제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

# 전자거래 인증서 관리를 위한 ClientCA 운영 메커니즘 설계

김 점 구*, 나 상 엽*
* 남서울대학교 컴퓨터학과

## 요 약

인증서는 PKI 시스템에서 사용자 인증 서비스를 제공하기 위한 중요한 매체이다. 본 논문에서는 인증서를 효율적으로 활용하는 방법의 일환으로 ClientCA라 불리는 도구를 전자거래 인증에 적용하는 방법을 제안하였다. 각종 인증서의 효율적인 관리와 활용을 통해서 정보화 시대의 근간을 이루고 있는 사용자 인증에 대한 서비스를 보다 효율적으로 이용할 수 있을 것이다. 특히, ClientCA는 특정 목적을 지니고 운영하는 소규모 단위의 PKI 시스템에 효율적으로 접목시켜 사용할 수 있음을 본 논문을 통해서 알 수 있게 된다.

# Design of ClientCA Operation and Mechanism for e-Commerce Certificate Management

Jeom Goo Kim*, Sang Yeob NA*

## ABSTRACT

A certificate is important media for the purpose of offering user-authentication service on PKI system. In the paper we analyzed management implement which could make the efficient use of a certificate. This implement called ClientCA will make efficient use of the service about user-authentication consisting of the basis in the age of information through efficient management and partial use of each certificates. Especially, ClientCA could be used efficiently by grafting a small group of PKI system which is operated with particular purposes.

※ 본 연구는 한국과학재단 목적기초연구(R05-2002-000-01244-0) 지원으로 수행되었습니다.

## 1. 서 론

이용 범위가 급격히 커지고 있는 인터넷 뱅킹, 전자상거래, 전자 결재 등과 같은 업무가 안전하게 진행되기 위해서는 반드시 인증서비스가 필요하다. 온라인 특성상 인증되지 않은 정보의 교환은 상대방으로 하여금 신뢰성에 의문을 제기하게 되고, 정보 및 문서의 변경, 불법 열람 등의 위험성을 초래하게 되므로, 보다 신뢰성을 가지고 안전한 정보의 교환을 위해서는 이들 정보를 법적 효력을 지니는 공식적인 인증서비스를 사용하는 것이 필요하다.

이에 IETF에서는 인증과 관련한 기반 기술을 RFC 표준으로 제정하였고, 국내에서도 1999년에 전자서명법을 제정하여 인터넷을 통해 교환되는 정보의 안전성과 신뢰성을 확보에 활용되어지고 있다. 그러나 국내·외적으로 늘어가는 인증서를 효율적으로 관리하고, 활용하기 위한 인증서 관리 도구의 개발은 현재까지 미흡한 실정이다. 특히, 특정 목적을 지닌 소규모에서 공개키 기반의 인증서비스를 사용하기 위해서는 절차상 또는 업무상으로 일반 사용자가 사용하기에 어려웠던 것이 사실이다.

이에 본 논문에서는 IETF의 RFC 표준을 통해서 공개키 기반 구조에 부합하는 인증서 관리 도구를 분석하여 효율적인 인증서 관리에 활용하도록 하고자 한다.

## 2. 관련 연구

### 2.1 인증서 관리 프로토콜

인증서 관리 프로토콜(CMP : Certificate Management Protocol)은 공개키 인증 시스템을 구성하고 있는 각 구성요소 상호간의 작용을 유기적으로 관리할 수 있는 기능을 규정하고 이들 기능을 그룹화 한다. 공개키 인증 시스템은 이를 관리하는 개인들의 타입에 맞추어 구성되어져야 하지만, 관리자에게 무제한적인 선택 기능을 제공한다면, 요구되어 지는 관리 소프트웨어가 매우 복잡해지고, 미묘한 실수에 대해 위험한 결과를 초래하게 된다. 또한, 관리자의 선택 기능을 지나치게 제한한다면, 인증기관, 등록기관, 최종 사용자들은 공개키 인증 시스템을 사용하지 않을 것이다. 그러므로 관리 프로토콜은 공개키 기반 구조를 구성하는 각 요소들의 온라인 상호작용이 반드시 이루어져야 하며, 인증서 관리 프로토콜은 인증서의 원활한 관리와 각 구성요소간의 유기적인 상호작용 지원을 위해서 ISO 9594-8 표준과 이와 관련된 수정안을 따라야 한다.

### 2.2 관리 프로토콜 주요 기능

공개키 인증 시스템을 구성하고 있는 각 구성요소간의 상호 작용과 관리 요구사항은 상위 레벨에서 다음과 같은 주요 관리 기능으로 그룹화 될 수 있다[1][3].

① 인증기관 설립 : 새로운 인증기관이 설립될 경우에는 초기 인증서 폐지 목록의 생성과 공개키의 발송과 같은 단계가 요구된다.

② 최종 사용자의 초기화 : 최종 사용자의 초기화는 최상위 인증기관의 공개키 획득과, PKI 관리 실체가 지원하는 선택 사항 정보를 요구하는 것을 포함한다.

③ 인증 : 최종 사용자와 인증기관, 혹은 등록기관과 인증기관에서 발생하는 관리사항을 포함하며, 새로운 인증서가 생성된다.

④ 인증서/CRL 공표 : 인증기관과 최종 사용자는 발행된 인증서와 인증서 취소 목록을 디렉토리나 데이터베이스를 이용하여 공개적으

로 공표해야 한다.

⑤ 인증서/CRL 조회 : 인증기관과 최종 사용자는 공개 저장소에 저장되어 있는 인증서와 인증서 취소 목록을 조회할 수 있어야 한다.

### 2.3 부가적 관리 기능

인증서버와 ClientCA간의 원할한 상호 작용과 이용의 효율성을 높이기 위해서는 기본적인 주요 관리 기능 이외에도 부가적인 관리 기능이 요구된다. 다음은 실제 운영에 필요한 부가적인 관리 기능을 그룹화한 것이다[1][3].

① 개인키 소유 증명 : 인증기관은 최종 사용자가 발급받은 인증서의 공개키에 대응하는 개인키를 소유하고 있는 사실을 확신할 수 있어야 한다.

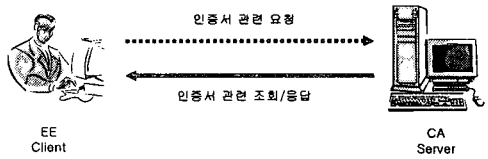
② 인증서 검증 : 최종 사용자는 이용하려는 인증서의 유효성 여부를 검증할 수 있어야 한다. 인증서 검증은 기본적으로 인증서에 포함된 유효기간을 통한 검증과 공개 저장소에서 인증서 폐지 목록을 다운받아 이를 검증할 수 있어야 한다.

## 3. ClientCA 분석

### 3.1 요구사항

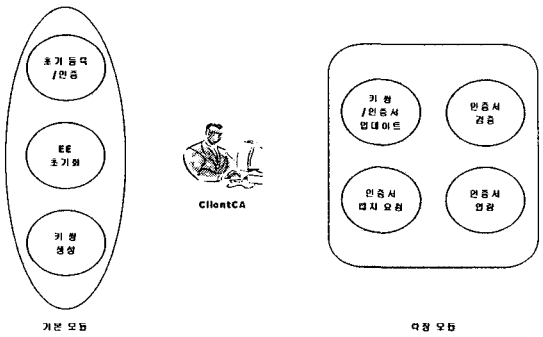
본 논문에서 분석하고자 하는 ClientCA는 공개키 인증 업무와 관련되어 있는 복잡한 과정을 단순화하고, 공개키 기반의 인증 시스템의 안전성을 파괴하지 않는 한도에서 각 과정과 책임을 부여하여 보다 간소화되고 효율적인 인증 업무를 구축하는데 목적이 있다. 또한, 최종 사용자가 인증서를 효율적으로 이용하고 관리할 수 있는 인증서 관리 도구를 분석하는데 그 목적이 있다. 이러한 목적을 달성하기 위해서는 ClientCA와 인증서버사이에 안전한 통신 채널이 확립되어 있어야 하며, 공개키 기반 인증 시스템의 신뢰성을 해치지 않는 한도 내에서 적절한 업무의 간소화가 이루어야 하고, 인증서버는 ClientCA의 인증 업무 요청에 대해서 즉각적인 응답이 가능해야 한다.

또한 효율적인 인증서 활용과 관리를 위해서 ClientCA는 자체적으로 인증서 생성을 위한 공개키 쌍 생성과 인증서의 유효성 여부를 검증할 수 있어야 하고, 공개 저장소에 접속하여 인증서 및 인증서 폐지 목록의 조회가 가능해야 한다. [그림 1]은 기본적인 ClientCA와 인증서버 사이의 관계 모델이다.




[그림 1] ClientCA 동작 모델

### 3.2 모듈 분석




[그림 2] ClientCA 관리 모듈

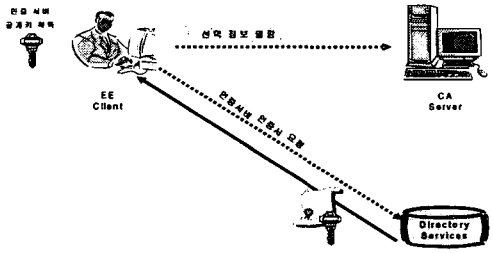
ClinetCA의 모듈은 크게 인증서 생성과 관리를 위한 기본 모듈과 인증서 활용을 위한 확장 모

듈로 나누어 볼 수 있다. 기본 모듈은 인증서의 초기 생성을 위한 초기등록/인증 모듈, EE 초기화 모듈, 키 쌍 생성 모듈로 나누어 볼 수 있으며, 확장 모듈은 인증서의 유효성을 검증하기 위한 모듈과, 키 쌍 업데이트를 통한 인증서 업데이트 모듈, 인증서 폐지 요청 모듈, 인증서 열람 모듈등이 있다. [그림 2]는 ClinetCA에서 요구되는 각각의 모듈이다.

가. 기본 모듈

1) ClientCA 초기화

ClientCA가 인증서버와 연계하여 인증업무를 수행하기 위해서는 인증서버의 공개키를 획득하고, 지원하는 선택 정보를 요구하여 확인해야 한다. ClientCA의 초기화기 이루어지는 과정은 [그림 3]과 같이 인증서버의 인증서를 공개 저장소에서 다운받아 인증서버의 공개키를 획득하게 되며, 선택 정보 역시 공개 저장소 또는 인증서버에서 발행한 문서를 통하여 확인하게 된다.



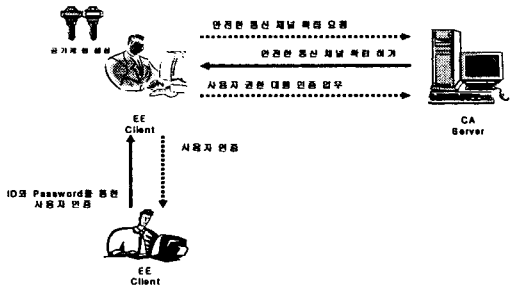

[그림 3] ClientCA 초기화

2) 키 쌍 생성

ClientCA에서는 인증서 발행을 위한 공개키/개인키 쌍은 [그림 4]와 같이 인증서버와 ClientCA 양측에서 생성할 수 있다. 키 쌍을 인증서버에서 생성시키는 것을 중앙키 생성방식이라고 부르며, ClientCA에서 생성시키는 것을 원격키 생성방식이라고 부른다. 인증서 발급을 위한 키 쌍 생성은 키 쌍의 생성 위치를 결정한 후에 키를 생성하는 순서로 진행된다

3) 초기 등록/인증

초기 등록 및 인증은 키 생성과정을 포함하며, ClientCA 또는 인증서버에서 생성된 키 쌍의 생성과 사용자 인증, 메시지 인증을 위한 모듈로 구성되어 있다. 사용자 인증은 인증서를 발급 받거나 활용하려는 최종 사용자의 아이디와 패스워드를 사용하여 ClientCA에 접근하면, 인증서버는 별도의 절차없이 해당 ClientCA를 인증하는 것으로 대신하게 된다. 또한 메시지 인증에 대해서는 ClientCA와 인증서버사이에 안전한 통신 채널을 확립하는 것으로 대신하게 된다. [그림 5]는 초기 등록 및 인증을 위한 모듈의 접근 방법이다.



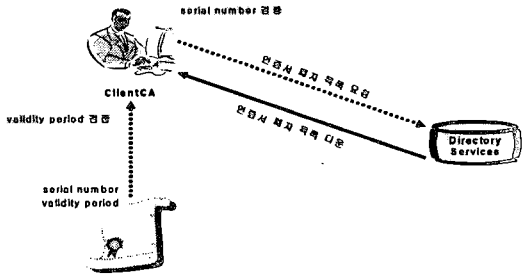

[그림 5] 초기 등록 및 인증

나. 확장 모듈

1) 검증

최종 사용자 디렉토리에 저장되어 있는 인증서의 공개키 값을 사용하기 위해서는 해당 인증서의 유효성 여부를 검증할 수 있어야 한다. 인증서 검증은 [그림 6]과 같이 해당 인증서의 유효기간을 검증한 후에 유효기간이 경과되었을

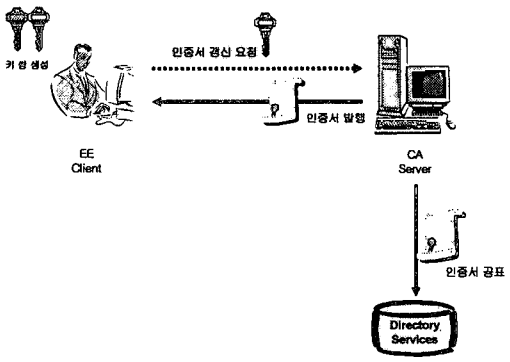
경우에는 바로 해당 인증서가 유효하지 않음을 검증하며, 다음으로 공개 저장소에 저장되어 있는 인증서 폐지 목록을 받아 해당 인증서의 고유번호가 포함되어 있으면, 유효하지 않은 인증서임을 검증하게 된다.




[그림 6] 인증서 검증

2) 업데이트

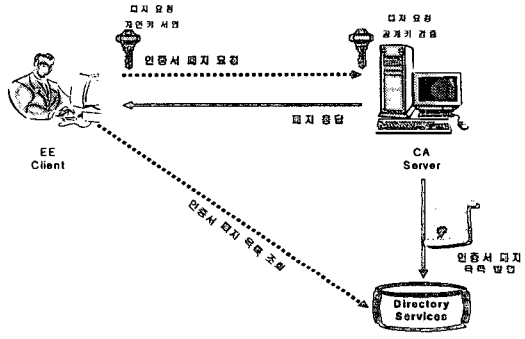
인증서 소유자의 부서 이동과 같은 환경변화 또는 키 손상 및 손실의 위험이 존재할 경우에는 해당 인증서를 효력정지 시키고, 업데이트 할 수 있는 요청 모듈이 필요하다. 인증서 업데이트는 [그림 7]과 같이 새로운 키 쌍을 생성 후에 인증서버에 새로운 키 쌍에 대한 인증서의 업데이트를 요청한다.




[그림 7] 인증서 업데이트

3) 폐지 요청

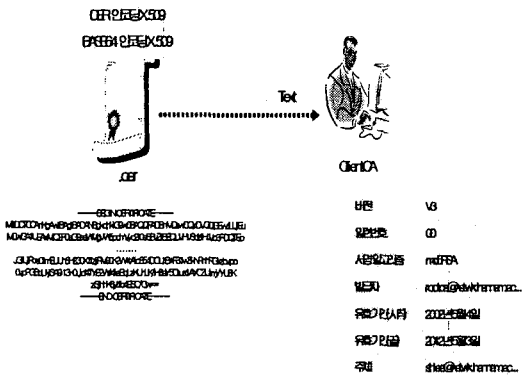
최종 사용자가 발급받아 소유하고 있는 인증서의 사용을 중지하고자 할 경우에는 ClientCA에서 인증서버로 폐지를 요청할 수 있다. 인증서의 폐지 요청은 [그림 8]의 경우와 같이 해당 인증서 소유자의 개인키로 서명한 폐지 요청서를 인증서버에 발송하고, 인증서버는 개인키에 대응하는 공개키로 이를 검증한 후 폐지 요청을 받아들이기 된다.




[그림 8] 인증서 폐지 요청

4) 열람

최종 사용자의 디렉토리에 저장된 인증서는 ClinetCA의 인증서 열람 모듈을 사용하여 해당 인증서의 내용을 확인할 수 있다. 인증서 열람은 [그림 9]와 같이 DER로 인코딩되어 있는 X.509 바이너리 또는 64 비트로 인코딩 된 X.509 형태의 인증서 필드의 내용을 열람할 수 있도록 일반 텍스트 형태로 바꾸어 각 필드값을 보여준다.




[그림 9] 인증서 열람

## 4. 결 론

본 논문에서는 공개키 인증 시스템의 구성 요소를 살펴보고, 이를 관리하기 위한 운영프로토콜을 적용한 ClientCA 응용을 분석하였다. 국내에서는 점차 이용이 확산되고 있는 인증서를 일반인이 효율적으로 관리하고, 활용할 수 있는 도구와 개념이 부족한 실정이다. 본 논문에서 분석한 ClientCA는 소규모, 특히 특정 집단에서 활용될 수 있는 공개키 기반 인증 시스템의 구축에 효율적일 것이다. 향후 본 논문에서 제안 설계된 메커니즘을 바탕으로, 실생활에서 활용할 수 있는 통합 인증서 관리 도구를 구현하는데 도움이 되었으면 한다.

## 참고문헌

[1] Jongho Yu, Heungyoul Youm, "인증서 관리 프로토콜(CMP)의 최근 동향", Journal of Korean Institute of Information of Security and Cryptography, Vol.10 No.4, 2000. 12

[2] RSA Data Security, Inc., Public Key Cryptography Standards #1-9, June 3, 1991.

[3] IETF, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999

[6] IETF, "Certificate Management Message over CMS", RFC 2797, April 2000

[7] Baltimore, Inc., "pki based e|security", 2000

김 점 구

광운대학교 전자계산학과 이학사
광운대학교 전자계산학과 이학석사
한남대학교 컴퓨터공학과 공학박사
(주) 제성프로젝트 연구원
(주) 시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수
<관심분야> 정보보호, 컴퓨터 네트워크, 무선통신

나상엽

동국대학교 전자계산학과(공학사)
동국대학교 컴퓨터공학과(공학석사)
동국대학교 컴퓨터공학과(공학박사)
현재 남서울대학교 컴퓨터학과 교수
<관심분야> 정보보호, 컴퓨터 네트워크, 무선통신