공개키인증서와 속성인증서 연동방법의 설계

진승헌 0 김희선, 조상래, 조영섭
한국전자통신연구원 인증기반연구팀
(jinsh0,sezsez,sangrae,yscho)@etri.re.kr

Design & Implementation of Binding method for PKC & AC

Seunghun Jin0 Heesun Kim, Sangrae Cho, Yeongsub Cho
ETRI, Certification Infrastructure Research Team

요 약

인터넷상의 안전한 전자상거래에 효과적인 인증/인가 서비스를 제공하기 위해서는 공개키기반구조와 권한관리기반기반구조의 효율적인 연동이 필요하며 이를 위해서는 먼저 공개키 인증서와 속성인증서의 연동이 필요하다. 그러나 현재까지는 공개키 인증서와 속성인증서의 프로파일에 대한 독자적인연구만 진행되고 상호간의 구체적인 연동방법 및 시나리오에 대하여 기술하고 있지는 않다.[6],[7] 따라서 본 논문에서는 공개키 인증서와 속성인증서의 연동 방법의 요구사항을 정의하고 설계와 모델을 보임으로써 효과적인 인증/인가 서비스 제공 모델의 가능성을 제시한다.

1. 서 론

최근 인터넷을 통한 전자상거래(Electronic Commerce)는 기존 상거래의 시간적 공간적 제약을 극복하며 유통, 물류 비용 등의 상거래 비용을 절감하고 기업의 유연한 경제활동이 가능하도록 하여 사이버 기업(Cyber Company), 사이버 마켓(Cyber Market), 사이버 거래사회(Cyber Trading Community) 등과 같은 신종 기업/비즈니스 문화를 탄생시키고 있다. 전자상거래는 인터넷 뱅킹, 사이버 증권거래, 전자결재 등과 같이 다양하게 기존 상거래를 대체하며 급속하게 확장하고 있다[1,2].

전자 상거래는 사이버 공간에서 수행되기 때문에 거래자의 위조, 거래 내용의 노출, 거래 내용의 변조, 거래 사실의 부인 등과 같은 다양한 위협에 노출될 수 밖에 없다. 따라서 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 거래자의 인증(Authentication), 거래 내용의 무결성(Integrity), 기밀성(Confidentiality), 그리고 거래자가 거래사실 자체를 부인하는 것을 방지하는 부인봉쇄(Non-Repudiation) 기능을 제공하는 보안 메커니즘이 필요하다[1,3].

PKI(Public Key Infrastructure)는 기본적으로 신원확인을 위한 기술로서 공개키인증서를 바탕으로 신원확인 이외의 기밀성,무결성,부인봉쇄 서비스를 제공하는 정보보호 기반구조이다. 그러나 최근 많은 데이터와 다양한 인터넷 정보가 인터넷을 통하여 유통됨에 따라 신원확인 기능만으로는 다양한 정보보호 서비스의 요구사항을 충족시키지 못하는 경우가 발생한다. 즉, 신원확인된 사용자에 대해 시스템 접근권한,지위,임무,신용상태와 같은 사용자 속성 정보를 세밀히 제어할 필요성이 커지고 있다. 따라서 사용자의 속성 정보에 대한 권한관리 서비스를 제공하기위한 기반 구조인 PMI(Privilege Management Infrastructure)에 관심이 증가되고 이에 대한 연구가 활발히 진행되고 있다.

그러나 최근까지 PKI와 PMI에 대한 연구는 독자적으로 진행되어 많은 응용에 활용되는 데는 제약이 따르고 있다. 즉 인증을 위한 기반 구조인 PKI와 권한관리를 위한 기반 구조인 PMI는 별도로 존재하여 서비스에 활용될 수도 있겠지만 실제 많은 응용서비스에서는 인증과 권한관리가 모두 필요한 경우가 일반적이다[1,2].

이러한 인증/인가 기반구조를 위해서는 먼저, 인증을 위한 기반 구조인 PKI의 공개키인증서(PKC: Public Key Certificate)와 권한관리를 위한 기반 구조인 PMI는 속성인증서(AC: Attribute Certificate)가 연동되어 사용되어지는 것이 필요하다[4,5]. 그러나 PKC와 AC 관련 표준 제안에는 프로파일만 언급되거나 이론적인 연동방법에 대한 분류와 특징에 대해서는 기술하고 있으나[7], 구체적인 연동방법과 운영 시나리오를 언급하고 있지는 않다. 따라서 본 논문에서는 PKC와 AC의 연동방법을 제안하고 설계한다. 또한 연동개념을 구현함으로써 인증/인가 모델을 제시한다..

본 논문은 구성은 다음과 같다. 2장에서는 PKC와 AC의 연동방법들의 특징을 정의하고 프로파일을 통해 설계와 구현을 기술하고 3장에서는 사용자가 PKC를 이용하여 AC를 발급받는 시나리오를 기술한다. 4장에서는 인증/인가 서비스 모델 제시를 통하여 본 논문에서 제안한 방법이 효과적으로 인증/인가 서비스를 제공하는 것을 보이고

5장에서는 결론 및 향후 연구 과제를 기술한다.

2. PKC와 AC 연동방법 설계

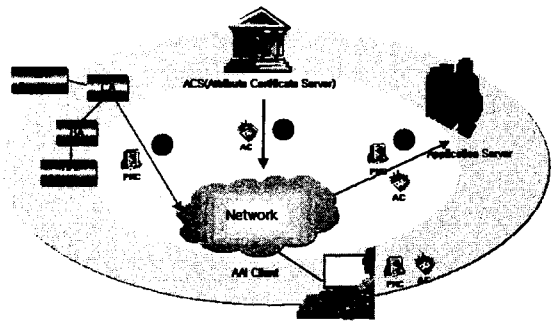

그림 1. PKC와 AC 연동 개념도

PKC와 AC의 연동 개념도는 그림1과 같다.
1) 먼저 사용자는 정해진 절차에 따라 PKI로부터 PKC를 받는다. 인증서는 CMP(Certification Management Protocol)를 통하여 발급 및 관리되어진다.[5]
2) PKC를 ACS(Attribute Certificate Server)에 제출하고 해당 AC를 발급 받는다. 이때, ACS에 사용자의 정보를 관리하는 방법은 별도의 처리 방법을 따른다.
3) 사용자가 응용서비스를 사용할 때, PKC를 응용 서버에 제출하여 인증을 하고 AC를 제출함으로써 서비스 접근 권한을 입증한 후에 서비스를 이용한다.

위와 같은 흐름을 가정할 때, 중요하게 고려하여야 할 부분분 중의 하나는 PKC와 AC의 연동 방법이다. 이에 관련된 연구는 [7]에서 기술한 바와 같이 3가지로 나누어 볼 수 있으며 아래와 같이 각각 장단점을 갖고 있다.

	통합된 서명 방법	선택적 서명 방법	연결된 서명 방법
CA 지원	단일	복수	복수
유효기간	동일	다름	다름
연결강도	강함	약함	강함
탐색용이성	쉬움	보통	어려움
재사용성	낮음	높음	보통

표1. PKC와 AC의 연결 방법 비교

첫번째 통합된 서명 방법은 속성정보를 저장 및 유통하기 위하여 AC의 기본적인 필요성에 위배되고 세번째 연결된 서명 방법은 연결 강도가 높아 AC와 PKC의 연결 관계를 검증하기가 용이하지 않고 재사용성이 비교적 낮아 다양한 서비스 환경에 적용하기에는 무리가 있어 보이므로 두번째 선택적 서명 방법을 본 설계에서는 적용하였다.

선택적 서명 방법은 통합된 서명 방법과는 달리 공개키인증서와 속성인증서를 분리한 형태이며 공개키 인증서로 부터 사용자의 신원과 관련되는 정보들을 속성 인증서에 포함시킴 으로서 공개키인증서와 속성인증서 사이의 연관관계를 설정하는 메카니즘으로서 가장 일반적인 형태라고 할 수 있다.

선택적 서명 방법은 공개키인증서가 포함하는 정보들의 일부부분만을 이용하기 때문에 공개키 인증서에서 속성 인증서가 연관관계를 설정하기 위하여 사용하는 정보들을 제외한 나머지 정보들은 CA 에 의하여 자유로이 수정될 수 있으므로 이는 공개키인증서의 재사용율을 높이는 장점을 가지고 있다.

구현단계에서는 AC 프로파일의 Holder 부분에 PKC 인증서의 DN과 Serial Number로 구성된 baseCertificateID 필드를 이용하여 PKC와 AC의 연결 관계를 설정하고 찾는다. PKC와 AC의 연결 관계를 설정하기 위하여 Holder에는 3가지 종류의 정보를 기술할 수 있는데 [5]에서 권고하는 바와 같이 objectDigestInfo는 사용을 배제하여 지원하지 않는다.

baseCertificateID	발급자 DN과 PKC의 일련 번호 PKC를 연계하여 인증할 때 사용	필수
entityName	AC의 소유자 또는 Role 이름	필수
objectDigestInfo	인증서나 공개키의 해쉬 값	지원안함

표 2 Holder 구성 필드

```
typedef struct IssuerSerial {
  unsigned char    bit_mask;
  # define IssuerSerial_issuerUID_present 0x80
  struct GeneralNames *issuer;
  CertificateSerialNumber serial;
  UniqueIdentifier issuerUID;
  /* optional; set in bit_mask */
  /* IssuerSerial_issuerUID_present if present */
} IssuerSerial;

typedef struct Holder {
  unsigned char    bit_mask;
  # define Holder_baseCertificateID_present 0x80
  # define entityName_present 0x40
  # define Holder_objectDigestInfo_present 0x20
  IssuerSerial     baseCertificateID;
  /* optional; set in bit_mask */
  /*Holder_baseCertificateID_present if present */
  struct GeneralNames *entityName;
  /* optional; set in bit_mask */
  /* entityName_present if present */
  ObjectDigestInfo objectDigestInfo;
  /* optional; set in bit_mask */
  /* Holder_objectDigestInfo_present if present */
}Holder;
```

3. 속성인증서 발급 시나리오

본 장에서는 사용자가 AC를 발급받는 과정을 기술한다. 먼저, ACS(Attribute Certificate Server) 관리자는 AC를 발급하기 전에 자신이 발급할 인증서에 적용되는 정책을 설정한다. 그 뒤에 사용자가 자신이 선택한 인증방법에 따라 AC의 발급을 요청하면 AC 발급자는 미리 설정되어진 인증 정보를 이용하여 요청한 사용자를 인증하고 해당하는 AC를 발급하여 준다. AC 발급을 요청하는 사용자를 인증하는 방법은 기존에 사용되고 있는 인증메카니즘을 수용할 수 있도록 ID/Password 방법과 PKC를 이용하는 방법을 모두 지원하도록 하였다.

4. 인증/인가 서비스 모델

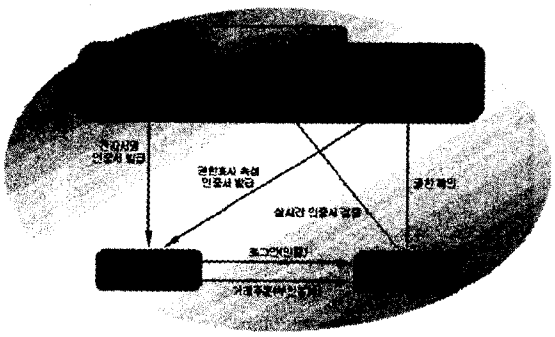

그림 2 인증/인가 서비스 모델을 이용한 증권거래 개념도

위에 그림2는 인증/인가 서비스 모델을 이용하여 증권주문 시스템을 구성한 것이다. 사용자가 PKC와 AC를 이용하여 증권거래 시스템에 연결하여 사용자에게 부여된 권한에 따라 구분되어진 서비스를 제공받을 수 있게하는 것을 보여 주는 것이 이 개념 구현의 시나리오이다.

먼저 사용자는 공개키기반구조(PKI)를 통하여 PKC를 발급 받는다. 발급 받은 PKC를 권한관리기반구조(PMI)에 제출하고 AC를 발급 받는다. 사용자가 증권 거래 서비스를 이용하고자 할 때, 먼저 PKC 인증서를 이용하여 증권서버에 인증을 요청한다. 증권거래서버(HTS Server)는 검증서버(VA : Validation Authority)를 통하여 인증서 검증을 한 후에, 인증이 통과하면 사용자가 서비스를 요청 받을 수 있는 상태로 전이를 하고 아니면 인증 실패 메시지를 사용자에게 보낸다. 인증이 성공하고 나면 사용자는 원하는 서비스를 선택하고 AC를 증권거래 서버로 전송한다.

증권거래 서버에서는 PMI내에 있는 Decision-Making Server를 이용하여 사용자가 요청한 서비스에 대한 권한을 소유하고 있는지 확인 한 후에, 권한이 있으면 서비스를 제공하여 주고 권한이 없으면 서비스 거절 메시지를 사용자가 보낸다.

5. 결론

인터넷을 통한 전자상거래가 활성화 되면서 정보보호 서비스의 중요성이 더욱 부각되고있다. 그러므로 현재 이런 한 인터넷에서 안전한 정보보호 서비스를 제공하기 위한 노력의 일환으로 PKI에 대한 많은 연구와 개발을 진행하고 있다. 그러나 PKI는 비대면한 상황에서 사용자의 인증을 위해서는 좋은 해결책을 제시하여주고 있지 만 인가에 대한 해결책을 제시하기에는 미흡한 것 또한 사실이다. 이러한 이유로 권한관리기반 구조가 제안되었고 이에 대한 연구가 활발히 진행중이다. 그러나 인증과 인가는 실제 서비스 적용 환경에서는 기술 적으로는 분리되어지지만 서비스로서 연동되어질 필요가 있다. 이에 본 논문에서는 공개키인증서와 속성인증서의 연동방법의 특징을 정의하고 설계하였다. 또한 속성인증서 발급 시나리오를 기술하고 연동개념 구현을 통하여 인증/인가 서비스 제공 모델의 가능성을 보였다. 향후에는 속성인증서의 관리 프로토콜과 속성정보관리 부분에 대한 연구가 필요하다.

6. 참고문헌

[1] 조영섭,최대선,진승헌,정교일, "Attribute Certificate과 PMI모델", 한국통신학회 학술대회, Vol 23, No. 2, July, 2001

[2] 김태성,노종혁,최대선,조영섭,진승헌, "통합형 Global 공개키 기반구조 시스템", 통신소프트웨어학술대회, pp , July, 2001

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

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

[5] RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", IETF PKIX Working Group, March 1999

[6] RFC 3281, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX Working Group, April 2002

[7] Joon S. Park, Ravi Sandhu, "Binding Identities and Attributes Using Digitally Signed Certificates", ACSAC, 2000