通信情報保護學會誌
第8卷 第3號, 1998. 9

공개키 기반구조에서 상호인증 구현을 위한 요구사항 분석

홍 기 웅*, 권 현 조*

요 약

인터넷 사용자의 증가와 더불어 보안의 중요성이 확산됨에 따라 공개키 기반구조(PKI:Public Key Infrastructure)하에서의 상호인증(Cross Certification) 기술이 요즘들어 정보보호 기반기술의 중요요소로 논의되고 있다. 이러한 상호인증과 관련한 문제는 현재 국내외적으로 활발히 연구중에 있으며 몇몇 회사에서는 이를 상용화 추진하고 있다. 하지만 상호인증을 실현하는데 있어, 인증기관들간에 호환성이라든가 정책 확장등의 문제를 감안할 때 실질적인 서비스의 완전한 구현은 당장은 어려울 것으로 생각된다. 만일 이러한 상호인증이 완벽한 호환성을 가지고 사용자들간에 상호연동될 수 있다면 늘어나는 인터넷 사용자들의 요구를 한층 더 충족시켜 줄 수 있게 될 것이다. 따라서 본 논문에서는 이와 관련한 요구사항이 무엇인지를 알아보고 현재 개발되고 있는 기술동향을 서술한다.

Ⅰ. 서 론

오는 2001년 인터넷을 통한 국제 상거래 규모가 2천억 달러를 돌파할 것으로 예측되는 가운데 현재 인터넷은 전 세계적으로 약 5000만 명의 사용자가 약 600만 대의 서로 다른 컴퓨터에 접속되어 지구 반대편의 세계를 한 눈에 바라보고 있다. 최근 글로벌 전자상거래의 출현과 더불어 인터넷은 전통적인 유통 체계를 붕괴시키며 인터넷이 새로운 유통채널로 급부상하여 전세계 전자상거래 시장이 45억달러대 거대시장으로 성장하고 있다. 선진국가들은 인터넷 상거래 시장의 주도권 장악을 위해 정보서비스산업 경쟁력을 강화하는 한편 전자상거래 지원을 위한 각종 법규정비와 세부정책 추진에 역점을 두고 있는 가운데 공개키 기반구조(PKI:Public Key Infrastructure) 구축을 위한 노력을 산업체와 협력하여 국가차원에서 중점적으로 기울이고 있다. 선진국에서 추진개발중에 있는 공개키기반구조 프로젝트로는 미국의 FPKI(Federal Public Key Infrastructure), 유럽의 ICE-TEL(Internetworking Public Key Certification Infrastructure), 캐나다의 GOC PKI(Government of Canada PKI), 호주의 PKAF(Public Key Authentication framework) 등이 있다. 현재 우리나라도 공개키기반 구축을 위해 한국정보보호센터를 중심으로 활발히 진행중에 있고 공개키기반 구축의 구성요소인 인증관리 업무를 시행하기 위하여 법제정을 추진중에 있다. 산업자원부는 법무부와 공동으로 "전자거래기본법(안)"을 마련하고 정보통신부에서는 "전자서명법(안)"

* 한국정보보호센터

을 마련하여 제정을 추진중에 있다.

앞서 서술한 바와 같이 공개키기반 구축을 위한 노력이 전세계적으로 진행되고 있는 가운데 공개키기반의 계층구조 유형에 따라 각기 분산되어 있는 인증기관(CA:Certification Authority) 사이의 서로 다른 인증관리 정책, 인증서 형식 등 공개키 기반구조 구성요소간의 차이로 인한 CA간 상호인증 서비스를 어떻게 제공할 것인지를 고려하여야 한다. 공개키 기반구조에서의 인증 서비스와 관련하여 그 유형을 크게 계층구조를 이용한 방식과 비계층구조를 이용한 방식으로 나눠볼 수 있는데 상호인증 서비스를 제공하기 위해서는 비계층구조가 유리하며 이러한 비계층구조를 상호인증(Cross-Certification)이라고 한다. 상호인증에 대한 논의는 현재 ISO X.509의 프레임워크내에서 활발한 연구가 진행중에 있으며, 보다 세부적인 인증서 형식과 프로토콜들은 미국의 NIST와 IETF에 의해 연구중에 있다.

본고에서는 상호인증을 이해하기 위해서 인증기관을 구성요소로 하는 PKI 구조에 대해 개략적으로 살펴보고 일본에서 진행중인 상호인증에 대한 가이드라인으로서 상호인증을 위한 요구사항을 분석하였다. 그리고 인증기관 서비스 제공자로서 선두역할을 하고 있는 Xcert사의 상호인증 기술 및 현재 기술 개발동향을 알아본다.

Ⅱ. PKI 구조

1. 구성요소

전자인증제도는 전자상거래 정보보호기술의 핵심기술인 전자서명 기술의 안전한 운영을 의미한다. 이러한 전자서명 기술의 안전한 운영을 위해 필요한 기반기술이 공개키 기반구조이다. 즉, 공개키 기반구조는 전자인증제도의 실체화된 정보보호망이다.

공개된 공개키의 무결성 문제를 해결하기 위하여 등장한 것이 공개키기반구조(PKI : Public Key Infrastructure)로 공개키 대신 인증서를 공개한다. 공개키 기반구조란 정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용분야에서 인증서의 사용을 용이하도록 하는 정책, 수단, 도구 등을 수립하고 제공하는 객체들의 네트워크이다.[1]

● 인증기관

공개키 기반구조를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 각 계층마다 다른 명칭을 가지고 있다. 이들 기관을 [표-1]에서 나타내었으며 이들 세 기관 모두를 포함해 인증기관이라고 한다.[2]

[표-1] PKI의 인증기관

인 증 기 관	역할 및 수행기능
정 책 승 인 기 관 (PAA : Policy Approving Authority)	○ PKI 전반에 적용되는 정책수립 ○ 루트 CA로서의 역할 ○ 수행기능 - 정책과 절차 생성 및 수립 - 하위 CA의 정책준수 및 적합성 감사 - 하위 CA의 공개키인증 - 상호인증을 위한 정책 수립 - 하위 CA의 인증서, 인증서 취소목록 관리

정책인증기관 (PCA : Policy Certification Authority)	○ PAA의 하부계층 ○ 수행기능(PCA 영역내의 CA 및 사용자) - 정책 수립 - 하위 CA의 공개키 인증 - 인증서, 인증서취소목록 관리
인증기관 (CA : Certification Authority)	○ PCA의 하부계층 ○ 수행기능 - 사용자공개키 인증서 발행 및 취소 - 자신의 공개키와 상위기관의 공개키를 사용자에게 전달 - 인증서 발행(등록기관(RA) 요청) - 상호인증서 발행 - 인증서와 소유자 정보 관리(디렉토리 관리) - 인증서, 인증서 취소목록 및 감사파일 보관

● 등록기관(RA:Registration Authority)

인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자사이에 등록기관을 두어 인증기관 대신 사용자들의 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행한다. 등록기관을 조직 등록기관(ORA:Organizational Registration Authority)이라고도 한다.

● 디렉토리

인증서와 사용자 관련 정보, 상호인증서 쌍 및 인증서 취소목록(CRL:Certificate Revocation List) 등을 저장, 검색하는 장소로 인증기관에서 관리한다.

● 사용자

공개키/비공개키 쌍을 생성할 수 있어야 하며 공개키 인증서를 요청하고 획득한다. 또한 전자서명 생성 및 검증 기능 이외에도 인증서 해석에 관한 여러 기능을 가지고 있어야 한다.

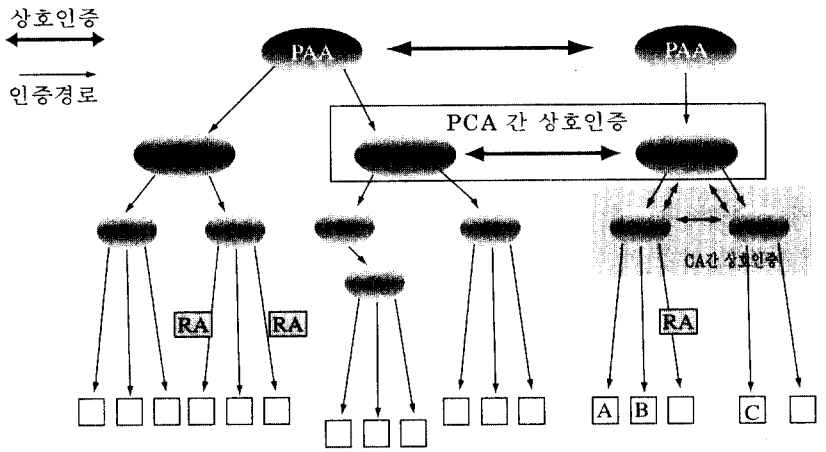


그림 1 PKI 계층구조

2. 인증방식

공개키 기반구조를 통한 공개키 인증서 획득 방식은 계층구조와 비계층구조로 분류되며 후자를 "상호인증(Cross-Certification)방식"이라고 부른다.

계층 인증방식은 최상위 계층을 최상위 인증기관(root CA)으로 두고, PKI내의 모든 사용자들간에 접속을 보장하는 전형적인 형태를 말한다. 이때 루트 인증기관 내에서의 모든 사용자들은 공개키 인증서 체인을 이용, 상대방의 공개키를 획득함으로써 인증이 가능해진다. 이에 반해 상호인증 방식의 경우는 공개키 기반구조의 계층구조에서 인증기관들간에 서로의 인증서를 발급하는 형태를 말한다. 보다 자세히 말하자면, 둘 이상의 인증기관들이 인증서를 서로 교환함으로써 신뢰성의 관계를 보다 확장한 방식이다. 따라서 계층구조에서 다양한 조합의 상호인증이 가능하며 상호인증하는 해당기관 사이에는 상대방의 정책 준수가 반드시 보장되어야 한다.[2] 이들 두가지 방식간의 장·단점을 [표-2]에 나타내었다.

[표-2] 인증방식의 비교

인증방식	장 점	단 점
계층구조	○ 계층적인 관리조직에 적합 ○ 계층적 디렉토리 이름 ○ 인증 경로탐색 용이 ○ 사용자 자신의 상위 공개키를 알고 있기 때문에 인증경로 제공 및 검색 가능	○ 전세계를 통합하는 하나의 최상위 CA가 존재해야 하는 불합리성 ○ 최상위 CA의 비밀키 안전성 문제 ○ 전자상거래에 적합하지 않음
비계층구조 (Cross-Certification)	○ 인증기관간의 상호 신뢰 ○ 신뢰성을 근간으로 한 CA간의 상호인증 ○ CA 비밀키 복구가 간단	○ 인증경로 탐색의 복잡성 ○ 단일 인증경로 불가능

Ⅲ. 상호인증

정보통신 기술의 급속한 발달로 인하여 지금까지 별개로 존재했던 각종의 기반구조가 하나의 단일한 정보기반구조로 통합되면서 국가의 경제와 국민생활에 미치는 영향이란 실로 대단하다. 특히 사이버시대가 도래하면서 전자상거래는 현실경제로 일반 사용자에게도 피부로 느껴지는 기술이며 이에 대한 안전·신뢰성을 제공하기 위한 기반 정보보호서비스들 중에 하나가 공개키 기반구조이다. 이는 세계 각국을 하나로 묶는 인터넷을 통해 사용자의 물리적 위치에 상관없이 안전하게 상거래를 할 수 있도록 해준다. 이를 위해서 해결해야 하는 가장 큰 문제중에 하나가 바로 상호인증 서비스이다. 일본의 ECOM에서는 전자상거래에 관한 기반연구를 진행하는 컴소시엄인데 여기서 1998년 7월 상호인증에 대한 가이드라인[3](Cross Certification Guidelines, Alpha

version)을 제안하였다. 본 절에서는 상호인증(cross-certification)에 대한 기본개념을 소개하고 상호인증에 대한 가이드라인에서 제안된 요구사항을 중심으로 서술하였다.

1. 상호인증의 개념

앞절에서 서술한 바와 같이 인증기관은 사용자의 공개키로 인증서를 발행하고 사용자는 이러한 인증서를 검증하기위해 인증기관의 공개키를 이용한다. 또한 검증된 인증서로 다른 사용자는 인증기관에 의해 실제로 인증서가 발행 되었는가를 확인하게 된다. 이러한 작업을 위해, 두 번째 사용자는 먼저 인증기관의 공개키를 확보해야만 한다. 단일 인증기관으로 소수의 사용자 그룹인 경우, 각 사용자는 곧바로 인증기관의 공개키를 확보할 수 있다. 하지만 이것은 실제 환경에는 적합하지가 않다. 그러므로, 대부분의 공개키 기반구조는 여러 인증기관으로 하여금 다른 인증기관들을 위한 인증서가 발행되도록 설계되고 있다. 이렇게 함으로써 한 인증기관이 다른 인증기관을 신뢰하게 되고 이와 더불어 사용자도 다른 인증기관에 속한 사용자를 신뢰할 수가 있다. 이와 같이 다른 사용자의 공개키를 검증하기 위해 사용자는 여러 인증경로를 거치게 된다. 이러한 처리과정을 "인증서의 체인"이라고 부른다. 따라서 "인증서의 체인"의 길이는 체인을 따라 여러 인증기관을 거치는 동안 검증되어야 할 인증서의 갯수로 정의할 수 있다. 결과적으로 이 "인증서의 체인"은 인증 기관의 계층구조내에 신뢰도를 검증하는데 있다고 볼 수 있다.

인증을 위한 이러한 계층은 공개키 기반구조에서 운영하기가 매우 용이하다. 예를 들어, 어느 한 사용자가 최상위 인증기관의 공개키를 안다고 할 경우에 이 계층구조내에 있는 어떤 사용자와도 손쉽게 인증이 가능하다. 하지만 이러한 방식에서, 문제점은 대부분의 "인증서의 체인"내에 최상위 인증기관이 최소한 반 이상 포함되어 있다는 데 있다. 또 다른 문제점으로 "인증서의 체인"이 점차적으로 늘어감에 따라 신뢰도는 점점 떨어져 간다. 이러한 이유들로 인해 "상호인증"에 대한 필요성이 대두하게 되었다. 기본적으로 상호인증은 동일 계층내지는 다른 계층의 임의 지점에 있는 다른 인증기관과의 신뢰 즉, 인증을 위해 단 한번의 처리 과정을 요한다. 다시 말해, 이것은 인증서 체인에 대한 지름길이라고도 말 할 수 있다.[4]

예를 들어 XYZ 는 인증기관이 X라는 인증기관과 곧바로 상호인증을 한다고 할 경우에, 이를 위해 사용자는 단 두번의 인증서 체인을 통과하면 된다.

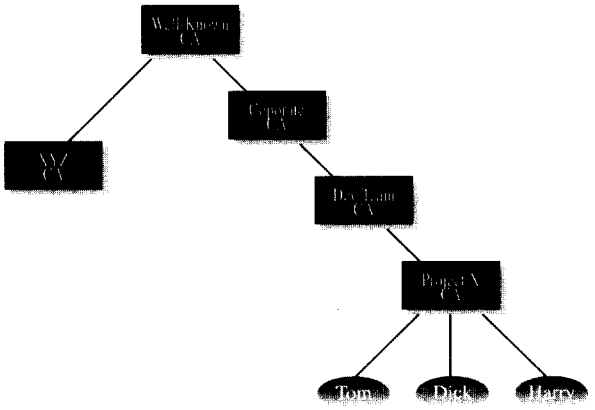


그림 2. 상호인증

(그림 3)에서와 같이 Tom이라는 사용자가 XYZ라는 인증기관에 속한 사용자와 상호인증을 한다고 할 경우에, Tom은 상위 인증기관인 X의 공개키를 알고 있다고 가정한다면 다른 사용자와 XYZ 인증기관, 그리고 XYZ 인증기관과 X 인증기관 사이에 인증만 확인되면 되는 것이다. 물론 이러한 경우는 두 인증기관들에 대한 신뢰가 상당수 확보되었거나 상호인증에 대한 협상이 사전에 이루어진 경우라야 가능할 것이다.

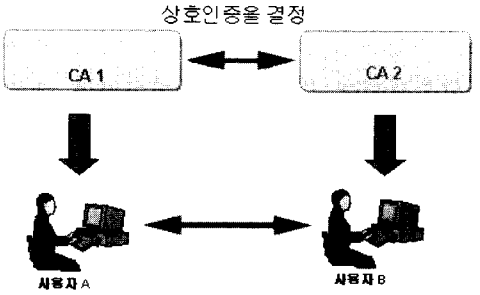
2. 상호인증을 위한 요구사항

상호인증은 전자상거래의 구성요소인 디지틀 인증에 대한 유효성을 향상시키는 중요기술로 인식되고 있으며 다음과 같은 세가지 관점에서 논의될 수 있다.

- CA간 상호인증 모델
- 상호인증을 수행하는 인증기관의 운영요구사항
- 상호인증의 기술요구사항
  - 상호인증, 인증서 취소목록(CRL) 형식
  - 상호인증을 위한 인터페이스
  - CRL의 운영

2.1 CA간 상호인증 모델

CA간 상호인증에서는 인증서 도메인의 범위에 따라 두가지 유형이 존재한다. 인증서 도메인이 같은 경우 상호인증서(cross certificate)를 분배하는 방법을 (그림 2)에서 표현하고 있는데 CA1와 CA2 모두의 통제영역내에 있는 인증서 도메인에서 인증정책 수준을 조정하고 인증절차를 감독한다. 인증기관에서 상호인증서를 생성하여 각 개체들에게 분배할 수 있으며 이 상호인증서는 다른 인증도메인에서도 유효하다.



같은 도메인에 있는 CA간의 상호인증

그림 2. CA간의 상호인증 모델

다른 하나의 방법으로 제 3의 신뢰기관을 이용한 모델이다. 원격지에 있는 사용자를 인증하기위해서 이 제 3의 신뢰기관을 이용하게 되는데 두 인증기간사이에 상호인증이 이루어지기만 하면 제 3의 신뢰기관을 세울 수 있다. 상호인증 서비스를 제공하는 인증기관은 신뢰도를 기초로 서로간의 호환성을 가질 수 있는 인증정책을 세워야 하며 인증기관에 속해있는 사용자에게 상호인증서를 분배해주기 위해서는 상호인증서를 상호인증 창구에게 신청하여야 한다.

Cross Certification Guideline[3]에서는 인증서 저장소(repository)가 존재하지 않기 때문에 인증기관이 사용자에게 인증서를 분배할 때 상호인증서가 같이 분배되는 것으로 가정한다.

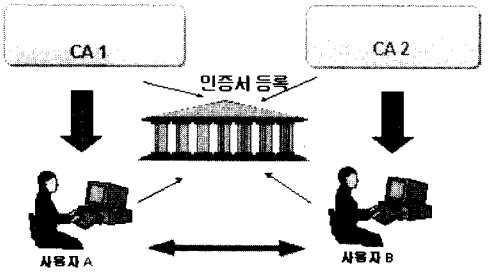


그림 3. 제 3의 신뢰기관을 이용한 상호인증 모델

2.2 상호인증을 위한 고려사항

- 상호인증 서비스를 제공하기 위해서 고려

해야할 사항
- 상호인증에 참여하는 인증기관의 수
- 상호인증을 위한 인증기관들간의 협약
- 협약에 대한 조건(예, 동일 계층내에서 상호인증/다른 계층간에 상호인증)
- 국제 상호인증
- 인증기관들에 대한 제약조건
- 인증서/인증서 취속목록(CRL) 형식
- 인증프로토콜
- 동일 프로토콜에 있어서의 상호인증
- 다른 프로토콜에 있어서의 상호인증
- 인증 정책
- 암호 알고리즘

3. 인증기관의 운영요구사항

이번 절에서는 어느 한 인증기관이 같은 혹은 다른 인증 도메인내에 있는 인증기관과 상호인증을 수행하기 위해서 제공하여야 하는 운영요구사항을 요약하여 표로 나타내었다.

[표-3] 상호인증 운영요구사항

요 구 사 항		내 용
관 리	Screening과 인증서 발행	○ Screening 표준과 인증서 발행 표준에 대한 상호 협정체결 (서면결의) ○ 인증기관이 신뢰도 등급이 다른 인증서를 발행하는 경우 신뢰도 등급에 대해 부분적으로 협정
	Disclosure와 Notification	○ CA 각 인증정책 발표 ○ 상호인증서 구현 기술 및 제약조건 ○ 상호인증서 명칭
인증서 도메인 신뢰도	호환성	○ 인증서 발행을 책임지는 screening의 등급에 의존 ○ 인증서 신뢰도(신용도 및 잔액 검사에 기초) ○ 인증서 응용분야에 따라 차등을 두어서 적용 ○ 같은 신뢰도를 가진 인증서에 대해 상호인증 체결
	공 표	○ 인증서 유형 공표(상호인증 분야, 신뢰도)
의 무		○ 인증기관과 상호인증을 담당하는 사람사이의 책임과 의무
감 사 (Audit)		○ 기술적 요소에대한 정기적인 감사 ○ 상호인증을 체결한 인증기간간 상호감사 메커니즘 ○ 미공개 감사에 대해서는 사전에 인증기간간 동의가 필요
상호 인증	승인조건	○ 운영조건 : 상호인증서 분배, 유효기간, 갱신, 취소절차, 책임/면제 조건 ○ 기술조건 : 인증서 형식, 상호인증서 분배, 사용자 인증서 검증방법
	분 배	○ 인증서 소유자 정보 ○ 인증서 전달방법(저장장소, 배달장소, 자격) ○ 공개키생성
	유효기간	○ 사용자 인증서 유효기간을 고려하여 상호인증서의 유효기간 설정 ○ 짧은 갱신기간
	갱 신	○ 유효기간 만료 ○ 인증서 재분배
	폐 지	○ 상호인증서 폐지 우선순위 결정 ○ 상호인증서 폐지절차/폐지된 인증서 발표절차
상호인증 취소		○ 상호인증 취소시 이에 대한 절차와 상호인증서 처리 문제를 상호인증 서비스 개시이전에 결정

상호인증이 성립되기 위한 중요한 요소로 인증기간 사이의 상호 신뢰도가 일치하여야 한다. 인증기간은 인증서 응용분야에 따라 인증서의 신뢰도 등급을 다르게 운영할 수 있으므로 이에 대한 상세한 협의가 이루어져야 한다. 다음은 신뢰도 등급에 따른 screening 내용을 [표-4]에서 정리하였고 [표-5]에서는 신뢰도와 상호인증서 사이의 관계를 보였다.

[표-4] 신뢰도 등급[4]

screening 등급	screening 내 용
하위 등급	◦ 인증된 이름/e-mail 주소 등의 존재여부
중간 등급	◦ 개인이나 회사등의 인증을 위한 문서와 제 3의 신뢰기관을 경유한 문서의 검증
	◦ 인증된 이름/e-mail 주소 등의 존재여부
상위 등급	◦ 개인이나 회사등의 인증을 위한 문서와 제 3의 신뢰기관을 경유한 문서의 검증
	◦ 주체와의 직접 접촉을 포함한 여러 수단들에 의해 주체의 신원을 설립

[표-5] 신뢰도 등급과 상호인증과의 관계[4]

	하위 등급	중간 등급	상위 등급
하위 등급	O	N	N
중간 등급	N	O	N
상위 등급	N	N	O

O : Preferable form. (각각의 등급범위내에서 서비스가 제공)
N : 상이한 등급간의 상호인증 (하위 등급쪽으로 조정)

4. 기술요구사항

이번 절에서는 기술적인 관점에서 요구될 수 있는 상호인증 형식과 상호인증 인터페이스 및 CRL 운영들에 관해 기술한다.

4.1 상호인증서

인증서의 형식은 X.509에 따라 다음과 같은 세 요소들로 분류할 수 있다.

- 사용자 인증서(User Certificate)
- 인증기관 인증서(CA Certificate)
- 상호인증서 쌍(Cross Certificate Pair)

X.509에서 정의하는 인증서 형식을 적용하여 상호인증서를 생성하기 위해서는 몇가지 필드를 설정해야 하는데 다음 [표-6]에서 이러한 필드를 나타내었다.

[표-6] 상호인증서 설정프로토콜[4]

분 류	필 드	상호인증서 설정 프로토콜
기 본 블 럭	Version No.(version)	○
	Serial number(serial Number)	○
	Signature information(signature)	○
	AlgorithmIdentifier	○
	Name of issuer(issuer)	○
	Validity period(validity) - notBefore / notAfter	○
	Owner name(subject)	○
	Owner public key information (subject PublicKey Info) - AlgorithmIdentifier	×
V2 확장블럭	Issuer unique identifier(Issuer Unique Identifier)	×
	Subject unique identifier(subject Unique Identifier)	

4.2 상호인증의 확장

일반적인 인증과는 달리 상호인증의 경우에는 확장된 부분이 상호인증 프로토콜로 이용될 수 있다. 향후 상호인증을 위한 인증정책과 관련한 필드가 추가될것이다. 하지만 이러한 필드의 이용은 현 상황에서는 명확하지 않으므로 임의로 허용되든지 아니면 운영관리자의 의견에 따라 정책의 호환성을 이룰 수 있도록 허용될 수 있을 것이다.

일반적인 인증서와는 달리 다음과 같은 특별한 필드가 요구된다.

- 인증기관 키 ID
- 인증 정책
- 정책 매핑

[표-7] 상호인증 설정프로토콜(V3확장 블럭)[4]

Category	Field	Critical	Cross Certification installation protocol	
Key and policy information	Authority KeyIdentifier	Ignore	O(C=Y)	
	● KeyIdentifier		O	X
	● authorityCertIssuer		X	O
	● authorityCertSerialNumber		X	O
	Subject Key Identifier	Ignore	A	
	Key Usage	Arbitrary	A(C=Y)	
	Private Key Usage Period	Arbitrary	A(C=N)	

	Certificate Policies	Arbitrary	A(C=Y)
	● Policy Identifier		A
	● PolicyQualifiers		A
	Policy Mappings	Ignore	A(C=Y)
Certificate Subject attribute Issuer attribute	Subject Alternative Name	Arbitrary	A(C=N)
	Issuer Alternative Name	Ignore	A(C=N)
	SubjectDirectoryAttributes	Arbitrary	A(C=N)
Constraint of certification path	Basic Constraints	Arbitrary	A(C=Y)
	● Certification authority(cA)		A
	● pathLenConstraint		A
	Name Constraint	Arbitrary	A(C=Y)
	● permittedSubtree		A
	● excludeSubtree		A
	Policy Constraints	Arbitrary	A(C=Y)
	● policySet		A
	● requireExplicitPolicy		A
	● inhibitPolicyMapping		A
CRL identifier	CRL Distribution Points	Arbitrary	A(C=N)
	● distributionPoint		A
	● reasons		A
	● CRL issuer(cRLIssure)		A

4.3 상호인증 인터페이스

상호인증 인터페이스에서는 상호인증을 하기위해 개체들간에 전송될 필요가 있는 정보들을 표시하고 특정 프로토콜에 독립적인 방식으로 상호인증을 수행하도록 하는 기술적 기본요소들을 서술하여야 한다. 상호인증 인터페이스는 다음 두 부분으로 정의 될 수 있다.

1. 인증 인터페이스의 설정(인증기관과 사용자대한 인증요구사항에 기초)
2. 인증서 취소목록(CRL) 분배 인터페이스

인증서 취속목록의 운영은 먼저 인증서를 폐지해야 할 대상에 대한 조사를 행한 후, 인증서 취소목록에 대한 분배 인터페이스를 설정하여야 한다. 인증서에 대한 취소는 상호인증의 경우 일반 인증서 취소와는 다르다. 예를 들어 인증서 취소목록 생성과 분배에 대한 시간 간격이 0 보다 클 경우에는 인증서 취소목록이 완전히 분배되어 서비스를 재개할 때까지 제공되고 있는 서비스를 중단해야 한다. 상호인증은 실제로 상호인증서내에 담겨져있는 CA 인증서의 취소에 의해 철회되기 때문에 상호인증서에 대한 인증서 폐지목록은 존재하지 않으며, 따라서 상호인증서의 폐지는 인증기관이 발행한 인증서의 인증서 취소목록의 제어에 의존한다.

Ⅳ. 상호인증 기술동향

1. 상호인증(Cross-Authentication)

상호인증은 실제로 하나의 인증기관이 다른 많은 인증기관들 사이에서 인증을 수행할 수 있다. 이러한 경우 해당 사용자는 보다 효율적인 상호인증이 이루어지기 위해 상호인증과 관련한 모든 사항들을 인지하고 있어야만 한다. 따라서 상호인증의 체인이 짧으면 짧을수록 공개키 기반구조 운영은 보다 어려워지게 된다. 실제로 공개키 기반구조에서 위와 같은 문제는 해결하기가 어렵다. 인증서 취소목록을 이용한 해결 방법이 있을 수 있다. 왜냐하면 인증서 취소목록내에는 유효하지 못한 인증서에 대한 목록들이 있으므로 이를 참조하여 즉각적인 상호인증을 가능케 할 수 있다. 하지만 이런 경우, 인증서 취소목록의 양이 많으면 많을수록 해당 사용자가 기억해 두어야 할 정보가 많아질 수 있으며, 보다 심각한 문제로 인증서의 폐지와 새로운 인증서 취소목록의 갱신간에 시간 차이가 발생할 수 있다. 이렇게 되면 사용자와 사용자간의 신뢰도를 위해 인증서 취소목록을 자주 갱신해야 하는 부담이 있게 된다.

인증기관 구현기술에서 앞서가고 있는 Xcert사에서는 상호인증(Cross-Authentication)을 제안하였는데 기본적인 아이디어는 인증권한을 상위 인증기관이 수행하도록 하는 것이다. 여기서 인증기관은 그들 스스로 다른 인증기관에 대한 신뢰여부 및 방법을 결정하게 된다. 예를들어 (그림3)에서 XYZ CA와 Project X CA가 인증체인을 거치지 않고 사용자들을 상호인증한다면, 이들 사용자들이 속한 CA가 가지고 있는 지식을 기반으로 상호인증을 수행한다. XYZ CA에 속해있는 사용자 A가 Project X CA에 속해있는 사용자 B로부터 메시지를 받는 경우에 이 메시지는 Project X CA가 발행한 인증서로 서명된 것이다. 메시지의 유효성을 검증하려는 사용자 A는 이 메시지에 포함된 인증서를 XYZ CA로 보내서 검증요청을 간단하게 할 수 있다. 그러면 XYZ CA는 이 인증서가 Project X CA가 발행한 인증서임을 인식하여 Project X CA에게 직접 인증서의 유효성에 대한 질의를 하게 되고 XYZ CA는 Project X CA로부터 받은 응답을 사용자에게 되돌려줄 것이다. 기본 방식의 경우, 해당 사용자는 다른 사용자와의 상호인증을 위해 인증서 체인에 대한 인증과정이 끝날때까지 참여해야 했다. 하지만 제안된 방식에 따르면 사용자 인증에 대한 모든 권한을 상위 인증기관에 일임하여 이 인증기관으로 하여금 인증과 관련한 모든 요청, 처리 및 응답을 할 수 있도록 함과 동시에 사용자는 다른 프로세스를 행할 수 있도록 하자는 데 있다. 이러한 경우에 장점은 첫째, 사용자가 인증처리에 대한 세세한 관리를 할 필요가 없고, 둘째로, 신뢰성과 관련된 어떤 변화들이 네트워크를 통해 즉각적으로 전파될 수 있다는 것이다. 따라서 온라인 및 실시간 프로토콜로 인해 사용자 인증에 관한 문제를 해결할 수가 있다.[3]

2. 상호인증 기술동향

Xcert사 이외에도 공개키 기반구조에서 상호인증을 구현하기 위한 기술들이 많이 연구되고 있는에 이를 살펴보면 아래 [표-8]과 같다.

Ⅳ. 결 론

공개키 기반구조하에서 상호인증에 대한 문제는 현재 국제적으로 활발히 연구중에 있으며 몇몇 회사에서는 이를 상용화 추진중에 있다. 하지만 상호인증을 실현하는데 있어, 인증기관들간에 호환성이라든가 정책 확장등의 문제를 감안할 때 실질적인 서비스의 완전한 구현은 당장은 어려울 것으로 생각된다. 1998년 6월 일본 ECOM에서는 상호인증을 위한 가이드라인을 제안하여 상호인증을 구현하기 위해

[표-8] 상호인증 기술동향

관련회사	현 동 향
xcert International Inc(미)[3]	- 현재 상호인증에 관한 솔루션으로 "Cross Authentication" 이라는 기술을 보유
ECom사(일)[4]	- 1997년, "Technical Comments on Cross Certification and Draft of Basic Specfication" 보고서 발표 - 1998년 6월 "Cross Certification Guide-lines" 발표
Entegrity Solutions Corp(미)[5]	- 1998년 현재, 상호 인증에 관한 솔루션으로, 최상위 인증기관의 공개키 교환과 direct trust model을 통해 인증서를 상호교환하는, "Entegrity"와 "Entrust"를 보유
JapanNet(일) & CommerceNet(미)[6]	- 미·일 국가간 상호 인증을 위한 계획 구상 - 계획을 위한 CA S/W는 Xcert사에서 지원
ISO x.509 v3[7]	- 인증서와 CRL에 대한 검증과 상호인증, 정책확장, 키 ID 확장 등, 인증서로 하여금 보다 다양한 정보를 처리할 수 있도록 인증서를 확장

고려하여야 할 사항들을 인증기관 운영과 상호인증 구현을 위한 기술적 요구사항들을 제시하였다. 현재 우리나라에서도 인증기관 구축을 위한 노력이 공공부분과 민간부분에서 활발히 진행중에 있으며 정부도 "전자상거래기본법(안)" 및 "전자서명법"을 마련하여 시행에 대한 준비를 하고 있다. 향후 상호인증이 실제로 구현되기 위해서는 기반기술뿐만 아니라 법·제도도 같이 뒷받침되어야 하기 때문에 공공기관과 민간분야가 공동관심을 가지고 공개키 기반구축에 박차를 가해야 할 것이다.

참 고 문 헌

[1] 한국정보보호센터, 정보보호 뉴스 통권 6호, 1997.9

[2] 한국정보보호센터, 공개키 기반구조 구축을 위한 디렉토리 서비스 구현, 1998.6

[3] Andrew Csinger, "InterSpect: Cross Certification- A 50% Solution", "http://www.xcert.com/support/papers/Cross__certification.html"

[4] ECOM, Cross Certification Guidelines (Alpha version), 1998.6

[5] http://www.entegrity.com

[6] http://www.commerce.net

[7] ISO/IEC 9594-8: 1995 | ITU-T Recommendation X.509 (1993E), Information Technology-Open Systems Interconnection - The Directory : Authentication Framework, 1993.11

□ 著者紹介

홍 기 웅

1985년 2월 전남대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산과(석사)
1994년 4월 정보처리 기술사
1996년 2월 아주대학교 컴퓨터 공학과 (박사)
1985년 9월 ~ 1995년 10월 한국전자통신 연구소 선임연구원
1992년 ~ 1993년 이태리, Alenia Spazio사 Senior Researcher
1995년 10월 ~ 1996년 4월 한국전산원 선임 연구원
1996년 4월 ~ 현재 한국정보보호센터 책임 연구원, 기술기준 팀장
※ 주관심분야: 컴퓨터 • 네트워크 보안, 정보시스템 위험분석 • 평가, 정보보호 표준화

권 현 조

1997년 2월 성균관대학교 정보공학과(학사)
1998년 3월 - 현재 성균관대학교 정보통신대학원 재학중
1997년 1월 - 1997년 7월 (주)나라계전 연구소, 연구원
1997년 7월 - 현재 한국정보보호센터 연구원
※ 주관심분야 : 정보보호시스템 평가체계, 네트워크 보안, 전자서명