XML을 이용한 PKI 기반 CA 설계

김환조, 김만수, 정목동
부경대학교 컴퓨터공학과
E-mail : {xxrcn, kmansoo}@mail1.pknu.ac.kr, mdchung@pknu.ac.kr

Design of PKI-based CA using XML

HwanJo Kim, Mansoo Kim, Mokdong Chung
Dept. of Computer Engineering, Pukyong National University

요 약

인터넷을 이용한 전자 상거래의 비중이 점차 증가하고 기업 활동 또한 인터넷으로 이동하고 있다. 인터넷을 이용하는 e-Commerce가 활성화됨에 따라 보안 관련 문제점들이 부각되고 있으며 이를 해결하기 위한 다양한 방법들이 제시되고 있다. 그 중에서 신뢰성과 안전성을 보장하는 공개키 기반 구조(PKI) 방법이 널리 사용되고 있다. 최근 e-Commerce에서는 XML 형식을 이용한 메시지 교환 방식이 널리 사용되고 있고 이에 대한 보안 역시 해결해야 할 문제이다.

본 논문에서는 XML을 이용하여 메시지를 전달하고 암호화를 통한 기밀성을 제공하고, PKI를 이용하여 신뢰성, 인증, 안전성을 제공하는 CA(Certificate Authority)를 설계한다.

1. 서론

인터넷의 보편화와 더불어 이를 이용한 e-Commerce 활동 역시 증가하고 있다. 그러나 이러한 e-Commerce의 발전에 가장 큰 장애는 보안 관련 문제들이다. e-Commerce 보안에 관련하여 기밀성, 인증, 신뢰성, 안전성의 기능들이 제공되어야 한다.

이런 문제점들을 해결하는 방법으로 공개키 기반 구조(PKI : Public Key Infrastructure)[1]가 널리 사용되고 있다. 공개키 기반 구조는 신뢰성과 안전성 그리고 인증 기능을 제공함으로서 e-Commerce 뿐만 아니라 인증을 필요로 하는 시스템 등에서도 널리 사용되고 있다.

또한 e-Commerce 시스템에서는 교환되는 메시지에 대한 보안 관련 문제들도 중요하다. 카드 번호, 카드 유효기간 등과 같은 민감한 정보들은 암호화 등을 통한 기밀성을 제공해야 한다.

본 논문에서는 XML을 이용하여 메시지를 교환하고 민감한 정보에 대해서는 암호화를 통해 기밀성을 제공하며, PKI를 이용하여 인증, 신뢰성, 안정성을 제공하는 CA(Certificate Authority)를 설계한다.

논문의 구성은 1절 서론에 이어, 2절 관련연구, 3절 XML을 이용한 PKI 기반의 CA 설계, 4절 결론 및 향후 연구에 대해서 논한다.

2. 관련 연구

2.1 XML(Extensible Markup Language)

W3C에서 1998년 제정한 XML[2]은 현재 웹에서 사용되고 있는 HTML의 한계를 극복하고 시스템 및 소프트웨어에 독립적인 문서와 메시지의 표현이 가능하도록 만든 표준이다. 서로 상이한 시스템을 연동하는데 매우 유용하기 때문에 다양한 전자상거래 분야에서 메시지와 문서 교환에 적당하다.

2.2 공개키 기반 구조(PKI : Public Key Infrastructure)

공개키 기반 구조(PKI)[1]는 사용자의 공개키를 안전하고 신뢰할 수 있게 공표하는 수단을 제공한다. 공개 키 기반 구조의 주요 구성 객체는 다음과 같다.

- 사용자(User) : 인증서를 발급받아 공개키 기반 구조를 이용하는 객체
- 등록기관(RA : Registration Authority) : 인증서를 요청한 사용자의 신분을 확인하고 등록하는 객체
- 인증기관(CA : Certificate Authority) : 사용자의 공개키와 정보를 이용하여 인증서를 생성, 검증, 폐기하는 객체
- 디렉토리(Directory) : 키의 관리, 인증서, 인증서 폐기목록(CRL)을 관리하는 객체

CA는 PKI에서 중요한 구성 요소로서 인증서의 생성 및 검증, 폐기를 담당한다. CA는 요구되는 서비스

에 따라 서로 다른 구성을 가질 수 있으며, 루트 CA의 하부에 다수의 하위 CA가 체인 형태로 존재할 수 있다.

PKI는 ITU-T의 X.509 방식과 비 X.509 방식으로 분류되며, X.509 방식은 인증기관에서 발행하는 인증서를 기반으로 상호인증을 제공하도록 하고 있으며, 비 X.509 방식은 국가별 지역별로 설정에 맞게 제공된다. Java에서는 J2SE 1.2, 1.3에서 java.security.cert 패키지를 이용해서 인증서와 CRL에 관한 API를 제공한다. 또한 J2SE 1.4에서는 "CertPath" API를 통해 인증서 경로 생성에 관한 API를 제공한다.

2.3 Pmart

Pmart[3]는 본 연구실에서 개발한 다중 변수 기반 에이전트 중재 e-Commerce 시스템이다. Pmart에서 매매는 판매 및 구매의 협상 정보를 가진 에이전트 간에 이루어진다.

Pmart의 협상 모델은 영역 지식과 일반지식을 동시에 사용할 수 있는데, 영역 지식은 MAUT(Multi-Attribute Utility Theory)[4]에 바탕을 두고 있고 일반지식은 기존의 구매 기록과 간결한 휴리스틱(simple heuristic)[5]에 바탕을 두고 있다.

2.4 CA관련 연구

인증서 폐지 목록(CRL)[1]은 인증기관이 폐기된 인증서에 대해 폐기 사유와 인증서의 일련번호 등의 정보를 포함하는 리스트를 주기적으로 생성하여 인증서 사용자들이 이를 이용하여 인증서를 검증할 수 있도록 하는 방식이다. 하지만 CRL은 주기적인 발행으로 인한 현재의 인증서 상태를 반영하지 못하는 문제점을 지니고 있다. 이를 해결하기 위한 방법으로 온라인 인증서 상태 검증 프로토콜(OCSP)[6]과 간단한 인증서 검증 프로토콜(SCVP)[7]이 널리 사용되고 있다.

OCSP는 온라인상에서 인증서의 상태 정보를 제공해 주는 OCSP 서버와 OCSP 클라이언트 간에 수행되는 프로토콜로서, OCSP 서버는 요청된 인증서의 상태 정보를 포함한 응답 메시지를 생성한 후 서명하여 클라이언트에 전달한다. 하지만 인증 경로에 대한 검증 정보를 제공하지 않는다는 단점이 있다.

SCVP는 인증서 상태 정보 외에 인증 경로에 관한 검증 정보들을 제공한다. SCVP는 클라이언트의 인증서 유효성 검증 관련 기능을 서버에게 위임함으로써 이의 구현을 간단히 하고 정책의 관리를 집중화 할 수 있다는 장점이 있다.

3. XML을 이용한 PKI 기반 CA 설계

3.1 시스템 구성

SecuPmart는 본 연구실에서 개발한 e-Commerce 시스템인 Pmart에 XML 전자 서명과 PKI를 적용한 시스템으로서 자체적인 CA를 운영한다. 각각의 SecuPmart는 CA로부터 인증서를 발급받고, 고객의 컴퓨터로 다운로드된 보안 모듈에서 SecuPmart의 인증서를 검증한다. 검증된 인증서의 공개키는 e-Commerce에서 안전한 거래를 위한 협상 정보, 결제 정보 등의 암호화에 사용된다.

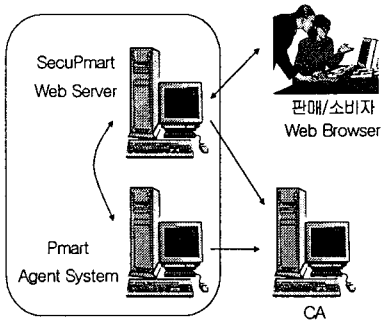

그림 1. SecuPmart 시스템 구성도

그림 1은 SecuPmart 시스템의 구성을 보여준다. 판매자와 구매자는 웹 브라우저를 사용하여 SecuPmart에 접속한다. SecuPmart와 Pmart 에이전트 시스템은 각각의 분리된 시스템일 수도 있고, 하나의 시스템으로 구성될 수 있지만, SecuPmart와 Pmart 에이전트 시스템은 반드시 방화벽이 있는 로컬 네트워크 안에 위치해야 한다.

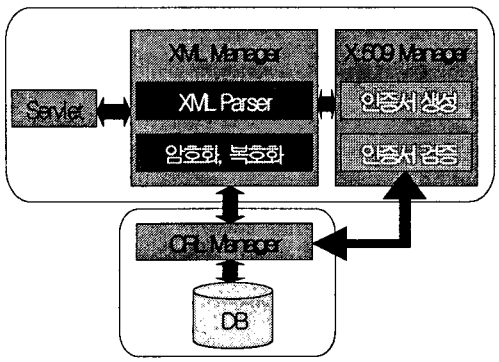

그림 2. CA 시스템 구성도

그림 2는 CA의 내부 구조를 보여준다. CA를 구성하는 요소는 크게 3개의 Manager로 구성된다. CLR Manager는 CA에게 가중되는 부담을 줄이기 위해 분리된 시스템에 위치시킨다. XML Manager와 X.509 Manager 그리고 CRL Manager는 반드시 방화벽이 있는 로컬 네트워크 내에 위치해야 한다.

각 Manager의 기능은 다음과 같다.

▪ XML Manager

SecuPmart로부터 전송된 정보를 CA의 개인키를 이용하여 복호화한 후 XML 문서의 내용을 분석하여 인증서의 생성, 검증, 폐기를 판별한다.

각 과정에 발생하는 메시지는 XML 문서로 변환한 다음 전송한다.

▪ X.509 Manager

실제적인 인증서의 생성을 담당한다. 인증서 생성에 필요한 정보를 체크하고 만약 올바르지 않다면 메시지를 생성하여 XML Manger에게 전달한다. 인증서 검증의 경우에는 CA의 공개키를 이용하여 서명을 검증하고 유효기간을 체크 한 다음 CRL Manger에게 전달한다.

▪ CRL Manager

인증서 폐기 목록(CRL : Certificate Revocation List)[1]을 관리하며 인증서 폐기를 담당한다. DB에는 인증서의 일련번호, 폐기 사유, 날짜 등의 정보가 저장된다. DB에 CRL 목록을 유지하고, 새로이 폐기되는 인증서의 정보를 다음 CRL 목록 생성일까지 유지함으로써 실시간 인증서의 상태 검증이 가능하다. X.509 Manger로부터 인증서 폐기 요청과 함께 관련 정보를 전달받아 이를 DB에 저장하고 결과 메시지를 XML Manager에게 전달한다. X.509 Manager로부터 인증서 검증 요청을 받을 경우 인증서의 일련번호가 DB에 존재하는지를 체크함으로서 폐기 여부를 확인 할 수 있다.

3.2 시스템 계수

표 1은 본 논문에서 인증서의 생성, 검증, 폐기에 필요한 시스템 계수이다.

▪ 표 1. 시스템 계수

계수	설명
CA	인증 기관
PM	SecuPmart
C_x	고객 x
PU_{C_x}	C_x의 Public Key
PR_{C_x}	C_x의 Private Key
$E_y(m)$	키 y를 사용해 메시지 m을 암호화
$D_y(m)$	키 y를 사용해 메시지 m을 복호화
$Info_{C_x}$	인증서 생성을 위한 C_x의 정보
$Cert_{C_x}$	C_x의 인증서

3.3 인증서 생성

사용자와 SecuPmart는 서로를 확인하는 과정을 거치고, SecuPmart의 인증서를 다운받아서 하드 디스크나 플로피 디스크에 저장한다(그림 3의 ①-④). 인증서 생성을 위해 SecuPmart에서 보안 모듈을 다운받는다(그림 3의 ⑤⑥). 이 보안 모듈은 PKI 기반 암호화를 위해 공개키와 개인키를 생성하고 이를 사용자의 하드 디스크나 플로피 디스크에 저장하고 이를 관리한다.

사용자는 보안 모듈을 이용해서 인증서 생성에 필요한 정보와 생성한 공개키를 XML 형식으로 변환하고 SecuPmart의 공개키를 이용하여 암호화한 후에 이를 전송한다(그림 3의 ⑦⑧). SecuPmart는 자신의 개인키로 복호화한 후에 CA의 공개키를 이용하여 암호화 시키고 CA로 전송한다(그림 3의 ⑨⑩).

XML Manger는 CA의 개인키로 복호화한 후에 XML 문서에서 필요한 정보를 추출하고 이를 X.509 Manager에게 전달한다(그림 3의 ⑪⑫). X.509 Manager는 인증서를 생성한 후에 이를 XML Manager에게 전달하고 XML Manger는 인증서를 XML 문서로 변환한 후에 Pmart의 공개키를 이용하여 암호화해서 전달한다.(그림 3의 ⑬-⑮). SecuPmart는 자신의 개인키를 이용해서 복호화한 후에 사용자의 공개키를 이용하여 암호화해서 사용자에게 전달한다(그림 3의 ⑯⑰). 사용자는 자신의 개인키를 이용해서 복호화한 후 인증서를 저장한다.

그림 3은 인증서 생성 과정을 보여준다.

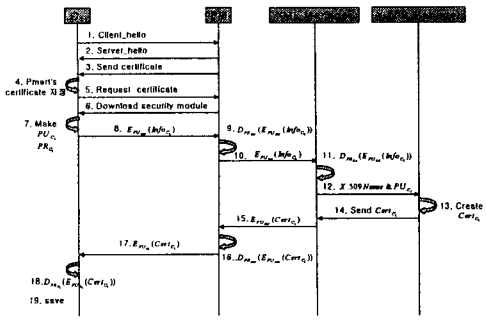

그림 3. 인증서 생성 과정

3.4 인증서 폐기

사용자는 인증서 폐기 요청과 인증서를 XML 문서로 변환한 후에 SecuPmart의 공개키로 암호화하여 전송한다(그림 4의 ①). SecuPmart는 자신의 개인키로 복호화한 후에 CA의 공개키를 이용하여 암호화해서 전달한다(그림 4의 ②③). XML Manager는 CA의 개인키로 복호화한 후에 XML 문서에서 인증서를 추출하고 이를 CRL Manager에게 전달한다(그림 4의 ④⑤).

CRL Manager는 인증서의 일련번호와, 폐기 날짜 등의 필요한 정보를 DB에 저장하고 결과 메시지를

XML Manager에게 전달한다(그림 4의 ⑥⑦). XML Manager는 메시지를 SecuPmart의 공개키로 암호화한 후에 전송한다(그림 4의 ⑧). SecuPmart는 자신의 개인키를 이용해서 복호화한 다음 사용자의 공개키를 이용하여 암호화해서 사용자에게 전송한다(그림 4의 ⑨⑩).

그림 4는 인증서 폐기 과정을 보여준다.

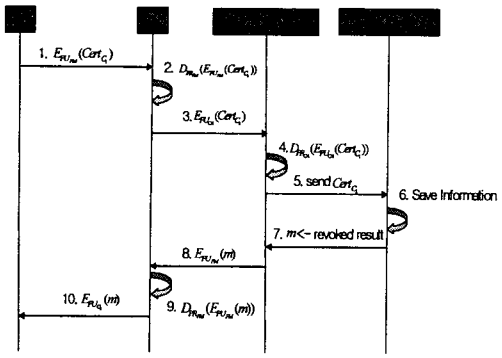

그림 4. 인증서 폐기 과정

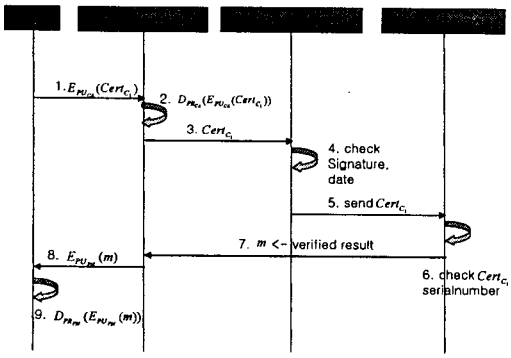

그림 5. 인증서 검증 과정

3.5 인증서 검증

그림 5는 인증서 검증 과정을 보여준다.

SecuPmart로부터 인증서 검증 요청이 전달되면 XML Manager는 CA의 개인키로 복호화한 후에 XML 문서에서 인증서를 추출한 다음 X.509 Manager에게 전달한다(그림 5의 ①-③). X.509 Manager는 CA의 공개키를 이용하여 서명을 검증하고, 인증서의 유효기간을 체크한 후에 CRL Manager에게 인증서를 전송한다(그림 5의 ④⑤).

CRL Manager는 인증서의 일련번호를 이용하여 현재의 CRL과 CRL 발행 후에 저장된 인증서 폐기 정보들을 검색해서 폐기 여부를 확인하고 결과를 XML Manager에게 전송한다(그림 5의 ⑥⑦). XML Manager는 결과를 SecuPmart의 공개키로 암호화 한 후에 SecuPmart에게 전달한다(그림 5의 ⑧). SecuPmart는 자신의 개인키를 이용해서 복호화한 후에 사용자의 개인키로 암호화해서 사용자에게 전송한다(그림 5의 ⑨).

4. 결론 및 향후 연구

본 논문에서는 안전하고 신뢰할 수 있는 e-Commerce를 위해 CA가 갖춰야 할 기능들을 제시하고 XML 및 PKI 기반의 CA를 설계했고, 중요 컴포넌트들은 구현하였다. 또한 교환되는 메시지는 모두 XML을 이용하여 이루어지며 암호화는 기밀 정보에 대해서만 이루어진다.

플랫폼 독립성 및 재사용성을 고려하여 Java를 이용하여 모듈별로 설계함으로써 PKI 기반의 e-Commerce 뿐만 아니라 기업 환경 내에서 공개키를 이용한 다양한 인증 시스템에 적용할 수 있다.

향후 연구 과제로서 CA의 키 갱신에 따른 기존 인증서를 효과적으로 갱신할 수 있는 방법에 대한 연구가 필요하다.

[참고 문헌]

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

[2] W3C, Extensible Markup Language(XML), http://www.w3c.org/XML, February 1998.

[3] Mokdong Chung and Vasant Honavar "A Negotiation Model in Agent-mediated Electronic Commerce," Proceedings of the IEEE International Symposium on Multimedia Software Engineering, Taipei, Dec. 2000, pp.403-410

[4] R.L.Keeney and H.Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley & Sons, New York, NY, 1976.

[5] G.Gigerenzer et al., Simple Heuristics That Make Us Smart, Oxford University Press, New York, 1999.

[6] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IEFT draft-ietf-pkix-rfc2560bis-01.txt, February, 2002

[7] C. Adams, P. Sylvester, M. Zolotarev and R. Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certificate Server Protocols", IETF RFC 3029, February, 2001