情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

PKI 표준화 동향과 PKI 영역간 상호 연동 방법

염 흥 열*

요 약

공개키 기반구조는 공개키 알고리즘을 이용하여 정보보호 서비스를 제공하는 정보처리 및 정보통신시스템에서 사용자 공개키의 무결성과 인증성을 제공하기 위한 중요한 기반 서비스이다. 공개키에 대한 무결성을 제공하기 위해서는 전자서명이 요구되며, 인증성을 제공하기 위해서는 제3의 신뢰기관이 요구된다. 제3의 신뢰기관이 통칭 인증기관이다. 사용자는 인증서를 이용하여 응용에게 공개키의 무결성과 인증성을 알려주며, 응용은 인증서에 포함되어 있는 공개키를 이용하여 정보통신 시스템에서 다양한 정보보호 서비스를 실현한다. 인증서 정책은 하나의 인증서를 특정 응용에 적용 가능한지를 알려주기 위한 법칙들의 집합이라고 될 수 있다. PKI 영역(Domain)은 하나의 통일되고 합의된 인증서 정책으로 구현되는 인증기관들과 사용자들의 집합이라고 볼 수 있다. PKI 응용 영역간의 상호 연동은 PKI 서비스를 확장하기 위하여 중요한 기술이다. 본 고에서는 PKI 영역간 상호 연동을 위한 공개키 기반구조의 개요와 필요성 등을 기술하고, IETF PKIX의 공개키 기반구조 표준화 동향을 분석하며, 상호 연동을 위하여 요구되는 인증서 정책과 인증서 확장자를 살펴보고, 대표적인 주요 인증서 정책들을 분석하며, 최근 PKI 포럼에서 연구된 PKI 영역간 상호 연동 방식을 살펴보고, 마지막으로 상호 연동 방식간의 특징과 장단점을 제시한다.

Ⅰ. 서 론

인터넷을 통한 전자거래는 온라인 뱅킹, 온라인 쇼핑, 온라인 주식거래, 기업간 응용, 전자지불 등이 있다. 인터넷은 근본적으로 보안이 고려되어 있지 않다. 또한 무선인터넷을 통한 정보교류나 전자거래도 수행되고 있고, 그 수요가 급증할 것으로 예측된다. 그러나 무선인터넷은 유선인터넷보다 보안에 더 취약하다고 알려져 있다. 따라서 유선은 물론 무선 인터넷을 통한 전자거래에도 정보보호 기술의 적용이 요구되고 있다.

공개키기반구조는 정보처리시스템 및 정보통신시스템의 안전성과 신뢰성을 제공하기 위한 중요한 기반 기술로써, 사용자에게 특정 클라이언트의 공개키에 대한 무결성과 인증성을 제공하기 위한 기술이다. 여기서 무결성은 공개키의 내용이 변경되지 않았음을 확인하며, 인증성은 공개키가 특정 사용자의 진정한 소유임을 확인한다. 공개키기반구조(PKI : Public Key Infrastructure)는 기본적으로 암호시스템 및 서명시스템에서 요구되는 사용자 공개키의 무결성을 보장하기 위하여 인증기관에 의하여 발행되는 인증서에 바탕을 두고 있다. 따라서 공개키 기반구조는 고객에게 인증서를 발행하고, 발행된 인증서를 신뢰 당사자에게 분배하며, 발행된 인증서를 취소하고, 인증서취소목록(CRL : Certificate Revocation List)을 발행하며, 인증서와 인증서취소목록을 공개하고, 신뢰의 확장을 위하여 인증기관간의 상호 인증서를 발행하는 기능 등을 수행하기 위한 정보보호 서비스 제공을 위한 기반기술이다[1-3].

PKI 인증서 정책(CP : Certificate Policy)은 하나의 인증서를 하나의 특정 응용에 적용 가능한가를 나타내는 법칙들의 집합이라고 할 수 있다. PKI 영역은 하나의 통일된 인증서 정책으로 구현된 인증기관들과 관련 개체들의 집합이라고 볼 수 있다. PKI 응용 영역간의 상호 연동은 PKI서비스를 확장하기 위한 중요한 기술로 최근에 대두되고 있다. PKI 상호 연동을 위해서는 상호 연동을 위한 통일되고 합의된 기준이 필요하며, 이 기준 중의 하나가 인증서 정책이다. 인증서 정책을 구체적으로 실현하기 위하여 인증기관이 채용한 업무 준칙이 인

* 순천향대학교 공과대학 정보보호학과 (hyyoum@sch.ac.kr)

증업무준칙(CPS:Certification Practice Statement)이다. 인증업무준칙은 각 조직이나 인증기관 단위로 운영되며, 비밀로 유지될 수 있다. 인증업무준칙의 이러한 특성은 인증업무준칙을 PKI 영역간 상호 연동의 기준으로 활용할 수 없음을 함축적으로 나타내고 있다.

또한 우리는 이미 민간 금융 및 전자상거래 분야의 공개키기반구조를 구축 완료했고, 현재는 정부 공개키 기반구조를 구축하고 있다. 기본적으로 민간분야 공개키기반구조를 NPKI(National Public Key Infrastructure)라고 통칭하고, 정부 공개키 기반구조는 GPKI (Government PKI)라고 통칭한다. 따라서 NPKI와 GPKI는 각각 서로 다른 인증서 정책으로 인증서를 발행하고 관리할 것이다. 그런데 정부와 민간분야의 거래 및 민원 서비스를 위해서는 인증서를 이용해야 하고, 이는 필연적으로 상대 영역에서 발행된 인증서를 이용하여 수행되어야 하며, 이는 상대 영역에서 다른 영역에서 발행된 인증서의 유효성을 검증하는 과정이 요구된다. 결국, 영역간 상호 연동(Interoperability)이 요구됨을 의미한다. 예를 들어, 민간이 정부로 전자 서명문을 보낼 수 있고, 반대로 정부가 민간으로 전자서명문을 보낼 수 있다. 이때 전자정부의 응용은 어떻게 민간분야의 공인 인증기관에서 발행된 인증서에 대하여 인증서의 유효성(인증서 수용 여부, 인증서 유효성 검증 여부 등)을 검증해야 하느냐에 대한 문제에 당면하게 될 수 있다. 이를 해결하기 위한 기술이 PKI영역간 상호 연동 기술이라고 할 수 있다.

본 고에서는 PKI영역간 상호 연동을 위한 공개키 기반구조의 개요와 필요성 등을 제시하고, IETF PKIX의 공개키기반구조 표준화 동향을 분석하며, 상호 연동을 위하여 요구되는 인증서 정책과 인증서 확장자를 살펴보고, 주요 인증서 정책을 분석하며, 최근 PKI포럼에서 연구된 PKI영역간 상호 연동 방식을 살펴보며, 마지막으로 상호 연동 방식간의 특징과 장단점을 제시한다.

II. 공개키 기반 구조 개요 및 상호 연동을 위한 요소 기술

2.1 인증서의 필요성

전자서명은 기본적으로 공개키 암호기술을 이용한다. 따라서 전자서명의 안전성을 공개키 암호기술의 안전성과 키관리 기술에 의존한다. 공개키 암호시스템을 이용하는 사용자는 공개키와 개인키로 구성되는 암호키 쌍을 생성하고, 공개키는 전화번호부와 같은 공개키 디렉토리에 저장하여 다른 사용자들이 액세스할 수 있도록 하며, 개인키는 비밀스럽고 안전하게 보관해야 한다. 공개키 암호시스템은 비밀통신을 목적으로 하는 암호시스템과, 메시지 변경 및 진위 여부의 확인과 부인방지를 목적으로 하는 전자서명시스템에서 널리 사용된다. 실제로 대부분의 정보보호시스템은 공개키 암호시스템을 사용하고 있다. 공개키 암호시스템을 위한 공개키는 디렉토리에 저장되어 있으며, 특정 사용자의 신분 정보와 연계되어 저장되어야 한다. 공개키는 암호문을 전송하고자 하는 사용자가 평문을 암호문으로 변환하는 암호화 과정에서 사용하며, 개인키는 암호문으로부터 평문으로 복구하기 위한 복호화 과정에서 사용된다.

전자서명시스템은 수신자가 특정의 메시지가 자신이 보냈다고 주장하는 사용자로부터 전송되었음을 증명하고, 메시지의 내용이 변경되지 않았음을 확인하며, 추후에 전송사실의 부인을 방지하기 위하여 사용된다. 다시 말해 서명시스템은 메시지에 대한 인증 기능, 무결성 기능, 그리고 부인방지 기능을 제공한다. 서명시스템인 경우 송신자는 개인키를 이용하여 특정의 메시지에 대한 서명문을 구한 뒤 수신자에게 원본 메시지와 서명문을 함께 보내면, 수신자는 공개키 디렉토리에서 송신자의 공개키를 구하여 서명문의 유효성을 검증한다.

그러나 공개키가 디렉토리에 저장되어 있다고 해도 사용자의 공개키가 적절하지 않게 관리되면 아무리 강력한 암호시스템을 채용한 정보시스템도 안전성과 신뢰성을 보장받을 수 없다. 공개키가 사용자의 신분 정보와 암호학적으로 안전하게 결합되어 있지 않으며, Man-in-the-middle 공격에 취약하여 전체 암호시스템의 안전성에 커다란 영향을 준다는 사실에 근거한다. 다시 말해, 사용자 공개키와 사용자 신분 정보가 긴밀하게 결합되어 있어야 한다는 것을 의미한다. 공개키기반구조 기술은 공개키 디렉토리에 저장되어 있는 사용자의 공개키의 안전성과 신뢰성을 보장하기 위하여 필요하며, 암호시스템을 채용한 모든 정보시스템의 기반 기술이다. 이 의미는 공개키기반구조가 먼저 구축되어야 사용자 및 메시지 인증 문제, 정보의 비밀성을 보장하기 위한 기밀성 문제, 그리고 전달된 메시지의 변경 여부를 확인하기 위한 전자서명 문제를 해결 할 수 있다는 것

이다. 공개키기반구조는 사이버 공간에서 전자적인 신분증과 같은 역할을 수행하는 공개키 인증서(Public Key Certificate)에 바탕을 두고 있다. 인증서는 기본적으로 모든 사용자가 신뢰하는 제삼의 기관으로부터 발행되어야 한다. 공개키기반구조는 제3의 기관인 인증기관이 발행하는 인증서에 바탕을 두며, 인증서는 기본적으로 사용자의 공개키와 사용자의 신분 정보, 인증서의 유효기간, 그리고 인증기관이 생성한 서명문으로 구성된다.

2.2 인증서와 인증서취소목록 내용

실세계에서 일반시민은 여권으로 신분을 확인받는데, 신분 확인정보는 이름, 생년월일, 사진, 서명, 발행국, 여권 일련번호, 여권 발행일시, 여권 유효기간, 공무원 서명, 패이지 번호 등이다. 인증서도 이와 비슷한 정보를 담고 있으며, 공무원의 서명 또는 공공기관의 도장이 인증기관의 서명문과 등가의 기능을 수행한다. 인증서에는 사용자 공개키(RSA 서명용 공개키)와 신분확인 정보(예를 들어, 전자메일 주소와 DN:Distinguished Name), 인증기관 정보, 정책 제한 및 이름 제한 등을 처리하기 위한 확장 필드, 그리고 인증기관의 서명문 등으로 구성된 복잡한 데이터 구조이다. 인증기관에 의한 서명문은 인증서의 유효성을 확인하기 위한 필드이다. 따라서 인증서 사용자는 인증기관이 발행한 서명문을 검증하기 위한 인증기관의 서명 검증용 공개키를 안전한 방법으로 인증기관으로부터 사전에 분배받아야 인증서의 유효성을 검증할 수 있다. 인증서는 RSA 등의 디지털 서명기술, SHA-1 알고리즘 등의 해쉬 기술, 그리고 DER(Distinguished Encoding Rule) 등의 부호화 기술 등이 적용되어 생성된다. 따라서 인증서를 생성하기 위해서는 반드시 해쉬 알고리즘과 서명 알고리즘, 그 외 다양한 요소 기술들이 요구되게 된다[4,26-27].

사용자의 개인키가 손상되거나 사용자의 직장이 변경되거나 이름이 변경되면, 해당 사용자 인증서는 유효기간이 경과하기 전이라도 인증기관에 의하여 취소되어야 한다. 따라서 인증기관은 자신이 발행한 인증서 중에서 특정 시점까지 유효기간이 경과되지 않은 취소된 인증서취소목록(CRL : Certificate Revocation List)을 공개 디렉토리로 공개하여 다른 신뢰 당사자가 취소된 인증서를 사용하지 말도록 해야 한다. 인증서취소목록은 서명 알고리즘의 종류, 인증기관 정보, 발행 일시, 취소된 인증서의 일련번호/취소 사유/조치사항 등을 포함한 취소된 인증서 관련 정보, 그리고 인증기관에 의하여 생성된 서명문으로 구성된다.

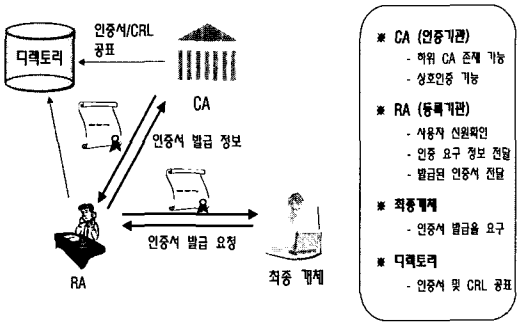
2.3 인증서의 일생

공개키기반구조는 인증서의 일생을 관리하는 역할을 수행한다. 따라서 인증서의 일생을 살펴보면 공개키기반구조의 주요 기능을 알 수 있다. 인증서 일생은 인증서를 발행하는 초기화 단계, 인증서를 사용하기 위한 동작 단계, 인증서 사용을 중단하기 위한 동작 중단 단계로 구성된다. 초기화 단계는 고객이 인증기관으로부터 인증서를 발행받고, 발행된 인증서를 고객에게 전달하기 위한 과정으로써, 다시 등록 과정, 인증 과정, 그리고 분배 과정으로 구성된다. 등록 과정은 인증서를 발행받기를 원하는 주체가 인증기관 또는 등록기관과 접촉하여 자신의 신원을 확인하고, 인증서 발행에 필요한 데이터를 수집하고 생성하며, 인증기관이 자신의 키를 최종 개체에게 안전하게 전달하고, 사용자가 자신의 키쌍을 생성하며 생성된 개인키를 안전하게 저장하는 기능과 관련된다. 인증 과정은 인증기관에 의하여 인증서를 발행하는 과정이다. 인증 과정은 인증기관에 의하여 주로 수행된다. 분배 과정은 최종 개체로 발행된 인증서를 전달하고, 디렉토리 형태의 저장소에 발행된 인증서를 공개하는 업무와 연관된다. 동작 단계는 통신 당사자의 인증서를 검색하고, 수신된 인증서 유효성을 검증하며, 키와 인증서를 다시 갱신받는 기능을 갖는다. 인증서 검색은 통신 주체가 자신이 원하는 인증서를 디렉토리에서 검색하며, 인증서의 유효성 검증은 인증서의 내용을 검사하고 인증 경로를 구성하며 인증 경로의 유효성을 검증하며, 인증서 취소 상태를 검증한다. 인증서 갱신은 기존의 키를 이용하여 새로운 인증서를 생성하는 과정을 포함한다. 동작 중단 과정은 인증서의 유효기간이 경과되거나, 키 손상, 인증서 내용의 변경, 최종 개체와 인증기관간의 신뢰 관계의 중단 등으로 인하여 이미 발행된 인증서에 취소 사유가 발생하여 유효 기간이 만료하기 전에 인증서를 취소해야 하는 기능과 관련된다.

2.4 공개키 기반구조 체계를 위한 구성 시스템

공개키 기반구조 체계를 위한 구성 시스템은 그림

1과 같이 인증서를 발행하고 발행된 인증서의 취소를 공표하기 위하여 인증서취소목록을 발행하는 인증기관(CA : Certificate Authority), 인증서를 인증기관으로부터 발행 받기를 원하는 최종 개체의 신분을 확인하는 등록기관(RA : Registration Authority), 공개키 인증서에서 주체이며 암호키 소유자인 최종 개체, 그리고 인증서와 인증서취소목록을 공개하고 분배하기 위한 디렉토리 등으로 구성된다. 우리나라 인터넷 뱅킹의 경우, 인증기관은 금융결제원이며, 등록기관은 은행이다.



〔그림 1〕 공개키 기반구조 구성 시스템

2.5 공개키 기반구조 제품 동향 및 구축 현황

미국의 공개키 기반구조를 살펴보면 정부기관 및 주 정부 차원의 공개키기반구조 구축을 완료하였고, 현재는 연방 정부, 주 정부, 그리고 민간 분야의 공개키 기반구조 간의 상호 연동이 가능하게 하기 위한 PKI 영역간 상호 연동방안이 마련하였으며, 브리지 인증기관을 이용하여 영역간 상호 연동 시험을 추진 완료한 바 있다.

우리의 공개키기반구조 체계를 살펴보면, 행정자치부가 주관하고 있는 전자정부를 위한 공개키기반구조 체계(전자관인 체계라고 명명되고 있음)와 정보통신부가 주도하고 있는 유무선인터넷을 망라한 전자서명인증 체계인 NPKI(National PKI) 체계로 구분되어 추진되고 있다. 1999년 7월에 발효된 전자서명법에 기초를 두고 구축된 NPKI 체계에서는 한국정보보호진흥원의 최상위 인증기관을 정점으로, 산하에 일반 전자 거래 분야를 담당하는 정보인증(주), 증권 분야를 위한 (주)증권전산, 인터넷 뱅킹 분야를 위한 금융결제원, 그리고 공공 영역의 인증서 발급 업무를 전담하고 있는 한국전산원, 전자상거래를 위한 한국전자인증, 무역망을 위한 한국무역정보통신 등의 6개의 공인 인증기관들로 구성되어 있다. 국내 공인 인증기관간의 영역 구분은 상호 연동이 가능한 인증서의 도입으로 점차로 희미해질 전망이다. 이는 인터넷 뱅킹을 이용한 인증서로 금결원 이외의 다른 공인 인증기관에서 발행된 인증서를 사용 가능토록 하는 정부의 상호 연동 확대 정책에 기인하고 있다. 현재 이용 가능한 공개키 기반구조 제품, 인증 서비스 기관, 국내외 공개키 기반구조 제품 제조업자, 그리고 이를 위한 표준 동향은 표 1과 같다.

〔표 1〕 공개키 기반구조 제품/서비스/표준 동향

동향	특 징
공개키 기반 구조 제품	- 메일보안(SMIME) 제품 : 네스케이프의 메신저, 마이크로소프트사 아웃룩, 로터스 노트 - 채널보안(SSL) 제품 : 네스케이프 네비게이터, 마이크로소프트사 인터넷 익스플로러 - 윈도우 2000의 보안 플래폼 - 프로그래머를 위한 툴킷 (마이크로소프트사의 CryptoAPI)
인증 서비스 제공자	- 국외: 미국의 베리사인, 벨지움의 글로벌사인, 독일의 Telesec - 국내: 한국정보보호진흥원 루트 인증기관, 정보인증, 금융결제원, 증권전산, 전산원, 무역정보통신
제품 제조 업자	- 국외 제품 제조업자: 볼티모아, 엔트러스트, IBM, RSA, Syprus - 국내 제품 제조업자: 드림시큐리티, 케이사인, 비시큐어, 소프트포럼, 시큐아이닷컴
표준	- PKI 표준안 : IETF의 PKIX 표준, ITU의 X.509 표준, PKCS 표준 - 응용 표준: S/MIME, PGP, SET, SSL/TLS, IPSec, WTLS - 기반 표준: X.500, LDAP/DAP, PKCS#11, PKCS#15 - 평가 표준: ITSEC, CC(Common Criteria), FIPS

2.6 인증서의 종류

인증서는 신분확인을 위한 신분확인 인증서와 권한을 나타내는 속성 인증서로 구분된다. 또한 인증서는 사용하는 주체에 따라서 개체 인증서와 인증기관 인증서로 구분될 수 있다. 신분확인용 인증서는 공개키기반구조의 기본 요소이며, 속성 인증서는 권한관리 기반구조의 기본 요소가 된다. 인증서는 용도에 따라서 전자메일용 인증서(PGP 인증서, PEM

인증서), 전자상거래에 널리 이용되는 SSL(Secure Socket Layer) 인증서, 안전한 전자지불을 가능케 하는 암호용 인증서와 서명용 인증서로 구성되는 SET(Secure Electronic Transaction) 인증서, 안전한 금융 정보 교류를 위한 금융 인증서, 소프트웨어 배포를 위하여 이용되는 소프트웨어 배포용 인증서 등이 있다. SSL 인증서는 서버용 인증서와 클라이언트용 인증서로 구분된다. 서버용 인증서는 SSL을 지원하는 서버를 위한 인증서로서, 클라이언트는 이를 이용하여 서버 인증 및 암호키 분배 기능을 수행한다. SSL 클라이언트 인증서는 서버가 사용자의 신원을 확인하고, 암호키를 분배하기 위하여 이용된다. 또한 최근에는 자바를 이용한 이동 코드의 활성화됨에 따라 악성 이동코드와 정상 이동코드를 구별하기 위한 인증서도 널리 사용될 전망이고, 특정 시점에 합법적으로 데이터가 존재했다는 사실을 제삼의 기관이 입증하는 데 이용되는 타임스탬프용 인증서, 그리고 온라인으로 인증서의 상태를 검증하기 위한 인증서 등에도 널리 활용될 전망이다. 또한 국내에서는 인터넷뱅킹을 위한 인증서가 국내 공인인증기관에 의하여 발행되고 있다. 또한 무선 인터넷을 위한 인증서도 발행되고 있다. 그리고 정부관인인증체계에서는 공무원을 위한 인증서가 2002년 9월 이내에 발행될 예정이다.

2.7 상호 인증의 필요성과 공개키 기반구조 형태

지구상에 존재하는 모든 사용자들이 하나의 인증기관으로부터 인증서를 발행받기란 사실상 불가능하다. 일반적으로 보안 영역(Security Domain)은 하나의 인증기관과 여기서 인증서를 발행받은 사용자들로 구성된다. 그러나 서로 다른 보안 영역에 존재하는 사용자간에 안전한 정보 유통이 요구된다. 이러한 요구는 인증기관간의 상호 인증으로 가능해질 수 있다. 상호 인증은 하나의 인증기관이 다른 인증기관에게 상호 인증서를 발행함으로서 보안 영역을 확대하기 위한 방법을 제공한다.

믿음의 확대 방법은 모든 인증기관들을 평면에 배치한 후 하나의 인증기관이 서로 다른 모든 인증기관에게 상호 인증서를 발행하는 평면형 형태, 인증기관들을 계층적으로 배열한 뒤 상위 계층의 인증기관이 하부 계층의 인증기관이나 사용자에게 인증서를 발행케 하는 계층형 형태, 그리고 이 두 방식을 적절히 혼용한 혼합 형태가 존재한다. 평면형 형태의 공개키기반구조는 확장이 용이하나 인증기관이 많을 경우 너무 많은 상호 인증이 요구되는 단점이 있고, 계층형 방법은 상호 인증의 수를 줄일 수 있으나 미리 계층 구조가 확고히 정해져 있어야 하는 단점이 있다. 국내는 두 개의 계층으로 구성된 계층형 공개키 기반구조를 채택하고 있다. 이는 1999년 7월에 발효된 국내 전자서명법에 의하여 체계화되었고, 최상위 인증기관으로 한국정보보호센터 인증기관을 선정하였으며, 그 하부 계층에 3개의 공인 인증기관을 선정하였다. 현재는 한국정보보호진흥원 산하에 6개의 공인 인증기관으로 확대되었다. 일반적으로 정부 공개키 기반구조는 계층형 형태를, 민간 공개키 기반구조는 혼합형 공개키 기반구조 형태를 갖는다.

2.8 공개키 기반구조 동작 과정

공개키 기반구조가 정상적으로 동작하기 위하여 요구되는 과정은 등록 과정, 초기화 과정, 인증 과정, 암호키 복구 과정, 키 생성 과정, 키 갱신 과정, 상호 인증 과정, 그리고 인증서 취소 과정 등이 있다. 등록 과정은 사용자가 인증서를 발급받기 전에 인증기관으로부터 사용자 식별 이름, 도메인 이름, IP 주소, 그리고 사용자 속성 정보를 제공받거나 제공하고, 이들의 유효성을 인증기관으로부터 검증받는 과정이다. 초기화 과정은 인증기관이 사용자에게 자신의 공개키나 인증서를 신뢰성 있는 방법으로 제공하며, 사용자는 자신의 공개키/개인키 쌍을 생성하는 과정이다. 인증 과정은 사용자의 요구에 의하여 인증기관이 인증서를 발행하고, 사용자로 생성한 인증서를 전달하며, 보관소에 인증서를 공표하는 과정을 나타낸다. 암호키 복구 과정은 선택적인 절차로 회사나 단체가 자신의 보안 정책으로 사용자의 개인키를 회사나 단체의 키 복구시스템에 보관할 것을 요구할 경우에 필요하다. 암호키 복구는 종업원이 병이 나서 회사에 출근할 수 없거나 회사를 퇴직하여 더 이상 회사에 나올 수 없을 경우에도 회사가 그 종업원에게 도착하는 회사 업무와 관련된 암호화된 메일을 읽을 수 있기를 원할 때 요구된다. 이를 위하여 인증기관은 사용자의 개인키를 인증기관이나 별도의 키백업 기관에 보관해야 한다. 만약 사용자나 고용주가 사용자의 백업된 사용자의 개인키를 원하는 경우 적법한 신분 확인 절차 후에 사용자의 개인키를 복구하여 전달해야 한다. 키쌍 생성 과정은

사용자의 공개키와 개인키를 생성하는 과정이다. 사용자의 개인키와 공개키는 사용자측에서 암호키 생성을 위한 독자적인 프로그램에 의하여 생성되거나 인증기관이 가지고 있는 안전한 키 생성 프로그램에 의하여 생성된다. 만약 인증기관에 의하여 사용자의 개인키와 공개키가 생성된다면, 인증기관은 사용자에게 인증기관의 공개키나 인증서를 등기 우편과 같은 안전한 방법으로 전달되거나 스마트카드와 같은 물리적 토큰을 이용하여 전달해야 한다. 대부분 암호키 쌍은 안전성을 보장하기 위하여 사용자에 의하여 생성됨을 원칙으로 하나 키 복구 기능이 요구되거나 사용자에 키 생성 모듈을 탑재할 수 없을 경우, 인증기관 또는 별도의 기관에 의하여 생성될 수 있다. 암호키는 한정된 수명을 가진다. 수명이 경과된 암호키는 안전성을 보장 받을 수 없다. 키쌍 갱신 과정은 모든 암호키 쌍이 수명이 경과하기 전에 새로운 암호키 쌍으로 대체되도록 하는 절차이며, 이때 인증기관은 새 공개키에 대응되는 새 인증서를 발급해야 한다. 키쌍 갱신 과정은 사용자 키쌍 갱신 과정과 인증기관 키쌍 갱신 과정으로 구성된다. 상호 인증은 하나의 보안 영역과 다른 보안 영역간의 믿음을 확장하기 위한 과정이다. 상호 인증은 하나의 인증기관이 다른 인증기관에게 발행하는 상호 인증서를 이용하여 실행된다. 상호 인증서는 하나의 보안 영역에 있는 사용자와 다른 보안 영역에 있는 사용자간의 안정한 정보 교환을 가능케 한다. 상호 인증서는 일방향 또는 양방향으로 발행될 수 있다. 인증서 취소과정은 사용자의 식별 이름이 변경되었거나, 회사원이 회사를 퇴직하여 직장이 변경되거나, 공개키에 대응되는 개인키가 누설되었다고 의심이 되는 경우 유효기간이 경과하지 않은 인증서를 취소하기 위한 과정이다.

III. 공개키 기반구조 표준화 동향

공개키 기반구조를 위한 표준으로는 미국 RSA 시큐리티사에서 제정한 PKCS 표준(표 2)[12-17], 인터넷에서 요구되는 표준을 제정하기 위하여 결성되어 운영되고 민간단체인 IETF에서 제정중인 PKIX 표준(표 3)[4-11], 정보시스템에 대한 표준을 정의하기 위한 ISO/IEC에서 제정한 공개키기반구조 표준[26-27], 그리고 각 국의 전자정부를 위한 공개키 기반구조 표준 등이 있다. 현재까지 널리 이용되고 있는 인증서 규격으로는 ITU의 X.500 인증서 규격과, IETF의 PKIX 인증서 규격 등이 있다. 국내에서도 정보보호 산업체와 한국정보보호진흥원, 한국전자통신연구원 등으로 구성된 인터넷보안기술포럼에서 전자상거래를 위한 유무선 인증서 및 CRL 프로파일, 공인 인증기관 상호 연동 규격 등에 대하여 표준화 작업을 완료했으며, 이는 TTA 단체 표준으로 확정되어 있는 상태이다.

3.1 PKCS 표준

PKCS(Public-key Cryptography Standards)는 표 2와 RSA 알고리즘의 구현 방법론 및 구문 표현 등을 정의한 표준으로서[12-17], 1991년 3월 NIST/OSI Implementor Workshop에서 문서 SEC-SIG-91-16으로 발표된 이후 1993년 11월까지 많은 수정을 거쳐 일관성 있는 문서로 개선되어 발표되었다. PKCS는 공개키 암호화를 위해 RSA에서 제안한 표준이다. APPLE, Microsoft, DEC, Lotus, Sun, MIT 등이 컨소시엄을 구성하여 PKCS를 채택하고 있다. 현재 전체 규격안은 PKCS#1에서 PKCS#15로 구성되어 있다. PKCS#2와 PKCS#4는 다시 PKCS#1에 통합되었고, PKCS#1은 RSA 암호화 표준, PKCS#3은 Diffie-Hellman 키 일치 표준, PKCS#5는 패스워드 기반 암호 표준, PKCS#6는 확장된 인증서 구문 표준, PKCS#7은 암호학적 메시지 구문 표준, PKCS#8은 개인키 정보 구문 표준, PKCS#9는 선택된 속성 타입, PKCS#10은 인증서 요구 구문 표준, PKCS#11은 암호 토큰 인터페이스 표준, PKCS#12는 개인정보 교환 구문 표준, PKCS#13은 타원 곡선 암호 표준, PKCS#14는 의사 랜덤 난수 생성기 표준, 그리고 PKCS#15는 암호학적 토큰 정보 구문 표준을 각각 규정하고 있다.

3.2 IETF PKIX 표준화

현재 인터넷을 위한 공개키 기반구조를 위한 IETF 보안 영역(Security Area) PKIX 워킹그룹에서는 인증서 및 CRL 규격, 운영 프로토콜, 관리 프로토콜, 인증서 정책, 온라인 인증서 상태 프로토콜, 간단한 인증서 검증 프로토콜, 타임 스탬프 프로토콜, 그리고 데이터 검증 및 인증 서비스 등의 사항을 표준화하고 있다. 이들 표준이 적용되어야 할 주요 응용분야는 그림 2와 같다.

가. 인증서 및 CRL 프로파일

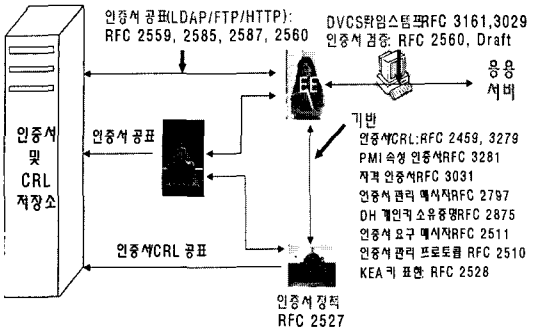
인증서 및 CRL 규격은 IETF RFC 2459와 최근에 이를 변경한 RFC 3280으로 표준화되었으며, 기본 필드와 다양한 확장 필드를 정의하고 있고, 인증서 규격으로 X.509 버전 3 인증서 규격을, 인증서 취소 목록 규격으로 X.509 버전 2 CRL 규격을 사용하고 있다[4].

〔표 2〕 IETF RFC 문서

구분	제 목	트랙	일 시
RFC 2459/3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	1999.1./2002.4.
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	표준	1999.3.
RFC 2511	Internet X.509 Certificate Request Message Format	표준	1999.3.
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	1999.3.
RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	정보	1999.3.
RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	표준	1999.4.
RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	표준	1999.5.
RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	표준	1999.6.
RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP	표준	1999.6.
RFC 2797	Certificate Management Messages over CMP	표준	2000.4.
RFC 2875	Diffie-Hellman Proof-of-possession algorithm	표준	2000.7.
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	실험	2001.2.
RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	표준	2001.1.
RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)	표준	2001.8.
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile	표준	2002.4.
RFC 3281	An Internet Attribute Certificate Profile for Authorization	표준	2002.4.
Draft	Simple Certificate Validation Protocol (SCVP)	-	2002.3.

〔표 3〕 PKCS 구성 및 현황

구분	제 목	내 용	버전	일시
PKCS #1	RSA Encryption Standard	RSA 공개키와 개인키에 대한 구문, 서명문 생성 과정, 서명문과 서명될 데이터의 형식을 정의함	2.1	1999.9.
PKCS #3	Diffie-Hellman Key-Agreement Standard	Diffie-Hellman 키 분배를 구현하는 방법 설명	1.4	1993.11.
PKCS #5	Password-Based Encryption Standard	패스워드로부터 파생된 비밀키(secret key)를 가지고 옥텟 스트링을 암호화시키는 방법 설명	2.0	1999.3.
PKCS #6	Extended-Certificate Syntax Standard	확장 필드를 갖는 인증서들에 대한 구문을 설명	1.5	1993.11.
PKCS #7	Cryptographic Message Syntax Standard	디지털 서명이나 디지털 봉투와 같은 일반적인 구문 표현에 대해 설명	1.5	1993.11.
PKCS #8	Private-Key Information Syntax Standard	개인키 정보, 암호화된 개인키 정보를 위한 구문을 정의	1.2	1993.11.
PKCS #9	Selected Attribute Types	PKCS#6의 확장된 인증서, PKCS#7의 디지털 서명된 메시지, 그리고 PKCS#8의 개인키 정보에서 사용될 선택된 속성 타입들을 정의	2.0	2000.2.
PKCS #10	Certification Request Syntax Standard	인증(certification) 요구를 위한 구문을 정의함. 인증 요구는 DN, 공개키, 속성 정보 집합, 인증서를 요청하는 개체에 의하여 서명된 서명문을 포함함.	1.7	2000.5.
PKCS #11	Cryptographic Token Interface Standard	일반적으로 CAPI라고 불리는 보안 서비스 API를 정의함. 암호키와 인증서를 가지고 있고 암호학적 동작을 수행하는 단일 사용자 장치를 위한 암호학적 API를 제공함	2.11	2000.11.
PKCS #12	Personal Information Exchange Syntax Standard	사용자가 개인 신분확인 정보(인증서, 개인키들, 여러 비밀정보 등)를 한 장치에서 다른 장치로 전달하기 위한 형식을 정의함	1.0	1999.6.
PKCS #13	Elliptic Curve Cryptographic Standard	현재 개발중인 표준으로, 타원 곡선 파라메터 생성 및 검증, 키 생성과 검증, 디지털 서명, 공개키 암호, 키 일치 등을 포함함	-	진행중
PKCS #14	Pseudo-random Number Generation Standard	암호 안전성에 중요한 영향을 주는 난수 생성기에 대한 표준으로, 현재 개발중임	-	진행중
PKCS #15	Cryptographic Token Information Syntax Standard	암호학적 토큰에 저장되는 암호학적 객체의 공통적인 형식을 정의함으로써, 암호학적 토큰의 상호 연동성을 증진하기 위한 표준임.	1.1	2000.9.



(그림 2) IETF PKIX 표준의 주요 적용 분야

나. 운영 프로토콜

IETF RFC 2585와 2559로 표준화되고 있는 운영 프로토콜은 인증서를 사용하는 시스템으로 인증서나 CRL을 전달하기 위한 방법을 기술하고 있다. 전달 방법에는 LDAP, HTTP, FTP, X.500 프로토콜에 기반을 둔 다양한 수단들이 이용될 수 있다[9].

다. 인증서 관리 프로토콜

관리 프로토콜은 사용자와 인증기관 간에 인증서를 발행을 요구하거나 인증기관 간에 상호 인증을 요구하기 위한 과정과 이를 위한 데이터 요소를 정의하는데 이용된다. 주로 관리 프로토콜은 사용자와 인증서의 발급 또는 취소 요구와 관련하여 온라인으로 동작되며, 상호 인증을 위해서는 인증기관사이의 온라인 동작으로 수행된다. 현재 RFC 2510으로 표준화되었다[5].

라. 인증서 정책

인증서 정책(RFC 2527)은 특정의 공개키 인증서를 적당한 가격의 전자 거래를 위한 인증서로 활용할 수 있는지를 판단할 수 있게 하는 규칙들의 집합이다[7]. 인증업무준칙은 인증기관이 공개키 인증서를 발급할 때 사용되는 자세한 세부 실행규칙이다. 인증서 정책은 물리적 및 개인 보안, 주체 신분확인 요구사항, 인증서 취소 정책 등의 규칙을 포함한다. 인증서 정책은 전자상거래를 위한 거래 금액이 크기에 따라 달라질 수 있다. 인증기관은 상대 인증기관의 인증서 정책을 검토하여, 상호 인증을 허용하기 위한 기준으로 인증서 정책을 활용할 수 있다. 인증기관이 공표하는 인증서 정책을 근거로 사용자는 해당 인증서의 특정 금융 거래로의 적용 여부를 판단할 수 있다. 일반적으로 인증서 정책에 따라서 인증서는 발행시 신분확인 방법, 공개키/개인키 생성방법, 인증서 전달 방법, 인증서 수명, 인증서 취소 방법 등의 절차가 달라진다. 인증서 정책 프레임워크는 IETF RFC 2527 문서로 마련되었다.

마. 온라인 인증서 상태 프로토콜

온라인 인증서 상태 프로토콜(RFC 2560)은 특정 인증서의 취소 상태를 시기적절하게 제공하기 위한 절차와 관련 데이터 구조를 정의한다[8]. 인증서 상태 프로토콜은 OCSP서버와 OCSP클라이언트간에 수행된다. OCSP클라이언트는 특정 인증서의 유효성과 취소 상태를 서버로 문의하고, 서버는 인증서 유효성과 취소 상태를 전달한다. 클라이언트는 서버로부터 인증서가 유효하고 취소되지 않았다는 정보를 수신한 후에야 해당 인증서를 이용하여 정보보호서비스를 제공할 수 있다. OCSP규격에서는 서버와 클라이언트의 기능과 인증서의 상태를 확인하기 위하여 교환해야 하는 데이터 형태를 정의하고 있다. 이는 실시간으로 인증서의 유효 상태를 확인할 수 있는 장점이 있다. 특히 2000년 이후 온라인 인증서 상태 프로토콜에 위임된 경로 발견 기능과 위임된 경로 검증 기능을 더한 차기 온라인 인증서 상태 프로토콜이 제안되고 있다. 따라서 온라인 인증서 상태 검증은 온라인 인증서 상태 프로토콜과 다음에 설명될 간단한 인증서 검증 프로토콜 중의 하나 또는 둘다 같이 채택되어 사용될 수 있다.

바. 간단한 인증서 검증 프로토콜

간단한 인증서 검증 프로토콜(IETF 드래프트)은 인증서 상태를 문의하거나 인증 경로에 대한 유효성을 문의하기 위한 프로토콜이다. 이는 SCVP(Simple Certificate Validation Protocol)서버와 클라이언트 간에 수행되며, 서버는 클라이언트로 인증서의 유효성과 취소 상태, 서명문 검증을 위한 인증서 체인의 유효성과 설정된 체인을 결과로 전달한다. SCVP는 응용이 공개키기반구조를 채용함에 따라서 추가적으로 요구되는 절차와 부담을 간단히 할 수 있는 방법을 제공한다. 온라인 인증서 상태 서비스와 간단한 인증서 검증 서비스는 무선 공개키기반구조에 유용하게 사용될 수 있는 프로토콜이다. 간단한 인증서 검증 서비스와 온라인 인증서 상태 서비스는 모두 인증서의 상태를 검증하기 위한 프로토콜로써,

현재 경쟁 관계에 있는 프로토콜이며, 앞으로의 논의 결과가 주목되고 있다.

사. 타임스탬프 프로토콜

타임스탬프 서비스(RFC 3161)는 제삼의 기관인 서버가 특정 메시지가 특정 시간 이전에 존재했음을 증명하기 위하여 사용된다[11]. 타임스탬프 서비스는 기본적으로 전자적인 데이터에 대한 존재 사실만을 증명하는 서비스라고 할 수 있다. 다시 말해, 타임스탬프 서버는 전자 문서의 내용에 대해서는 확인하지 않는다. 타임스탬프 기관은 모두가 믿는 제3의 기관이며, 특정 데이터에 대한 타임스탬프 토큰을 생성하다. 클라이언트는 메시지 자체를 서버로 보내는 것이 아니라 메시지에 대한 해쉬 값만을 서버로 전송한다. 따라서 서버는 메시지에 대한 구체적인 내용을 알지 못한다. 타임스탬프 기관은 사용자 메시지를 해쉬한 값과 이를 서명한 서명문을 포함한 타임스탬프 토큰을 클라이언트로 전달한다.

아. 데이터 검증 및 인증 서비스

데이터 검증 및 인증 서비스(RFC 3029)는 타임스탬프 서비스를 확장한 인증 응용 서비스이다. 클라이언트는 데이터 자체나 데이터의 해쉬값, 데이터에 대한 서명문, 서명문 검증을 위한 인증경로 등을 서버로 전달한다. 모든 클라이언트가 믿는 서버는 타임스탬프 서비스와 마찬가지로 특정 데이터가 소지 사실을 증명하거나, 특정 데이터 자체가 존재했음을 확인하거나, 특정 데이터에 대한 서명문이 유효함을 검증한다.

IV. 상호 연동을 위한 인증서 정책과 인증서 확장자

본 장에서는 상호 연동을 위하여 IETF PKIX에서 규정한 인증서 정책과 인증서 정책 관련 확장자의 특성을 분석한다.

4.1 인증서 정책과 인증업무준칙

인증서 정책은 IETF RFC 2527에서 나타난 바와 같이 다음과 같이 정의된다.

> 특정 인증서를 공동체 또는/그리고 공통의 요구사항을 갖는 응용에 적용 가능성 여부를 나타내는 이름을 갖는 법칙들의 집합. 예를 들어, 특정의 인증서 정책은 특정 인증서가 정해진 가격 내에서 상품을 거래하기 위한 전자 데이터의 교환을 위한 인증에 이용될 수 있는 지 여부를 나타낸다.

인증서 정책은 두개 이상의 PKI 영역 간의 상호 연동을 위한 기준으로 이용될 수 있다. 각 인증서 정책은 유일한 객체 확인자(OID)로 확인된다. 이 말은 인증서 정책은 제3의 신뢰 기관에 등록하여 사용되어야 함을 의미한다. 인증서, 상호 인증서, 또는 인증서 정책 수단을 전달하기 위한 다른 수단에 최종 개체 인증서가 호환 가능한 인증서 정책과 일치하게 사용되게 하기 위하여 적당한 OID가 존재할 것이다. 인증업무준칙은 "인증기관이 인증서를 발행할 때 적용하는 구체적이고 세부적인 업무 준칙"으로 정의되고 있다. RFC 2527이 언급했듯이, 1995년 ABA 가이드라인 초안은 위의 정의를 다음과 같이 확대 정의하였다.

> 인증업무준칙(CPS)은 인증기관에 의한 공표될 것이다. 이 선언에는 신뢰 시스템의 세부적인 사항과 인증서 발행을 지원하고 운영하기 위하여 이용되는 준칙을 포함할 것이다. 또는 이는 인증기관에 적용될 수 있는 정관이나 규칙이 될 것이다. 이는 클라이언트와 인증기관 사이에 이루어지는 계약의 일부가 될 것이다. 인증업무 준칙은 여러 문서, 여러 공공 법령, 사적 계약, 그리고 선언으로 구성된다.

그러므로, CPS는 인증기관의 동작과 관련되는 지극히 세부적인 사항을 다룬다. 이는 CPS가 상호 연동 협정을 확고하기 위하여 요구되는 제삼의 감시자의 기반으로써 이용될 수 있음을 의미한다.

인증서 정책과 인증업무준칙의 내용은 서론, 일반 규정, 신분확인 및 인증, 운영 요구사항, 물리적/절차적/개인적 보안 제어, 기술적 보안 관리, 인증서 및 CRL 프로파일, 그리고 규정관리 부분들로 구성된다. 서론에서는 개요, 문서 확인, 공동체, 응용 분야 등을 기술하고, 일반 규정은 책임과 의무, 해석 방법, 요금, 공표 및 보관소, 지적 재산권 등을 다루며, 신분확인과 인증은 초기 등록, 리키, 취소후 리키, 취소 요구를 위한 신분 확인 방법과 인증 방법을 기술하며, 동작 요구사항에서는 인증서 신청, 인

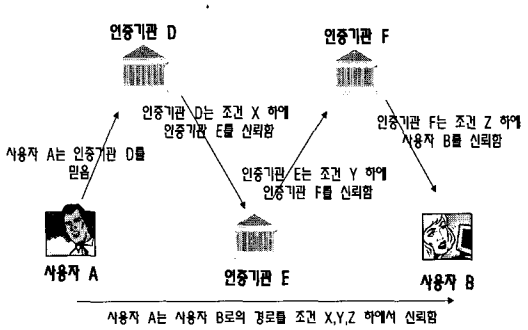
증서 발행, 인증서 수용, 인증서 동작정지 및 취소, 보안 감사 과정, 레코드 보관, 누설 및 재해 복구, 인증기관 업무 정지 등을 포함하고, 물리적/절차적/개인적 보안 관리에서는 비기술적 보안 제어를 포함하며, 기술 보안 제어에서는 키상 생성 및 설치, 개인키 보호, 활성화 데이터, 컴퓨터 보안제어, 네트워크 보안 제어, 암호학적 모듈 공학 제어 등을 포함하고, 인증서 및 CRL 프로파일에서는 인증서와 CRL 프로파일에 대하여 다루며, 마지막으로 문서 관리를 포함하고 있다.

4.2 인증 경로의 신뢰 모델과 상호 연동 관련 인증서 확장자

가. 전진적으로 제한된 신뢰 모델

인증 경로는 하나의 인증서 사용자가 믿는 신뢰점(Trust Point)에서 다른 인증기관이 발행하는 최종 개체 인증서까지의 믿음을 확장하기 위한 여러 개의 인증기관 인증서들과 하나의 최종개체 인증서로 구성되어 있는 인증서 체인(Certificate Chain)이다. 두 개의 인증서 간에 인증 경로 제한은 인증기관의 신뢰 경로 확장을 신뢰성 있고 의미 있게 연결할 수 있게 한다. 즉, 하나의 CA가 자신이 믿는 신뢰점에서 다른 CA로부터 발행되는 인증서까지의 인증 경로를 안전하고 신뢰성 있게 확장해 갈 수 있는 방법을 제공한다. 또한 인증서에는 인증서 주체가 CA인지 아니면 최종 개체인지를 확인할 수 있는 확장자가 있다. 이것을 이용하며, 최종 개체가 마치 인증 경로 상에 존재하는 또 다른 인증기관이 것처럼 가장하여 부정한 추가적인 인증 경로를 설정하는 것을 방지하기 위해서 사용된다. 인증서 제한 확장자를 이용하면, 하나의 인증기관은 특정한 이름 공간으로만 또는 인증 정책들의 집합을 따르는 인증서로만 인증 경로가 확장될 수 있다. 또한 인증 경로의 최대 길이를 제한할 수 있다. 이렇게 함으로써 인증 경로의 길이가 무한대로 확장되는 것을 방지할 수 있다. 인증 경로 제한 확장 영역은 상호 인증 환경 하에서 적절한 조건을 만족하도록 하는 인증기관으로만 인증 경로를 확대하기 위하여 사용된다. 이러한 기능을 수행하기 위하여 필요한 확장자가 기본 제한(Basic Constraints), 이름 제한(Name Constraints), 그리고 정책 제한(Policy Constraints) 등이다.

인증 경로는 그림 3과 같이 전진적으로 제한된(Progressive-constraint) 신용 모델을 채용한다. 사용자 A는 인증기관 D를 자신의 루트 인증기관으로써 사용하고, 사용자 A는 인증기관 D를 완전히 신뢰한다. 인증기관 D는 다른 인증기관 E를 특정 조건 하에 신뢰한다. 예를 들면 인증기관 D는 인증기관 E가 다른 인증기관을 위한 인증서를 발행할 때만 CA E를 신뢰한다.(중간 인증서는 반드시 인증기관 인증서야 한다는 조건) 즉, 조건 X는 인증기관 E가 다른 인증기관을 위해 CA 인증서를 발행하는 경우에만, 인증기관 D가 인증기관 E를 신뢰한다는 것이다. 인증기관 E는 인증기관 F가 이름 영역이 전자메일 주소 sch.ac.kr 내의 사용자들을 위하여 인증서를 발행하는 경우만 인증기관 F를 신뢰한다는 조건 하에 인증기관 F에게 인증기관 인증서를 발행한다(이름 제한 이용). 따라서 조건 Y는 인증기관 F에 의해 발행된 인증서가 최종 개체를 위한 인증서이고, 사용자 이름이 sch.ac.kr 영역에 있을 경우에만, 인증기관 E가 인증기관 F가 발행한 인증서를 신뢰한다는 것을 의미한다. 마지막으로 인증기관 F는 사용자 B에 대한 인증서를 발행하지만 보통 전자메일에 대한 인증서 만의 경우만 사용자 B를 신뢰한다(정책 제한 이용). 그래서 조건 Z는 인증기관 F에 의해 발행된 사용자 B의 인증서가 전자메일에 대해서만 사용될 수 있음을 의미한다. 이런 방법으로 인증 경로가 증가되면서 인증 경로는 점점 제약이 가해진다. 사용자 A 가 사용자 B에 대한 인증서를 가졌을 경우, 사용자 A는 사용자 B의 인증서를 단지 보통 전자메일에 대해서만 사용해야 한다는 것을 미리 알고 있다. 그리고 인증 경로를 따라 어떻게 신뢰경로가 형성되었는지를 알 수 있기 때문에 신뢰경로에 대한 확신을 가질 수 있다. 이런 제한들을 만족하는 경로에 대해서만사용자 A는 인증기관 F가 발행한 사용자 B 인증서를 신뢰한다.



〔그림 3〕 전진적으로 제한된 신뢰 모델

따라서 인증서의 기본 제한, 정책 제한, 그리고 이름 제한으로 인증 경로를 안전하고 신뢰성 있게 만들 수 있다.

나. 기본 제한

기본 제한은 기본적으로 인증 경로의 길이를 제한한다. 기본 제한의 경로길이 제한 값보다 긴 인증경로는 유효하지 않다는 것을 의미한다[11]. 기본 제한 확장자는 인증서 주체가 인증기관인지 최종개체인지 여부와 해당 인증서를 포함하는 인증 경로의 최대 길이를 나타낸다. 기본 제한자는 cA 와 pathLen Constraint 라는 두 필드로 구성된다. cA boolean 은 인증기관 인증서인지 최종개체 인증서인가를 나타내는 값이다. pathLenConstraint 필드는 cA boolean 이 주장되고 키 사용 확장자인 keyCertSign이 주장되었을 때만 의미를 갖는다. pathLenConstraint 필드는 인증 경로에서 이 인증서 뒤에 오는 비자체 서명된 중간 인증서의 전체 개수를 나타낸다. 만약 인증서의 주체 필드와 발행자 필드 내의 두 DN 들이 동일하면, 이 인증서는 자체 서명된 인증서가 될 것이다. "0" 값을 갖는 pathLenConstraint 필드는 오직 하나의 인증서 만이 뒤의 인증 경로 상에 나타날 수 있음을 의미한다. 이 확장자는 인증서 서명문의 유휴성을 검증하기 위한 서명용 공개키를 포함하는 모든 인증기관 인증서의 경우 임계성 확장자로 나타나야 한다. 만약 cA boolean가 주장되어 있지 않고 키 확장 필드가 keyCertSign 비트가 주장되지 않았다면 인증기관은 인증서에 pathLenConstraint 필드를 포함하지 않아야 한다.

다. 이름 제한

이름 제한은 기본적으로 인증 경로상의 인증기관이나 최종 개체의 이름을 제한하는 기능을 수행한다. 이름 제한(Name Constraints) 확장자는 인증기관 인증서에서만 사용되며, 이름 제한 확장자는 인증 경로 상의 이후에 나타날 모든 인증서 들의 주체 이름이 이 인증서 확장자의 이름 공간 내에 존재해야 함을 의미한다. 이름 제한은 주체의 구별 가능한 고유 이름(SubjectName)과 주체대체이름(SubjectAltName)에 대하여 적용된다. 이름 제한은 허용된 서브트리 (permittedSubtrees) 또는 배제된 서브트리(excludedSubtrees)에 대하여 정의되어야 한다. excludedSubtrees 필드의 제한과 일치하는 어떤 이름도 유효하지 않다. 이 확장자는 Criticality 이 TRUE 이다.

이름 제한은 호스트나 도메인, 그리고 전자메일 주소, 그리고 DNS 등의 형태에 적용될 수 있다. 이름 제한은 하나의 호스트나 하나의 도메인에 대하여 적용될 수 있다. 예를 들어, "sch.ac.kr"와 ".sch.ac.kr" 경우를 보자. 이름 제한이 마침표로 시작되면, 이는 하나 이상의 서브 도메인으로 확장될 수 있다. 다시 말해, 이름 제한 ".sch.ac.kr"는 elec.sch.ac.kr과 dis.asan.sch.ac.kr를 만족하나 제한 ".sch.ac.kr"는 "sch.ac.kr"를 만족하지 않는다. 이름 제한이 마침표로 시작하지 않는다면, 이는 특정의 호스트를 명시한다.

인터넷 메일 주소에 대한 이름 제한은 특정의 메일 주소, 특정 호스트 상의 모든 주소들, 또는 하나의 영역에서 모든 메일 주소들을 규정할 수 있다. 특정 메일 주소를 명시하기 위해서는 제한이 완전한 메일 주소 형태이어야 한다. 예를 들어, "root@sch.ac.kr"는 호스트 "sch.ac.kr" 상의 루트(root) 메일 주소를 나타낸다. 특정 호스트 상에 모든 인터넷 메일 주소를 나타내기 위하여, 제한은 호스트 이름으로 규정되어야 한다. 예를 들어, 이름 제한 "sch.ac.kr"은 호스트 "sch.ac.kr" 상의 모든 메일 주소들(hyy@sch.ac.kr)에 의하여 만족된다. 특정 도메인 내에서 임의의 인터넷 주소를 만족하기 위하여, 이름 제한은 마침표로 시작되도록 해야 한다. 예를 들어, ".sch.ac.kr"은 도메인 "sch.ac.kr" 내의 모든 인터넷 메일 주소를 나타내며(이는 hyy@elec.sch.ac.kr을 만족한다는 의미임), 이는 특정 호스트 "sch.ac.kr" 상의 인터넷 메일 주소를 나타내지 않는다.

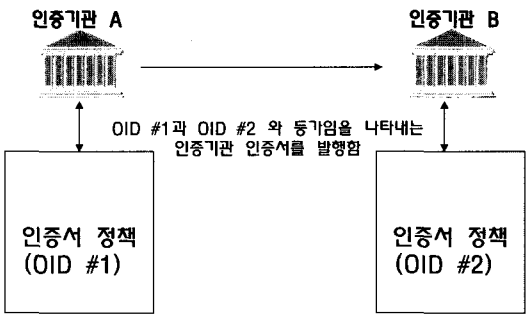
라. 인증서 정책 확장자

인증서 정책 확장자는 최종개체 인증서와 인증기관 인증서에서 모두 존재할 수 있다. 최종 개체 인증서의 경우 정책 확장자는 인증서가 발행되었을 때 적용되었던 인증서 정책으로 주로 인증서가 사용되어야 할 목적을 나타내고 있다. 인증기관 인증서의 경우 이 인증서를 포함하는 인증 경로에 대한 정책 집합을 제한(limit)한다. 다시 말해 추후의 인증 경로가 가져야할 인증서 정책들을 제한하는데 이용한다. 하나의 인증기관은 다른 인증기관에게 인증서를 발행하면서 수용 가능한 인증서의 집합을 이 정책 확장자를 이용하여 제한할 수 있다. 인증서 정책 확

장자는 하나 이상의 정책정보(PolicyInformation)들의 계열(Sequence)이다. 각각의 정보요소는 특정의 인증서 정책(CertPolicyId)을 나타내는 객체 확인자(OID)와 선택 항목인 서술자(PolicyQualifier Info)로 구성된다. 선택 항목인 서술자는 앞서는 인증서 정책에 대한 정의를 변경하지 않고 정책을 추가적으로 설명하는데 이용된다. 특정 정책을 만족하도록 요구하는 응용은 자신이 받아들일 수 있는 정책들의 목록을 가지고 있다가 자신이 허용하는 정책 목록과 인증서가 포함하고 있는 인증서 정책을 비교하여, 동일하면 해당 인증서를 받아들일 것이다. 정책 서술자(PolicyQualifierInfo)는 인증업무준칙의 위치를 응용에게 알려주는 CPS 참조 서술자(CPSuri) 또는 인증서 사용자에게 보여주는 해당 인증서에 대한 부가 정보를 보여주기 위한 사용자 공표(NoticeReference)를 갖는다. CPS 참조 서술자는 인증기관이 발행한 인증업무준칙을 알려주기 위한 참조자를 포함하며, URI 형태를 갖는다. 사용자 공표(NoticeReference) 서술자는 해당 조직과 조직에서 발행한 번호를 나타내는 noticeRef와, 사용자에게 직접 보여지는 explicitText 의 두 가지 필드를 가질 수 있다. noticeRef 필드는 조직과 확인자를 지칭한다. 확인자는 조직이 미리 마련한 여러 문자 성명서 중에서 특정의 문자 성명서를 확인하기 위하여 사용된다. 예를 들어 조직이 "KISA"이고 공표 번호가 "1"인 경우, KISA에서 발행한 번호 "1" 이라는 문자 성명서를 나타낸다. 일반적으로 응용 소프트웨어는 KISA에서 발행된 모든 문자 성명서의 집합을 담고 있는 파일을 가지고 있다가 인증서의 사용자 공표 필드에서 획득한 값을 참조로 하여 특정의 공표 문서를 확인하고 이를 인증서 사용자에게 보여주어야 한다. 문자 성명서는 여러 언어로 작성되는 것을 허용한다. 이는 소프트웨어가 자신의 환경을 위한 특정 언어를 선택할 수 있게 한다. explicitText 필드는 인증서 내에 직접적인 문자 형태로 전달되는 성명서를 포함한다. 이 확장자는 최대 200문자를 갖는 문자열 형태이다.

마. 정책 매핑

정책 매핑은 기본적으로 발행 인증기관의 인증서 정책과 등가인 주체 인증기관의 인증서 정책을 나열하기 위함으로써, 미국 연방정부 브리지 인증기관에서 널리 이용되고 있는 필드이다. 정책 매핑(Policy Mapping) 확장자는 인증기관에게 발행되는 인증기관 인증서에서만 사용된다. 이 확장 영역은 CA 인증서에서 사용되며, 발행 인증기관이 사용하는 인증서 정책과 타 인증기관에서 사용되는 정책이 서로 등가임을 알리기 위하여 사용된다. 정책 매핑 확장 영역은 발행 인증기관의 정책을 나타내는 issuer DomainPolicy 서브필드와 발행 인증기관으로부터 상호 인증서를 받은 인증기관의 인증서 정책을 나타내는 subjectDomainPolicy 서브 필드로 구성된다. 예를 들어 그림 4에서 인증기관 A가 발행 인증기관이 되고, 인증기관 A가 인증기관 B를 위한 상호 인증서를 발행할 때 정책 매핑 필드에 발행 인증기관의 인증서 정책 #1이 인증기관 B의 인증서 정책 #2와 등가임을 인증기관 A의 사용자나 응용에게 알리기 위하여 이용된다. 인증기관 A의 사용자는 자신의 정책 필드에 인증기관 B의 인증서 정책을 나타내는 OID를 갖는 인증서를 받아들일 때, 인증기관 A가 인증기관 B로 발행한 상호 인증서의 정책 매핑 필드에서 인증기관 A의 인증서 정책과 인증기관 B의 인증서 정책이 매핑되어 있으므로 해당 인증서를 받아들인다. 발행 기관 인증서 사용자는 발행기관의 인증서 정책을 갖는 인증서를 받아 드리도록 구성되어 있다. 정책 매핑 확장 영역은 응용이 자신이 보관하고 있는 인증서 정책이 아닌 특정의 정책을 담고 있는 인증서를 수신할 때 만약 수신된 인증서에 포함된 인증서 정책이 인증 경로 상에 존재하는 상호 인증서의 정책 매핑 필드에서 자신의 인증서 정책과 등가 인증서 정책이라고 선언된 정책으로 발행된 인증서를 수용하도록 하기 위한 경우에 매우 유용하게 활용될 수 있다. 정책 매핑 확장자에서 이름지어진 issuerDomainPolicy는 동일한 인증서에서 인증서 정책 확장자에 나타나야 한다. 정책들은 anyPolicy로 매핑되거나 anyPolicy 로부터 매핑되어서는 않된다.



〔그림 4〕 인증서 정책 매핑

바. 정책 제한

정책 제한 확장자는 인증기관 인증서에서만 사용될 수 있다. 정책 제한 확장자는 두 가지 방법으로 인증 경로를 제어한다. 하나는 인증 경로 상에서 임의의 정책 매핑을 금지하게 하는 것이고, 다른 하나는 인증서 경로 상의 각각의 인증서들이 수용 가능한 정책 확인자를 반드시 포함해야 한다는 것이다. 정책 제한 영역(Policy Constraints)은 인증기관 인증서에만 적용된다. 정책 제한 영역은 inhibit PolicyMapping 서브 필드와 requireExplicit Policy 서브 필드를 이용하여 실현된다. 첫 번째 방법은 inhibitPolicyMapping 서브 필드는 더 이상의 정책의 매핑이 수행되는 것을 방지하는 것이고, 두 번째 방법은 requireExplicitPolicy 서브 필드를 이용하여 실현된다. inhibitPolicyMapping 서브 필드는 인증 경로 상에서 현재부터 시작하여 새로운 정책 매핑이 금지되어야 하는 추가적인 상호 인증서의 개수를 나타낸다. 만약 이 값이 "1"이면, 이 인증서의 인증기관이 발행한 인증서에서만 정책 매핑이 가능하며, 더 이상의 상호 인증서에서는 정책 매핑이 수행될 수 없음을 의미한다. requireExplicit Policy 필드는 전체 인증 경로 상에서 분명한 인증서 정책이 나타나기 이전에 인증 경로 상에 나타날 수 있는 추가적인 인증서의 개수를 나타낸다. 분명한 인증서 정책이 요구될 경우, 경로 상의 모든 인증서에는 인증서 정책 확장자에 수용 가능한 정책 확인자를 포함해야 한다. 수용 가능한 정책 확인자는 인증 경로 사용자가 요구하는 정책의 확인자이거나 정책 매핑을 통하여 등가라고 선언된 정책의 확인자이다.

사. Inhibit Any-Policy

inhibit any-policy 확장자는 인증기관 인증서에서 적용된다. inhibit any-policy 확장자는 {2 5 29 32 0} 값을 갖는 anyPolicy OID가 다른 유효한 인증서 정책이 일치한다고 간주하지 않기 전에 나타날 수 있는 인증경로 상의 인증서의 개수를 의미한다. 다시 말해, 이 값은 anyPolicy가 허용되지 않기 이전에 나타날 수 있는 인증서의 개수를 나타낸다. 예를 들어, "1" 이라는 값은 anyPolicy 가 이 인증서의 주체에 의하여 발행된 인증서에서만 처리될 수 있고, 인증 경로 상의 추가적인 인증서에서는 처리될 수 없음을 의미한다.

4.2 인증서 정책 예

가. IETF 인증서 정책

IETF PKIX WG에서 예를 들고 있는 인증서 정책은 전자메일을 보호하기 위하여 발행되는 인증서에 적용될 수 있는 범용 정책(General-Purpose Policy)과 금융거래를 위하여 발행되는 상용 정책으로 구분될 수 있다. 범용 정책으로 발행된 인증서와 이에 대응되는 개인키는 일반적으로 소프트웨어로 보관되며, 이는 웹 상에서 전자우편의 안전한 교환을 위한 인증서로 활용된다. 상용 정책에 의하여 생성될 사용자의 공개키/개인키 쌍은 안전한 하드웨어 키 토큰에서 생성되고 보관되어야 하고, 사용자의 인증서도 엄격한 보안 관리 하에서 인증기관에서 발급되어야 한다. 인증서 정책 확장자는 하나의 인증서가 여러 응용에 활용될 수 있도록 하는 역할을 수행한다. 인증서 정책 확장 필드는 인증서가 사용자에게 발급되었을 때 사용되었던 인증서 정책과 인증서가 적용될 수 있는 서비스의 종류를 정의한다. 인증서에는 여러 개의 인증서 정책들이 포함될 수 있다. 이는 인증서에 포함된 인증서 정책들이 서로 상충되지 않는 다면 하나의 인증서가 여러 용도의 인증서 정책을 지원하는 서비스에 적용될 수 있음을 의미한다.

나. 미국 브리지 인증기관에서 정의된 인증서 정책

미국 연방 정부 내에서 또는 연방정부와 민간 분야의 공개키 기반구조를 상호 연동하기 위한 미국 브리지 인증기관을 위한 인증서 정책이 있다[28]. 정부 부처와 기관간의 브리지 인증기관을 통하여 연동을 위한 인증서 정책은 표 4와 같이 기초, 기본, 중급, 고급 등의 4가지 인증서 정책 레벨을 갖는다. 여기에 시험은 시험용으로 할당된 정책이다. 따라서 정부 기관의 인증서 정책은 고유의 객체 확인자를 가지며, 다음 4 가지 인증서 정책으로 매핑되어 상호 연동의 기준이 된다. 브리지 인증기관은 PKI 영역 간의 가교(Bridge) 역할을 하며, 이는 기본적으로 인증서 확장자의 정책 매핑 필드를 이용하여 실현된다.

〔표 4〕 인증서 정책의 종류

보장 레벨	설 명
시험	이 레벨은 FBCA(Federal Bridge CA)와 PCA(Principal Certification Authority) 간의 상호 호환성 시험용으로 사용된다. 이는 이는 시험용으로만 사용되고, 어떤 정보의 전달용으로 사용되지는 않는다.
기초	이 레벨은 개인의 신원과 관련하여 가장 낮은 보장 정도를 제공한다. 주요 기능들의 하나는 서명되는 정보에 대한 데이터 무결성을 제공하기 위함이다. 이 레벨은 악의적인 위협이 낮다고 여겨지는 환경과 적용된다. 이 레벨은 인증을 요구하는 거래에 불충분하며, 일반적으로 기밀성을 요구하는 거래에 불충분하며, 그 보다 높은 보장 레벨이 유용하지 않는 환경에서 기밀성을 위하여 사용될지도 모른다.
기본	이 레벨은 결과가 중요하다고 여겨지지 않은 데이터 손상의 결과와 위협이 존재하는 환경과 관련되는 기본 보장 레벨이다. 이는 악의적인 가능성이 높지 않은 환경에서 개인 정보로의 액세스를 제어하기 위하여 사용된다. 이 레벨에서는 사용자는 악의적이지 않다고 가정한다.
중급	이 레벨은 데이터 손상의 결과와 위협이 적절하게 존재하는 환경과 관련된다. 이는 상당한 금전적인 가치가 있고, 사기 위험이 있으며, 악의적인 액세스가 상당한 환경에서 개인 정보로의 액세스와 관련된 거래를 포함한다.
고급	이 레벨은 데이터로의 위협이 높고, 보안 서비스의 실패 결과가 높은 환경에 사용하기가 적절하다. 이는 거래 가격이 높고 고 레벨의 사기 위협을 포함한다.

초기 등록 시에 고객에 대한 신분 확인은 인증서 정책마다 표 5와 같은 요구사항을 갖는다. 리키 인증서는 새로운 인증서가 새로운 공개키 및 개인키 쌍을 갖고, 새로운 일련번호를 가지는 것을 제외하고, 새로운 유효 기간으로 옛 인증서와 동일한 보장 등급과 특성을 갖는 새로 생성된 인증서이다. 리키 인증서를 발행하기 위한 사용자 인증 방법은 표 6과 같다.

개인키 생성 메카니즘은 표 7과 같다. 연방 브리지 인증기관과 기관 인증기관에 의하여 발행된 인증서가 취소되어야 할 때, 인증서 취소는 표 8과 같은 시간 내에서 수행되어야 한다. 기관 CRL(ARL: Authority Revocation Lists)과 CRL 발행 주기는 표 9와 같다.

〔표 5〕 신분확인 요구사항

보장 레벨	설 명
시험	양해 각서로 설정됨.(시험 환경에 종속됨)
기초	신분확인 요구사항 없음, 신청자는 자신의 전자메일 주소를 제공함으로써 인증서를 신청하고 받을 수 있음.
기본	신분확인이 RA에 직접 출두하여 수행됨. 방법은 신청 데이터와 데이터베이스 정보를 비교하거나, 신분을 확인하기 위하여 도장, 또는 다른 수단을 사용하는 신분을 확인할 권한이 주어진 감독자, 정보보호 관리자, 연방 기관이나 주 정부에 의하여 검증된 사람에 의해 발행된 증명서에 의하여 수행됨.
중급	신분을 확인하기로 인가 받은 RA, 신뢰 기관, 또는 주 또는 연방 기관에 대면 출두로 신분이 확인됨. 제공된 정보는 합법성을 보장하기 위하여 검사된다. 자격증은 연방 정부-발행 사진이 있는 신분증, 두 개의 비 연방 정부 신분증(하나는 운전면허증)
고급	신뢰기관이나 등록 기관에 직접 출두로 신분이 확인됨, 제공된 정보는 합법성을 위하여 검사됨. 자격증은 연방정부-발행 사진이 있는 신분증, 두 개의 비 연방 정부 신분증(하나는 운전면허증)

〔표 6〕 리키 인증서를 위한 신분확인 요구사항

보장 레벨	설 명
시험	양해 각서로 설정됨.(시험 환경에 종속됨)
기초	현재의 서명키를 이용하여 신분이 확인될 수 있음.
기본	현재의 서명키의 사용을 통한 신분 확인, 초기 등록 시간으로부터 적어도 15년 마다 한번 초기 등록 과정을 통한 신분을 재확인함
중급	현재의 서명키의 사용을 통한 신분 확인, 초기 등록 시간으로부터 적어도 9년 마다 한번 초기 등록 과정을 통한 신분을 재확인함
고급	현재의 서명키의 사용을 통한 신분 확인, 초기 등록 시간으로부터 적어도 3년 마다 한번 초기 등록 과정을 통한 신분을 재확인함

〔표 7〕 개인키 생성 메카니즘

보장 레벨	설 명
시험	MOA에서 구축됨
기초	HW 또는 SW
기본	HW 또는 SW
중급	HW 또는 SW
고급	HW만

〔표 8〕 취소 시간 주기

보장 레벨	설 명
시험	MOA에서 구축됨
기초	요구되지 않음
기본	6시간 이내
중급	2시간 이내
고급	30분 이내

〔표 9〕 CRL 발행 주기

보장 레벨	정기적인 발행 주기	개인키 손실이나 손상으로 인한 발행주기
시험	양해각서에서 정의됨	양해각서에서 정의됨
기초	적용 않함	적용 않함
기본	기관이 정함	신고 후 24시간 이내
중급	적어도 하루 한번	신고 후18시간 이내
고급	적어도 하루 한번	신고 후 6시간 이내

V. PKI 영역간 상호 연동 방법

신뢰 영역은 하나의 인증서정책(CP)으로 관리되는 인증기관과 사용자 집합으로 구성된다. 인증서 정책은 하나의 인증서가 특정의 응용에 적용 가능한지를 전달하기 위한 것으로써, 보안 영역 내에 있는 여러 참여 주체들의 협력으로 작성될 수 있다. 인증업무준칙(CPS)은 인증서 발행을 위하여 인증기관이 채용한 업무준칙이다. 신뢰 영역은 하나의 기업과 같은 자치권을 갖는 기반구조이고, 일관된 인증서 정책과, 비슷한 인증업무준칙 하에 운영되는 인증기관과 최종개체 들의 집합으로 볼 수 있다. 따라서 다른 영역에서 발행된 많은 인증서들과 서로 연동될 수 있는 상호 연동은 인증서 사용의 이점을 최대로 확대할 수 있다.[18-19] 상호 연동은 서로 다른 신뢰 영역에 있는 사용자간의 전자거래가 증가하면서 필요성이 증가하고 있다. 서로 다른 신뢰 영역간의 상호 연동을 달성하기 위해서는 기술적/프로토콜 차원의 기술적 요구사항, 자국의 정책과 외부 영역 정책간의 정책 매핑과 외부 영역에서 발행된 인증서의 사용 가능성 여부를 결정하는 정책 또는 사업 요구사항, 그리고 디지털 서명법의 존재 여부와 전자서명법의 적용 여부를 결정하는 법률적 요구사항 등이 고려되어 수행되어야 한다. X.509 v3 인증서는 인증서 발급 시에 적용되었던 정책들의 명단을 포함한다. 이 정책들은 사용자 인증서가 특정의 목적에 적합하게 발행되었는지를 결정할 수 있게 한다. 예를 들어, 어떤 정책에서는 공개키가 전자메일을 위해 사용될 수 있고, 다른 경우에는 금융 거래를 위한 응용에 사용될 수 있다. 따라서 전자메일을 위하여 발행된 인증서는 전자 거래를 위한 인증서로 사용될 수 없음을 의미한다. 일반적으로 인증서 정책은 사용자에 대한 인증 절차, 주체에 대한 신분확인 방법, 법적 권리 및 의무 사항 등을 규정한다. 여기서 정책매핑이란 한 인증기관의 인증서 정책이 다른 인증기관 인증서 정책과 등가임을 알려준다.

본 절에서는 상호 연동을 위한 프레임워크과 여러 가지 상호 연동 방법들, 그리고 이들 상호 연동 방식들간의 특징을 비교한다.

5.1 상호 연동을 위한 프레임워크

PKI 포럼에서 채용한 PKI 상호 연동 프레임워크는 NIST의 Tim Polk 에 의한 제안에 바탕을 두고 있다. 상호 연동을 위한 차원은 구성 요소-레벨 상호 연동, 응용-레벨 상호 연동, 그리고 영역간 상호 연동으로 구분된다[20].

가. 구성 요소-레벨 상호 연동

구성 요소-레벨 상호 연동은 PKI 관련 서비스를 직접 지원하고 사용하는 시스템간의 상호 동작을 다룬다. 영역 내 상호 연동을 위해서는 하나 이상의 인증기관들의 존재한다고 가정한다. 여기서, 하나의 PKI 영역 내 상호 연동이란 하나의 기업이나 공통의 관리 기관의 제어 하에 있는 여러 구성 요소간의 상호 연동을 의미한다. 또한 신뢰(Trust)나 신뢰관계(Trust Relation)의 의미는 일반적으로 글로벌 차원에서 합의되어 있지는 않지만, 하나의 개체가 다른 개체가 자기가 기대하는 대로 행동할 것이라고 믿으면, 한 개체는 두 번째 개체를 신뢰한다고 할 수 있다. 구성 요소-레벨 상호 연동은 다음의 고려사항을 포함한다.

- 인증기관, 등록기관, 그리고 최종 개체 등으로 구성되는 PKI 구성 요소들은 공통의 프로토콜, 메시지 포맷, 그리고 인증서 포맷을 이용하여 구현되어야 한다. 이는 인증기관과 인증기관간, 인증기관과 등록기관간, 최종개체와 인증기관간, 또는 최종개체와 등록기관간의 메시시지 교환 시에 호환성을 달성할 수 있다.

- 개체 인증과 PKI 구성 요소간에 교환되는 데이터를 보호하기 위하여 공통의 알고리즘이 사용되어야 한다.
- PKI 구성요소간의 인증서를 저장하고 검색하며 인증서의 상태 정보를 제공하기 위한 방법이 지원되어야 한다.
- 인가된 최종 개체는 개인키는 저장 방법(소프트웨어, 스마트카드, 또는 하드웨어 토큰)에 무관하게 안전한 방법으로 접근할 수 있어야 한다.

나. 응용-레벨 상호 연동

응용-레벨 상호 연동은 응용의 공급자 또는 응용을 보조하는 데 사용되는 부수적인 기반 요소와 무관하게 두 개의 개체간의 호환성을 달성하기 위함이다. 예를 들어, 두 개의 S-MIME 클라이언트들은 응용 소프트웨어가 서로 다른 벤더로부터 제공되고, 응용이 서로 다른 플래폼 상에서 동작되며, 각 응용이 서로 다른 PKI 제조업자부터 공급받은 PKI 기술로 실현되더라도 다른 클라이언트와 상호 동작할 수 있어야 한다. 이를 위한 기능이 응용-레벨 상호 연동을 위한 기능이다.

- 인증서와 인증서 상태 정보의 형식이 호환 가능해야 한다.
- 비지니스 제어가 인증서의 키 사용과 정책 및 이름 제한을 만족하도록 실현되어야 한다. 이는 비즈니스에 적합하게 키가 사용되어야 하고, 정책 제한과 이름 제한이 비즈니스 제어에 적합하도록 사용되어야 함을 의미한다.
- 암호 알고리즘의 종류와 키의 크기를 포함한 알고리즘 규격이 호환되어야 한다.
- 파일 포맷과 메시지 포맷을 포함하는 데이터 캡슐화 방법과 데이터 엔코딩 방법이 호환되어야 한다.
- 등위간의 정보를 교환하기 위한 기반 통신 프로토콜들이 호환되어야 한다.
- 공개키 관련 정보(최종 개체 인증서와 인증기관 인증서, 인증서 상태 정보 등)를 공유하기 위한 임의의 인밴드 방법이 호환되어야 한다.

다. 영역간 상호 연동

영역간 산호 연동에서는 두 개의 서로 다른 PKI 영역간에 상호 연동성을 위한 여러 문들과 여러 상호 연동 방법들을 다룬다. 이는 동일한 PKI 영역 내에서 존재하는 상호 연동 문제와는 근본적으로 다르다. 여러 가지 영역간의 협조가 필요하므로, 영역간 상호 연동은 세 가지 상호 연동 레벨 중에 가장 복잡한 부분이다. 신뢰 관계를 구축해야 하는 이유는 두 개의 영역 사이에서 하나 이상의 응용이 지원될 필요성이 있을 때 요구된다. 영역간 상호 연동을 위해서는 다음과 같은 문제들이 다뤄져야 한다.

- PKI 영역간의 신뢰 관계를 구축하는 방법이 선행되어야 한다.
- 하나의 PKI 영역의 PKI 관련 정보가 다른 PKI 영역에서 사용 가능해야 한다.
- 각 PKI 영역은 하나의 일관된 인증서 정책을 가져야 하며, 각 PKI 영역은 합의된 정책에 따라서 적절하게 시행되도록 감시하는 방법 또는 메카니즘을 가지고 있어야 한다.

표 10은 각 상호 연동에 적용될 수 있는 기술적 측면을 요약하였다.

〔표 10〕 상호 연동 레벨별 주요 기능

주요 기능	구성 요소 레벨	응용 레벨	영역간
공통의 프로토콜, 메시지 포맷, 인증서 프로파일	○	○	○
PKI 구성 요소간 개체 인증과 교환되는 데이터의 보호를 위한 공동 알고리즘 실현	○	○	○
인증서의 저장/검색, 인증서 상태 정보를 제공하기 위한 공통의 프로토콜과 인증 기법이 지원되어야 함	○	○	○
개인키가 안전한 방법으로 인가된 사용자에게만 접근되어야 함	○	○	○
하나 이상의 인증서 상태 검사 검증 메카니즘이 제공되어야 함	○	○	○
인증서 및 인증서 상태 정보가 호환성이 있어야 함		○	○
응용이 인증서 발행 목적대로 사용되도록 보장해야 함		○	○
암호 알고리즘 호환성		○	○
데이터 캡슐화와 엔코딩 방법 호환성		○	○
기반 통신 프로토콜 호환성		○	○
PKI 정보 공유를 위한 인밴드 방법 호환성		○	○
PKI 영역간의 신뢰 관계의 구축 방법			○
다른 영역의 PKI 정보 사용 가능성			○
PKI 영역간 합의된 특정 정책이나 메카니즘의 적절한 유지			○

5.2 영역간 상호 연동방법

PKI 영역간 상호 연동방법은 크게 상호 인증(Cross Certification), 브리지 인증기관, 상호 인정, 인증서 신뢰 목록, 인가 인증서, 그리고 엄격한 계층 구조 등이 있다[21]. 상호 연동방법을 위한 여러 대안 등의 장점과 단점을 검토하기 위하여서는 적어도 다음과 같은 기술적, 비즈니스적, 법률적 고려사항이 검토되어야 한다. 기술적 고려사항은 상호 연동을 위하여 요구되는 프로토콜, 데이터 구조, 그리고 또 다른 측면 들(예를 들어, 인증서의 공유와 인증서 취소 정보의 공유) 등을 다룬다. 비즈니스적 고려사항은 두 PKI 영역들간의 관계를 구축하기 위한 비지니스 관련 세부 사항을 다룬다. 영역간(또는 기업간) 관계를 구축하기 위한 근본 이유는 두 영역간의 사용자간에 전자적인 정보 교환의 필요성에 기인한다. 이를 전자적 관계의 구축이라고 할 수 있으며, 기존의 비즈니스 요구사항에서부터 도출되거나 새로운 비즈니스 요구사항/관계로부터 생성될 수 있다. 따라서 상호 연동을 위해서는 비즈니스적 요구사항이 선행되어야 한다. 법률적 고려사항은 상호 연동과 관련되어 가장 중요하게 다루어져야 할 것으로써, 디지털 서명문의 인정 여부에 달려 있다. 미국 내에서 가장 최근에 전자 서명법이 통과되었고, 유럽에서도 전자 서명법이 도입되고 있다. 전자 서명법에서는 수기 서명의 신뢰성과 전자 서명의 신뢰성을 동일하게 법률적으로 보장해 주어야 한다. 또한 PKI 구성 요소간에 책임과 의무에 분담하기 위하여 신뢰 당사자에게 추가적인 의무을 주어 인증기관의 의무를 감소하는 법률적 고려도 요구된다.

가. 상호 인증

상호 인증은 하나의 인증기관이 신뢰관계를 구축하려는 다른 인증기관에게 매쉬 형태로 상호 인증서를 발행함으로써 달성된다. 즉, 실질적인 절차는 하나의 인증기관이 다른 인증기관에게 인증서를 발행해줌으로써 완료될 수 있다. 상호 인증서는 하나의 인증기관이 다른 인증기관으로부터 발행받은 인증서이며, 이 경우 주체가 인증기관이 되는 인증서라고 할 수 있다. 상호 인증서는 통상 인증기관에게 발행되므로 인증기관 인증서라고 불리어진다[24].

> 상호 인증서 : 발행자와 주체가 서로 다른 인증기관일 경우 이 인증서는 상호 인증서이다.

> 인증기관은 주체 인증기관의 존재를 인증하거나(순수한 계층 구조에서) 주체 인증기관을 인식하기 위한(분산된 신뢰 모델에서) 메카니즘으로 다른 인증기관에게 인증서를 발행한다. 상호 인증서는 이 두 환경에서 사용된다.

상호 인증의 근본적인 목적은 두 개의 인증기관간에 신뢰를 구축하는 것이다. 이는 서로 다른 두 개의 PKI 영역 사이나 동일한 PKI 영역내의 인증기관 사이에 하나 이상의 응용을 위한 상호 연동 경로를 구축하기 위하여 발행된다. 전자는 영역간에 상호 인증이라고 하고, 후자는 영역내 상호 인증이라고 한다. 상호 인증은 일방향(Unilateral)일수도 양방향(Mutual)일수도 있다. 양방향인 경우, 대칭적인 관계가 인증기관 간에 대칭적인 관계가 구축된다. 하나의 인증기관은 다른 인증기관에게 인증서를 발행하고, 또 반대로 다른 인증기관이 하나의 인증기관에게 인증서를 발행한다. 자국 인증기관이 원격 인증기관에게 발행해준 인증서는 자국 인증기관 관점에서 보면 역방향상호인증서(Reverse Cross-certificate)가 된다. 원격 인증기관이 자국 인증기관에게 발행해준 인증서는 자국 인증기관 관점에서 보면 순방향상호인증서(Forward Cross-certificate)가 된다. 역방향상호인증서와 순방향상호인증서는 디렉토리의 DN 속성에 쌍으로 보관될 수 있다. 일방향 상호 인증은 단순히 하나의 인증기관이 다른 인증기관에게 상호 인증서를 발행함을 의미하며, 반드시 그 역이 있어야 함을 의미하지는 않는다. 일방향 상호 인증은 상위 인증기관이 하위 인증기관에게 인증서를 발행해주는 엄격한 계층구조에서 전형적으로 적용된다.

이러한 상호 인증은 PKI영역간 상호 연동을 위한 방법으로 사용될 수 있다. 상호 인증의 가장 큰 단점은 다중 PKI영역간에 원하지 않은 믿음의 확장을 도입할 수 있다는 것이다. 다른 말로 하면, 만약 A가 B를 믿고, B가 C를 믿는다고 가정하며, 어떻게 A가 그렇게 하기 원해서 C를 믿지 않게 할 것인가? 상호 인증서는 다음과 같은 확장자를 이용하여 원하지 않은 믿음의 확장을 막을 수 있다.

- 이름 제한: 이는 외부 PKI 영역에 있는 주체의 이름을 하나 이상의 가능한 이름 공간을 한정하기 위하여 사용될 수 있다. 예를 들어, A가 B를 믿되 조직 B 내의 재무 부서 내의 주

체만을 믿도록 한정할 수 있다. 또한 주어진 인증 경로에서 이후의 특정 인증서 발행자를 제외하거나 허용하는 등으로 주체의 이름을 제한할 수 있다.

- 정책 제한: 외부 PKI 영역에 주체에게 발행된 인증서의 사용을 제한하기 위하여 사용될 수 있다. 예를 들어, 외부 영역 B에 존재하는 주체에게 발행된 인증서가 전자메일용으로만 사용되도록 한다. 그리고/또는 다중 PKI 영역간에 원하지 않은 신뢰 확장을 막기 위하여 정책 매핑을 금지하기 위하여 사용된다.
- 인증경로 길이 제한(기본 인증서 확장자에서): 인증 경로에서 상호 인증서의 수를 제한하기 위하여 사용된다. 예를 들어, 값이 "0 인 경로 길이 제한은 분명히 A와 C간의 B에 의한 부정한 믿음의 확장을 막을 수 있다.

PKI영역간 상호 연동을 위한 상호 인증은 두 개의 인증기관간에 믿음을 확장하기 위하여 서로 간에 상호 인증서를 주고받는 행위로 볼 수 있다. 가장 일반화된 상호 연동 방식이라고 할 수 있으며, PKI 영역의 수가 증가하며, 상호 인증을 위한 부가적인 처리가 기하급수적으로 증가하는 단점이 있다.

나. 브리지 인증기관

상호 인증 방식은 작은 PKI 영역을 갖는 구조에서 잘 동작할 수 있다[25]. 그러나 PKI 영역의 수가 증가하면, 상호 인증의 수가 급격히 증가하게 되는 단점이 있다. 브리지 인증기관은 중앙화된 상호 인증을 위한 기관으로, 이의 목적은 상호 인증서를 발행하여 인증 경로에 대한 루트를 제공하는 것이다. 다시 말해, 인증 경로를 확장하는 것이다. 브리지 CA는 허브 노드라고 하며, PKI 영역간에 신뢰 관계를 구축하기 위한 중계소 역할을 수행한다. 현재의 브리지 CA 이니셔티브는 PKI 영역간 상호 연동을 위하여 상호 인증을 이용하는데 바탕을 두고 있다. 양방향 상호 연동의 가장 큰 단점은 매쉬형 상호 인증의 경우, 인증기관의 수가 n이면 요구되는 상호 인증의 수가 n(n-1)/2 가 되어 상호 인증을 위하여 요구되는 오버헤드가 감당할 수 없을 정도가 증가하게 된다는 것이다. 이러한 문제는 상호 인증 과정 자체를 너무 복잡하게 한다. 이러한 문제점을 해결하기 위하여 제안된 상호 연동 구조가 브리지 인증기관을 이용한 상호 연동 기법이다. 브리지 CA는 하나의 조직이나 기업을 다른 조직이나 기업에 소개하는 조직이거나 이를 실현하는 세삼의 신뢰된 중개 조직이라고 볼 수 있다. 따라서 브리지 CA는 일반적으로 중립성을 보장받을 수 있기 위하여 국가에 의하여 운영되고 있는 추세이다. 브리지 CA가 하나의 조직을 다른 조직으로 소개하므로, 하나의 조직이 다른 각각의 조직과 양방향 상호 인증 협정을 별도로 체결할 필요가 없다. 각 조직은 하나 이상의 인증서 정책을 갖고 브리지 CA와 상호 인증을 위한 협정을 체결할 수 있다. 인증서 정책이 등가라고 간주되면, 각 조직은 브리지 CA를 통하여 다른 조직과 인증 경로를 가질 수 있다. 각 기업 입장에서 보면, 이 신뢰 관계를 구축하기 위한 오버헤드가 크게 줄일 수 있다. 즉, 하나의 조직이 브리지 CA와 신뢰관계를 맺음으로써, 다른 모든 조직으로의 믿음의 경로를 확장할 수 있음을 의미한다. 브리지 CA가 하나의 인증서 정책 하에 존재하는 조직의 수가 클 때 상호 연동과 관련되는 오버헤드를 크게 줄일 수 있음을 의미한다. 브리지 인증기관은 PKI 영역이 증가하는 경우 가장 바람직한 상호 인증 방식으로써, 조직간의 호환성이 있는 인증서 정책의 실현을 가능케 한다.

다. 상호 인정

상호 인정은 APEC 통신 워킹 그룹에서 고려되고 있는 개념이다. 상호 인정의 개념은 다음과 같다. 한 PKI 영역 내에 존재하는 신뢰 당사자가 다른 PKI 영역 내에 존재하는 주체를 인증하기 위하여 필요한 다른 PKI 영역의 PKI 관련 정보를 상호 연동 협정을 체결을 통하여 이용하겠다는 것이다. 상호 인정은 상호 인증과 몇 가지 측면에서 다르다. 여기서는 인증기관간 상호 인증이 없다. 상호 인정은 독립적인 인증기관이 상호 믿음이 있는 신뢰 기관(인가 기관이나 감독기관)에 의하여 허가되고 감독된다는 개념에 바탕을 두고 있다. 특별히, APEC은 다음과 같이 언급하고 있다. 만약 인증기관이 인가/승인 기관에 의하여 인가/승인되었거나 독립적인 믿을 수 있는 신뢰기관에 의하여 인가/승인되었다면 인증기관은 신뢰적이라고 간주된다. 또 다른 중요한 차이점은 신뢰 당사자가 직접 인증기관에 대한 신뢰 여부를 판단해야 하는 것이다. 신뢰 당사자가 인증서의 유효성을 판단하기 위하여 필요한 PKI 정보를 획득하는 방법은 글로벌하게 아직 분명하게 결정되지 않았으나, 인증서의 확장자나 다른 방법을 사용

하여 신뢰 당사자에게 전달될 수 있도록 하는 방법이 제안되고 있다. APEC은 상호 인정이 신뢰 당사자에게 추가의 부담을 초래하며, 고신뢰 정도를 요구되는 환경에서 수용 가능한 해법으로 볼 수 없는 것으로 인정한다.

라. 인증서 신뢰 목록

인증서 신뢰 목록(CTL:Certificate Trust Lists)은 부라우저에서 널리 사용하는 방식이다. 이 방식은 여러 응용 분야에서 이용되고 있는 일반화된 방식이다. 클라이언트는 신뢰된 루트의 공개키들이 제공되고, 하나의 인증서는 이 신뢰된 인증기관의 공개키와 연결되어야 하며, 상호 연동을 위한 인증기관은 자신의 공개키를 인증서 신뢰목록에 삽입하기 위하여 제3의 신뢰기관으로부터 검증 받아야 한다. 인증서 신뢰목록은 "신뢰된 인증기관"의 공개키를 제삼의 신뢰기관의 개인키로 서명된 PKCS#7 데이터 구조이다. 신뢰된 인증기관은 주체 CA의 공개키 형태로 CTL 내 포함된다. PKI 영역간 상호 연동의 관점에서, CTL은 근본적으로 상호 인증서 쌍을 대체한 것이다. 이 방식에서는 신뢰 당사자가 CTL을 발행하는 제삼의 신뢰기관인 CTL 발행자를 믿는다는 것에 바탕을 두고 있다. 신뢰 당사자에게 CTL을 분배하는 방법은 여러 가지 방법으로 수행될 수 있다. 이는 PKIX 워킹그룹에서 표준화되고 있는 운영 프로토콜 중의 하나 이상을 이용하거나 out-of-band 방법을 통하여 실현될 수 있다. 이 방법 역시 PKI 영역의 수가 증가하면 인증서 신뢰 목록의 수가 증가하게 되며, 또한 이를 위한 추가적인 관리 기능이 요구된다는 점이다. 또한 어느 조직이 CTL 발행자가 되어야 하는 문제도 해결되어야 한다.

마. 인가 인증서

인가 인증서를 이용하는 방법은 호주 정부에서 이용되는 방식이다.[22-23] 상호 연동을 위하여 특정의 인증기관이 호주 정부에 의하여 인가되었음을 나타내는 인가 인증서을 이용한다. 기본적으로 각 인가된 인증기관들은 GAC(Gatekeeper Accreditation Certificate)를 호주 정부로부터 발행 받음으로써 해당 인증기관을 위한 인가된 공개키를 가질 수 있음을 의미한다. 다시 말해, 각 인증기관이 호주정부가 발행한 인증서를 가지고 있음을 의미한다. 서명 확인 과정은 신뢰 당사자에게 주체 인증기관이 호주 정부에서 요구하는 모든 인가 기준을 만족했다는 것을 보증한다. 신뢰 당사자가 신뢰 원천으로서 GAC를 믿는다면, 신뢰 당사자는 호주정부에 의하여 인가된 임의의 인증기관을 믿게 된다. 이 상호 연동 방법은 루트 인증기관을 갖는 계층 구조와 근본적으로 동일하다고 볼 수 있으나, 이 연동 방식과는 두 가지 관점에서 차이점이 존재한다. 첫째, 호주 정부에 의하여 인가된 각각의 인증기관들이 독립적이고 구별 가능한 인증서 정책과 인증업무준칙을 가질 수 있다는 것이다. 이는 각 인증기관에 독립적인 인증서 정책의 설정을 허락하는 것이다. 둘째, 각 인증기관은 자신의 자가 서명된 공개키 인증서를 가질 수 있다는 것이다. 이런 의미에서, 인가된 인증기관은 자치권을 갖는 독립된 PKI 영역을 구축할 수 있는 하나의 개체라고 할 수 있다. 상호 인정은 인가 인증서를 발행 받도록 요구하지 않는다. 인가 인증서는 인증기관간의 신뢰 관계를 구축하는데 이용된다. 즉, 인증기관이 인가 기관으로부터 인증서를 받으며, 이 인가 인증서가 신뢰 당사자가 해당 인증기관을 믿어야 하는지에 대한 판단 근거가 될 것이다. 인가 여부는 호주 정부에 의하여 정의된 기준을 근거로 결정된다.

바. 엄격한 계층 구조

엄격한 계층 뒤의 개념은 모든 신뢰가 하나의 공통된 인증기관으로부터 나온다는 것에 개념을 두고 있다. 이것은 루트 인증기관이 그 영역 내에서 모든 신뢰 당사자를 위한 신뢰 원천지가 됨을 의미한다. 하부의 인증기관으로의 신뢰된 인증 경로는 최상위 인증기관으로부터 시작됨을 알 수 있다. 엄격한 계층 구조는 하부의 인증기관은 오직 하나의 상위 인증기관을 갖는다. 또한 하부 인증기관은 자신의 자가 서명된 인증서를 가질 수 없다. 오직 루트 인증기관만이 자신의 자가 서명된 인증서를 갖는다. 엄격한 계층은 하나의 루트 인증기관에 여러 개의 하부 인증기관으로 구성된다. 이 경우에, 최상위 인증기관은 여러 개의 레벨 1 하위 인증기관에게 인증서를 발행한다. 레벨 1 인증기관은 차례로 여러 개의 레벨 2 하위 인증기관에게 인증서를 발행한다. 상위 인증기관이 하부 인증기관에게 인증서를 발행하는 것은 일방향 상호 인증과 근본적으로 동일하다. 엄격한 계층 구조에서는 하나의 루트 인증기관만이 자가 서명 인증서를 가질 것이고, 자가 서명된 최상위 인증기관 인증서는 루트 인증기관의 인증서 속성에 저장된다. 이는 X.500 디렉토리에서 DN 에 대응

하는 속성 정보로 최상위 인증기관의 인증서가 저장될 수 있음을 의미한다. 엄격한 계층은 정책 제어가 하향식으로 수행되어야 하는 환경에 적합하다. 엄격한 계층 구조의 단점은 최상위 인증기관의 개인키 손상의 결과가 모든 하부 인증기관의 인증서를 변경해야 하는 치명적인 결과를 초래 한다는 것이다. 또한 하나의 최상위 인증기관만이 허용되므로 어느 인증기관이 최상위 인증기관이 되어야 하는지에 대한 합의가 매우 힘들다는 단점이 있다.

5.3 상호 연동 방식의 비교 분석

상호 연동 방식간의 특성은 표 11과 같이 요약될 수 있다. 또한 주요 상호 연동 방식의 주요 관점별 특징 비교는 표 12와 같다.

5.4 영역간 상호 연동 방식 선정을 위한 위한 지침

영역간 상호 연동 방식은 각자 장단점이 있다. 따라서 환경을 살펴보고, 그에 적합한 상호 연동 방식을 선정해야 할 것이다. 위의 분석 결과를 바탕으로 제시한 상호 연동을 위한 주요 지침은 다음과 같이 제시한다.

〔표 11〕 상호 연동 방식 종류와 특징

종 류	동 작	특징 또는 장단점
상호 인증	- 인증기관간의 상호 인증서 발행 - 인증기관간의 상호 인증 협정이 요구됨	- PKI 영역의 수가 증가하면 상호 인증의 수가 기하급수적으로 증가함 - 따라서 상호 인증을 위한 경비가 큼 - 영역의 수가 작은 경우 유리함
브리지 인증 기관	- 미국 정부의 브리지 인증기관 이용 - 미국 연방 정부와 민간 PKI 간의 상호 연동 방식	- 정책 매핑이 용이한 상호 연동 방식 - 영역의 수가 증가하더라고 상호 인증의 수를 크게 증가하지 않음 - 브리지 인증기관이라는 별도의 조직과 관리 기관이 요구됨
상호 인정	- 하나의 PKI 영역이 다른 PKI 영역 정보 사용하기 위하여 협정 체결 - 제삼의 신뢰 기관이 특정 인증기관을 믿을지 여부를 결정해야 함	- 상대 영역의 PKI 정보 전달 방법이 개발되어야 함 - 고가 거래에 부적합함 - 글로벌 차원의 상호 인정을 위한 기준이 합의되기가 어려움
인증서 신뢰 목록 (CTL)	- 신뢰 인증기관 목록을 포함하는 인증서 신뢰 목록이라는 데이터 구조 이용 - CTL 발행자가 신뢰 당사자에게 믿어야 할 인증기관의 인증서 목록을 전달해야 함 - 상호 연동을 원하는 하나의 인증기관과 CTL 내의 신뢰 인증기관 간의 신뢰 경로가 먼저 구축되어야 함 - 기존의 메일 브라우저에서 사용하는 방법임	- PKI 영역의 수가 작다면 효율적임 - 많은 PKI 영역이 존재하는 경우, 추가적인 관리 부하가 요구됨 - CTL 생성 주체가 결정되어야 함 - 신뢰 당사자에게 CTL 전달이 어려움 - PKI 영역의 수가 증가하면 관리가 어려움
인가 인증서	- 호주 정부에서 개발된 방법임 - 일정한 기준을 만족하는 인증기관에게 호주 정부가 인가 인증서를 발행함 - 인증기관에게 좀더 많은 자치권 부여함	- 인가 인증서 소지 여부로 신뢰 여부를 판단함 - 각 인증기관이 독립적인 PKI 영역의 구축이 가능함 - 각 인증기관이 독자적인 인증서 정책과 인증업무준칙을 가질 수 있음 - 인가 기준이 전체적으로 유일함
엄격한 계층 구조	- 믿음의 원천으로 최상위 인증기관을 이용함 - 하부 인증기관은 상위 인증기관 정책을 사용해야 함 - 경로 처리가 간단함	- 인증 경로 길이가 상대적으로 짧음 - 루트 인증기관의 합의가 어려움 - 루트 키 손상이 치명적이며 전체 기반구조에 영향을 줌

〔표 12〕 주요 상호 연동 방식의 특징 비교

비교 항목	계층적 구조	상호 인증	브리지 CA	CTL
신뢰점 공개키	계층적 구조의 최상위 인증기관 공개키	자국 인증기관 공개키	자국 인증기관 공개키	CTL 발행자가 인정된 인증기관들의 공개키
기업간 지원	공통의 최상위 인증기관을 넘는 인증기관의 경우 약함	적당한 수의 기업 간에 좋음	큰 규모에 대해서도 아주 우수	영역의 수가 작은 경우 간단, 영역 수가 증가하면 복잡: CTL에 대한 집중적인 관리가 요구됨
경로 구성	간단(최상위 인증기관으로부터 시작되는 경로 구성)	어려움(여러 개의 인증 경로가 존재할 수 있음)	간단(모든 자기 영역이 아닌 경로도 브리지 인증기관을 통과해야 함	간단하나 제한적임(모든 인증 경로는 CTL 목록 내의 CA에서 시작되어야 함)
디렉토리(인증서, CRL) 종속성	낮음(최상위 인증기관 디렉토리 이용)	높음(여러 개의 디렉토리에 접근 가능해야 함)	중간(브리지 디렉토리 이용)	낮음(다중 신뢰점에서부터 경로가 생성되므로)
새 영역의 상호 연동 확장	상위 인증관으로부터 인증서를 발행 받음	원하는 인증기관 쌍이 상호 인증서 교환	브리지 인증관과 인증기관 인증서의 교환	제삼의 신뢰 기관인 CTL 발행자에 의한 CTL에 상호 연동을 위한 공개키를 추가함
별도 조직의 필요성	없음(기존 루트 인증기관이 수행)	없음	브리지 인증기관 운영 조직	CTL 발행기관(기존의 기관 선정 가능)

① 상호 연동의 평가 기준은 인증서 정책을 이용한다. 일반적으로 인증업무준칙은 상호 연동을 위한 기준이 될 수 없다. 그러나 인증업무준칙이 공개가 가능한 경우, 인증업무준칙을 이용한 평가를 통하여 수행하는 것도 가능하다. 상호 연동 기준으로 인증업무준칙을 이용하는 것은 하나의 정부나 하나의 회사의 여러 PKI영역간에 상호 연동에 적합하다.

② 독립적인 제3의 신뢰 기관에 의한 PKI영역에 대한 감사는 대부분의 상호 연동 방식에 대하여 적용되어야 한다. 이는 상호 연동을 허락하는 초기 과정에서뿐만 아닐라 인증 서비스를 수행하는 동안에 주기적으로(1년, 또는 6개월 단위로) 지속적으로 수행되어야 한다.

③ PKI 영역이 많은 경우 가장 바람직한 방법은 브리지 인증기관 방식을 위한 상호 연동 방식이다. PKI 영역이 작은 경우, 상호 인증, 브리지 인증기관, CTL 방법을 통한 상호 연동이 가장 적절할 것이다. 또한 협정을 통해 간단히 달성할 수 있는 인가 인증서를 이용한 상호 연동 방식의 이용도 가능하다.

VI. 결 론

상호 연동은 공개키기반구조의 응용 영역을 확대하기 위한 중요한 기술로 부각되고 있다. 최근 우리나라에서도 전자정부를 위한 공개키기반구조 영역과 민간 분야를 위한 공개키기반구조 영역으로 나타나고 있다. 정부 PKI는 전자정부법에 기반을 두고 구축되고 있고, NPKI 체계는 전자서명법에 기초를 두고 구축되었다. 이와 같이 여러 PKI영역에서 발행되는 인증서에 대한 활용성을 증가시키기 위해서는 이들 영역간의 인증서의 상호 연동이 가능해야 한다. 인증서의 상호 연동은 여러 가지 방법으로 달성될 수 있다. 따라서 공개키기반구조 체계가 서로 호환이 가능한 상호 연동이 가능한 구조를 가져야 한다. 이는 독립적으로 운영되던 기존의 공개키기반구조 체계가 상호 연동이 가능한 체계로 발전되어야 함을 의미한다. 상호 연동은 인증서 정책에 바탕을 두고 있으므로 상호 연동을 위한 널리 인정되는 인증서 정책이 개발될 전망이다. 상호 연동 방식의 채택은 정책적 사항, 기술적 사항, 그리고 국제 사회의 채택 동향을 고려하여 결정되어야 한다. 따라서 장단기적 관점에서 상호 연동 방식 채택과 관련 기술의 개발이 이루어져야 한다. 또한 모든 참여 주체가 참여하는 상호 연동을 위한 국가 차원의 인증서 정책에 대한 연구도 시급히 추진되어야 할 것이다. 우리나라의 경우 현재 상호 상동 방식으로 신뢰된 인증서 목록 방식을 이용하는 것으로 알려지고 있

다. 그러나 이 방식은 소규모나 신뢰 영역의 수가 작은 경우에 단기적으로 적용할 수 있으나, 영역의 크기가 증가하게 되는 경우 복잡한 관리 문제를 초래한다. 영역의 수가 증가하게 되면 브리지 인증기관을 이용한 상호연동 방식이 여러 가지 이점이 있으며, 이 방식이 국제적인 추세이기도 하다. 이는 미국, 일본, 캐나다 등 대부분의 나라에서 상호 연동을 위한 방법으로 채택하고 예에서도 알 수 있다. 따라서 장기적 관점에서 브리지 인증기관 방식을 이용한 상호연동 방식도 고려되어야 하며, 브리지 인증기관 방식으로 진화하기 위한 단계와 진화 모델을 포함한 체계적인 연구도 필요한 시점이라고 생각된다.

마지막으로 본 고의 결과가 국가 차원의 상호 연동을 위한 인증서 정책 개발과 상호 연동 방식을 개발하고 연구하는데 도움이 될 수 있으리라고 기대한다.

참고문헌

[1] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자상거래 보안 기술," 생능출판사, 1999

[2] 염흥열외, "선진국의 정보보호기술 개발사업 동향분석 및 국내 대응방향 연구," 정보통신진흥원, 2000.2.

[3] 염흥열외, "유·무선 PKI 운용환경 분석 및 연동방안 제시에 관한 연구," 한국전자통신연구원, 2001. 11.

[4] RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile., R. Housley, W. Ford, W. Polk, D. Solo, January, 1999.

[5] RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", IETF PKIX Working Group, March, 1999, http://www.ietf.org/rfc/rfc2510.txt

[6] RFC 2511, "Internet X.509 Certificate Request Message Format", IETF PKIX Working Group, March 1999, http://www.ietf.org/rfc/rfc2511.txt

[7] RFC 2527, "Internet Public Key Infrastructure Certificate Policy and Certification Practies Framework", IETF Network Working Group, March, 1999, http://www.ietf.org/rfc/rfc2527.txt

[8] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", Network Working Group, June, 1999, http://www.ietf.org/rfc/rfc2560.txt

[9] RFC 2559, "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2," IETF PKIX Working Group, April, 1999.

[10] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", IETF Network Working Group, August, 2001, http://www.ietf.org/rfc/rfc3161.txt

[11] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R. Housley, W. Ford, W. Polk, D. Solo, 2002.4.

[12] PKCS #5, "Password-Based Cryptography Standard", RSA Laboratories.

[13] PKCS #7, "Cryptographic Message Syntax Standard", RSA Laboratories.

[14] PKCS #8, "Private-Key Information Syntax Standard", RSA Laboratories.

[15] PKCS #10, "Certification Request Syntax Standard", RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs/index.html

[16] PKCS #11, "Cryptographic Token Interface Standard", RSA Laboratories.

[17] PKCS #12, "Personal Information Exchange Syntax Standard", RSA Laboratories.

[18] John Linn, Trust Models and Management in the Public-Key Infrastructures", 2001.

[19] A. Nash, W.Duane, C.Joseph, and D. Brink, PKI Implementation and Managing E-Security, RSA Press, 2001.

[20] PKI forum White Paper, "PKI Interoperability Framework," PKI forum, 2001.3.

[21] PKI forum White Paper, "CA-CA Interoperability," PKI forum, 2001.3.

[22] Gatekeeper Certificate Management

Infrastructure Gatekeeper Accreditation Certificate Concept of Operations, Department of Communications Information Technology and the Arts, Version 0.9.1a, 6 October 2000

[23] Gatekeeper: A strategy for public key technology use in the Government, Australian Office of Government Information Technology, 6 May 1998

[24] Government of Canada Public-Key Infrastructure Cross-Certification Methodology and Criteria, Draft Version dated April 2000

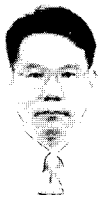
[25] X.509 Certificate Policy for the Federal Bridge Certification Authority, NIST, 2000.12.

[26] ITU-T Draft Revised ITU-T Recommendation X.509(2000 E) : Information Technology Open Systems Interconnection - The Directory : Public-Key and Attribute Certificate Frameworks

[27] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition.

[28] Michael. S. Baum, Federal Certification Authority Liability and Policy, NIST-GCR- 94-654, June 1994.

〈著者紹介〉



염 흥 열 (HeungYoul Youm)
종신회원

1981년 : 한양대학교 전자공학과 졸업
1983년 : 한양대학교 대학원 전자공학과 석사
1990년 : 한양대학교 대학원 전자공학과 박사
1982년~1990년 : 한국전자통신연구소 선임연구원
1990년~현재 : 순천향대학교 공과대학 정보기술공학부 교수, 정보보호학과 학과장
1997년~2000년 : 순천향대학교 산업기술연구소 소장
2000년~현재 : 순천향대 산학연컨소시엄센터 소장
1997년~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안