E-PMI의 설계

김희선 조상래 조영섭 진승헌

한국전자통신연구원

(sezsez, sangrae, yscho, jinsh)@etri.re.kr

Design of ETRI Privilege Management Infrastructure

Heesun Kim, Sangrae Cho, Yeongsub Cho, and Seunghun Jin

Electronic and Telecommunication Research Institute

요 약

응용 서비스 측면에서는 서비스를 이용하고자 하는 사용자들의 신원확인 뿐만 아니라 이러한 그들이 어떠한 서비스를 이용할 수 있는 권한을 갖고 있는가를 반드시 확인해야 한다. 응용에 따라서는 신원 확인보다도 권한 확인을 더 중요하게 처리하고자 하는 경우도 있다. 이런 의도에서 권한 인가와 권한 정보의 관리는 매우 중요한 보안 서비스의 하나로 인식되고 있다. 본 논문에서는 이러한 권한관리 메카니즘의 하나로서 제시된 권한관리기반구조 개념에 대하여 살펴보고, 이를 바탕으로 설계한 E-PMI에 대해 설명하고자 한다. E-PMI에 대해서는 구조 및 시나리오, 시스템 특징에 관하여 기술한다.

I. 서론

1. 배경

인터넷 상의 전자 거래가 증가함에 따라 오픈 네트웍에 대한 안전성을 제공하기 위한 보안 서비스의 필요성은 나날이 증가되고 있다. 이러한 보안 서비스의 기반 기술인 공개키 암호 기술은 공개키 기반구조(Public Key Infrastructure: PKI)의 구축을 통해 이미 전자거래의 필수 요소가 되었다.

PKI에서 관리되는 공개키 인증서(Public Key Certificate : PKC)는 인증(Authentication) 서비스를 제공하기 위한 중요한 수단이 되기도 한다. 인터넷 뱅킹, 전자 민원 서비스 등은 이용자의 신원 확인 과정이 필수적이며, 이미 실제 응용에서도 PKC를 통해 '인증' 서비스가 처리되고 있다.

실세계에서의 또 다른 응용을 생각해 보자. 사용자 '갑'이 쇼핑몰 '을'과 1억짜리 물건 구매 계약을 성사시키려고 한다. '갑'은 '을'에게 PKC 등을 이용하여 자신이 누구인지를 확인(인증)시켰다. 그러나 계약 체결 시, '을'은 '갑'이 정말 그 구매 계약을 이행할만한 1억의 구매력이 있는지와 구매 계약을 수행할 만한 자격자(회사에서의 계약 체결 권한 직위자)인지 알 수 있는 정보가 필요하다. 그러면, 그러한 권한 정보는 어떻게 전달하고 관리할 수 있을 것인가.

이와 같은 문제 해결을 위해 '인가' 서비스가 요구된다.

2. PMI 개요

인가란 사용자에게 사용자가 가진 권한 속성 등을 부여하는 것을 의미한다. 이러한 권한 속성을 관리해 주는 메카니즘 중에서 권한관리기반구조(Privilege Management Infrastructure: PMI)가 제시되고 있다[1]. PMI에서는 이러한 권한 속성들을 X.509 속성 인증서(Attribute Certificate : AC)를 이용하여 관리하도록 채택하고 있다[2]. PMI는 PKI를 통해 인증 과정을 수행한 사용자의 인가 정보를 확인한다.

이를 기반으로 하여 우리는 E-PMI(ETRI PMI)를 설계하고 각 구성 요소의 기능 및 운영 동작을 정의하였다. 본 논문에서는 본문을 통해 설계한 E-PMI의 구조 및 기능, 운영 시나리오를 살펴보고, 시스템의 특성을 설명하고자 한다.

II. E-PMI 설계

1. E-PMI 구조 및 기능 정의

E-PMI는 AA 서버, PMI 클라이언트, Decision-Making 서버, LDAP 서버로 구성되어 있으며, 그 각각의 기능은 다음과 같이 정의된다.

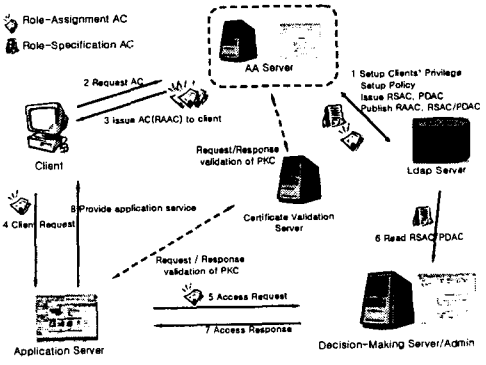
1) AA 서버
- AC의 발급 정책 정의 및 게시
- 클라이언트에게 권한을 부여
- 부여되는 권한 속성 관리 및 정의
- AC 발급 및 게시
- AC 폐기
- AC 갱신

2) PMI 클라이언트
- AA 서버에게 AC 요청
- AA 서버에게 AC 폐기 요청
- AA 서버에게 AC 갱신 요청

3) Decision-Making 서버
- AC 검증
- 응용 서비스 이용에 따른 권한 판단

4) LDAP 서버
- AC 저장
- 사용자 정보 및 권한 정보 관리
- AC 관련 정책 저장

이와 같은 기능을 가진 E-PMI의 각 요소들은 권한관리를 통해 서비스 접근 및 이용을 허용하는 응용 서비스에 적용된다. [그림 1]은 E-PMI의 구성 및 운영 시나리오를 나타낸 것이다.



[그림 1] E-PMI 구조 및 동작

AA 서버는 LDAP 서버를 통해 PMI 클라이언트들의 정보 및 권한 정보를 부여하고 저장한다. AC의 발급은 PMI 클라이언트가 AA 서버에게 AC 발급을 요청함으로써 이루어진다. 클라이언트는 먼저 PKC 혹은 ID/Password로 자신의 신원을 확인 시킨 다음, AA 서버로부터 자신에게 부여된 권한 속성에 대해서 AC를 발급받는다. 그런 다음, 클라이언트는 발급 받은 AC를 응용(Application) 서버의 서비스를 이용 요청과 함께 제시한다. 응용 서버는 클라이언트가 접근하려는 서비스 제공을 위해 제시한 AC를 이용하여 클라이언트의 권한을 검사한다. 응용 서버는 Decision-making 서버에게 권한 판단을 요청하기 위해 AC와 접근하려는 서비스를 전달한다. Decision-making 서버는 AC의 유효성을 검증하고, 접근하려는 서비스가 허용된 것인지를 확인하기 위해 필요한 정책 정보 등을 LDAP 서버로부터 읽어와 검사한다. 검사 결과에 따라 Decision-making 서버는 "허용/거부" 메시지를 응용 서버에게 전달하게 된다. 응용 서버는 Decision-making 서버의 권한 판단 결과에 따라 클라이언트에게 서비스 제공여부를 결정하게 된다.

2. E-PMI의 특징

E-PMI는 다음과 같은 특징을 지닌다.

1) X.509 AC 이용

사용자의 속성 관리를 위해 X.509 AC를 이용한다. PKC를 이용한 속성 관리는 공개키와 속성의 lifetime이 다르고, 하나의 인증서에 여러 속성 정보를 담는 것으로 발생할 수 있는 프라이버시 정보의 침해 우려가 있으며, 공개키와 속성 정보를 다루는 인증기관이 상이하다는 것에 문제점이 있다. 반면, X.509 AC는 권한 관리 기능을 수행하는 신뢰받는 인증기관의 서명으로 클라이언트와 클라이언트의 권한 속성간의 바인딩을 신뢰하도록 해준다. 따라서, AC를 권한 속성 전달의 매개체로 선택한 이유는 AC가 단순히 속성 전달의 하나의 도구이기보다는 정보의 신뢰성을 보장할 수 있다는 측면을 고려한 것이다. 또한, 프라이버시 정보의 보호를 위해 E-PMI에서는 하나의 인증서에 하나의 속성만을 저장하도록 하고 있다.

2) Short lived AC 생성

AC의 검증은 AC의 각 필드의 유효성을 검사하고, AC가 폐기되었는지의 여부를 확인하는 것으로 이루어진다. AC의 폐기 여부는 ACRL (Attribute Certificate Revocation List)에서 검색한다. 이는 PKI의 CRL을 관리하는 기법과 동일하게 처리된다[3]. 그러나 CRL이 배포의 문제점과 폐기 정보의 실시간 반영 문제가 PKI에서의 큰 문제점이 되었던 것처럼 AC에 대해서도 동일한 문제점이 발생하게 된다. 그러나, 속성 정보라는 것은 일반적으로 공개키보다 생명주기가 더 짧다고 보기 때문에, 그만큼 인증서의 잦은 폐기가 예상되어 ACRL 배포 및 폐기 정보에 대한 실시간 반영 문제는 더 심각해 질 수 있다고 여겨

진다. 따라서, 이러한 문제점을 PMI에서는 short lived AC를 통해 다소 해소시키려 하고 있다. Short lived AC는 짧은 유효기간을 갖는 인증서를 폐기없이 발급 주기마다 다시 발급해 주면 된다. E-PMI는 short lived AC를 발급하므로써 ACRL 생성 및 배포의 문제점과 폐기 정보의 관리에 대한 부하를 줄였다.

3) 두 가지 인증방식 지원

X.509 AC는 AC holder field를 통하여 PKC와의 연결관계를 유지하며, PKC를 통한 사용자 인증을 수행할 수 있다. 그러나, PKI를 지원하지 않는 환경에 속한 클라이언트에게도 권한 관리 서비스를 제공하기 위해서 가장 많이 이용되고 있는 인증메카니즘인 ID/Password 방식을 지원하고 있다. 즉, 선택적으로 PKC 혹은 ID/Password를 이용한 인증방식을 지원한다.

4) Push/Pull model 지원

다양한 응용 환경에의 적응성을 고려하여 AC의 분배 모델에 대하여 Push/Pull 모델을 모두 지원하도록 설계하였다. 이는 클라이언트가 권한 판단을 수행하는 주체에게 AC를 직접 전달 하거나, 권한 판단 주체가 LDAP으로부터 클라이언트의 AC를 읽어와서 권한 판단을 수행하는 가에 따라 구별될 수 있다. Push 모델과 pull 모델은 PMI가 적용되는 응용의 범위나 요구되는 응용 서비스의 처리 성격에 따라 알맞게 적용되어야 한다.

5) Decision-Making 기능의 독립 서버 구축

Decision-Making 서버는 PMI 적용 환경 및 정책에 따라 그 위치를 다양화시킬 수 있다. Decision-Making 서버는 응용 도메인이나 AA 서버의 일부 기능으로 구현될 수도 있으며, 독립된 서버로 구현될 수도 있다. AA 서버에서 구현되는 Decision-Making 기능은 서버 기능의 병목이 되어 성능 저하를 가져올 수도 있다. 응용 서버에 구현되는 Decision-Making 기능은 기존 응용들에 대한 변경을 요구하게 되며, 여러 응용들에게 반복적인 기능의 별도 구축을 요구하게 된다. 물론, 별도의 서버로서의 구축은 AA 서버 및 응용 서버와의 신뢰관계의 형성이라는 문제점을 안고 있지만, 추후 확장성과 기능성을 고려하여 별도의 서버로 구축하고 있다.

6) RBAC 모델 지원

E-PMI에서 관리되는 권한 속성 타입 중에서 role 타입은 role-based access control 메카니즘에 의해서 관리된다. 이를 위해 클라이언트에게 부여되는 role에 따라 RAAC (Role Assignment Attribute Certificate)를 발급하며, role에 대한 permission에 따라 RSAC (Role Specification Attribute Certificate)를 발급한다.

III. 결론

지금까지 권한 관리 기능을 제공하는 E-PMI에 대하여 살펴보았다. E-PMI는 X.509 AC를 이용하여 PMI 클라이언트의 응용 환경 리소스에 대한 권한 관리를 수행하여 준다. 이를 위해, E-PMI는 AA 서버 및 Decision-Making 서버의 구성요소를 필요로 하고 있다. E-PMI는 이외에도 Push/Pull model 지원, 다양한 인증 메커니즘 지원, Decision-Making 기능의 독립서버 구축, RBAC 지원 등의 특징을 가지고 있음을 알아보았다.

권한 관리 기능을 제공하기 위한 솔루션으로서 PMI만이 만능은 아니다. 중요한 것은 응용 환경에 이것을 얼마나 잘 적용하여, 응용 환경에서의 효율적인 권한 관리를 제공할 것이냐 하는 것이다. 이를 위해, 권한관리를 필요로 하는 응용들과 각 응용 환경에 따른 적합한 권한관리 솔루션의 모델 연구가 지속되어야 할 것이다.

참고문헌

[1] ITU-T Recommendation X.509 | ISO/IEC 9594-8 : Information Technology Open Systems Interconnection The Directory Public-Key and Attribute Certificate Frameworks , Draft ISO/IEC 9495-8, May 3, 2001

[2] S. Farrell, R. Housley,An Internet Attribute Certificate Profile for Authorization, RFC3281, April 2002

[3] Housley, R., Ford, W., Polk, W., and Solo, D., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999.