웹 기반의 인증서 관리 시스템에 관한 연구

김지현*, 채철주*, 최병선*, 이재광*

*한남대학교 컴퓨터공학과

A Study on Certificate Management System base on Web

Ji-Hyeon Kim*, Cheol-Joo Chae*, Byeoung-Seon Choi*, Jae-Kwang Lee*

*Dept. of computer engineering, Hannam University.

요 약

최근 국내외적으로 인터넷 기술 및 기반 시설의 증가와 이러한 인프라를 바탕으로 인터넷 뱅킹, 전자상거래와 같은 다양한 서비스의 이용률이 높아지고 있다. 그러나 이러한 시스템을 사용하기 위해서는, 서비스 제공 업체에게 일정의 금액을 지불해야 하거나 인증서 관리 및 확장에 있어 개발 업체의 규정에 준수해야 하는등 몇몇 불편한 사항이 있다. 따라서 본 논문에서는 국제 표준 규격을 따르며 편리하고 효율적으로 인증서를 확장할 수 있는 인증 체계와 중/소규모(small and medium) 인증 시스템에 적용할 수 있는 인증서 관리 시스템을 연구하고자 한다.

I. 서론[1)]

최근 인터넷을 이용한 민감한 정보 교환이 급속히 증가함에 따라 정보 교환에 대한 유효성 보장은 더욱 중요한 의미를 가지게 되었다. 해당 교환에 대한 유효성 보장을 효과적으로 제공하기 위해서는 교환 당사자의 신원확인, 교환 데이터의 무결성 및 기밀성 보장, 교환에 대한 부인방지 기능 등을 제공할 수 있는 인증서 시스템이 요구된다.

인터넷 상에서의 서비스와 업무가 안전하게 진행되기 위해서는 서로를 인증할 수 있는 서비스가 절대적으로 필요하게 된다. 따라서, 보다 신뢰성을 가지고 안전한 신상 정보의 교환을 위해서는 안전하고 신뢰성 높은 인증 서비스를 사용하여야 한다. 이에 IETF에서는 인증서비스와 관련한 기반 기술을 RFC 표준으로 제정하여 공표하고 있으며, 국내에서도 1999년에 전자서명법을 제정하여 공표함으로써 인터넷을 통하여 교환되는 정보의 안정성과 신뢰성을 확보하고 있다.

따라서, 본 논문에서는 앞서 언급한 표준안을 토대로 하여 자바 기반의 암호 API 및 이를 활용한 CA 및 인증 시스템을 구축하는 것을 목표로 한다. 자체 개발한 자바 기반의 암호 API를 통하여 적의 방해 및 가로채기, 불법수정, 위조 등의 보안 공격에 대해서 효과적으로 방지할 수 있는 보안 서비스를 구축할 수 있도록 모듈을 작성하고, 이를 활용하여 PKI를 구성하는 객체인 인증기관(CA), 등록기관(RA), 디렉토리, PKI를 사용하는 응용, 보안 서비스 시스템 등을 구현하여 보다 안전한 정보통신망 구축을 목표로 한다.

1) 본 연구는 산업자원부의 지역혁신 인력양성 사업의 연구결과로 수행되었음.

II. PKI 시스템

2.1 PKI의 기능

PKI는 인증 서비스의 기반을 이루는데 [표 1]과 같이 기본적으로 인증서 관리 기능과 암호 기능과 부가기능으로 구분할 수 있다.

인증서 관리 기능	인증서 발행
	인증서 폐지
	인증서 공표
	인증서 저장
	정책 수립/승인
암호 기능	공개키 쌍 생성
	전자서명 생성
	전자서명 유효성 검사
	관용키 생성 및 분배
부가 기능	등록
	데이터 저장
	공증
	키 복구
	디렉토리

[표 1]. PKI의 기능

2.2 X.509 v3 인증서

X.509 v3 인증서는 X.509 v2 인증서에 비해 많은 새로운 개념들이 도입되었다. 근본적 변화는 확장자를 도입한 것이다. 이는 X.509 실현자가 그들의 용도에 적합하게 인증서 내용을 정의할 수 있게 하기 위함이다. 표준 확장자(standard extension)들은 인증서 정책 정보, 주체(subject) 디렉토리 속성, 인증 경로 제한, 확장된 인증서 폐지 목록(CRL : Certificate Revocation List) 기능들을 제공한다.

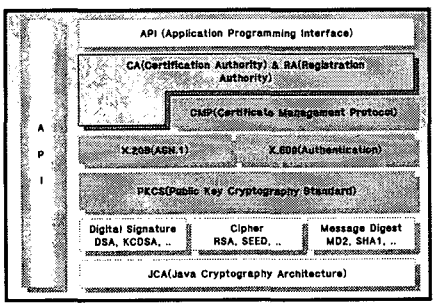

그림 1. PKI API 구조

2.3 API 구조

JCA는 특정 암호화 알고리즘에 독립적인 인터페이스를 제공하여 다양한 제품의 알고리즘을 이용할 수 있는 구조를 가지고 있다. 이러한 구조를 바탕으로 PKI와 관련한 API에서 제공하는 API 구조는 (그림 1)과 같이 정의하였다. 또한, 별도도 접근 제어와 로그 분석 및 감사 등의 보안 서비스를 제공하기 위해서 JDK를 기준으로 작성한 보안 서비스 API의 구조는 (그림 2)와 같이 정의하였다.

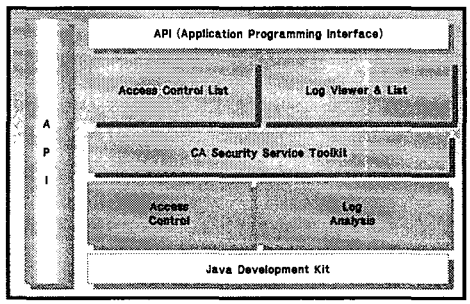

그림 2. 보안 서비스 API 구조

2.4 PKI 시스템 개요

본 논문에서의 PKI 시스템은 인터넷 환경에서 송신자와 수신자가 자료를 주고받을 때 서로 상대방의 신원정보를 확인하고 정보를 안전하게 주고 받을 수 있는 인증서비스를 제공해 준다. PKI 시스템은 오프라인상의 사용자 인감이나 서명을 공개키 알고리즘을 이용해서 전자적으로 구현한 사용자 인증 시스템이다. 본 시스템을 사용하는 사용자는 인증, 무결성, 부인방지, 접근통제 등 인터넷환경에서 요구되는 다양한 보안서비스를 제공받게 된다.

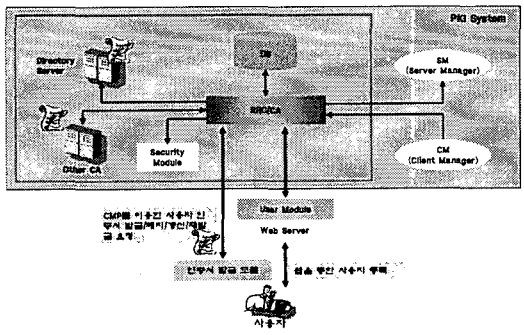

그림 3. CA 서버의 역할 및 구성

2.5 CA 서버 구성

CA 서버의 핵심 기능은 인증서 발급/갱신/

재발급/폐지와 관련된 기능으로 사용자 인증서의 발급과 이와 관련한 관리 업무를 수행할 수 있다. 자세한 동작 모델은 (그림 3)에서 보여진다.

III. 제안한 PKI 시스템의 설계

3.1 인증서 발행과 관리 모듈

PKI에서 인증서의 발급과 관리를 위한 모듈은 (그림 4)와 같은 구성 체계를 가진다.

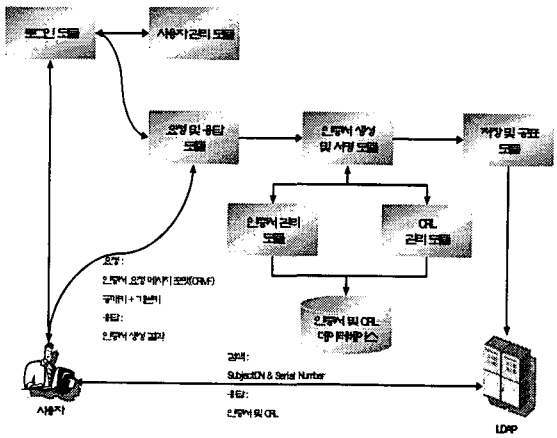

그림 4. 인증서 발행 및 관리 모듈

각 세부 모듈에 대한 기능 설명은 다음과 같다.

· 로그인 모듈 : RRC CA의 웹 인터페이스에 접근을 허가하기 위한 모듈로 ID와 패스워드를 통하여 로그인을 설정한다.

· 사용자 관리 모듈 : 사용자의 정보를 입력받아 ID와 패스워드를 발행하기 위한 모듈이다.

· 요청 및 응답 모듈 : 사용자로부터 인증서 발행을 요청받기 위한 데이터 입력 필드를 구성하며, 인증서가 발행된 결과를 사용자에게 응답하기 위한 모듈이다.

· 인증서 생성 및 서명 모듈 : 인증서를 발급하기 위한 키 쌍 생성 모듈과 이를 통한 인증서 발행, 발행된 인증서에 인증기관의 서명을 하기 위한 모듈이다.

· 인증서 관리 모듈 : 발행된 인증서를 관리하기 위한 모듈로 데이터 관리 기능, SubjectDN 관리 기능, 키 쌍 관리 기능 등을 제공하기 위한 모듈이다.

· CRL 관리 모듈 : 인증서의 폐기 기능을 담당하는 모듈이다.

· 인증서 및 CRL 데이터베이스 : 발행된 인증서와 CRL에 대한 정보를 저장하기 위한 모듈이다.

· 저장 및 공표 모듈 : 발행된 인증서 또는 CRL을 사용자들이 활용할 수 있도록 공개 저장소 또는 데이터베이스에 저장 또는 공표하기 위한 모듈이다. public directory

· LDAP : 인증서 및 CRL에 대하여 사용자들의 활용을 지원하기 위한 모듈로 검색, 결과의 응답 등의 기능을 지원한다.

3.2 사용자 클라이언트를 위한 웹 모듈

CA와 사용자 간의 정보 교환과 인증서의 발행 요청 및 응답을 얻기 위한 클라이언트 모듈의 데이터 흐름은 (그림 5)와 같은 흐름을 가지고 있다.

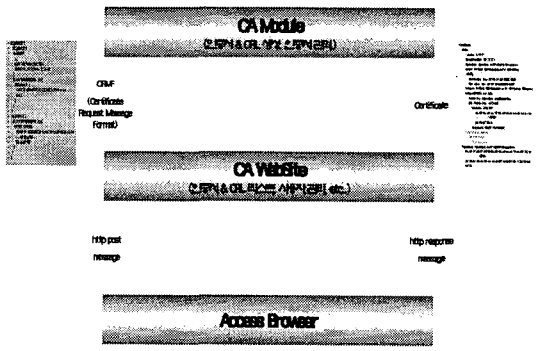

그림 5. 사용자 클라이언트의 데이터 흐름

위 그림에서 인증서를 발급받기 위한 사용자가 입력한 정보는 3 단계의 계층을 거쳐서 서로 다른 데이터 포맷으로 변경된다. 각 단계의 데이터 흐름에 대한 설명은 다음과 같다.

· Access Browser -> CAA WebSite : 일반적인 웹 서버에서 이루어지는 데이터 흐름과 같은 과정을 거친다. 사용자의 호스트에서 사용되는 웹 브라우저를 통하여 입력된 결과는

HTTP Post Message 형식으로 변환되고, CA 웹 인터페이스가 동작하고 있는 서버로 전송된다.

· CA WebSite -> CA Module : 서버로 전송되어진 정보는 CA의 각 모듈에 정보를 전달하기 위한 고유한 메시지 포맷으로 변경된다. 예를 들어, 인증서의 발급을 요청할 경우에는 CRMF(Certificate Request Message Format)의 형태로 변환되어 전송된다.

· CA Module -> CA WebSite : 발급된 인증서는 일반적인 base64 형태로 인코딩되어 전송된다.

· CA WebSite -> Access Browser : 첫 번째 단계와 역으로 데이터의 흐름이 정의된다. HTTP Response Message 형식으로 변환되어 전송된다.

IV. 결론

인터넷을 통한 정보 교환은 물론 금융 거래나 개인 신상 정보등의 신중히 처리되어야 할 여러 가지 일들을 인터넷을 통해 처리하는 일이 빈번한 현재 사회에서 정보를 보호하고, 사용자를 인증할 수 있는 인증서의 필요성은 말할 필요가 없을 것이다. 본 연구를 통해서 구현된 PKI 시스템은 각 기관이 가지는 사용자, 주 활용 형태, 기관 특성 등에 맞게 구축할 수 있는 중소규모의 인증 체계를 수립하는 것을 목표로 연구하였다. 본 연구의 성공적인 수행을 위해서 표준에 따라 자바 기반의 암호 알고리즘을 설계 및 개발하였으며, 이를 응용하여 다양한 보안 서비스를 제공할 수 있는 핵심 API 체계를 수립하였다. 또한, 암호 알고리즘과 PKI 시스템 구축을 위한 핵심 클래스의 결합을 통해서 인증서를 발행 및 관리를 자유롭게 할 수 있는 PKI 체계를 구축하였다. 향후로는 추가적인 연구를 통해 구현한 PKI 시스템을 바탕으로 다양한 기관의 특성에 맞추어 필요에 따라 알맞은 기능을 갖춘 인증 체계와 시스템을 구성하는 것이다.

[참고문헌]

[1] 송유진, 김선호, "전자거래 인증서 보안 요구사항 연구", *한국정보시스템학회 종합학술대회논문집, 1999. 11*

[2] 은유진, "X.509 인증서 및 인증서 폐지 목록 프로파일 분석", 전자서명인증 관리센터, 1999. 6.

[3] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신 보안", 그린출판사, 2001.

[4] 류종호, 염홍렬, "인증서 관리 프로토콜(CMP)의 최근 동향", *정보보호학회지, 제 10권 제 4호, 2002. 12.*

[5] 한국정보통신기술협회, "전자서명 인증서 효력정지 및 폐지목록 프로파일 표준", TTSS.KO-12.0013, 2001. 8

[6] 한국정보보호진흥원, "인증업무준칙 Ver 1.1", 2001. 11

[7] RSA Data Security, Inc., "Public Key Cryptography Standards #1-12", June 3, 1991

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

[9] IETF, "Internet X.509 Public Key Infrast- ructure Certificate Management Protocols", RFC 2510, March 1999.