논문 2004-41TC-1-5

OCSP 서버를 이용한 인증서 결합방안

김 지 홍*, 지 준 웅**

Certificates Binding Method Using OCSP Server

(JiHong Kim and JunWoong Chi)

요 약

정보통신기술의 발달로 인하여 인터넷상의 공개키인증서를 이용한 전자상거래가 범용적으로 사용되고 있다. 또한 공개키인증서와 별도로 사용자의 권한에 대한 속성정보를 가진 속성인증서를 이용한 웹서버 혹은 데이터베이스 서버 접근제어를 위한 연구도 매우 활발히 진행되고 있다. 본 논문에서는 사용자인증을 위한 공개키인증서와 권한인증을 위한 속성인증서를 결합하기 위한 방안으로서 OCSP 서버를 이용한 웹서버 접근제어 방법을 제시한다.

Abstract

With the development of Information Communication Technique, electronic commerce is widely used in Internet using public key certificates. And the study on access control for web server or database server is also progressed actively. In this paper, we analyze the proposed access control method for server and the binding method between public key certificates and attribute certificates using OCSP server.

Keywords: PKI, PMI, Access Control, PKC, AC, OCSP

I. 서 론

위성영상정보의 활용분야는 환경에서부터 토목, 농업, 해양, 지질, 임업, 수산업 등 각 분야에 걸쳐 급속도로 확산되어 가고 있으며, 이에 따라 위성영상정보의 효과적인 관리 및 서비스에도 많은 관심이 집중되고 있다. 위성영상정보 통합관리기술은 위성영상정보의 체계적인 활용, 자원공급의 증대, 환경오염의 감시 및 통제, 지도 제작 등에 요구되는 다양한 위성영상 관련 정보를 구축하고 관리함으로써 신속하고 정확하게 사용자가 원하는 위성영상 관련 정보를 검색하고 이를 제공받게 해주는 서비스로 커다란 잠재력을 가지고 있는 기술 로 각광받고 있다. 이에 따라 2002년에 정부는 정보통신부, 건설교통부, 환경부, 해양수산부, 기상청 등 관계부처와 한국전자통신연구원, 한국과학기술연구원, 한국항공우주연구원, 국립지리원, 농업과학기술원, 국방과학연구소, 한국지질자원연구원 등 연구소로 구성된 '위성영상정보 운영위원회' 를 발족하고 2004년까지 위성영상정보 통합관리시스템을 구축키로 하는 등 위성영상정보 통합관리사업을 확정했다[8].

이와 같은 위성영상정보 통합관리사업의 목표는 국가차원에서 위성영상정보를 네트워크로 통합 관리함으로써 관련 연구 및 산업 활성화에 기여하는 것을 목표로 하고 있다. 향후에는 공공기관의 각 부처와 일반 사용자를 대상으로 위성영상 및 검색· 전송·소프트웨어 공급 시스템 등 다양한 맞춤형 솔루션을 제공할 예정이다.

현재 위성영상정보 통합관리시스템 구축을 위한 주관연구기관으로 선정된 한국전자통신연구원는 1차 연도인 2002년에 Landset MSS/TM/ETM+, SPOT-1, JERS-1, 코로나, 아리랑 1호 등 위성으로부터 획득한

* 정회원, 세명대학교 정보보호학과
(Dept. of Information Security, Semyung University)
** 정회원, 세명대학교 대학원 전기전자공학과
(Dept. of Electrical, Electronics Engineering, Semyung University)
※ 접수일자 : 2003년 8월 14일, 수정완료일:2004년 1월 16일

위성영상 DB 및 관련 메타데이터 DB 구축을 위한 통합관리체계와 기반 시스템을 설계하고 관련 소프트웨어를 개발하였으며, 2003년부터는 자원탐사위성(Landsat 7) 영상을 신규로 직접 수신하여 정부 및 공공기관을 대상으로 위성영상정보 통합관리 웹서비스를 시범 서비스할 계획이다.

본 논문은 이러한 위성영상정보 통합관리시스템에 대한 효율적인 보안방안으로서, 현재 증권, 금융분야 등에서 다양하게 적용되고 있는 공개키기반구조(PKI : Public Key Infrastructure)의 공개키인증서를 이용하여 사용자에 대한 인증방법을 제시하고, 또한 현재 연구중인 권한인증기반구조(PMI : Privilege Management Infrastructure)의 속성인증서를 이용하여 분산된 위성영상정보 데이터서버를 통제하기 위하여 웹서버를 이용한 접근통제방안을 제시한다.

공개키기반구조는 인증기반구조[6]로서, 비대면 거래 당사자들 간의 신뢰성과 안전성을 제공하기 위한 기능을 제공한다. 공개키기반구조는 계층구조 형식의 인증기반구조를 채택함으로서, 하위 계층의 인증기관 혹은 사용자에게 공개키 인증서를 발급하고, 이를 이용하여 온라인상의 안전한 전자거래를 할 수 있도록 하는 방식이다. 따라서 공개키기반구조 상에서의 모든 사용자는 공인인증기관으로부터 사용용도에 부합되는 공개키 인증서를 발급받고, 이를 이용하여 자신이 정당한 사용자임을 입증할 수 있다.

그러나 이러한 공개키 인증서를 이용한 기술은 공개키 정보를 이용하여 사용자 인증정보를 제공하므로 비대면 인터넷 통신에서의 사용자 신원을 입증하기 위해서 유용하게 사용될 수 있지만, 실제 시스템에서의 접근통제를 위한 정보는 포함하고 있지 않으므로, 접근통제를 필요로 하는 분야에서는 속성인증서와 같은 별도의 형태의 인증서를 이용한 구조가 제안되고 있다.

권한인증기반구조의 속성인증서는 사용자의 속성정보를 저장하는 인증서로서, 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공한다. 속성인증서에 대한 연구는 ITU-T, IETF 등에서 진행되고 있으며, IETF에서는 Internet Draft 문서[4]와 RFC 3281[5]를 통하여 표준화가 진행되고 있다. 이러한 속성인증서는 사용자의 속성정보와 같은 유용한 정보를 저장하고 있지만, 사용자에 대한 공개키 정보를 가지고 있지 않다. 따라서 속성인증서를 접근통제 분야에 적용하기 위해서는 공개키 기반구조상의 PKI 인증서를 첨부하여 접근하거나, 혹은 PKI 인증서와 속성인증서를 결합한 형태에 관한 많은 연구가 진행되고 있다[2,3].

Ⅱ. 기초이론

1. 속성인증서

인증서란 여권과 같이 자기 자신의 신분을 증명하기 위해 사용되는 증서로서, 인터넷상에서 신뢰성있는 통신을 위하여 개개인을 입증하기 위해서 사용된다. 이와 같이 인터넷상에서 사용되는 인증서는 크게 PKI 인증서, 속성인증서, SPKI 인증서로 분류할 수 있다. 속성인증서에 대한 표준을 미국 재정산업국(U.S financial industry)에서 1998년 ANSI X9 위원회를 통하여 발표하였다. 이는 기존의 ANSI X9.57 표준과 X.509 표준을 복합한 형태로 구성된다. 속성인증서란 인증서 주체와 주체에 대한 속성인증정보를 결합시킨 인증서로서, 속성정보 형태를 등록하여 사용할 수 있도록 규정한다. 속성인증서는 속성인증당국(Attribute Authority)으로부터 서명되어 발급되는 인증서로서, 구성은 기본적으로 PKI 인증서 형식과 유사하지만 사용자의 공개키를 포함하고 있지 않다.

속성인증서는 서버 혹은 데이터베이스 등 시스템 자원에 대한 접근통제를 목적으로 하기 때문에, 인증서 발급주기를 가급적 짧게 하고, CRL(Certificate Revocation List)은 가능하면 사용하지 않는 것을 권장하고 있다.

2. 기존의 방식

전 절에서 설명된 바와 같이 속성인증서에는 사용자의 공개키 정보가 포함되어 있지 않다. 이러한 단점으로 인하여 속성인증서를 사용하기 위해서는 사용자인증을 위한 공개키 인증서를 획득하여야 한다. 또한 공개키 기반구조상의 공개키 인증서를 이용함으로서, 상대방의 공개키를 이용하여 암호 및 인증기능을 제공받을 수 있다. 이와 같이 기존의 속성인증서를 이용하여 서버시스템에 대한 접근통제를 수행하기 위한 방법으로 속성인증서 분배 방식의 서버 Pull 방식과 사용자 Pull 방식이 있다. <그림 1>은 이와 같은 절차는 다음과 같다.

① 사용자는 인증기관(CA)으로부터 신원확인을 통해 공개키 인증서를 요청한다.

② 인증기관에서는 사용자의 신원확인, 키 발급절차를 거쳐, 사용자에게 공개키 인증서를 발급한다.

③ 사용자는 속성인증서를 발급하는 속성인증기관(ACA)에 속성인증서를 요청한다. 이때 사용자는 자신의 공개키인증서를 첨부하여 신원확인을 한다. 사용자의 접근권한 확인과정을 거친 후, 발급된 속성인증서를 사용자가 보관하는 경우에는 User Pull 모드라 하고, 발급된 속성인증서를 별도의 속성인증서 저장소에 보관하는 방법을 Server Pull 모드라 한다.

④ 사용자가 서버에 접속하는 경우, User Pull 모드에서는 자신의 공개키인증서와 속성인증서 및 서비스 요구패킷을 함께 제출하며, Server Pull 모드에서는 자신의 공개키인증서와 서비스 요구패킷을 전달한다.

⑤ Server Pull 모드에서 서버가 직접 속성인증서버에 접속하여 사용자에 대한 속성인증서를 획득한다. 반면에 User Pull 모드에서는 본 과정은 생략된다.

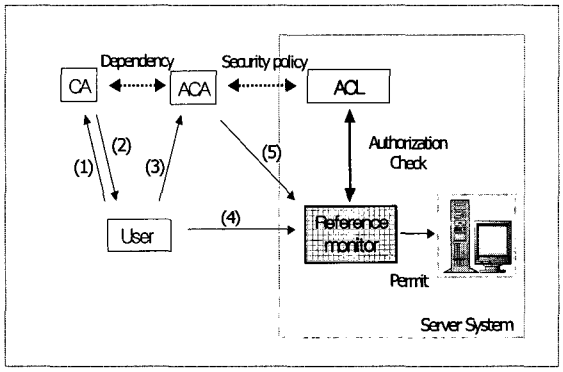


그림 1. 속성인증서 획득방법
Fig. 1. The AC Aquisition Method

이와 같은 절차를 통하여 서버에서는 공개키인증서, 속성인증서, 서비스 요구패킷을 수신한 후, 각각의 인증서에 대한 검증을 위하여 공개키인증서 CRL에 접속하여 공개키인증서의 유효성을 체크하고, 속성인증서 CRL에 접속하여 속성인증서의 유효성을 체크하여 적법성를 검증한 후, 서비스 요구패킷을 허용하거나 거부한다.

3. 속성인증서와 PKI 인증서의 결합방법

속성인증서는 사용자에 대한 공개키 정보를 가지고 있지 않기 때문에 암호 및 인증서비스를 사용하기 위해서는 공개키인증서와 병행하여 사용하여야 한다. 공개키인증서와 속성인증서를 병행하여 사용하는 방법이 가장 명확한 방법이기는 하지만 실제로 접근제어를 원하는 서버에서는 인증서 검증절차를 두 번해야 된다는 단점이 있다. 그러므로 최근 발표된 논문[3]에 의하면, 이러한 절차를 간략화시키기 위한 방법으로서, 속성인증서에 공개키인증서를 결합하기 위한 방법이 제안되고 있다.

① Monolithic Signature 방식 :

인증기관(CA : Certificate Authority)과 속성인증서 발급하는 인증기관(ACA : Attribute Certificate Authority)의 역할이 동일한 인증기관에서 행하여지는 경우에 적용될 수 있는 방법이다. 본 논문에서는 속성인증서를 발급하는 인증기관을 속성인증기관이라 칭한다. Monolithic Signature 방식은 PKI 인증서의 확장자 영역에 속성인증서를 포함하여 1개의 인증서로 구성하고, CA 서명문을 첨가하는 형태이다.

② Automatic Signature 방식 :

CA와 ACA가 서로 다른 별도의 인증기관으로 구성되어 있는 경우, 이를 결합할 수 있는 방법으로서, PKI 인증서와는 별도로 속성인증서에 PKI 인증서를 결합하기 위하여 PKI 인증서의 일련번호, 발급자 ID 등의 일부정보를 포함시키는 방법이다.

③ Chained Signature 방식

Automatic Signature 방식과 마찬가지로 CA와 ACA가 서로 다른 별도의 인증기관으로 구성되며, 이를 결합할 수 있는 방법으로서 속성인증서에 PKI 인증서의 서명문 부분을 포함시키는 방법이다.

이러한 방법들은 모두 기존의 PKI 인증서에 역할, 책임과 관련된 속성정보를 포함할 수 없다는 단점에 기인하여, PKI 인증서와 속성인증서를 결합시킬 수 있는 방법으로 제시되고 있다. 이와는 별도로 PKI 인증서의 확장자 영역에 다중 속성인증서 기능을 할 수 있도록 여러 개의 ACA에서 발행한 속성인증서를 다중으로 첨부할 수 있는 스마트인증서(Smart Certificate)라는 방법도 제시되고 있다[2].

4. OCSP 인증방식 소개

2절 3절에서 제시된 형태의 속성인증서는 수신측에서, 공개키인증서와 속성인증서를 각각 검증하여야 하는 단점이 있다. 예를 들면 공개키인증서와 이를 이용한 속성인증서가 발행된 후, 공개키인증서에 대한 취소사유가 발생될 때, 즉, 속성인증서는 정상적인 상태이지만, 공개키인증서가 취소되었을 경우에 발생되는 문제점을 지적한 논문이 있다[1].

본 논문에서는 이와 같은 절차를 제거하기 위하여 OCSP(Online Certificates Status Protocol) 서버를 이용하여 두 가지 검증과정을 한번의 검증과정으로 줄이고, 이에 대한 방법을 제시한다.

일반적으로 사용자가 특정인증서에 대한 유효성을 확인하기 위한 절차는 인증서 자체 정보의 유효성을 확인하는 절차와 인증기관이 발행하는 인증서 취소목록(CRL)에 자신이 사용하고자 하는 인증서가 포함되었는지를 확인하는 방법이 있다.

첫 번째 인증서에 대한 내용을 확인하는 절차에 의한 인증서 자체 정보의 유효성을 확인하는 방법과, 두 번째로 인증서의 상태를 체크하기 위하여 온라인으로 인증기관에 접속하여 CRL을 통하여 인증서의 취소여부를 확인하거나, 별도의 OCSP 서버[7]를 통하여 인증서 상태를 문의하는 방법이 사용되고 있다.

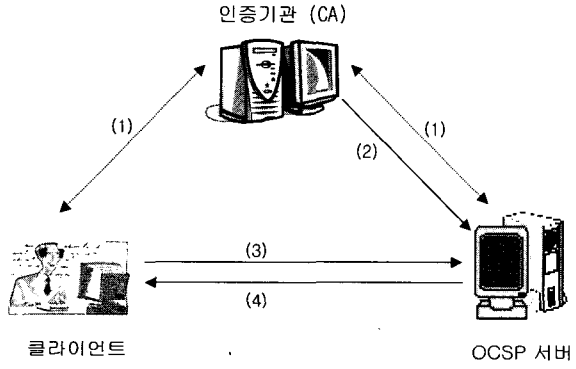


그림 2. OCSP 서버를 이용한 인증서 검증
Fig. 2. Certificate Verification Using OCSP Server

(1) 공개키 인증서 요청 및 발급
(2) 인증서 및 인증서 상태정보 저장
(3) 사용자의 인증서 상태정보 요청
(4) OCSP 서버는 클라이언트의 OCSP 요구메세지의 적절성 여부에 대한 응답메시지 전송여부 결정.

Ⅲ. 제안 방법

전 절에서 지적된 공개키인증서와 속성인증서의 상태정보를 확인하기 위해서는 각 인증기관별 CRL에 접속하여 상태정보를 문의하여야 하는 단점과 공개키인증서와 속성인증서의 상태정보를 실시간으로 동기된 상태정보를 받을 수 없다는 단점을 제거하기 위하여 본 논문에서는 OCSP 서버를 이용하여 각 인증서의 상태정보를 동기화하는 방법을 제안하였다. 본 논문에서 제안된 방법은 다음과 같다.

(사전단계_공개키인증서 발급)

(1) 공개키 인증서 발급단계 :

사용자는 사용자들에 대한 속성인증서를 발급하고, 관리하는 기관인 속성인증기관(ACA), 웹서버, 기타 공간정보제공을 위한 아카이빙시스템은 <그림 3>과 같이 공개키 기반구조상의 인증기관으로 인증서를 요청하고, 신원확인과정을 거친 후에 공개키 인증서를 발급받는다.

(2) 공개키인증서 상태정보 저장단계 :

CA는 주기적으로 자신이 발급한 공개키인증서에 대한 상태정보를 CA의 개인키로 서명하여, OCSP에 전달한다. OCSP 서버는 수신된 인증서 상태정보 패킷의 서명문을 확인하고, 이를 저장한다.

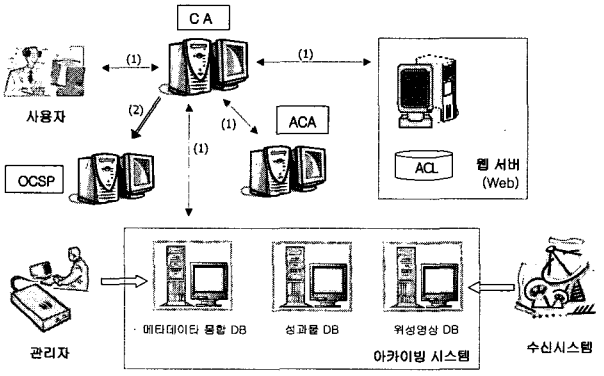


그림 3. 공개키인증서 발급을 위한 사전단계
Fig. 3. Prior step for PKC Issuance

(사전단계_속성인증서 발급)

(3) 아카이빙 시스템

아카이빙 시스템은 수시로 수신된 정보를 추가하고, 저장된 정보를 수정 보완하여야 하는 부분이다. 위성영상정보의 유통을 위하여 위성영상정보 수신시스템으로부터 수신된 정보를 위성영상 DB에 저장하고, 또한 성과물 혹은 기타 위성영상정보 자료들을 관리자에 의해 아카이빙 시스템에 등록하는 단계이다. 또한 등록된 위성영상정보에 대한 메타데이타를 작성하여 메타데이타 통합 DB에 저장하여야 한다.

(4) ACA 보안정책 설정 :

관리자는 웹서버를 통하여 위성영상정보를 저장하고 있는 분산된 아카이빙 시스템에 접근할 수 있도록 사

용자별 접근제어 정책을 설정한다. 즉, 아카이빙 시스템에 저장된 위성영상정보에 대한 접근통제리스트(ACL : Access Control List)를 작성하고, 이러한 정보는 ACA에서 사용자의 속성인증서 발급을 위한 정보로 사용된다.

(5) 속성인증서 요청단계 :

사용자는 접근하고자 하는 아카이빙시스템의 서비스를 요청하기 위하여, ACA에 접속하여 자신의 공개키인증서와 속성인증서 요청패킷에 서명하여 이를 ACA에 전송한다. ACA는 사용자의 공개키를 이용하여 사용자의 신원을 확인하고, 사용자로부터 속성인증서 요청패킷의 서명문을 확인하고 서명문을 추출한다. 사용자의 요청패킷에는 사용자가 접속하고자하는 서버와 응용서비스에 대한 요구내용이 포함된다. ACA에서는 시스템 관리자가 설정한 보안정책을 검토하여, 사용자의 요구가 적합한 지를 확인하고 적법한 경우에는 속성인증서를 발급하고 이를 보관하며, 이에 대한 상태정보를 서명하여 OCSP 서버에 전달한다.

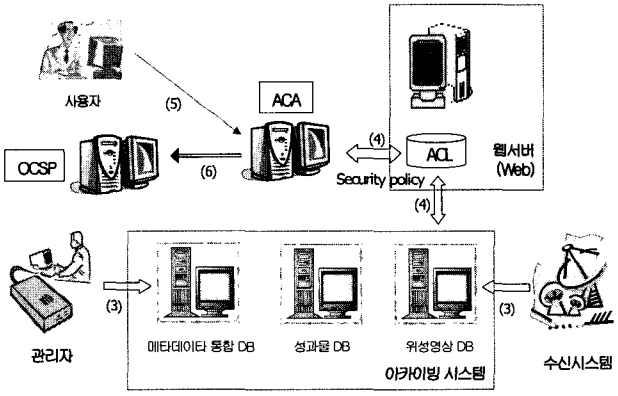


그림 4. 속성인증서 발급을 위한 사전단계
Fig. 4. Prior step for AC Issuance

(6) 속성인증서 상태정보 저장단계 :

OCSP 서버는 수신된 상태정보를 저장한다. OCSP 서버는 주기적으로 CA 및 ACA로 부터 사용자의 인증서(공개키인증서 및 속성인증서)에 대한 상태정보를 수신하여 사용자의 요구에 대하여 신속하게 응답하여야 한다. 또한 ACA는 발급된 속성인증서를 보관하고, 사용자에게 속성인증서가 발급되었음을 고지한다.

(웹서버 접근단계)

(7) 웹서버 접속단계 :

사용자는 자신의 공개키인증서와 아카이빙 시스템에 접속하여 사용하고자 하는 서비스에 대한 서비스요구패킷을 웹서버에게 보낸다.

(8) 인증서 상태확인 단계 :

웹서버는 사용자의 공개키인증서와 서비스요구패킷에 대한 서명문을 확인하고, 사용자의 속성인증서를 확인하기 위하여, OCSP 서버에 접속하여, 두 개의 인증서(공개키인증서, 속성인증서)에 대한 상태정보를 동시에 확인하여야 한다. 웹서버는 OCSP 서버에 접속하여 사용자의 공개키인증서와 속성인증서의 유효성을 검증한다. 이러한 두 가지의 인증서 검증을 위하여 OCSP 서버에 사용자 ID에 대한 두 개의 인증서(공개키인증서, 속성인증서) 상태정보를 통합하여 제공하는 기능을 부가한다.

(9) ACL 확인단계

웹서버는 사용자의 공개키인증서와 속성인증서를 검증한 후, 적법한 서비스요구이면 ACL에 설정된 서비스권한과 사용자의 요구를 비교하고 이에 해당되는 서비스 티켓을 발급한다. 서비스 티켓에는 아카이빙시스템의 해당서비스에 대한 접근허용시간과 접근권한을 허용하는 내용을 포함한다.

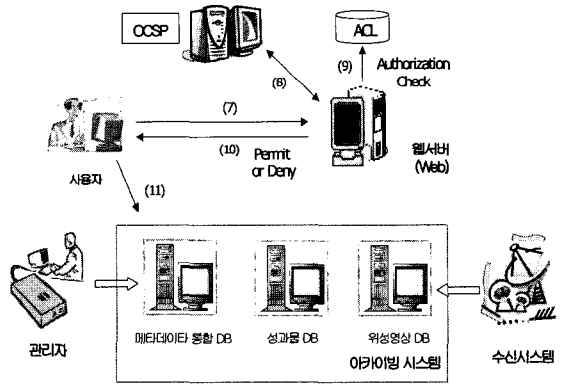


그림 5. 웹서버 및 아카이빙시스템 접근단계
Fig. 5. Access on Web Server System

(10) 티켓 전달 및 아카이빙시스템 접속단계

사용자는 웹서버로 부터 수신된 패킷을 자신의 개인키를 이용하여 복호하여 티켓을 추출하고, 이를 이용하여 아카이빙시스템에 접속한다.

Ⅳ. 제안 방식의 특징

본 논문에서 제안한 분산시스템구조에서의 속성인증서를 이용한 접근통제방안은 기존의 제안된 방식에 비해 다음과 같은 특징을 가진다.

(1) 단일 절차에 의한 속성인증서와 공개키인증서 검증

OCSP 서버를 이용한 단일 절차에 의한 속성인증서와 공개키인증서 검증방법을 제시하기 위하여 OCSP 서버내에서 사용자 DN(Distinguished Name)별로 공개키인증서와 속성인증서에 대한 상태정보를 결합함으로서, 기존의 인증서 검증을 위한 각 인증당국으로 접속하여 CRL을 조회하는 과정을 1번으로 단일 절차로 제안하였다.

(2) 공개키 인증서와 속성인증서간의 결합방법 제시

본 논문에서 제안된 방식에서는 사용자가 속성인증서를 발급받기 위하여 ACA에 접속하는 단계에서 사용자의 공개키인증서를 요구한다. ACA에서는 사용자의 속성인증서를 발급하기 위하여 사용자의 공개키인증서를 이용하여 사용자의 신원확인 작업을 수행하고, 공개키인증서에 대한 인증서 상태정보를 확인한 후에 속성인증서를 발급하며, 또한 속성인증기관도 CA로부터 인증된 기관이어야 하기 때문에 속성인증서에 대한 신뢰도를 높일 수 있다.

(3) OCSP 서버에서의 사용자별 인증서 통합관리기능

본 논문에서는 OCSP 서버에서 공개키인증서와 속성인증서에 대한 상태정보를 각각 CA 와 ACA로부터 주기적으로 수집하여, <표 1>과 같이 사용자별 인증서 상태정보에 대한 데이터베이스를 구축한다. .

표 1. OCSP에서의 공개키인증서와 속성인증서 상태표

Table 1. The State Table for PKC and AC in OCSP

사용자 DN (X.500 이름)	공개키인증서				속성인증서				적합성
	CA DN	일련번호	유효기간	취소사유	ACA DN	일련번호	유효기간	취소사유	

이로써 사용자의 인증서 상태정보 요구에 대하여 공개키인증서와 속성인증서의 상태정보를 통합 처리할 수 있다

(4) 속성정보의 실시간 처리

제안된 방식은 OCSP 서버를 이용하여 공개키 인증서와 속성인증서를 통합관리 할 수 있는 Server Pull 방식을 이용하여 사용자의 신분변경이나, 권한변경 등에 따른 속성정보에 대한 변경여부가 신속하게 적용될 수 있으며, 공개키 인증서와 속성 인증서간의 상태정보를 동기화 시킬 수 있다.

(5) 제안방식과 기존방식과의 비교

제안된 방식과 기존의 방식은 <표 2>와 같이 비교할 수 있다.

표 2. 제안방식과 기존방식의 비교

Table 2. A Comparison between suggested method and original method

분류	기존방식	바인딩방식	제안 방식
CRL	별도의 보관소를 가져야함	별도의 보관소를 가져야함	OCSP 통합 관리
상태정보 요구절차	공개키인증서와 속성인증서에 대한 검증절차를 별도로 수행	공개키인증서와 속성인증서에 대한 검증절차를 별도로 수행	공개키인증서와 속성인증서에 대한 상태정보를 동시에 검증.
취소사유 발생시 처리방법	공개키인증서와 속성인증서간의 동기문제 발생	공개키인증서와 속성인증서간의 동기문제 발생	OCSP 서버를 이용하여 주기적인 갱신으로 동시성
서버접속 방법	공개키인증서와 속성인증서를 모두 필요로 한다.	바인딩된 인증서 만을 이용하여 서버에 접근한다.	공개키인증서만 필요로 한다.

V. 결 론

최근 공개키 인증서를 이용한 인증기반구조와는 별도로, 응용서버에 대한 접근권한을 허용하기 위한 방안으로 제시되고 있는 PMI 기반구조의 속성인증서에 대한 내용을 검토하였다. 속성인증서는 자체적으로 사용자의 공개키 정보를 포함하지 않고 있기 때문에, 접근통제를 위한 응용시스템에 사용하기 위해서는 공개키 정보를 포함하고 있는 공개키 인증서와 함께 사용되어야 한다. 그러므로 두 개의 인증서를 사용하기 위해서는 공개키 인증서에 대한 검증과정과 함께, 부가적으로 속성인증서에 대한 유효성을 검증하여야 한다. 이와 같은 이유로 최근에는 두 개의 인증서를 결합하기 위한 인증서 바인딩기법에 관한 많은 연구가 진행되어 왔다.

본 논문에서는 각각의 인증서에 대한 CRL 정보를 획득하기 위한 과정을 OCSP 서버를 이용하여 단일화함으로서, 공개키인증서와 속성인증서간의 동기문제를 해결하였다. 또한 CA, ACA, OCSP 서버 및 위성영상 통합시스템을 위한 실제 시스템 구조를 제안하였으며,

또한 OCSP 서버에서 속성인증서와 공개키인증서를 결합하여 보관하는 데이터구조를 제안하였다. 이와같은 과정을 통하여 인증서 검증과정을 단일화하여 속도를 향상시키고, 비용을 절감시키는 효과를 발생할 수 있다.

마지막으로 본 연구 결과는 보다 섬세한 프로토콜 제안을 통하여 많은 보완되어야 할 것으로 생각되며, 기존의 사용자 인증과 권한 인증을 동시에 필요로 하는 응용시스템에 적극 적용될 수 있을 것으로 보인다.

참 고 문 헌

[1] Himanshu Khurana and Virgil D. Gligor, "Enforcing Dependencies between PKI Certificates in ad-hoc networks", IEEE International Conference on Telecommunications, Buchartest, Romania, pp. 293-298, June 2001.

[2] Joon S. Park and Sandhu, "Smart Certificates: Extending X.509 for Secure Attribute Service on the Web", NISSC / 1999

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

[4] Internet Draft "An Internet Attribute Certificate Profile for Authorization", S.Farrel, June 2001.

[5] RFC 3281 "An Internet Attribute Certificate Profile", S.Farrell, April 2002.

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

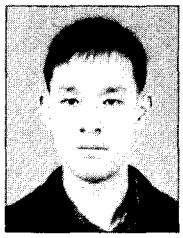
[7] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocols - OCSP", IETF PKIX Working Group, 2001.

[8] 한국전자통신연구원 컴퓨터소프트웨어연구소, "위성영상정보 통합관리사업", 공간정보기술센터 GIS 팀, 2002.

저 자 소 개

김 지 홍(정회원)

한양대학교 전자공학과 졸업, 한양대학교 전자통신공학 석사, 한양대학교 전자통신공학 박사, 1982 - 1991 엘지전선 연구소 근무, 1995.2 - 정보통신기술사, 1991 - 2002.8 세명대학교 전자공학과 교수, 2002 - 현재 세명대학교 정보보호학과 교수, <주관심분야: 공개키기반구조, 접근제어, 네트워크보안>



지 준 웅(정회원)

1996년 상지대학교 자원공학과 학사. 2001년 세명대학교 전기전자공학과 석사. 2003년 11월 현재, 세명대학교 전기전자공학과 박사과정.