PKI 기반의 안전한 인증서 관리 시스템에 관한 연구

최병선*, 채철주*, 이재광*
*한남대학교 컴퓨터공학과
e-mail:bschoi@netwk.hannam.ac.kr

A Study on Secure Certificate Management System base on PKI

Byeoung-Seon Choi*, Cheol-Joo Chae*, Jae-Kwang Lee*
*Dept of Computer Engineering, Han-Nam University

요 약

암호 API 및 PKI 클래스를 토대로 하는 PKI 시스템의 개발은 암호 알고리즘을 활용한 보안 서비스의 중요한 위치를 차지하고 있으며, 현재 네트워크 기반의 각종 서비스에서 강력한 보안 기능을 제공하는 부분으로, 각종 보안 서비스의 제공을 위해서 가장 먼저 구축되어야 할 부분이다. 본 논문에서는 자바 암호 API 및 PKI 관련 클래스를 바탕으로 사용자 인증(User Authentication), 인가(Authorization), 부인-방지(Non-Requdation), 전자서명(Electronic Signature) 등의 보안 서비스를 제공할 수 있는 X.509 전자인증서를 발행하는 PKI 시스템을 연구하였으며, 향후 각종 보안 서비스의 제공에 있어서 중요한 위치를 차지할 수 있을 것이다. 또한, 자바 기반의 PKI 시스템은 이식성이 매우 높으며, 개별 서비스에 대한 모듈 형식으로 구성되어 있어, 그 활용의 범위가 고정되지 않고 다양한 시스템 및 서비스에 적용할 수 있는 장점을 가지고 있다.

1. 서론

인터넷상에서 전자거래 행위가 이루어지기 위해서는 비대면 특성을 보완하고 신뢰성을 보장하기 위한 거래 당사자간의 신분확인이 전제되어야만 하며, 이는 인증, 무결성, 부인봉쇄 등의 서비스를 제공하는 전자서명 기술을 활용함으로써 해결 가능하다. 전자서명 기술을 효과적으로 이용하기 위해서는 공개키 암호 방식이 필요하며, 공개키 암호 방식을 이용한 인증 방법을 구현하기 위한 기술적, 제도적 기반이 요구되는데 이를 공개키 기반구조(PKI: Public Key Infrastructure)라고 한다. 또한 공개키 기반구조는 정보시스템 보안, 전자거래, 안전한 통신 등의 여러 응용 분야에서 신원 확인이 용이하도록 하는 정책, 수단, 도구 등을 수립 및 제공하는 객체들의 네트워크 집합으로 볼 수 있다[1][2]. 공개키 기반구조에서는 거래 당사자의 신분을 증명해주는 수단으로 인증서(Certificate)를 활용하고 있으며, 이를 관리하고 지원하기 위해서 IETF(The Internet Engineering Task Force)는 RFC 문서를 통하여 표준으로 제정하고 있다[1]. 다시 말해, 공개키 기반구조란 실체가 드러나지 않는 사이버 공간에서 공인된 인증기관이 사용자에게 법적 효력이 있는 인증서를 제공함으로써 비인가로부터 개인의 프라이버시 정보와 인터넷상에서 유통되는 전자거래 정보의 위·변조를 방지하기 위한 보안 인프라이다. 따라서 공개키 기반구조는 인증기관이 사용자들에게 인증서를 발급하여 전자서명의 공개키와 관련된 정보를 제공함으로써 사용자들이 통신상대방을 인증하고 안전한 메시지 교환을 가능케 해주는 공개키 관리 시스템으로 정의할 수 있다[2].

따라서 본 논문에서는 표준안을 기반으로 하여 자바기반의 암호 API와 이를 활용한 CA 및 인증 시스템을 구축하고자 한다. 암호 API를 통하여 적의

본 연구는 산업자원부에서 시행한 산업기술개발사업 (2003-61-10009504)에 의해 지원되었음

방해 및 가로채기, 불법수정, 위조 등의 보안 공격에 대해서 효과적으로 방지할 수 있는 보안 서비스를 구축할 수 있는 모듈을 작성하고, 이를 활용하여 PKI(Public Key Infrastructure)를 구성하는 객체인 인증기관(CA: Certification Authority), 등록기관(RA: Registration Authority), 디렉토리, PKI를 응용하는 이용, 보안 서비스 시스템 등을 구현하여 보다 안전한 정보통신망 구축할 수 있다.

2. 관련연구

2.1 PKI와 인증서비스

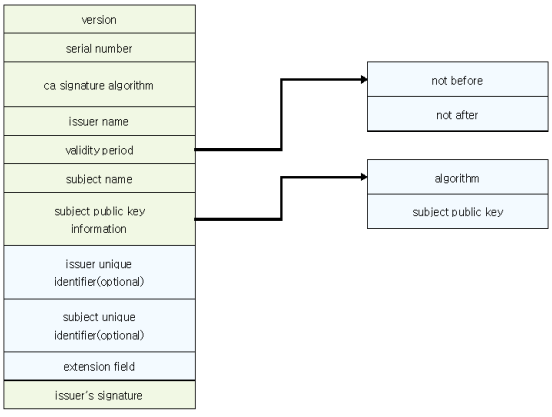
인터넷 상에서 송수신되는 전자문서의 송수신자 확인 및 송수신 내용을 확인해주는 서비스를 인증서비스라 부르며 공개키 암호 기술을 사용한다. 공개키 시스템에서는 두 종류의 키를 필요로 하는데, 하나는 송신자가 전자서명을 생성할 때 사용하는 개인키(private key)이고, 다른 하나는 수신자가 송신자의 전자서명을 검증할 사용하는 공개키(public key)이다. 개인키는 인감도장과 마찬가지로 개인이 안전하게 보관하는 키정보인 반면, 공개키는 네트워크상의 누구나 접근할 수 있도록 공개해 놓는 키 정보이다. 이 키쌍의 합치여부를 통하여 송수신 메시지의 위·변조를 확인하는 서비스를 제공한다[3][5].

이러한 인증 서비스를 제공함에 있어서 공개키는 필요할 때 통신하고자 하는 상대방에 전달할 수도 있지만, 통신 전에 상대방과 접촉하여 키를 교환해야 하는 번거로움이 있고, 또한 상대방이 자신의 키를 속이거나 타인이 신분을 위장할 수도 있으므로 신뢰할 수 있는 제3자(Trusted Third Party)가 필요하게 된다. 이러한 기능을 담당하는 시스템을 CA 시스템이라 부르고, 이를 위한 지원 시스템, 시설, 제도 등을 통틀어 PKI라 부른다.

2.2 X509 v3 인증서 및 X.509 v2 CRL 형식

(1) X.509 v3 인증서

전자서명은 물리적인 형태의 인감 도장이나 수기로 생성된 서명과 같은 역할을 수행한다. CA의 역할은 인감 도장에 대한 인감증명서를 발급하는 동사무소와 동일하다. 여기서 CA는 사전에 정해진 방침에 따라서 거래 당사자의 신원을 증명하는데, 인증서를 발급 받고자 하는 자는 주민등록증과 같이 그의 신분을 증명할 신분증을 CA에게 제시하면 CA는 그의 신분에 관한 정보와 공개키를 담은 메시지를 생성한다. 이러한 메지지를 인증서(Certificate)라고 하며, CA는 이 메시지에 대해서 전자적으로 서명하여 인증서의 유효성을 보증한다[4][6][8]. 인증서는 특정한 공개키가 특정한 개인에게 종속된다는 사실을 확인하는 수단을 제공하여 다른 사람이 특정인의 공개키를 도용하거나 공개키 자체를 변조하지 못하도록 한다. 이러한 체계가 효과적으로 운영되기 위해서는 CA의 공개키가 가급적 널리 알려져야 된다. 인증 구조의 최상단에 위치하는 인증기관은 다른 인증기관의 인증서가 없이도 신뢰할 수 있는 기관이어야 한다. 최상위의 인증기관은 공개키는 사전에 널리 공개되어 있어야 한다[7]. 가장 널리 인정되는 인증서의 형식은 ITU-T X.509 국제 표준에 의해 정의된다. ITU 권고 X.509는 디렉토리 서비스를 정의하는 X.500 시리즈 권고사항의 일부로서 디렉토리에 의해 유지되는 인증 정보의 형식을 설명하며, 인증정보가 디렉토리에서 어떻게 얻어질 수 있는지를 설명한다. 또한 디렉토리에서 인증 정보가 어떻게 형성되고 바뀌는지에 대하여 가정을 설정하고, 응용프로그램들이 인증을 수행하기 위해 이 인증 정보를 이용할 수 있는 세 가지 방법을 정의하고 있으며 다른 보안 서비스들이 인증에 의해서 어떻게 지원되는지를 기술하고 있다. X.509는 처음 1988년에 버전 1(v1)이 발행되었고, 1993년에 버전 2(v2), 1996년에 버전 3(v3) 표준이 완결되었다. X.509는 인증구조를 정의하고 있으며, 디렉토리는 공개키 인증서의 저장소 역할을 할 수 있다. 인증서는 최소한 다음의 항목을 포함하여야 한다. X.509 v3의 인증서 형식은 (그림 2)와 같다[8][9][10].



(그림 1) X.509 v3 인증서 필드

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 하

기 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.

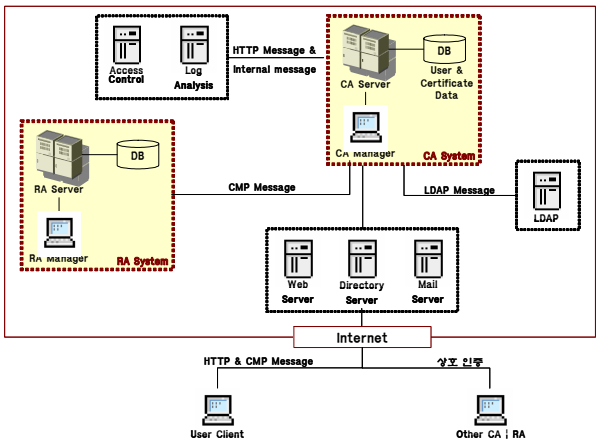
3. PKI 시스템 설계

3.1 PKI 시스템 개요

본 논문에서의 PKI는 인터넷 환경에서 송신자와 수신자가 자료를 주고받을 때 서로 상대방의 신원정보를 확인하고 정보를 안전하게 주고 받을 수 있는 인증서비스를 제공해 준다. PKI 시스템은 오프라인 상의 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.

(1) 구성 및 기능

본 논문에서 연구한 PKI 시스템은 (그림 2)와 같은 시스템 구성을 가지고 있다.

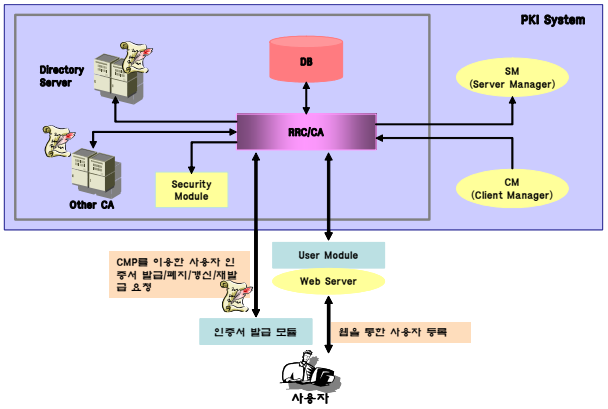


(그림 2) 시스템의 구성

- CA Server : 인증서를 발급하고 관리하는 인증 시스템의 핵심으로 다양한 공개키 알고리즘을 통하여 사용자 인증서를 발급한다.
- RA Server : 사용자 정보를 등록하고 관리하는 시스템으로 CA 서버와 연계하여 사용자 인증서에 대한 발급 업무를 보조해준다.
- LDAP : CA 서버에서 발급한 인증서를 공표하기 위한 시스템으로 공개저장소의 개념을 포함한다.
- Admin Tool : CA 서버에 대한 운영 및 관리를 위한 관리자 전용 도구로 CA 서버에 대한 전반적인 운영을 제어할 수 있다.

(2) CA 서버의 구성

본 논문에서 연구한 PKI 시스템에서 CA 서버가 가지는 역할은 절대적이라고 할 수 있다. CA 서버는 PKI 시스템의 근본을 이루는 사용자 인증서를 발행하기 위한 서버로, 이를 위해서 다양한 구성 요소를 가지게 된다. CA 서버의 역할 및 기능 구성은 (그림 3)과 같다.

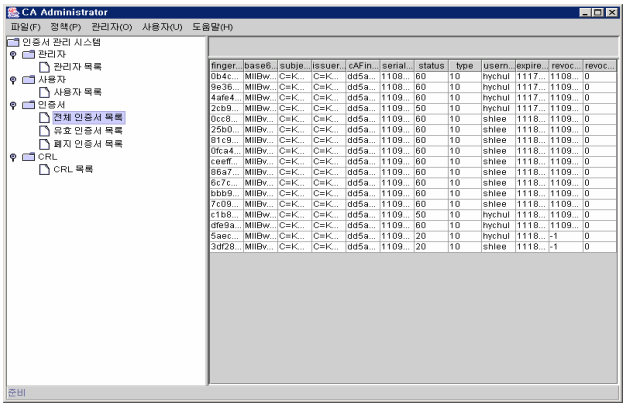


(그림 3) CA 서버의 역할 및 구성

4. PKI 시스템 구현

4.1 관리자 도구

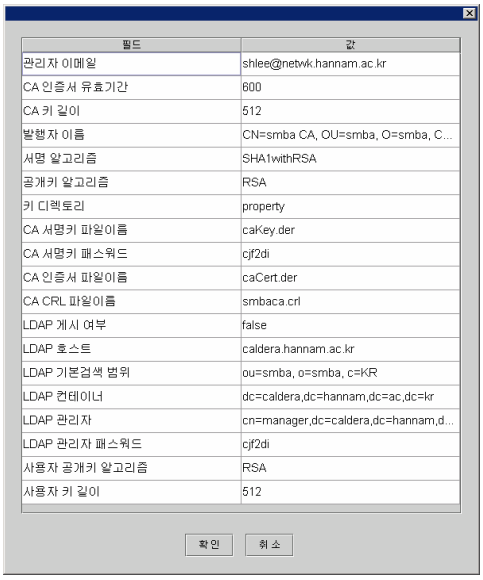
관리자 도구는 본 논문에서 구현한 CA에 대한 운영 및 인증서 발급 업무, 사용자 관리, 정책 설정 등과 관련한 업무를 수행하기 위한 인터페이스이다. 자바를 기반으로 스윙을 사용하여 구현하였다. (그림 4)는 관리자 도구의 인터페이스 예이다.



(그림 4) CA의 관리자 인터페이스

4.2 정책 설정

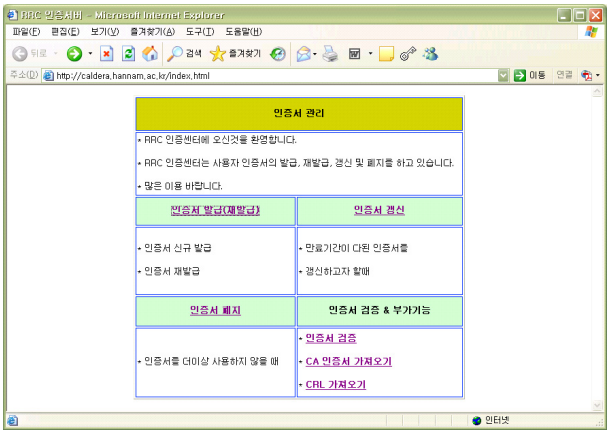
정책은 이전에서 설명한 것과 마찬가지 CA 시스템을 운영하기 위한 핵심 정보를 설정하고 관리하기 위한 일종의 가이드라인이다. (그림 5)는 본 논문의 CA에서 적용되고 있는 정책의 일부 예이다.



(그림 5) CA의 정책 파일

4.3 사용자 웹 인터페이스

사용자 웹 인터페이스는 본 논문에서 구현한 CA와 사용자를 연결하는 매개 역할을 하며, 간단한 인터페이스를 통하여 CA의 복잡한 프로세스를 수행하기 위한 핵심 기능을 포함하고 있다. 사용자 웹 인터페이스에서는 인증서 발급/재발급, 갱신, 폐지, 검증, 열람등과 같은 핵심 사용자 기능을 포함하고 있으며, (그림 6)과 같이 웹 기반으로 작성되어 있다.



(그림 6) 사용자 웹 인터페이스

5. 결론 및 향후 연구

급격히 발전하고 있는 인터넷을 통한 전자거래, 인터넷뱅킹, 전자문서 교환과 같은 서비스는 교환되는 메시지의 암호화와 함께 송·수신하거나 결제하는 사람의 신원에 대한 인증 문제가 매우 중요하다. 인증서는 개인 또는 기관에서 서명 및 암·복호화에 사용되는 공개키와 이에 대응한 개인키의 소유 증명을 확인해 주는 전자문서로써 각 구성원의 신원을 증명하기 위한 중요한 수단이다. 본 연구를 통해서 구현된 PKI 시스템은 각 기관이 가지는 사용자, 주 활용 형태, 기관 특성 등에 맞게 구축할 수 있는 중·소규모의 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. 본 연구의 향후 연구 방향은 구현한 PKI 시스템을 각 기관의 특성에 맞게 자유로운 모듈의 추가·제거 및 기능 변경이 용이한 맞춤형 인증 체계를 구성하여 이를 제품화 하는 것이다.

참고문헌

[1] 최용락, 소우영, 이재광, 이임영, “컴퓨터 통신 보안”, 그린출판사, 2001.

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

[3] 송유진, 김선호, “전자거래 인증서 보안 요구사항 연구”, 한국정보시스템학회 종합학술대회논문집, 1999. 11

[4] 은유진, “X.509 인증서 및 인증서 폐지 목록 프로파일 분석”, 전자서명인증 관리센터, 1999. 6.

[5] 김지연, “PKI 구성 객체의 상호연동을 위한 명세서 분석”, 한국정보보호진흥원, 1998. 7

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

[7] 한국정보보호진흥원, “인증업무준칙 Ver 1.1", 2001. 11

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

[9] IETF, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 2459, January 1999

[10] IETF, “Internet X.509 Public Key Infrastructure Certificate Management Protocols”, RFC 2510, March 1999.