E-PMI의 소개

김희선1) 조상태 조영성 전승현
한국전자통신연구원
(sesez@, sangrae, yscho, jinsh)@etri.re.kr

Introduction of ETRI Privilege Management Infrastructure

Heesun Kim3) Sangrae Cho Yeongsu Cho Seunghun Jin
Electronic and Telecommunication Research Institute

요 약

권한관리 기반구조를 이용한 온라인 서비스의 보안을 관리하기 위한 인프라로서 인가서비스를 제공한다. 전자상거래의 유효화 및 탈중앙화, 기업의 무형자산, 부인 등을 보안 서비스의 필요성은 이미 중요하게 부각되어 왔다. 공개화 보안 기술은 이러한 보안 서비스의 제공에 핵심이 되었고, 이를 지원하기 위한 공개키 기반구조가 주요 인프라로 제시되었다. 특히, 온라인에서의 인증의 필요성은 이미 중요한 요소가 되었다. 그러나, 보안 서비스에서 사용자들의 권한에 대한 요구가 증가함에 따라 권한 관리에 대한 연구가 활발해져 오고 있다. 이에 대한 해결방안으로 제시되고 있는 E-PMI 스토러스는 이미 네트워크의 보안시스템을 위한 필수 요소로 인식되고 있다. 본 논문은 이러한 E-PMI 구축의 실제로서 ETRI에서 개발하고 있는 E-PMI를 소개한다.

1. 서론

인터넷을 이용한 인터넷 기술의 발전은 다양한 컨텐츠의 제공을 가능하게 하고, 요구가격의 정보도 타는 일이 증가함에 따라, 서비스를 제공하는 리소스에 대한 접근 가능성을, 즉 권한 확인에 대한 요구가 증가할 수밖에 없었다. 이에 대한 해결방안으로 권한관리 기반구조를 이용하여 ETRI에서는 이를 제공하기 위한 인프라 스토러스로서 E-PMI를 개발 중에 있다. 이를 통해, 사용자들이 보안된 접근을 위해 인증한 사용자에게 등록한 사용자에 대한 권한을 제공하는 것이다. ETRI에서는 이와 같은 권한 관리 스토러스로서 E-PMI를 개발 중에 있다. 이를 통해, 사용자들에게 권한에 대한 인증과 관리를 제공하고자 한다. 본 논문에서는 E-PMI의 구조 및 개발한 관리를 통해 E-PMI를 소개하고자 한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 E-PMI의 개요와 구성의 개요에 대한 설명한다. 3장에서는 E-PMI의 구조 및 운영 시나리오를 소개하고, 4장에서는 결론을 맺도록 한다.

2. PMI 개요

최근 인가 서비스는 인증 서비스와 함께 중요한 보안 요구사항으로 인식되고 있다. 여러 가지 서비스를 제공하는 사용자들에게 기존의 서비스에 접근하고자 하는 사용자들이 무단 접근 문제, 즉 사용자들의 인증이 필요한 문제 등이 중요하게 인식되어 왔다. 그러나, ETRI 관리에 대한 접근 권한을 가진 자에 대한 문제가 인증을 주로 사용하지 않게 중요하게 인식되면서 이러한 권한을 보다 신중하게 고려하고, 고해결적으로 통합 관리를 필요로 한다. ETRI는 E-PMI에 대한 해결방안으로 제시된 관리체계를 요구하게 되었다. PMI는 이에 대한 해결방안으로 제시된 개념이다. 현재 PMI는 IETF와 ITU-T에서 표준화가 추진 중이며, 최근, 이러한 노력의 일환으로 RFC3281가 발표되었다 [1, 2].
2.1 AC의 개념
X.509 기반의 인증서를 이용하여 권한 속성을 관리하는 것은 단순한 속성 관리 수단 이외의 의미를 갖는다. 이는 속성 소유자와 그가 지닌 속성 간의 관계를 신뢰하는 인증기관의 서명으로 신뢰성을 보장한다는 것에 그 의미가 있다고 할 수 있다. X.509 PKC에서는 확장 필드를 이용하여 속성 정보를 저장할 수 있도록 지원하고 있다. 그러나, PKC를 이용하여 권한 속성을 관리하는 것은 공개키와 속성 정보의 서로 다른 lifetime으로 인해 같은 인증서 폐기 문제를 야기시킬 수 있다. 그러므로, AC를 이용하여 권한 속성을 관리하는 것은 공개키와 속성 정보의 서로 다른 lifetime으로 인해 같은 인증서 폐기 문제를 야기시킬 수 있다. 그러므로, 다음과의 속성 정보를 이용하여 공개키를 여러 번 발급하지 않는다면 하나의 인증서에 여러 속성 정보를 저장하도록 해야 한다. 이것은 프라이버시 정보의 침해 가능성을 낮게 한다. 또한, 공개키와 속성 정보를 다루는 인증 기관에 상이하다는 문제점이 있다. 따라서 X.509 AC를 도입하여 권한 관리 기능을 수행하려는 의견이 보다 설득력있게 제시된 것이다.

3. E-PMI 구조 및 운영 시나리오
이러한 PMI에 대한 연구의 한 실례로서 ETRI에서는 E-PMI (ETRI PMI)를 개발 중에 있다. 본절에서는 E-PMI의 구조와 운영 시나리오에 관하여 간략히 소개하고자 한다.

3.1 E-PMI 구조
E-PMI에서는 PMI client의 권한 속성을 X.509 AC를 이용하여 관리한다.

[그림 1] ETRI PMI 구조도

608
3.2 E-PMI의 권한관리 시나리오


1) AC 요청

PMI client는 AA server에게 자신의 권한에 대한 AC를 요청한다. Client는 PKC를 이용하여 AA server에게 자신을 인증한다 (ID/Password를 이용한 인증도 지원).

2) AC 발행

AA server는 PMI client를 인증하고, 요청에 따라 X.509 AC를 발행하며, client에게만 속성 인증서를 전달한다.

3) 리소스 접근

PMI client는 Application server의 서비스를 이용하기 위해 자신의 AC와 함께 서비스를 요청한다.

4) AC 검증 요청

Application server는 서비스를 요청한 client를 인증한다. 그리고, client의 서비스 이용에 대한 권한을 체크하기 위해, Decision-Making server에게 AC를 전달하여 검증을 요청한다.

5) 권한검증 및 리소스 접근 허용

Decision-Making server는 AC의 유효성을 검증하고, 속성 정보를 통해 client가 요청한 서비스를 이용할 자격이 있는지의 권한 체크를 수행한다. 이에 따라, Decision-Making server는 Application server에게 서비스 요청 여부에 대한 응답을 보내준다 (허용/거부).

6) 권한 검증 결과에 따른 서비스 제공

Application server는 Decision-Making server의 응답에 따라 client에게 요청된 서비스를 제공하거나 혹은 거부한다.

4. 결론


참고문헌