情報保護學會論文誌
第11券 第5號, 2001. 10

속성인증서 프로화일 연구

윤 이 중*, 류 재 철**

Attribute Certificate Profile Research

E-Joong Yoon*, Jae-Cheol Ryou**

요 약

속성인증서는 사용자의 속성정보를 저장 관리하는 인증서로서 기존 공개키인증서가 사용자의 공개키 정보를 통해 인증 정보를 제공한 것과는 달리 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공한다. 최근 국제적인 표준 단체에서 속성인증서에 대한 표준이 제정되고 있으며 국내외적으로 속성인증서에 대한 연구 및 개발이 시작되고 있으며 인증뿐만 아니라 인가정보가 필요한 많은 실응용 분야에서 활용될 수 있을 것으로 예상된다.

따라서 본 고에서는 이와 같은 속성인증서의 출현배경, 표준화 동향에 대하여 고찰하며 현재 IETF에서 제정중인 속성인증서의 프로화일과 관련 기술에 대하여 설명한다. 또한 속성인증서를 이용한 접근통제 시스템을 소개하여 속성인증서의 활용에 대하여 기술한다.

ABSTRACT

Existent public key certificates provide authentication information through some information on user's public key. However, an attribute certificate which stores and manage user's attribute information, provides various privilege information such as position, privilege and role. In recent, international organizations establishes standards on attribute certificate, and the researches and developments on attribute certificate have been widely made. In addition it may be expected to be used many real application areas requiring for authorization information as well as authentication information.

Therefore, this paper considers background and standardization trends of attribute certificate and describes the profile and related techniques of attribute certificate currently established by IETF. In addition, it introduces an access control system using attribute certificate and specifies applications of attribute certificate.

keyword : *Certificate, PMI, privilige, PKI, Authentication, Public Key*

Ⅰ. 서 론

최근 인터넷의 급격한 성장에 따라 전자상거래는 기존 상거래를 보안하거나 대체하면서 급속한 성장을 보이고 있다. 그러나 인터넷은 공개네트워크(Open Network)라는 특성으로 인해 정보의 변조, 위조, 누설 등의 위협에 노출되어 있다. 따라서 인터넷 상의 정보보호는 전자상거래의 활성화를 위해 필수적인 요소로 자리잡고 있다[1,2]. 이러한 정보보호를 제공하기 위해 많은 연구가 진행되고 있으며 특히 최근에는 사용자에 대한 인증 정보를 제공하는 PKI (Public Key Infrastructure)에 대한 연구 및 개발이 활발히 진행되고 있다[3].

PKI는 사용자에 대한 공개키 소유여부에 대한

* 국가보안기술연구소 기반기술연구부장(yej@etri.re.kr)
** 충남대학교 정보통신공학부 부교수(jcryou@esperosun.chungnam.ac.kr)

인증 정보를 제공하며 정보에 대한 인증(Authentication), 무결성(Integrity), 비밀성(Confidentiality), 부인봉쇄(Non-repudiation) 기능을 제공하며 정보보호 기반구조로 활용되고 있다[2]. 그러나 일반 응용 환경에서는 이와 같은 정보보호 기능뿐만 아니라 사용자에 대한 권한관리를 요구한다. 즉 일반적인 전자상거래에서 사용자가 어떤 물품을 주문했을 때, 서버 시스템에서 물품을 배달할 것인지 결정하는 과정은 물품을 주문한 사용자에 대한 신원확인을 수행하는 인증 정보뿐만 아니라 사용자가 주문한 물품의 대금을 지불할 능력이 있는지를 확인하는 인가(Authorization) 정보가 매우 중요하다.

이와 같은 사용자의 권한은 초기에 공개키인증서(Public Key Certificate, PKC)를 통해 제공하려는 연구가 수행되었다. 그러나 공개키에 대한 발급주체가 사용자의 속성을 발급하는 주체와 다르고 공개키의 유효기간과 사용자 속성의 유효기간이 서로 다르기 때문에 실제 활용되지 못하고 있다.
따라서 최근에는 사용자의 임무, 지위, 접근권한 등과 같은 속성 정보를 별도의 속성인증서(Attribute Certificate, AC)에 저장 관리하며 유통하는 속성인증서에 대한 연구가 활발히 진행되고 있다[4,5]. 현재 속성인증서는 ITU-T, IETF, ANSI에서 표준화가 진행되고 있으며 일부 업체에서 속성 인증서 발급 시스템을 개발하고 있다[6~9]. 또한 사용자의 속성을 키와 바인딩하는 인증서 구조를 통해 속성 정보를 제공하는 SPKI(Simple PKI)에 대한 연구도 진행되었다. 그러나 SPKI의 실제 응용이 아직은 미흡한 실정이다[10,11].

따라서 본 논문에서는 사용자의 다양한 속성 정보를 제공하는 속성인증서에 대한 연구동향을 고찰한다.

본 논문의 구성은 다음과 같다. 2장에서 속성인증서의 출현 배경 및 표준화 동향에 대하여 고찰한다. 3장에서는 IETF에서 제정 중에 있는 속성인증서 프로화일에 대하여 기술하고 4장에서 속성인증서와 관련된 기술적 사항에 대하여 설명한다. 5장에서 속성인증서를 이용한 RBAC 시스템에 대하여 기술하고 마지막으로 6장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 속성인증서의 출현 배경과 표준화 동향에 대하여 고찰한다.

2.1 속성인증서 출현배경

일반적인 전자상거래에서 사용자가 어떤 물품을 주문했을 때, 서버 시스템에서 주문한 물품을 배달할 것인지 결정하는 과정은 물품을 주문한 사용자에 대한 신원확인을 수행하는 인증이 필요하다. 또한 사용자가 주문한 물품의 대금을 지불할 능력이 있는지를 확인하는 인가도 필수적이다. 대부분의 응용 환경에서는 이와 같이 사용자 인증과 사용자의 임무, 지위, 접근 권한 등의 사용자 인가를 통해 시스템의 접근을 통제하게 된다. 사용자 속성 정보를 기존의 PKC에 저장 관리할 수 있다. 즉 PKC는 사용자 속성 정보를 저장 관리하기 위해 확장 필드 중 SubjectDirectoryAttribute 예약해 놓고 있다. SubjectDirectoryAttribute 필드를 통해 사용자의 속성 정보를 저장할 경우 기존 PKI 시스템의 변경 없이 사용자 속성을 제공할 수 있다는 장점을 가지고 있다.

그러나 속성 정보를 PKC에 저장하는 방식은 속성정보의 유효기간과 공개키인증서의 유효기간이 불일치하고 발행주체가 다르다는 문제로 인하여 실제 활용되기 어렵다는 단점이 있다[2,8,9]. 즉 공개키인증서의 유효기간은 대부분 유효기간이 1년 이상으로 상당히 긴 반면에 사용자의 속성 정보는 상대적으로 변경이 자주 발생한다는 특징을 보인다. 따라서 PKC에 사용자의 속성 정보를 저장할 경우 사용자 속성의 변경에 따라 PKC도 함께 폐지해야 하는 문제가 발생한다. 일반적으로 PKC의 발급에 많은 시간과 비용이 발생하고 사용자에게 불편을 초래하기 때문에 이는 시스템의 가용성과 시스템의 전체적인 효율을 떨어뜨리는 문제를 발생시킨다.

또한 PKC에 사용자 속성을 관리할 경우 PKC의 발급기관인 인증기관(Certificate Authority)이 사용자의 속성을 발급하는 주체가 된다. 그러나 사용자의 속성은 실제 인증기관이 아니라 사용자가 속한 기관에서 발급하는 것이 일반적이다. 즉 사용자의 신용도는 사용자가가 거래하는 은행이 사용자 권한을 발행하며 사용자의 지위는 사용자가 속한 조직에서 권한을 발행하는 것이 일반적이다. 이와 같은 사용자 권한 발급을 인증기관에 위임하는 것은 조직 고유의 정보를 인증기관에 전달하는 것이 되어 실제적으로 구현되기 어렵다.

2.2 속성인증서 표준화동향

속성인증서에 대한 표준에 대한 작업은 ANSI, Open

Group, ITU-T, IETF 등과 같은 국제 단체에서 진행하고 있다. 이 중 ITU-T는 X.509 Version 4에서 속성인증서와 이를 이용한 권한관리기반구조인 PMI(Privilege Management Infrastructure)에 대하여 기술하고 있다. 또한 IETF에서는 Attribute Certificate Profile에 대하여 표준을 제정하고 있으며 현재 Version 9 드래프트가 발표되었다.

인터넷상의 전자상거래 정보보호를 위해 일반적으로 복잡한 ITU-T 표준보다 IETF의 RFC나 드래프트가 활용되고 있는 것이 현실이다. 따라서 본 고에서는 IETF의 AC 프로화일을 위주에 속성인증서에 대한 프로화일과 관련 기술을 설명한다.

Ⅲ. 속성인증서 프로화일

본 장에서는 인터넷 환경에 적합한 IETF의 속성인증서 프로화일에 대하여 기술한다.

3.1 표준 필드

본 절에서는 IETF의 속성인증서 프로화일에서 표준 확장 필드에 대하여 간략히 기술한다. 속성인증서에 대한 ASN.1 문법은 다음 [그림 1]과 같다.

```
AttributeCertificate ::= SEQUENCE {
   acinfo                AttributeCertificateInfo,
   signatureAlgorithm    AlgorithmIdentifier,
   signatureValue        BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
   version     AttCertVersion -- version is v2,
   holder      Holder,
   issuer      AttCertIssuer,
   signature      AlgorithmIdentifier,
   serialNumber      CertificateSerialNumber,
   attrCertValidityPeriod
                  AttCertValidityPeriod,
   attributes  SEQUENCE OF Attribute,
   issuerUniqueID UniqueIdentifier OPTIONAL,
   extensions      Extensions OPTIONAL
}
```

[그림 1] 속성인증서 프로화일

속성인증서는 [그림 1]에서와 acinfo, signatureAlgorithm, signatureValue, 로 구성되어 있다. acinfo는 속성인증서 정보를 포함하는 필드이다. signatureAlgorithm은 속성인증서를 서명하는 서명 알고리즘이며 속성인증서의 서명 값은 signatureValue로 표현된다. PKC에서와 같이 서명 값을 계산하기 위해 acinfo는 DER로 인코딩되어야 한다.

acinfo는 다음과 같은 필드로 구성되어 속성인증서를 구성한다. Version은 속성인증서의 버전을 나타내는 필드이며 값으로 v2를 가져야한다. Holder는 속성인증서의 소유주를 나타낸다. Holder는 baseCertificateID, entityName, objectDigestInfo로 구성될 수 있다. baseCertificateID는 속성인증서 소유주의 PKC를 발급한 issuer와 PKC의 일련번호로 구성된다. entityName은 소유주 PKC의 subject 필드는 subjectAltName과 일치해야 한다. objectDigestInfo는 속성인증서가 PKC에 연결되지 않고 공개키나 오브젝트코드와 같은 것에 연결될 때 그것들의 해시 값을 저장하여 속성의 소유주를 연결시키기 위한 필드이다. Issuer는 속성인증서의 발급자를 나타내는 필드이다. Signature는 속성인증서의 서명 값을 검증하는데 사용되는 알고리즘 식별자와 그것에 따른 파라미터를 저장하는 필드이다. Serial Number는 issuer에 의해 발급된 속성인증서 들 중에서 해당 속성인증서를 유일하게 식별할 수 있는 일련번호를 나타낸다. Validity Period는 속성인증서의 유효기간을 나타낸다. Attributes 필드는 속성인증서의 소유주에 대한 속성 정보를 제공하는 필드이다. Issuer Unique Identifier는 속성인증서 발급자를 식별하는 용도로 사용될 수 있지만 실제 사용되지 않아야 한다. Extensions 필드는 속성인증서 자체에 대한 다양한 부가 정보를 제공하는 필드이다.

3.2 속성 필드

본 절에서는 속성인증서의 Attributes 필드를 자세히 기술한다. 속성 필드는 속성들의 집합으로 구성되어 있다. 속성은 속성의 타입과 속성 값으로 구성되며 속성 값은 반드시 하나이상의 값을 가져야 한다. 속성 타입은 Object Identifier로 표현되며 속성 값은 속성 타입에 따라 결정된다. 속성 필드는 [그림 2]와 같은 ASN.1 문법으로 표현된다.

또한 IETF에서는 속성 정책 관리기관과 속성인증서 발급기관을 분리하도록 규정하고 있다. 이는 하나의 기관에서 속성인증서 정책을 관리하고 여타 다른 기관에서 속성인증서를 발급할 수 있도록 지원하기 위해서이다. 이를 위해 다음 [그림 3]과 같은 문법을 사용한다.

```
attributes  SEQUENCE OF Attribute,
   Attribute ::= SEQUENCE {
        type      AttributeType,
        values    SET OF AttributeValue
         -- at least one value is required
   }

AttributeType  ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY
                   AttributeType
```

〔그림 2〕 IETF 속성인증서의 속성 필드

```
IetfAttrSyntax ::= SEQUENCE {
   policyAuthority [0] GeneralNames
                              OPTIONAL,
   values   SEQUENCE OF CHOICE {
              octets    OCTET STRING,
              oid       OBJECT IDENTIFIER,
              string    UTF8String }
}
```

〔그림 3〕 IetfAttrSyntax

현재 속성인증서의 속성 필드 중에서 표준화된 속성 필드는 다음과 같다.

■ **Service Authentication Information**

이 필드는 서버 또는 서비스에게 소유주를 식별할 수 있도록 하는 정보를 포함한다. 또한 이 필드는 선택적으로 서비스에 고유한 인증정보를 포함할 수 있으며 이 정보는 일반 응용을 위해 사용자 ID와 패스워드를 포함할 수 있다.

```
name          id-aca-authenticationInfo
OID           { id-aca 1 }
Syntax        SvceAuthInfo
values :      Multiple allowed

SvceAuthInfo ::=   SEQUENCE {
   service      GeneralName,
   ident        GeneralName,
   authInfo  OCTET STRING OPTIONAL
}
```

■ **Access Identity**

이 필드는 소유주를 서버/또는 서비스가 식별할 수 있도록 고안된 필드이다. 이 필드에서는 authInfo 필드가 존재해서는 안된다. 이것은 이 필드는 속성인증서 검증자(Verifier)가 소유주를 인식하고 그의 권한을 인가하기 위해 제공되는 필드이기 때문이다.

```
name          id-aca-accessIdentity
OID           { id-aca 2 }
syntax        SvceAuthInfo
values:       Multiple allowed
```

■ **Charging Identity**

이 필드는 서비스 시스템이 속성인증서 소유주에게 과금(Charging)을 할 수 있도록 고안된 필드이다. 일반적으로 과금 대상은 소유주와 다를 수가 있다. 예를 들어 소유주가 소속된 회사에서 서비스에 대한 과금을 책임질 수 있다.

```
name          id-aca-chargingIdentity
OID           { id-aca 3 }
syntax        IetfAttrSyntax
values :      One Attribute value only,
      multiple values within the IetfAttrSyntax
```

■ **Group**

이 필드는 속성인증서 소유주가 속한 그룹에 대한 정보를 제공한다.

```
name          id-aca-group
OID           { id-aca 4 }
syntax        IetfAttrSyntax
values:       One Attribute value only:
      multiple values within the IetfAttrSyntax
```

■ **Role**

이 필드는 속성인증서의 소유주에게 할당된 Role을 포함한다.

```
RoleSyntax ::= SEQUENCE {
  roleAuthority [0] GeneralNames OPTIONAL,
  roleName      [1] GeneralName
}
```

위에서 roleAuthority는 role을 기술하는 속성인증서의 발급 기관을 나타내는데 사용될 수 있다. 또한 roleName은 roleAuthority에 의해 규정되어진다.

■ **Clearance**

이 필드는 소유주의 보안 등급에 대한 정보를 포함한다.

name	{ id-at-clearance }
OID	{ joint-iso-ccitt(2) ds(5) module(1) selected-attribute-types(5) clearance (55) }
syntax	Clearance - imported from {X.501-1993}
values	Multiple allowed

위에서 Clearance는 보안 등급과 관련된 보안 정책을 지칭하는 policyID 필드와 각각에 허용되는 보안등급을 나타내는 classList 그리고 선택적인 securityCategories로 구성된다. classList는 각각의 조직에서 결정할 수 있지만 상위 6bit은 unmarked, unclassified, restricted, confidential secret, top-secret로 예약되어 있다. 또한 securityCategories는 부가적인 인가정보를 제공한다.

3.3 확장 필드

속성인증서의 확장 필드에는 다음과 같은 확장이 포함될 수 있다.

■ **Audit Identity**

이 필드는 사용자의 감사기록을 나타내기 위한 것이다. 일부 응용에서는 속성인증서 소유주가 자신의 신원 정보를 응용 서버에 알리지 않기를 원한다. 이와 같은 환경에서 속성인증서 소유주의 신원확인을 응용 서버에 알리지 않고 응용 서버에서 감사기록을 남길 때 일 필드가 활용될 수 있다. 소유주의 비정상적인 행동이 있을 때, 응용 서버에서는 속성인증서 발급자와 협동으로 이 필드를 이용하여 소유주의 신원을 확인할 수 있다.

name	id-pe-ac-auditIdentity
OID	{ id-pe 4 }
syntax	OCTET STRING
criticality	MUST be TRUE

■ **AC Targeting**

이 필드는 속성인증서 발급시 속성인증서가 사용될 수 있는 응용 서비스인 목적(Target) 서비스를 기술하는데 사용된다. 응용 서버에서는 속성인증서 검증시 이 필드에 속한 서비스에 자신이 포함되지 않을 경우 속성인증서 검증을 실패로 하여 사용자에게 자신의 서비스를 제공해서는 않된다.

name	id-ce-targetInformation
OID	{ id-ce 55 }
syntax	SEQUENCE OF Targets
criticality	MUST be TRUE

위에서 Target은 다음과 같은 문법을 가진다.

```
Target ::= CHOICE {
  targetName          [0] GeneralName,
  targetGroup         [1] GeneralName,
  targetCert          [2] TargetCert
}
TargetCert ::= SEQUENCE {
  targetCertificate       IssuerSerial,
  targetName        GeneralName OPTIONAL,
  certDigestInfo ObjectDigestInfo
   OPTIONAL
}
```

이 필드는 여러 개의 Target으로 구성될 수 있으며 각각의 Target은 targetName, targetGroup, targetCert 중에 하나를 선택하여 값을 가진다. targetName은 속성인증서의 target이 되는 응용 서비스 이름이 된다. targetGroup은 속성인증서의 target이 되는 그룹이 된다. 예를 들면 "Printer"와 같은 그룹을 가질 수 있다. targetCert는 향후 ITU-T X.509와의 호환을 위해 만든 필드로써 현재는 사용하면 않된다.

■ **Authority Key Identifier**

이 필드는 속성인증서 검증 모듈이 속성인증서를 검증할 때 속성인증서의 발급자를 식별할 때 사용되는 필드이다.

name	id-ce-authorityKeyIdentifier
OID	{ id-ce 35 }
syntax	AuthorityKeyIdentifier
criticality	MUST be FALSE

■ **Authority Information Access**

이 필드는 속성인증서 검증시 속성인증서의 폐기 상태를 검증할 때 사용된다. OCSP를 이용할 경우 AuthorityInfoAccessSyntax에는 OCSP responder의 URI를 값으로 가져야 한다.

name	id-ce-authorityInfoAccess
OID	{ id-pe 1 }
syntax	AuthorityInfoAccessSyntax
criticality	MUST be FALSE

■ CRL Distribution Points

이 필드는 속성인증서의 폐기 여부를 인증서폐기 목록의 분배점을 이용하여 검사할 때 사용된다.

name	id-ce-cRLDistributionPoints
OID	{ id-ce 31 }
syntax	CRLDistPointsSyntax
criticality	MUST be FALSE

■ No Revocation Available

이 필드는 속성인증서 발급자가 별도의 인증서 상태 검증을 위한 정보를 제공하지 않는다는 것을 나타낸다.

name	id-ce-noRevAvail
OID	{ id-ce 56 }
syntax	NULL (i.e. '0500'H is the DER encoding)
criticality	MUST be FALSE

Ⅳ. 속성인증서 관련 기술

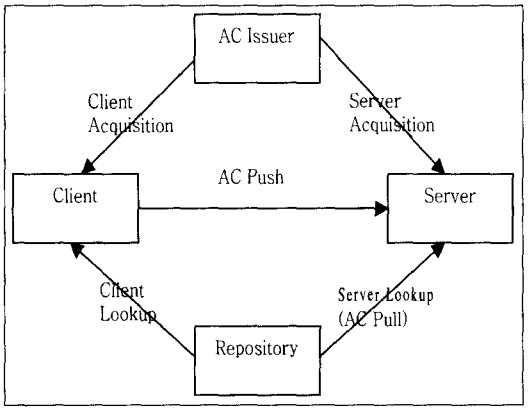
본 장에서는 속성인증서에 관련된 기술적인 이슈에 대하여 설명한다.

4.1 속성인증서 분배 방식

속성인증서가 실제 응용 환경에서 활용되기 위해서는 응용 서비스에 전달되어져야 한다. 이와 같이 속성인증서를 응용 서비스에 전달하는 속성인증서 분배 방식은 pull 모델과 push 모델로 분류될 수 있다.

pull 모델은 속성인증서가 생성될 때, 속성인증서 발급자가 응용 서비스에서 검색 가능한 디렉토리에 발급된 속성인증서를 게시하는 방식이다. 이와 같은 방식에서는 응용 서비스에서 사용자에 대한 접근 권한 등을 통제할 때 필요한 속성인증서를 디렉토리에서 검색한다. pull 모델은 기존 클라이언트-서버 모델을 변경시킬 필요가 없다는 장점을 가진다. 또한 클라이언트 사용자의 속성 권한을 할당하는 도메인이 응용 서비스 도메인과 동일할 때 장점을 가질 수 있다. 이것은 동일한 도메인을 가지는 응용 서비스에서 이미 디렉토리에 대한 정보를 가지고 있기 때문에 추가적인 비용일 발생하지 않기 때문이다. 그러나 속성인증서 검증시 매번 디렉토리에서 인증서를 검색하기 때문에 추가적인 통신 부하가 발생한다는 단점이 있다.

push 모델은 사용자가 응용 서비스에 접근할 때 속성인증서를 직접 전달하는 방식이다. 이 방식은 사용자가 응용 서비스에 접근할 때 사용자 이름과 패스워드를 전달하는 것과 같은 방식이다. push 모델은 기반구조를 단순화시키고 디렉토리를 필요로 하지 않는다는 장점을 가지고 있다. 또한 디렉토리 서버에서 속성인증서 검색을 위한 서버의 추가적인 통신비용이 필요하지 않기 때문에 시스템 성능이 개선될 수 있다는 장점을 가지고 있다. 특히 속성 권한을 할당하는 도메인과 응용 서비스 도메인이 달라 디렉토리 정보를 알리는데 추가적인 비용이 필요한 환경에서 활용될 수 있다. 다음 [그림 4]는 속성인증서의 분배 방식을 나타낸다.



[그림 4] 속성인증서 교환 방식

[그림 4]에서 AC Issuer는 속성인증서 발급 기관이며 Repository는 속성인증서를 게시하는 디렉토리이다. Server가 Repository에서 속성인증서를 검색하는 방식이 Pull 방식이며 Client에서 Server에 접속할 때 직접 속성인증서를 전달하는 방식이 Push 방식이다. 이와 같은 Push 모델과 Pull 모델은 응용 서비스 환경에 따라 선택적으로 활용될 수 있다.

4.2 속성인증서 검증

속성인증서 검증 모듈은 기본적으로 속성인증서의 다음과 같은 항목을 검사하며 하나라도 실패하면 전체 검증은 실패한다.

1. 속성인증서 소유주가 속성인증서 검증자에게 인

증을 위해 PKC를 사용할 경우 PKC에 대한 인증경로를 구성하고 RFC 2459[12]의 인증경로 검증 방법에 따라 검증한다.
2. 속성인증서의 서명 값을 검증한다.
3. 속성인증서를 발급한 발급자 인증서가 유효한지 검증한다.
4. 속성인증서 발급자가 응용 서비스 환경 설정이나 여타 다른 방법으로 속성인증서 발급자로 신뢰되어 있는지 확인한다.
5. 속성인증서를 유효기간이 올바른지 검증한다.
6. 속성인증서의 Targets 필드와 부합되는지 확인한다.
7. 속성인증서에 검증 모듈이 지원하지 않는 critical 확장이 있으면 속성인증서의 검증은 실패한다.

이외에도 다음과 같은 추가적인 검증이 설정될 수 있다.

1. 응용 서비스는 속성인증서 검증시 검증에 대한 환경을 설정할 수 있다. 즉 속성인증서가 특정한 속성을 포함하도록 또는 포함하지 않도록 설정할 수 있다.
2. 만약 검증 모듈이 응용 서비스가 속성인증서의 내용을 질의할 수 있도록 허용한다면 검증 모듈은 설정되어 있는 환경 정보에 따라 속성을 필터링할 수 있다. 예를 들어 검증 모듈이 어떤 응용 서버에게는 특정한 속성을 반환하지 않도록 설정될 수 있다.

4.3 속성인증서 생명 주기

속성인증서는 일반적으로 PKC에 비해 짧은 생명주기를 가진다. 이와 같은 특성 때문에 속성인증서 발급은 빈번하게 발생할 수 있다. 따라서 인증서 발급 프로세스는 가능하면 가벼운 프로세스(light process)로 구성되어야 한다. 또한 속성인증서 생명 주기가 짧은 경우에는 기존의 PKC 폐기목록 관리와는 다른 방식의 처리가 가능하다. 즉 유효기간이 아주 짧으면 인증서폐지목록이 필요 없는 Short-lived 인증서로 속성인증서를 발급할 수 있다.

반면 속성인증서가 PKC와 같이 상대적으로 긴 유효기간을 가지는 경우가 있다. 이는 속성인증서가 소유주의 지위 같은 속성을 포함할 경우이다. 소유주의 지위는 일반적으로 그 유효기간이 길다. 따라서 속성인증서의 생명 주기와 이에 따른 속성인증서 발급 시스템은 응용 환경에 따라 다양한 기능을 제공할 수 있어야 한다. 또한 속성 인증서의 폐지는 PKI의 인증서 폐지 메커니즘과 동일한 방식을 사용한다.

V. Case Study : 속성인증서를 이용한 RBAC 시스템

RBAC(Role Based Access Control)은 기존의 MAC(Mandatory Access Control)과 DAC (Discretionary Access Control) 방식과는 달리 사용자에게 role을 할당하고 role에 의해 시스템 접근제어를 수행하는 방식이다[13]. 본 장에서는 속성인증서를 이용하여 RBAC 시스템의 시스템 구성과 기능을 간략히 소개한다[14].

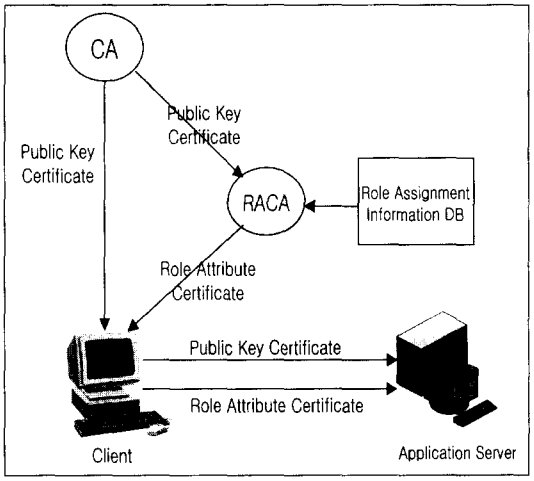
RBAC에서 권한 할당에 대한 정보를 관리하는 방식은 일반적으로 두 가지가 있다. 첫 번째 방식은 정보가 응용 서비스 의존적인(Application-dependent) 방식이다. 이 방식은 응용 서버 사이트에 정보를 관리하는 방식이다. 두 번째 방식은 접근 제어 정보가 실제 접근 기능이 수행될 때 요구되는 것으로 간주하고 중앙 집중형(centrally managed)으로 임무 권한 풀(role privileges pool)에 관리하는 방식이다.

사용자에 대한 권한 정보를 지역 사이트에 관리하는 첫 번째 방식은 이 정보를 원하는 곳과 정보를 저장하고 있는 곳이 일치한다는 장점을 가지고 있다. 따라서 중앙 집중형 방식에서 정보가 필요할 때 매번 중앙 관리 서버에 부가적인 통신을 해야하는 부하를 방지할 수 있다는 장점이 있다. 그러나 이 방식은 관리되는 사용자 정보가 미리 지역 사이트에 등록되고 저장되어야 한다는 단점을 가지고 있다.

중앙 집중형으로 관리하는 방식은 정보의 효과적인 등록과 효율적인 저장 관리가 가능하다는 장점을 가지고 있다. 그러나 응용 서버가 사용자 할당 정보를 검색하기 위해 부가적인 통신 부하가 필요하다는 단점이 있다.

이와 같은 문제를 해결하기 위해 다음 [그림 5]와 같이 속성인증서를 이용하는 RBAC 시스템의 구성할 수 있다.

[그림 5]에서 RACA는 사용자의 role에 대한 할당 데이터베이스를 접근하여 사용자의 속성을 속성인증서 형태로 발급한다. 그리고 발급된 인증서를 사용자에게 전달한다. 이 시스템에서 사용자는 응용



(그림 5) Role 속성인증서를 이용한 접근 제어 시스템

서버에 접근할 때 신원확인을 위해 PKC를 제출하고 서비스 접근을 위해서 RACA에서 발급 받은 속성인증서를 제출한다.

이 시스템은 시스템 사용자에 대한 role 관리를 중앙 데이터베이스에서 관리하기 때문에 지역 서버에 미리 저장 관리할 필요가 없어진다는 장점을 가지게 된다. 또한 응용 서버 측에서는 사용자의 권한 검사시 중앙 서버에 직접 통신하지 않고 사용자가 제출한 속성인증서의 role을 검사할 수 있다. 이와 같은 방식은 중앙 서버에 부가적인 통신 부하가 발생하지 않기 때문에 시스템 효율을 증가시킨다.

6. 결 론

본 고에서는 일반적인 응용 서비스에서 필요로 하는 인가 정보를 제공하기 위해 최근 그 연구가 시작되고 있는 속성인증서에 대하여 고찰하였다. 먼저 속성인증서의 출현 배경과 표준화 동향에 대하여 기술하였다. 그리고 속성인증서 프로화일과 관련 기술에 대하여 설명하였다. 또한 속성인증서를 이용한 RBAC 시스템에 대하여 설명하였다.

속성인증서는 사용자의 다양한 속성 정보를 제공하기 때문에 많은 실응용 환경에서 활용될 수 있을 것이다. 향후에는 속성인증서를 PKI 시스템과 연동하여 인증과 인가를 통합적으로 제공하는 연구가 필요하다. 또한 다양한 응용 환경에서 필요한 속성에 대한 요구 사항을 분석하여 속성인증서가 보다 많은 응용 환경에서 수용될 수 있도록 하는 연구가 필요할 것이다. 또한 속성 인증서에 담긴 사용자 속성 정보의 유통에 따른 정보 유출 문제에 대한 효율적인 처리 방식이 연구되어져야 할 것이다.

참 고 문 헌

[1] Computer Technology Research Corp. "Global Network Security : Threats and Countermeasure", 2000.

[2] W. Ford, M. S. Baum, Secure Electronic Commerce , Prentice Hall, 1997.

[3] NIST PKI Program web site, http://csrc.nist.gov/pki.

[4] Baltimore "Attribute certificate - a new initiative in PKI technology", http://www.baltimore.com/library/whitepapers/acswp-hm.html.

[5] Risa Pretty, "Attribute Certificate", NIST, TWG-99-67, 1999.

[6] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8, "INFORMATION TECHNOLOGY. OPEN SYSTEMS INTERCONNECTION. THE DIRECTORY : PUBLIC-KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS", 2001.

[7] Internet Draft, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX Working Group, 2001.

[8] Baltimore, http://www.baltimore.com/, 2001.

[9] Entrust, http://www.entrust.com/, 2001.

[10] RFC 2693, "SPKI Certificate Theory", IETF SPKI Working Group, September, 1999.

[11] Toni Nykanen, "Attribute Certificates in X.509", Seminar on Network Security, HUT TML, 2000.

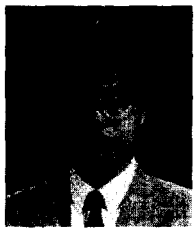
[12] RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF PKIX Working Group, January, 1999.

[13] Ravi S. Sandhu and Pierangela Samarati, "Access Control : Principles and Practice", IEEE Communications Magazine, pp. 40~48, 1994.

[14] Jing-Jang Hwang, Kou-Chen Wu, Duen-Ren Liu, "Access control with role attribute certificates", Computer Standards & Interfaces, Vol. 22, pp. 43~53, 2000.

〈著者紹介〉

윤 이 중 (E-Joong Yoon) 정회원
1990년 2월 : 인하대학교 전산과 석사
1997년 2월~현재 : 충남대학교 컴퓨터과학과 박사과정
1990년 2월~2001년 2월 : 한국전자통신연구원 정보보호시스템연구부장
2001년 2월~현재 : 국가보안기술연구소 기반기술연구부장
〈관심분야〉 정보보호, PKI, 컴퓨터네트워크, 데이터베이스



류 재 철 (Jae-Cheol Ryou)
1985.2 한양대학교 산업공학과 졸업
1988.5 Iowa State Univ. 전산학 석사
1990.12 Northwestern Univ. 전산학 박사
1991.2~현재 : 충남대학교 정보통신공학부 부교수
〈관심분야〉 인터넷 보안, PKI, 스마트카드 보안