PMI 인증서 등에 대한 적합성 평가

이승훈*, 정구완*, 송주용*, 송주석*, 박정환**, 이재일**

*연세대학교 컴퓨터과학과

**한국정보보호진흥원

Interoperability Compliance Test for PMI

SeungHoon Lee*, GuWan Jung*, JooYong Song*, JooSeok Song*,

JungHwan Park**, JaeIl Lee**

*Dept of Computer Science, Yonsei University

**Korea Information Security Agency

요 약

권한 관리 기반 구조(PMI: Privilege Management Infrastructure)란 공개키 기반 구조(PKI: Public key Infrastructure) 와 연동되어 온라인 상에서 사용자의 신원정보와 권한 또는 속성 정보를 연결하여 자원에 대한 접근 관리를 효율적이고 안전하게 할 수 있도록 해주는 정보 보호 인프라이다. 이러한 권한 관리 기반 구조에서 사용되는 인증서를 속성 인증서(Attributc Certificate) 또는 PMI 인증서라고 부른다. 속성 인증서가 기반 구조 내에서 통용되어 사용되기 위해서는 표준화 기관에서 정의한 표준 규격을 따라야 하며 유효성을 해치지 않는 올바른 값들로 인증서 내용이 채워져 있어야 한다. 이와 같이 특정 단체나 어플리케이션에 의해 생성·사용되는 속성 인증서 등이 기반 구조내의 개체들 간에 서로 호환되어 사용될 수 있는지 검사하는 것을 적합성 평가라고 한다. 본 연구에서는 속성 인증서 및 인증서 요청 메시지의 적합성 평가를 위한 평가 시스템을 구성하고 평가 시 요구되는 평가 항목 및 평가 기준을 정의한다.

I. 서 론

인터넷의 혁신적인 발달과 기하급수적인 사용자 증가는 일상생활의 많은 부분에 영향을 미치고 있다. 인터넷 뱅킹, 인터넷 주식 거래, B2B·B2C 전자 상거래, 온라인 결재가 생겨나는 등 여러 분야에서 삶의 방식을 바꾸어 놓고 있다. 그러나 이와 같이 사람들에게 많은 편리함을 가져다 주는 네트워크 상의 정보 처리는 온라인 상에서 상대방의 신원과 속성을 확인할 수 없다면 불가능한 일일 것이다. 물리적 접촉을 통하지 않고서도 상대방의 신원과 속성을 확인 할 수 있는 방법은 다양한 통신망 서비스를 제공하기 위한 기본 요구 사항이라고 할 수 있다. 오래 전부터 이러한 요구 사항을 충족시키기 위한 많은 연구가 진행되고 있으며 그 성과 중의 대표적인 것으로 PKI와 PMI의 등장을 들 수 있다.

PKI(Public Key Infrastructure), 즉 공개키 기반 구조는 온라인 상에서 상대방의 신원을 확인하기 위한 기반 모델로서 생겨나게 되었다. 공개키 기반 구조에서는 사용자의 공개키에 대해 신뢰할 수 있는 인증기관이 서명을 하여 보증함으로써 보증된 공개키와 쌍을 이루는 비밀키를 가지는 사용자에 대해 신원 인증 기능을 제공하게 된다.

PMI(Privilege Management Infrastructure), 즉 권한 관리 기반 구조란 사용자에 대한 역할, 지위, 그룹, 과금, 감사 등의 정보를 신뢰할 수 있는 기관이 보증하고 유지함으로써 보안을 책임지는 기반구조로서 공개키 기반 구조(PKI : Public Key Infrastructure)와 함께 사용되어지는 정보보호 인프라를 의미한다. 그림 1은 PKI와 PMI가 연동되어 작동하는 구조에서 공개키 인증서와 속성 인증서를 가지고 사용자가 자신이 가지고 있는 권한을 행사하는 모습을 보여주고 있다.

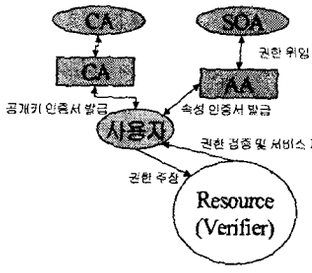

그림 1 PKI와 연동된 PMI 구조

PKI 및 PMI가 기반 구조로서 제대로 작동하기 위해서는 PKI 및 PMI 인증서가 기반 구조내의 각 개체들 사이에서 통용될 수 있도록 그 규격과 내용에 대한 규칙이 약속되어져야 한다. 즉, 각 인증서에 대한 표준화 작업이 이루어 져야 하며 실제 사용환경에서도 표준 문서에 따라 인증서를 생성하고 처리할 수 있도록 해야한다. PKI는 이미 오래 전부터 표준화 작업이 수행되어오고 있다. 또한 각 국가나 단체 등 PKI를 구축한 환경에서 상호간의 호환성을 위해서 적합성 평가 방법을 수립하고 시행하고 있다. 그러나 PMI의 표준화는 현재 초기 단계이며, 아직까지는 널리 사용되고 있지 못한 점 때문에 여러 업체들에서 개발한 PMI 관련 제품들이 PMI 표준을 따르고 있는지 그리고 서로 다른 제품들간에 호환성을 가지고 있는지의 검증은 이루어지지 않고 있다.

인증서의 규격이 표준을 따르지 않게 되면 인증서 정보가 잘못 전달되게 되며 필요한 곳에서 인증서를 처리하지 못하여 사용이 불가능하게 될 수 있다. 또한 다양한 인증서 발급 기관이 발행한 인증서들이 서로 호환성을 갖추지 못하면 권한 정보의 교류 및 사용자 속성의 상호 인정 등이 이루어지지 않게 되며 인증서의 사용에 큰 제약을 받게 된다. 그리고 또 하나 중요한 문제는 표준의 잘못된 구현으로 인해서 여러 가지 보안 취약성을 야기할 수 있다는 점이다. 따라서 표준을 따르는 PMI 인증서가 널리 사용되어지고 인증 주체 서로간의 PMI 인증서를 확인 할 수 있도록 하기 위해서는 여러 제품들이 만들어낸 인증서가 관련 PMI 표준을 따르는지 그리고 상호 호환성을 갖추고 있는지 여부를 검증할 수 있는 방법론의 수립이 요구된다.

II. PMI 표준

속성 인증서의 표준 규격은 ITU-T의 X.509 3판(1997년)에서 처음 정의가 되었다. 그러나 이 때는 단순히 속성 인증서의 구조만 정의했을 뿐 PMI전반에 대한 표준화 작업은 이루어지지 않았다. X.509 4판(2000년)이 나오면서 비로소 기반 구조로서의 PMI가 정의되었다. X.509 4판에서는 PMI에서 사용될 수 있는 4가지 모델인 일반 모델, 역할 모델, 제어 모델, 위임 모델을 제시하고 있으며 속성 인증서의 구조를 개선하여 v2 표준 규격을 정의하였다. 또한 PMI에서의 위임 경로 처리, 속성 인증서 검증 절차, 표준 확장 필드 및 표준 속성 필드 등에 대해서도 정의하고 있다. 그림 2는 속성 인증서의 표준 규격을 나타내고 있다.

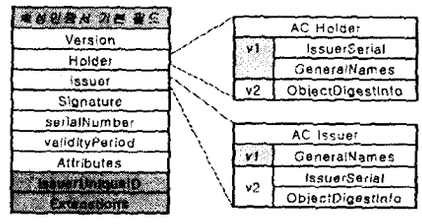

그림 2 속성 인증서 표준 규격

그림 2에는 속성 인증서의 버전이 v1에서 v2로 개선되면서 Holder와 Issuer 필드에 새롭게 추가된 옵션들을 보여주고 있다. 버전 2 속성 인증서에서 추가된 옵션들은 신원 인증서(공개키 인증서 등)와 속성 인증서(AC)를 좀더 강하게 연결할 수 있도록 지원한다.

ITU-T의 X.509는 다른 산업 표준들의 기본이 되고 있으며, 산업 표준화 기관들에서는 X.509를 바탕으로 해서 산업 영역에 맞게 PMI에 대한 산업 표준 문서들을 만들게 된다. PMI에 대한 표준화 작업을 진행하고있는 산업 표준 기관으로는 IETF가 있으며, IETF 내의 PKIX 작업 그룹에서는 PKI 및 PMI와 관련된 다양한 표준 문서들을 발표하고 있다. IETF에서는 RFC 3281 문서를 통해 인터넷에서 사용 가능한 표준 속성 인증서 규격을 제시하고 있으며 기본적인 규격은 X.509의 속성 인증서 규격과 동일하다. 다만 RFC 3281에서는 속성 인증서가 인터넷 환경에서 사용될 수 있도록 상호호환성을 강조하여 다양한 표준 속성들을 정의하고 있다. 또한 IETF에서는 PMI 환경에서 필요한 다양한 프로토콜 및 인증서 요청 메시지 등의 표준 규격을 정의하고 있다.

III. PMI 인증서 적합성 평가

PMI 인증서에 대한 표준 적합성 평가를 위해서는 평가 시스템 구성, 평가 항목, 평가 기준 등에 대한 정의가 이루어져야 한다. 평가 시스템의 구성은 그림 3과 같다. 표준 적합성 평가 시스템은 검증 주체와 검증 대상 사이의 상호작용으로 구성되어진다. 검증 주체는 검증 대상에게 검증에 필요한 속성 인증서, 공개키 인증서 등의 정보를 요청하며 이렇게 요청된 정보에 따라 검증 대상은 필요한 인증서 등의 정보를 검증 주

체에게 전달하게 된다. 적합성 평가 주체는 평가 대상이 되는 속성 인증서를 대상으로 표준을 준용하고 있는지를 검증하게 된다.

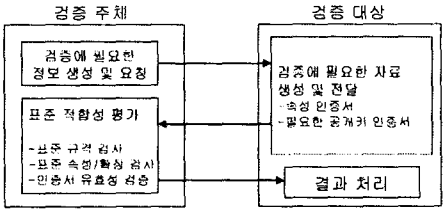

그림 3 적합성 평가 시스템

PMI 인증서에 대한 표준 적합성 평가는 표준 규격 검사, 표준 속성 및 확장 필드 검사, 인증서 유효성 검사의 순서로 이루어진다.

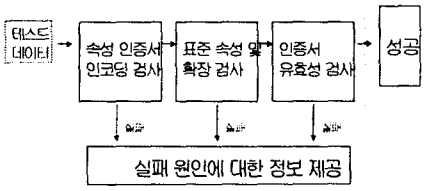

그림 4 PMI 인증서 적합성 평가

그림 4는 평가 절차에 대한 처리 과정을 나타내 주고 있다. 각각의 단계에서 인증서가 요구되는 조건을 만족하지 못하면 실패 처리와 함께 실패 원인을 제공해 주어야 한다.

인증서 표준 규격 검사에서는 인증서의 각 필드가 순서에 맞게 구성되어 있는지, 그리고 규칙에 맞게 제대로 인코딩 되었는지를 검사한다. 인코딩 규칙이 정확하게 이루어지지 않으면 인증서의 기능을 할 수가 없게된다. 인증서의 서명은 인증서 정보의 DER 인코딩 값에 대해 계산되어지는데, 인코딩이 잘못된다면 서명이 제대로 되었는지 알 수가 없기 때문이다.

표준 규격 검사를 만족하는 인증서에 대해서는 표준 속성 및 표준 확장 필드에 대한 검사를 수행한다. 각각의 인증서가 상호 호환성을 가지고 사용될 수 있기 위해서는 인증서에서 사용되는 속성 필드 및 확장 필드가 PMI 사용자들에 의해 합의된 것이어야 한다. 표준 속성 및 확장 필드 검사에서는 ITU-T X.509 및 RFC 3281 등 준용한 표준 프로파일에서 정의된 속성이나 확장 필드들에 대해 제대로 구현이 되었는지 여부에 대해 검사를 수행한다. 즉, 표준에 정의된 표준 속성들이 올바른 개체식별자(Object Identifier)를 가지고 있고 해당 개체에 대해 정의된 문법에 맞게 구성되어지고 인코딩 되어졌는지 여부를 검사한다. 또한 확장 필드의 경우 critical 값이 제대로 설정되어 있는지를 검사한다. 표 1은 표준 확장 필드들을 보여 주고 있으며 괄호 안의 c, x, n은 각각 critical, 정해져 있지 않은 경우, Non-Critical을 의미한다.

표준 확장 필드
Time specification(c)
Targeting information(c)
User notice(x)
Accept privilege policies(c)
CRL distribution points(x)
No revocation information(n)
SOA identifier(n)
attribute descriptor(n)
Role specification certificate identifier(n)
Basic attribute constraints(x)
Delegated name constraints(x)
Acceptable cert polices(c)
Authority. attribute identifier(n)
Audit Identity(c)
AC targeting(c)
authority key identifier(n)
authority information access(n)
CRL Distribution Points(n)
No Revocation Available(n)

표 1 표준 확장 필드

인증서 규격 검사와 속성 및 확장 필드 검사를 모두 통과한 인증서는 최종적으로 유효성 검증을 받는다. 인증서의 규격이 표준 규격을 따르고 있고 표준 문서에 정의된 속성 및 확장 필드들이 올바르게 구현되어 있다하더라도 인증서의 내용이 올바르지 못하다면 그 인증서는 사용될 수 없다. 유효성 검사에서는 각 필드 제약 사항 검사, 권한 위임 유효성 검사, 서명 값 검사 등을 수행하게 된다. 표 2는 기본 필드 및 확장 필드에 대한 유효성 검사 항목이다.

기본 필드 유효성 검사	
version	값이 v2를 나타내는 정수 1인지 검사
holder	baseCertID, entityName, objDigestInfo 등 3가지 옵션 중 적어도 하나 이상이 나타나는지 검사
issuer	옵션 중 적어도 하나 이상 사용 여부 검사
serial Number	양수이며 20 Octet을 넘지 않는지 검사
확장 필드 유효성 검사	
Time Speccification	시간 구성이 올바른지 검사, SOA Identfier 확장 필드가 존재하지 않는지 검사
User Notice	SOA Identfier 확장 필드가 존재하지 않는지 검사
Audit Identity	값이 0~20 Octet 사이에 존재하는지 검사
AC Targeting	taget 필드가 targetName 또는 targetGroup 둘 중 하나로 나타나는지 검사
Authority Info Access	accessMethod가 OCSP인 경우 accessLocation은 HTTP URL 값을 가지는 URI를 포함하는지 검사

표 2 기본 필드 및 확장 필드 유효성 검사

권한 위임 유효성 검사는 발급기관이 자신이 가지고 있는 권한의 범위에서 하위 개체들에게 권한을 부여했는지 여부를 검사하는 것이다. 검사 항목 및 평가 기준은 표 3과 같다.

Clearance 속성	발급 기관의 Clearance level이 하위 개체의 Clearance level 보다 높은지 검사
Role, Group 속성	Role 또는 Group이 계층적으로 정의되어 있는 경우 상위 기관의 Role 또는 Group이 하위 개체보다 높은 계층인지 검사
Basic Attribute Constraints 확장	발급 기관의 인증서이 이 확장 필드가 있으면 authority 값이 true 인지 *pathLenConstraint* 값이 0이상인지 검사

표 3 권한 위임 유효성 검사

서명 값 검사는 PMI 인증서의 서명이 발급 기관의 비밀키(서명키)에 의해 올바르게 서명되었는지 검사하는 것이다. 서명 값 검사는 검증 시 계산된 해쉬 값과 인증기관이 생성한 해쉬 값이 같은지를 비교함으로서 이루어진다. 아래의 등식이 참인 경우 서명 값은 유효하다.

Hash[Certificate Info] = D_{AApub}[Signature]

(D_{AApub} : 인증기관의 공개키로 복호화)

IV. 속성인증서 요청 폼 적합성

속성 인증서 요청 폼에 대한 적합성 평가 역시 인코딩 검사와 요청 메시지의 유효성 검사로 이루어진다. 인코딩 검사에서는 표준에 정의된 내용에 따라 정확하게 인코딩 되었는지를 검사한다. 유효성 검사에서는 인증서 요청 메시지가 인증서 발행에 필요한 최소한의 정보들을 포함하고 있는지 여부를 가린다. 인증서 요청 메시지는 대부분의 필드가 선택적으로 사용하도록 정의되어있다. 그러나 모든 필드가 생략된다면 정보가 충분하지 않아 인증서 발행이 불가능할 수 있다.

선택 필드의 필요 유무는 OldCert ID control 필드의 사용 유무에 따라 분류하였다. OldCert ID control 필드는 이전에 발행된 사용자 속성 인증서에 대한 정보를 담고 있기 때문에 이 필드의 존재하게 되면 선택필드들의 정보를 대체할 수 있어 생략이 가능해지기 때문이다. 표 4. 는 OldCert ID 사용 유무에 따른 필요한 선택 필드들을 나타내었다.

OldCert ID 존재	OldCert ID 부재
validity period	Holder Validity Period Attributes Extensions

표 4. 필요한 인증서 요청 폼 선택 필드

V. 결론

권한 관리 기반 구조는 아직 초기 단계이지만 많은 연구가 이루어지고 있으며 빠른 속도로 그 사용이 늘어날 것으로 기대되고 있다. 그러나 현재 사용중인 속성 인증서 등은 표준의 임의적인 해석이나 잘못된 이해로 인해 잘못된 구조를 가진 경우가 많은 것으로 알려져 있다. 따라서 PMI가 보안 기반 구조로서 널리 통용되어 사용될 수 있도록 표준을 정확히 이해하여 구현하는 것이 필요하다. 본 연구에서 정의된 적합성 평가 항목 및 기준들은 PMI 인증서 등의 정확한 구현을 검사하는 기초 자료로서 사용될 수 있을 것으로 기대한다.

참 고 문 헌

[1] ITU-T Recommendation X.509, "Public-Key and Attribute Certificate Frameworks", ISO/IEC 9594-8, May 2001

[2] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public-Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile", IETF PKIX RFC 3280, April 2002

[3] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX RFC 3281, 2002

[4] P. Yee, "Attribute Certificate Request Message Format", IETF PKIX Internet-Draft, March 2002

[5] DOD, "Interim External Certification Authority (IECA) X.509 Certificate Compliance Test Plan", 1999

[6] DOD, "Guidelines for External Certification Authority Interoperability With Department of Defense Public Key Infrastructure", version 0.7, 1999

[7] Denis Pinkas, "Certificate Validation Protocol", IETF PKIX Internet-Draft, June 2002.

[8] A. Arsenault, S. Turner, "Internet X.509 Public Key Infrastructure: Roadmap", IETF PKIX Internet-Draft, July 2002.

[9] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", IETF PKIX Internet-Draft, December 2001.