Issuer Unique Identifier Subject Unique Identifier
	Signature	Extensions(14)	Extensions(16)
		Signature	Signature

이 영역의 사용은 바람직하지 않다. PEM (privacy enhanced mail)의 설계 및 구현시 인증서 규격 버전 1과 버전 2만으로는 여러 관점에서 부족함이 증명되었다. 이러한 새로운 요구사항을 반영하기 위하여 ISO/IEC/ITU와 ANSI X9는 인증서 규격 버전3을 개발하였다. 인증서 규격 버전 3은 버전2에 추가 소유자 확인 정보, 키 속성 정보, 정책 정보, 그리고 인증서 경로 제한 정보 등 14개의 확장영역을 포함하고 있다[12]. 2000년에는 인증서 정책 및 인증서 효력정지 및 폐지정보를 획득하기 위한 방법을 보완하기 위하여 새로 두 개를 확장필드를 추가하여 총 16개의 확장필드를 표준으로 발표하였다[13].

특히, IETF PKIX 작업반에서는 ITU-T x.509를 기반으로 인터넷, 전자메일, IPSec 등의 응용에 적합한 프로파일을 만들기 위한 작업을 진행중이며 1999년 RFC2459(Proposed standard)를 발표하였고 2000년 3월 ITU-T x.509 4번째 판의 발표에 따라서 RFC2459를 일부 개정하여 인터넷 드래프트로 발표하였다[9, 10]. 결과적으로 추가 요구사항이 필요한 환경의 변화에 의해 인증서 프로파일 규격은 개정될 수 있다.

2. 공개키 인증서 효력정지 및 폐지목록 표준화 동향

공개키 인증서는 발급 후에 유효기간 동안 사용 가능하지만 소유자의 이름 변경, 소유자와 인증기관 사이의 관계 변화, 그리고 인증서의 공개키에 대응되는 비밀키의 누설 등 여러 가지 환경의 변화에 의해 유효기간 만료 전에 해당 인증서가 유효하지 않을 수 있다. 이러한 환경의 변화가 발생한 경우 인증기관은 공개키 인증서를 폐지할 필요가 있으며 이를 위하여 x.509에서는 공개키 인증서 폐지 방법을 정의하였다. 이 방법에 의해 인증기관은 주기적으로 인증서의 효력정지 및 폐지사실을 자신의 전자서명 생성키로 전자서명한 인증서 효력정지 및 폐지목록(CRL)을 발급한다. 또한 인증기관은 가입자가 자유롭게 인증서의 폐지 사실을 확인할 수 있도록 CRL을 안전·신뢰성 있는 공개 저장소에 공고한다. CRL의 규격 및 개정과정은 표 2와 같다.

CRL은 세 차례 변경되었으며 1993년 CRL 버전 1을 발표하였고 이어서 확장영역을 추가하여 1997년 CRL 버전 2를 발표하였다[12]. 2000년에는 CRL 버전 2의 확장영역에 CRL의 범주, Base CRL 갱신 영역 등을 포함하여 6개의 확장영역을 추가하였다[13]. 또한 IETF PKIX 작업반은

표 2. 인증서 효력정지 및 폐지목록 규격의 비교

ITU-T X.509(1993)	ITU-T X.509(1997)	ITU-T X.509(2000)
Version	Version	Version
Signature Algorithm	Signature Algorithm	Signature Algorithm
Issuer Name	Issuer Name	Issuer Name
This Update	This Update	This Update
Next Update	Next Update	Next Update
Revoked Certificates	Revoked Certificates	Revoked Certificates
User Certificate	User Certificate	User Certificate
Revocation Date	Revocation Date	Revocation Date
Signature	CRL Entry Extensions(4)	CRL Entry Extensions(4)
	CRL Extensions(5)	CRL Extensions(11)
	Signature	Signature

x.509의 CRL 버전 2를 인터넷 PKI에 적합한 프로파일로 만들기 위하여 11차례의 드래프트 개정을 통하여 1999년에 RFC2459(Proposed Standard)를 발표하였다[9].

3. 인증서 관리 프로토콜 표준화 동향

3.1 인증서 관리 프로토콜의 구성 요소

인증서 관리 프로토콜(CMP: Certificate Management Protocol)은 인증서를 발급하고 발급된 인증서를 사용자에게 전달하는 절차, 인증기관간의 믿음을 확장하기 위한 상호 인증과 관련된 절차, 인증기관이 인증서를 발급받는 최종개체의 공개키에 대응되는 개인키를 소유하고 있음을 증명하는 개인키 소유 증명(POP: Proof of possession) 절차, 인증기관의 암호키 갱신을 위한 절차 등으로 구성된다.

인증서 관리 프로토콜의 구성 시스템은 그림 1과 같이 최종개체에게 인증서를 발행하는 인증기관(CA: Certification Authority), 인증기관의 일부 기능인 신원 확인 기능을 대신하는 등록기관(RA: Registration Authority), 인증기관에게 인증서의 발행을 요구하고 발행된 인증서를 수신하는 최종개체(EE: End Entity), 그리고 인증서와 인증서 폐지목록을 저장하는 저장소(Repository)들로 구성된다[14]. 인증서 관리 프로토콜은 이들

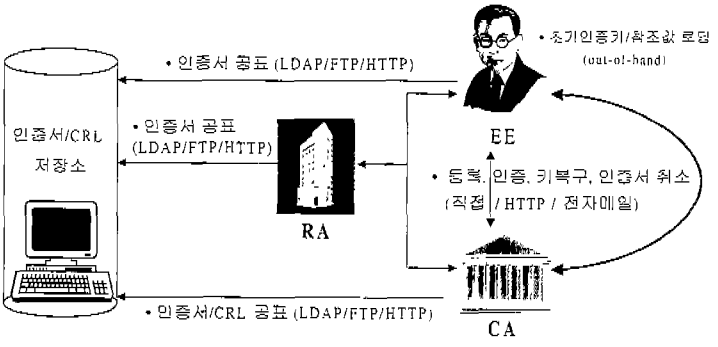

그림 1. 인증서 관리를 위한 요소 시스템

구성 요소간의 인증서의 관리를 위하여 요구되는 다양한 기능과 이를 위한 메시지 형식을 정의하고 있다. 그림 1에서 초기 인증키와 참조값은 인증서 발급시에 필요한 비밀정보로써, 관리 메시지의 무결성 서비스를 제공하기 위하여 최종개체와 인증기관간에 사전에 안전한 방법(out-of-band)으로 공유되는 비밀정보이다.

본 논문에서는 IETF PKIX 작업반에서 제안된 표준들을 근거로 하여 인증서 관리의 주요기능, 초기등록/인증 방법, 개인키 소유증명 등에 내용을 살펴본다.

3.2 인증서 관리를 위한 주요 기능

인증서 관리 주요 기능은 인증기관을 설립하는 기능, 최종개체를 초기화하는 기능, 인증서를 발급받는 기능, 발행된 인증서와 인증서 폐지목록을 확인하기 위한 기능, 최종개체의 암호키의 분실이나 손상으로 인하여 새로운 암호키를 복구하는 암호키 복구 기능, 그리고 생성된 인증서를 폐지하기 위한 인증서 폐지 기능 등으로 구성된다. 또한 인증서 관리는 인증서를 발급 받는 과정, 인증서를 공표하는 과정, 상호 인증서를 요청하는 과정, 그리고 인증기관의 키를 갱신하는 과정 등으로 구성된다.

3.3 초기 등록/인증 방법

IETF에서는 인증서 관리 프로토콜 규격을 RFC2510(Proposed Standard)으로 표준화하였고 최근 일부 내용을 개정하여 인터넷 드래프트(2000. 3)로 발표하였다[3, 4]. RFC2510과 비교하여 인터넷 드래프트에서 가장 큰 변화는 기본 인증 방법을 이용한 초기 등록/인증 방법에서 최종개체가 인증서 수령 후 확인 메시지를 일방적으로 인증기관에 전송하던 프로토콜을 확인 메시지 및 확인 메시지에 대한 인증기관의 응답 메시지로 나누어 교환하는 프로토콜로 변경되었다는 사실이다. 그림 2는 그 차이를 설명한 것이다.

3.4 개인키 소유 증명

인증기관/등록기관은 최종 개체가 인증서에 포함될 공개키에 대응되는 개인키를 가지고 있다는 것을 검증할 수 있다면 여러 가지 공격에 효율적으로 대처할 수 있다. 인증기관이나 등록기관에 의해 개인키의 소유가 증명되지 않고 발행된 인증서는 의미없는 인증서가 될 것이다. 소유 증명은 인증서에 포함될 공개키의 유형(서명용, 암호용, 키일치용)에 따라 여러 가지 방법으로 수행될 수 있다.

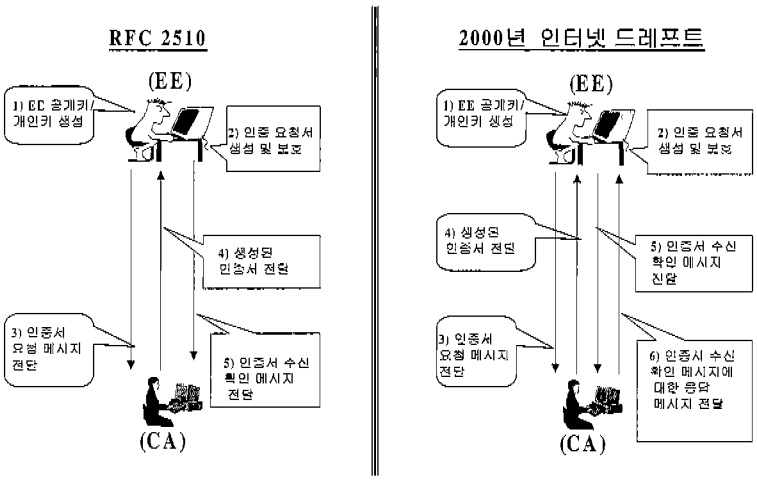

그림 2. 초기 등록 및 인증 방법 비교

4. 인증서 유효성 검증 기술 표준화 동향

인증서 유효성 검증의 첫 번째 목적은 소유자 DN(Distinguished Name) 혹은 소유자 대체 명과 소유자 공개키의 관련성 확인하는 것이다. 이러한 관련성을 확인하기 위해서는 신뢰할 수 있는 인증기관의 공개키를 근거로 하여 인증서 검증 경로를 형성하여야 한다. 인증서 유효성 검증 기술을 설명하기 전에 인증경로에 대하여 설명하고자 한다.

그림 3과 같은 공개키기반구조에서 갑이 을로부터 받은 문서의 전자서명에 대해서 유효성을 검증한다고 생각해보자. 갑은 자신에게 인증서를 발급한 CA1을 신뢰하지만 CA2는 신뢰하지 않는다. 따라서 CA2가 발급한 을의 인증서를 신뢰할 수 없다. 그러나 CA2의 공개키에 대해서는 갑이 신뢰하는 인증기관인 CA1이 인증서를 발급하였기 때문에 갑은 CA2가 을에게 발급한 인증서와 CA1이 CA2에게 발급한 인증서에 대해 유효성 검증을 실시하여 2개의 인증서가 모두 유효할 경우에는 을의 전자서명을 신뢰할 수 있다. 이와 같이 자신이 신뢰하는 인증기관으로부터 발급된 인증서로부터 시작하여 사용자의 인증서까지 형성되는 경로를 인증경로라 하며, 인증경로를 구성하는 인증서들의 유효성을 검증하는 기술을 인증서 유효성 검증이라 한다[15].

이 절에서는 인증서 유효성 검증 방법으로서 IETF PKIX 작업반에서 진행 중인 세가지 방법에 대하여 설명하고자 한다. 첫째 클라이언트에서 직접

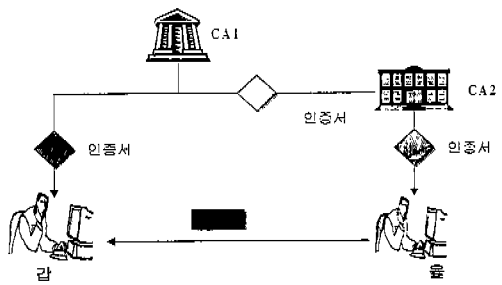

그림 3. 인증경로

수행되는 인증서 경로 검증 절차를 설명하고, 둘째 인증서 경로 검증 방법 중에서 온라인 상에서 인증서의 상태를 검증해 주는 방법을 설명하고, 셋째 단순 인증서 검증 방법에 대하여 설명하고자 한다.

4.1 인증서 경로 검증 절차

인증서 경로검증을 위한 기술은 비록 x.509에 기반하고 있지만 인터넷 분야의 응용에 있어서는 IETF PKIX 작업반의 인증서 경로 검증 기술을 사용하는 흐름으로 변하고 있다. 본 고에서는 2000년 3월에 인터넷 드래프트로 발표된 인증서 경로 검증 절차에 대하여 설명하고자 한다[10]. 인증서 경로 검증 절차는 그림 4와 같다.

인증서 경로 검증 절차는 입력변수 설정에서부터 결과출력까지 6단계로 구성되어 있다. 입력변수 설정에서는 인증서 유효성 검사 과정에서 필요한 예측되는 인증경로 길이, 처리되는 인증서의 유효기간이 인증서 유효성을 결정하는 시점에 포함되었는지를 판단하기 위한 유효성 결정 시점, 사용자가 수용가능한 인증서 정책들을 지정하는 부분, 신뢰할 수 발급자명 및 공개키 정보 등 인증기관의 정보, 인증서 정책 매핑 허용 여부를 나타내는 변수 등과 같은 인증서 정책관련 변수 등을 포함한다. 상태변수 초기화 과정에서는 입력변수 설정과정에서 획득한 신뢰할 수 있는 인증기관 정보 및 예측되는 인증경로 길이를 이용하여 공개키 정보, 인증서 발급자 명, 인증서 검증경로 길이를 초기화하고 인증서 정책과 관련된 6개의 상태변수를 지정된 값으로 초기화한다.

인증서 유효성을 검증하는 실질적인 과정은 지정된 순서의 인증서 유효성을 검증하는 기본 인증서 처리과정, 인증 경로상에서 순차적으로 다음 인증서를 처리하기 위하여 준비하는 상태변수 갱신 과정, 마지막 인증서를 처리하는 과정으로 나눌 수 있다. 기본 인증서 처리 과정에서는 인증서의 전자서명, 인증서 효력정지 및 폐지상태 등을 확인하는 기본 인증서 정보 검증 과정, 인증서 소유자 명과 그 소유

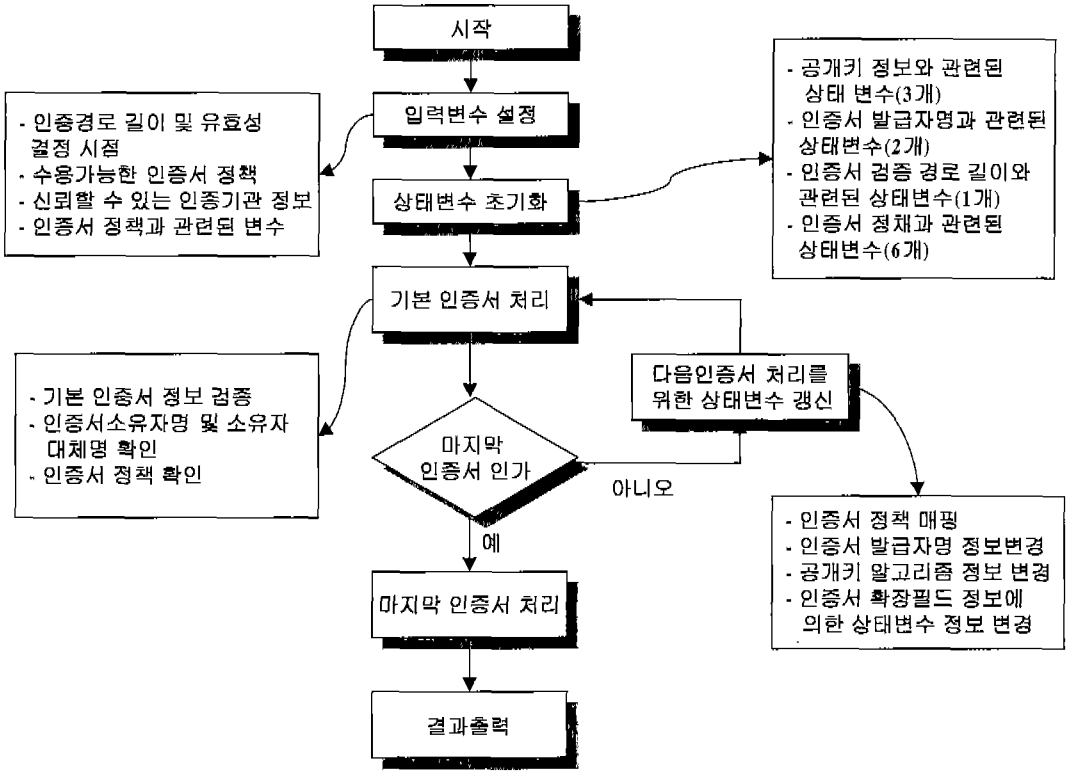

그림 4. 인증서 경로 검증 절차

자의 대체명의 정당성을 확인하는 과정, 인증서의 정책 확장영역과 상태변수로 보유하고 있는 인증서 정책을 이용하여 인증서 정책의 유효성을 검사하는 과정 등을 포함한다. 상태변수 갱신과정에서는 인증서의 정책매핑 확장영역, 유효한 인증서 정책을 지정하는 상태변수 및 인증서 매핑가능여부를 나타내는 상태변수를 이용하여 유효한 인증서 정책을 지정하는 상태변수를 변경하는 인증서 정책 매핑 과정, 기타 상태변수의 정보를 변경하는 과정을 포함한다. 마지막 인증서를 처리하는 과정에서는 사용자가 수용가능한 인증서 정책들과 유효한 인증서 정책을 지정하는 상태변수를 비교하여 마지막 사용자 인증서의 인증서 정책 유효성을 검사하는 부분을 포함한다.

이와 같은 인증서 경로 검증 과정을 통하여 거래 당사자가 전송한 인증서를 받아들일지 여부를 판단하게 된다. 다음 절에서는 인증서 경로 검증에 대한 클라이언트 시스템의 부담을 줄일 수 있는 방법에 대하여 설명하고자 한다.

4.2 온라인 인증서 상태 검증 프로토콜

인증서 경로검증 과정에서 실시간으로 해당 인증기관의 CRL들을 획득하여 인증서의 상태를 검증하는 것은 클라이언트 입장에서 매우 부담스러운 일이다. 따라서 실시간으로 인증서의 상태 정보를 확인할 수 있도록 지원하는 서비스가 필요하며 이러한 서비스를 지원하기 위한 프로토콜이 온라인 인증서 상태 검증 프로토콜(OCSP : Online Certificate Status Protocol)이다[6].

OCSP는 IETF PKIX 작업반에서 1997년 첫 번째 인터넷 드래프트를 제안한 이래 9번의 개정을 통하여 RFC 2560(Proposed Standard:

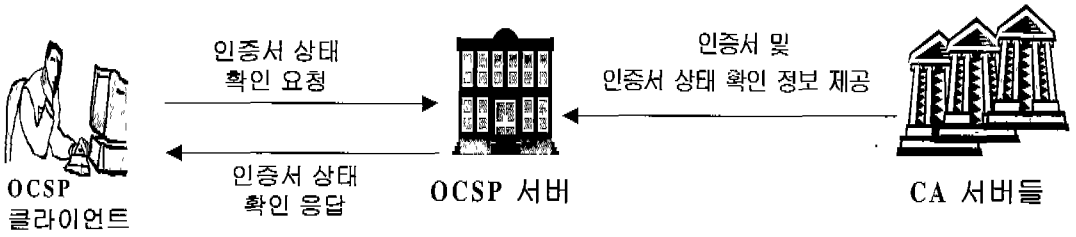

그림 5. 온라인 인증서 상태 검증 프로토콜

1999)으로 발표되었다. OCSP는 OCSP 클라이언트, OCSP 서버, 인증서버로 구성되며 그 관계는 그림 5와 같다. 그림 5에서 OCSP 클라이언트는 거래 당사자 인증서의 유효성 검사를 위하여 OCSP 서버에게 해당 인증서의 상태 확인 정보를 요청하고 그 응답을 얻는다. OCSP 서버는 CA로부터 인증서 상태 정보를 전달받아 이를 관리 유지하며 OCSP 클라이언트에게 해당 정보를 전자서명하여 전달한다. OCSP 서버는 전자서명을 위하여 인증기관에 의해 OCSP 서버용으로 발행된 공개키 인증서를 사용하게 된다. OCSP 서버용 인증서는 확장 영역 중 "Extended Key Usage" 영역에 OCSP 서명용 인증서를 나타내는 아래와 같은 OID (Object Identifier)를 사용하게 된다.

id-kp-OCSPSigning OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechani는(5) pkix(7) kp(3) 9}

OCSP 서버를 이용하여 인증서 상태정보를 획득하는 경우 CRL을 통하는 것보다 더 적시에 폐지정보 획득이 가능하고 고액 자금이체 혹은 대형 주식거래 시에 유용하며 또한 OCSP 서버를 통하여 부가 정보 획득이 가능한 장점이 있다. 다음은 OCSP 서버 구현시 고려사항이다.

- OCSP 서버는 항시 이용할 수 있어야 한다.
- 동시에 대량 인증서 상태 확인 요청이 있는 경우 서비스의 장애가 발생할 수 있다.
- 미리 계산된 응답 사용 시 응답 유효기간동안 인증서가 폐지되었음에도 불구하고 그 응답이 재 사용될 가능성이 있다.
- 상태 확인 요청에 응답 OCSP 서버의 정보가 포함하여 있지 않기 때문에 하나의 요청이 많은 OCSP 서버에 재 사용될 수 있다.

4.3 단순 인증서 검증 프로토콜

인증서는 다양한 응용 및 환경의 어플리케이션에서 널리 사용될 수 있다. 각 어플리케이션은 상대방 인증서를 받아들이기 전에 인증서 유효성을 확인하여야 만 한다. 그러나 인증서의 유효성을 확인하기 위해서는 많은 처리를 필요로 하기 때문에 어플리케이션은 인증서 검증에 대한 과다한 부담을 가지게 된다. 또한 인증서 유효성을 확인할 수 있는 능력은 있지만 상대방 인증서부터 신뢰된 인증서까지 모든 인증서를 획득할 믿을 만한 방법이 없는 어플리케이션도 존재한다.

SCVP 프로토콜은 SCVP 서버를 이용하여 인증서 처리에 대한 클라이언트의 부담을 줄이는 것이다. SCVP 서버는 인증서의 유효성 혹은 신뢰할 수 있는 인증서까지의 인증경로 등 인증서에 관한 가치 있는 다양한 정보를 줄 수 있다. SCVP는 클라이언트의 구현을 단순화시키고 기업 내에서 신뢰 및 정책관리를 중앙 집중식으로 처리할 수 있도록 허용하는 등의 목적이 있다. 따라서 SCVP는 두 가지 목적으로 사용될 수 있다. 처째는 스스로 대부분의 PKI 처리를 수행하고 단순히 정보 수집을 위하여

유용하지만 신뢰하지 않는 서버를 필요로 하는 클라이언트에 의해 사용된다. 둘째는 인증서 검증에 대한 부담을 덜고 한 기업내에서 일치된 형태의 정책이 반영된 충분히 신뢰성 있는 서버를 필요로 하는 클라이언트에 의해 사용될 수 있다.

첫 번째 SCVP 서버는 고객에게 경로 검증을 위한 인증서 경로 정보를 제공하고 CRL 및 OCSP 응답과 같이 고객의 경로검증에 필요한 폐지정보를 제공한다. 이러한 서비스는 전체 경로 검증을 위하여 필요한 매개 인증서, CRLs 및 OCSP 응답 등을 찾아서 다운로드하는 프로토콜을 지원하지 않는 고객 시스템에서 도움이 된다. 두 번째 SCVP 서버는 클라이언트를 위하여 충분한 인증서 검증을 수행한다. 클라이언트가 이 서비스를 사용하는 경우 SCVP 서버를 자신이 소유한 경로 검증 소프트웨어와 동일한 수준으로 신뢰해야 한다.

SCVP는 IETF PKIX 작업반에서 첫 번째 인터넷 드래프트를 제안하였고 2000년 3월 세 번째 드래프트가 제안된 상태이다[2]. SCVP의 구성요소는 SCVP 클라이언트, SCVP 서버, CA 서버로 구성된다. SCVP 클라이언트는 경로검증이나 폐지상태 등을 확인하고자하는 정보를 포함한 요청을 SCVP 서버로 전송한다. SCVP 서버는 요청된 내용의 결과를 SCVP 서버의 전자서명생성키로 전자서명한 응답을 SCVP 클라이언트에 전송한다.

5. 국외 인증기술 개발 동향

인증서비스에 필요한 PKI 제품은 CA, RA, 디렉토리, 클라이언트 등으로 구성된다. 국외에는 캐나다의 Entrust, 미국의 Baltimore를 비롯하여 많은 PKI 제품 개발업체들이 있으며 이러한 업체들은 공개키기반구조(Public Key Infrastructure) 구축을 위한 토탈 솔루션을 제공하고 있다. 또한, SSL, S/MIME, OFX, SET, IPSec 등의 응용에서 인증서 발급이 가능하도록 다양한 PKI 제품을 제공하고 있다. PKI 제품 개발하는 대표적인 업체는 표 3과 같다.

표 3. 국외 PKI 개발 업체 동향

국 가	업체명	제품명
캐나다	Entrust Tech.	Entrust/PKI5.0
	Xcert	Sentry CA 4.0
미 국	GlobeSet	GlobeSet CA
	Certco	CertAuthority 3.0
	Baltimore	UniCert v3.0.5
아일랜드	Siemens	Trusted CA 2.14

※ http://www.pca.dfn.de/dfnpca/pki-links.html
http://www.qmw ac.uk/~tl6345/ca.html

표 4. 국외 인증 서비스 제공업체 현황

국 가	회사명	홈페이지
미국	DST	http://www.digsigtrust.com/
	ARCANVS	http://www.arcanvs.com/
	USER Trust	http://www.usertrust.com/
	VeriSign	http://www.verisign.com
	ID Certify	http://www.idcertify.com/
독일	Deutche Telekom	http://srv15.telesec.de/
	Deutche Post	http://www.signtrust.deutchepost.de/
	TC Trust Center	http://www.trustcenter.de/
	IKS CA	http://www.iks-jena.de/
영국	Trustwise	http://www.trustwise com/
프랑스	Certplus	http://www.certplus com/
	Thawte Francophone	http://www.fr.thawte.com/
오스트리아	a-sign	http://a-sign.datakom.a/
	globalsign	http://www.globalsign.at/
일본	VeriSign Japan	http://www.verisign.co.jp/
	Thawte	http://www.jp.thawte.com/
	CA Japan	
대만	HiTRUST	http://www hitrust.com.tw/
말레이지아	Digicert	http://www.digicert com.my/
	mTrust	http://www.mtrust.com.my/
남아공	SACA	https://www.saca.net/
	Thawte	http://www.thawte.com/

Global 서비스 업체인 VeriSign 및 Thawte, 유럽지역에서 Global 네트워크를 형성하고 있는 GlobalSign, 국제 무역거래의 인증업무를 수행하는 Bolero.net 등을 비롯하여 다수의 인증서비스 업체들이 있다. 특히 미국의 경우 현재 유타 주 정부에서는 4개의 공인인증기관(DST, Arcanvs, USERTrust, VeriSign), 워싱턴 주 정부에서는 3개의 공인인증기관(VeriSign, ID Certify, Arcanvs) 등을 운영하고 있으며 그 외의 몇몇 주 정부에서도 공인인증기관을 운영하고 있다. 공인인증기관을 운영하는 미국, 독일을 비롯하여 인증서비스를 수행하는 나라와 인증기관은 표 4와 같다.

Ⅲ. 국내 전자서명 인증기술 현황

1. 전자서명 인증관리체계 기술 현황

국내에서는 전자서명법(1999. 2), 동법 시행령(1999. 6) 및 시행규칙(1999. 8)을 제정하여 정보통신망을 통한 비대면 전자문서 교환 및 전자상거래의 안전·신뢰성 확보를 위한 국가차원의 전자서명 인증제도를 마련하였다. 공개키기반구조(Public Key Infrastructure)에 기반한 국내 전자서명 인증관리체계의 구축·운영, 공인인증기관에 대한 인증서 발급 및 관리 등의 인증업무, 그리고 전자서명 인증기술의 개발 및 규격·표준화를 목적으로 한국정보보호센터내에 국가 최상위 인증기관인 전자서명인증관리센터가 출범하였다(1999년 7월).

한국정보보호센터는 임무와 역할에 따라 국내 전자서명 인증관리체계의 인증업무 수행에 필요한 전자서명 알고리즘(KCDSA), 해쉬함수(HAS-160), 블록암호알고리즘(SEED), DN(Distinguished Name), OID(Object identifier) 등의 기술규격을 정립하고 키생성시스템, 인증서 생성·관리시스템, 등록관리시스템 등을 자체 개발하였다.

또한, 한국정보보호센터에서는 인증기관사이의 인증서 생성 및 인증서 처리에 대한 상호 연동성을 보장하고 국제적인 호환성을 유지하기 위하여 전자서명용 인증서 프로파일에 대한 규격을 정의하고 국내 표준화를 추진하고 있다. 현재 전자서명 인증관리체계내의 인증서 프로파일 표준(안)은 인증기관 인증서, 가입자용 인증서, 시점확인용 인증서로 나누어진다.

2. 국내 인증서버 현황

국내 개발 업체들은 현재 SSL이나 S/MIME용 인증서 발급이 가능한 인증서버(CA 서버)를 개발한 상태이며, 아직까지는 다양한 인증서 발급 서비스(예:IPSEC, OFX 등)들을 지원하는 인증서버는 개발되지 않은 상태이다. 현재 국내 인증서버 개발 현황은 시장 형성 초기 단계를 지나고 있다. 표 5은 국내의 대표적인 인증서버 개발업체 및 제품명이다. 이 이외에도 많은 국내 업체들이 인증서버 및 인증관련 기술개발을 위해 노력하고 있다.

표 5. 국내 PKI 개발 업체 현황

업체명	제품명
소프트포럼	SFCA V3.0 SPKI
이니텍	이니텍 CA V1.0
삼성SDS(SECUI.COM)	TrustPro 2.0
장미디어인터렉티브	JCA Server V2.1
펜타시큐리티	ISSAC
세넥스	Assure Web CA
시큐어소프트	SecurePKI
케이사인	KSignPKI

전자서명 인증제도에 따라서 2000년 8월 현재 3개 기관이 공인인증기관으로 지정되었고 일반 전자거래분야, 증권거래분야, 은행거래분야, 공공분야 등에서 공인인증서를 이용한 서비스를 진행중이다.

표 6. 공인인증기관 지정 현황

업 체	지정일
한국정보인증(주)	2000. 2. 10
한국증권전산(주)	2000. 2. 10
금융결제원	2000. 4. 12

Ⅳ. 결 론

현재 국내 전자서명 인증관리체계는 한국정보보호센터를 중심으로 국제 기술 규격 및 표준을 준용하여 공인인증기관들 사이의 공개키 인증서의 상호연동성을 보장하기 위하여 노력하고 있다. 그러나 국내에는 많은 PKI 제품업체들이 존재하고 그들은 제각기 서로 다른 시각에서 국제 기술규격 및 표준을 준용하고 있기 때문에 서로간의 호환성 유지가 어려운 상태이다. 따라서 한국정보보호센터 및 인터넷 보안기술 포럼 등을 통하여 국내 기술규격 및 표준화를 추진해야 할 것이다.

또한, 향후 국경 없는 사이버공간에서 국내 전자상거래 시장이 세계 시장으로 진출할 수 있도록 국가간의 전자서명 상호인증을 조속히 추진하여야 하며, 이를 위해 국가간 상호인증을 위한 상호협력 방안 및 관련 기술의 개발을 통하여 국제 전자상거래 시장을 선점하도록 하여야 한다. 이러한 요구를 만족시키기 위해서는 첫째, 상호인증 관련 국제 표준화 기구활동 및 PKI 관련 포럼 등에 적극 참여하여 국제적인 기술 규격에 대한 동향을 파악하고 국내실정에 맞는 기술 요구사항을 적극적으로 반영하여야 하며, 둘째, 국외 상호인증 기술에 대한 최신 기술을 분석하여 국가 최상위인증기관 및 인증기관과의 상호인증 실현에 필요한 다양한 프로토콜 및 소프트웨어를 개발하여야 하며, 셋째, 실제 국가간 상호인증용 시스템을 구축하여 실증 프로젝트를 수행함으로써 국가간의 파트너쉽을 만들어나가는 등의 국가적인 차원의 체계적인 기술개발 노력이 절실히 필요하다.

따라서, 국내 전자서명 인증관리체계의 인증시스템간의 호환성을 보장하기 위해서는 인증서 관리 프로토콜, 데이터 검증 및 인증 서비스, 시점확인 서비스 등 새로운 인증기술 및 서비스에 대하여 상호호환성 시험을 위한 환경 구축을 통한 관련 기술 규격 · 표준화를 지속적으로 추진해야 한다. 또한 국외 전자서명 인증기관과의 상호협력을 통하여 상호인증을 위한 기술적 · 정책적 토대를 만들어야 할 것이다.

※참고문헌

[1] A. Arsenault, S. Turner, "Internet X.509 Public Key Infrastructure PKIX Roadmap", *IETF PKIX Internet-Draft*, March 10, 2000

[2] Ambarish Malpani, Paul Hoffman, "Simple Certificate Validation Protocol(SCVP)", *IETF PKIX Internet-Draft*, June 12, 2000

[3] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", *IETF PKIX RFC2510*, March. 1999.

[4] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", *IETF PKIX Internet-Draft*, March. 2000.

[5] M. Myers, C. Adams, D. Solo, D. Kemp, "Internet X.509 Certificate Request Message Format", *IETF PKIX RFC2511*, March. 1999.

[6] M. Myers, R. Ankney, A. Malpani, S.Galperin, C. Adams, "Internet X.

509 Public Key Infrastructure Online Certificate Status Protocol-OCSP", *IETF PKIX RFC 2560*, June, 1999

[7] M.Wahl, A.Coulbeck, T.Howes, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", *IETF PKIX RFC2252*, Dec. 1997.

[8] M.Wahl, T.Howes, S.Kille, "Lightweight Directory Access Protocol (v 3)", *IETF PKIX RFC2251*, Dec. 1997.

[9] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", *IETF PKIX RFC2459*, Jan. 1999.

[10] R. Housley, W. Ford, W. Polk, D. Solo, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile", *IETF PKIX Internet-Draft*, March, 2000

[11] S. Chokhani, W. Ford, "Internet Public Key Infrastructure. Certificate Policy and Certification Practies Framework", *ETF PKIX Internet-Draft*, Sep. 30, 1997

[12] ITU-T Recommandation X.509 (1997)| ISO/ IEC 9594-8:1997, "Information technology-Open Systems Interconnection-The Directory :Authectication Framework", August, 1997.

[13] Draft Revised ISO/IEC-9594-8, "ITU-T Recommandation X.509| ISO/ IEC 9594-8:, Information technology-Open Systems Interconnection-The Directory :Public-Key and Attribute Certificate Frameworks", March, 2000.

[14] 염흥렬, "인증서 관리 프로토콜의 표준화 동향", *한국정보보호센터 정보보호뉴스*, 8월호, pp. 26-28, 2000. 8.

[15] 류재철, "인증서 확인 검증 기술 표준화 동향", *한국정보보호센터 정보보호뉴스* 4월호, pp21-22, 2000. 4.

[16] http://csrc.nist.gov/pki/

[17] http://www.standards.com.au

[18] http://www.cio-dpi.gc.ca/pki/home_e.html

[19] http://www.bolero.net

[20] http://www.verisign.com

[21] http://www.thawte.com

[22] http://www.globalSign.com

이 재 일

1986년 서울대학교 계산통계학과 졸업
1988년 서울대학교 계산통계학과 석사
1999년~현재 연세대학교 컴퓨터과학과 박사과정
1991년~1996년 한국 IBM
1996년~현재 한국정보보호센터 선임연구원/팀장
관심분야 : 유·무선 PKI, 전자상거래 보안

고 승 철

1981년 연세대학교 졸업
1983년 연세대학교 이학석사
1992년 포항공대 이학박사
1984년~1996년 한국전자통신연구소 책임연구원
1996년~현재 한국정보보호센터 책임연구원/부장
1999년~현재 광운대학교 전산과학과 겸직교수
관심분야 : 침입탐지시스템, 전자서명기술

이 석 래

1992년 한양대학교 전자통신공학과 졸업
1994년 한양대학교 전자통신공학과 석사
1994년~1999년 LG 전자
1999년~현재 한국정보보호센터 연구원
관심분야 : 데이터 보안, 통신공학