情報保護學會論文誌
第14券 第6號, 2004. 12

AC 기반의 인증서 검증 모델

박 종 화[a)†], 김 지 홍[a)‡], 이 철 수[b)], 김 동 규[c)]
세명대학교[a)], 경원대학교[b)], 아주대학교[c)]

A Certificate Verification Method based on the Attribute Certificates

ChongHwa Park[a)†], JiHong Kim[a)‡], ChulSoo Lee[b)], DongKyoo Kim[c)]
Semyung University[a)], Kyungwon University[b)], Ajou University[c)]

요 약

인터넷과 정보통신의 발달과 더불어, 공개키 기반구조를 이용한 전자상거래가 광범위하게 사용하고 있으며, 또한 웹 응용 및 DB 시스템에 대한 접근제어에 관한 연구가 활발히 진행되고 있다. 공개키 인증서에 대한 검증방법으로는 CRL, OCSP, SCVP 등의 방법이 있으나, PKI 기반구조에서 사용되고 있는 인증서 검증방법이 권한제어를 필요로 하는 PMI 시스템에서 적용되기 위해서는 두개의 인증서에 대한 검증방법이 서로 연계되어야 한다. 왜냐하면 속성인증서는 권한제어를 위한 사용자의 속성정보를 저장하고 있는 반면에, 서명, 암호화 기능 등에 사용될 수 있는 공개키 정보를 포함하지 않고 있기 때문이다. 본 논문에서는 이와 같은 PKC와 PMI 간의 인증서 사용에서의 문제점을 분석하고 이를 해결하기 위하여 PMI 기반에서의 속성인증서를 중심으로 한 통합인증서 검증모델을 제안한다.

ABSTRACT

Electronic commerce is widely used with the development of information communication technologies in internet using public key certificates. And the study for access control in Web application and DB system is also progressed actively. There are many verification method for PKC(Public Key Certificates), which are CRL, OCSP, SCVP and others. But their certificates verification methods for PKC cannot to be applied to PMI(Privilege Management Infrastructure) which is using AC(Attribute certificates) because of synchronization of PKC and AC. It is because AC has no public key, AC Verifier must get the PKC and verify the validity on PKC and AC. So in this paper we proposed the new AC-based certificate verification model, which provide the synchronization in two certificates(AC and PKC).

Keywords : *PKI, PMI, Certificate Verification, PKC, AC*

Ⅰ. 서 론

정보통신 기술의 발달로 사회의 모든 분야에서 인터넷의 활용이 급속히 확산되어 전자상거래, 인터넷 뱅킹 등의 편리한 서비스가 제공되고 있다. 그러나 인터넷을 이용한 모든 거래는 거래 당사자간 비접촉, 비대면을 특징으로 하기 때문에, 온라인상의 편리함을 추구할 수 있는 반면에 거래 당사자간의 상호신뢰에 있어서 취약성을 가진다. 이러한 단점을 해결하기 위하여 전세계적으로 공개키기반구조(PKI: Public Key Infrastructure)라는 인증기반구조[7]를 도입함으로서 거래당사자들 간의 신뢰성과 안전성을 추구하고 있다. PKI는 계층구조 형식의 인증기반구조를 채택함으로서, 하위 계층의 인증기관 혹은 사용자에게 공개키인증서(PKC: Public Key Certificates)

접수일 : 2004년 5월 7일 ; 채택일 : 2004년 12월 6일
† 주저자 : chpark@semyung.ac.kr
‡ 교신전자 : jhkim@semyung.ac.kr

를 발급하고, 이를 이용하여 안전한 전자거래를 할 수 있도록 하는 방식이다. 따라서 PKI 상에서의 모든 사용자는 공인 인증기관(CA: Certification Authority)으로부터 사용용도에 부합되는 PKC를 발급받고, 이를 이용하여 자신이 정당한 사용자임을 입증할 수 있다.

그러나 이러한 PKC를 이용한 기술은 공개키 정보를 이용하여 사용자 인증정보를 제공하므로 비대면 인터넷 통신에서의 사용자 신원을 입증하기 위해서 유용하게 사용될 수 있지만, 실제 시스템에서의 접근제어를 위한 정보는 포함하고 있지 않으므로, 접근제어를 필요로 하는 분야에서는 속성인증서(AC: Attribute Certificates)와 같은 별도의 형태의 인증서를 이용한 구조가 제안되고 있다.

AC는 속성인증기관(ACA: AC Authority)에서 발급하는 사용자의 속성정보를 저장하는 인증서로서, 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공한다. AC에 대한 연구는 ITU-T, IETF 등에서 진행되고 있으며, IETF에서는 Internet Draft 문서[4]와 RFC 3281[6]를 통하여 표준화가 진행되고 있다. 이러한 AC는 사용자의 속성정보와 같은 유용한 정보를 저장하고 있지만, 사용자에 대한 공개키 정보를 가지고 있지 않다. 따라서 AC를 접근제어 분야에 적용하기 위해서 AC에 PKC를 첨부하거나 혹은 기타 결합방법을 통해 PKC와 AC를 결합하기 위한 많은 연구가 진행되고 있다[2,3].

본 논문은 이와 같이 접근제어를 요구하는 응용시스템에서 PKC와 AC를 검증하는데 있어서 발생되는 문제점을 밝히고, 이를 해결하기 위하여 기존의 PKC 인증서 검증에 사용된 OCSP(Online Certificate State Protocol)[8] 서버에 추가적인 기능을 부가하여 PKC 검증과 AC 검증을 함께할 수 있도록 함으로서, PKC와 AC간의 동기성 문제를 해결할 수 있는 방법을 제안한다.

II. 본 론

인증서(Certificate)란 여권과 같이 자기 자신의 신분을 증명하기 위해 사용되는 증서로서, 인터넷상에서 신뢰성있는 통신을 위하여 개개인을 입증하기 위해 사용된다. 이와같이 인터넷상에서 사용되는 인증서는 크게 PKC, AC, SPKC 등으로 분류할 수 있다. PKC(Public Key Certificate)란 현재 공개키 기반구조(PKI: Public Key Infrastructure)에서 범용적으로 사용되고 있는 신원 증명을 위한 인증서를 말하며, SPKC는 소규모 망에 적합하도록 PKI 기반구조를 간략화하고, 위임등의 기능을 구현한 SPKI[5] 구조에서 사용되는 인증서를 말한다. 본 논문에서는 PKC[7]와 SPKC에 관한 설명은 생략한다.

AC(Attribute Certificates)는 사용자의 속성정보를 저장하는 속성인증서로서, 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공하며, AC에 대한 표준화기관으로는 IETF(Internet Engineering Task Force)와 ITU-T(International Telecommunication Union)가 있다. IETF에서 제안된 AC 표준은 RFC 3281[6]이며, ITU-T와 ISO/IEC에서는 X.509 v4.0 AC와 권한기반구조인 PMI(Privilege Management Infrastructure)에 대하여 기술하고 있다. 두 개의 표준은 상당부분 유사한 구조를 가지고 있으며, IETF에서 제안된 AC에 대한 형식[6,7,10]은 표 1과 같다.

표 1. AC 기본형식

기본영역	사용용도
버전	X.509 V2.0인 경우 "2"
사용자(holder) 이름	AC 사용자이름(X.500 이름)
발급자(issuer) 이름	AC 발급자이름(X.500 이름)
서명알고리즘	서명알고리즘 ID 및 관련파라미터
일련번호	AC 일련번호
유효기간	시작일자와 만료일자
속성정보	사용자의 속성정보
발급자 고유 ID	발급자에 대한 부가정보
확장자	AC에 대한 부가정보
서명문	인증서발급자의 서명문

AC의 구성은 기본적으로 PKC의 형식과 유사하다. 그러나 사용자의 공개키 정보를 포함하고 있지 않으며, 사용자의 이름(holder)에는 BaseCertificateID 값으로 AC와 결합되는 PKC ID 번호, 사용자 이름, 사용자의 공개키 정보 등을 기록한다. 마지막으로 사용자의 속성정보에는 ID 및 비밀번호를 보관하는 "Service Authentication Information", AC holder에 대한 정보를 보관하는 "Access Identity", 과금정보를 처리하기 위한 "Charging Identity", 사용자가 속한 그룹을 표시하는 "Group", 사용자의 역할을 표시하는 "Role", 사용자의 보안인가 등급을 표시하는 "Clearance"로 구성된다.

1. 속성인증서의 발급과 응용서버접속방법

AC 분배 방식으로 Pull 방식과 Push 방식이 있다[6].

가. Push 방식을 이용한 접근제어 모델

Push 방식은 기본적으로 사용자가 AC를 소지하고 있으며, 사용자의 응용 프로토콜의 일부로서 권한 제어를 필요로 하는 응용서버에 접속할 경우에 AC를 제출하는 방식이다. 그림 1은 Push 방식을 이용한 접근제어 모델을 도식화하고 있으며, 이와 같은 절차는 다음과 같다.

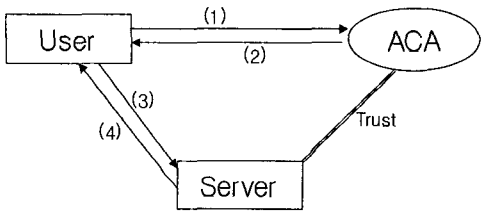


그림 1. Push 방식을 이용한 AC 획득방법

① 사용자는 ACA에게 AC 발급을 요청한다.
② 사용자의 접근권한 확인과정을 거친 후, 발급된 AC는 사용자에게 전달된다.
③ 사용자가 서버에 접속하기 위하여 자신의 AC와 접속요구 패킷을 보낸다.
④ 서버는 검증자로서 사용자의 AC와 접속요구 패킷을 수신하고 다음을 확인하고, 사용자에게 AC의 인증결과에 따라 접속허용여부를 알려준다.
- AC 서명문 확인 : AC 발급자인 ACA에 대한 PKC 획득과 ACA의 공개키를 이용한 서명문 확인
- 사용자 권한확인 : AC의 주체인 사용자의 권한 확인

나. Pull 방식을 이용한 접근제어 모델

Pull 방식을 이용한 서버 접속방식은 그림 1의 ②과정에서 발급된 AC는 ACA의 별도 저장소에 보관하고, 사용자에게 AC 발급상태를 통보해 주는 것 외의 모든 절차는 동일하다. 또한 사용자의 서비스 요구가 있을 경우, 응용서버는 사용자의 접속요구에 대한 권한여부를 확인하기 위하여 ACA의 AC 보관소로 접속하여 AC를 획득하는 방법이다.

다. 응용서버 접근절차

PKI 기반하에서 접근통제를 필요로 하는 응용에서 PKC와 AC를 이용한 사용자의 응용서버 접근절차를 도식화하면 그림 2와 같다.

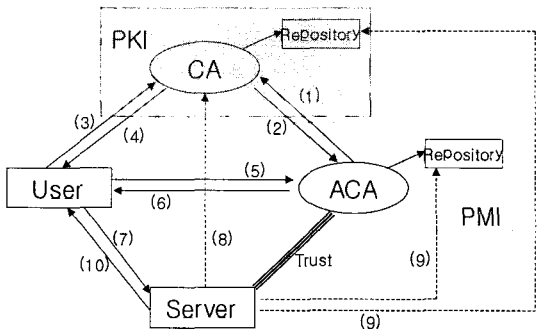


그림 2. 서버 접속절차

(ACA, 사용자, 서버에 대한 PKC 발급절차)
①,② ACA은 CA에게 PKC 발급을 요청하고, CA는 ACA의 신원확인, 키발급 절차를 거쳐 PKC를 발급한다.
③,④ 마찬가지 방법으로 사용자와 서버시스템도 CA로부터 PKC를 발급받는다.

(사용자의 AC 발급절차)
⑤ 사용자는 ACA에게 AC 발급을 요청한다. PKC ID 등의 신원확인을 위한 자료를 AC 발급 요청서에 작성하여 ACA에게 송부한다. 이때 지정된 PKC의 공개키는 이후, 사용자가 서버에 접속할 때 사용되는 각종 패킷에 대한 서명문 작성을 위해 사용되는 개인키와 결합된다.
⑥ ACA는 사용자에 대한 신원확인 과정과 접근권한 확인과정을 거친 후 AC를 발급한다. 발급된 AC의 사용자(holder) 항목에는 PKC에 대한 일련번호(BaseCertificateID)가 저장된다. push 방식인 경우에는 발급된 AC를 사용자에게 전달하고, pull 방식인 경우에는 발급사실을 사용자에게 통보하고, 발급된 AC는 ACA 보관소에 보관한다.

(서버 접속단계)
⑦ 사용자가 서버에 접속하는 경우로서, push 방식인 경우에는 사용자는 자신의 개인키로 서명한 서버접속요구 패킷과 자신의 AC를 서버로 전송한다. 그러나 pull 방식인 경우에는 사용

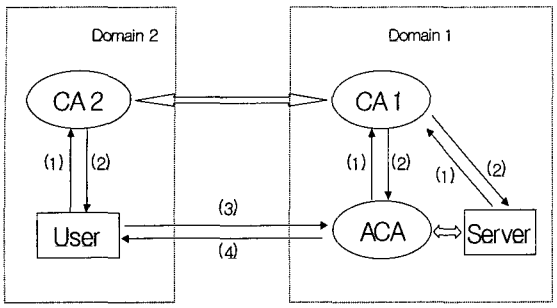


그림 4. 타 도메인에서 발급된 PKC 사용자

자는 자신의 개인키로 서명한 서버접속요구 패킷을 전송하고, 서버는 ACA 보관소에서 사용자의 AC를 취득한다.

⑧ 서버에서는 사용자의 AC 서명문 확인과 권한 확인작업을 시행한다.
- AC 서명문 확인 : AC 발급자인 ACA에 대한 PKC 획득과 ACA의 공개키를 이용한 서명문 확인
- 사용자 서명문 확인 : AC 주체인 사용자의 공개키를 이용한 사용자 인증
- 사용자 권한 확인 :

⑨ 서버는 사용자의 AC와 PKC 인증서에 대한 상태를 조회한다. 이때 PKC 혹은 AC가 취소된 상태이면, 사용자의 접속요구를 거절한다. 또한 사용자의 PKC 는 이후 사용자의 서명문 확인 및 암호문 전송에 사용될 수 있다.

⑩ ACA는 사용자에게 접속허용여부를 알려준다. 접근이 허용된 경우에는 이후 사용자와 서버간의 패킷에는 서명문과 암호문이 사용될 수 있다.

이와 같은 응용서버에 대한 접근절차에서 다음과 같은 인증서의 유효성검증절차와 서명문 확인을 위한 PKC 인증서 획득절차가 필요하다.

표 2. 단계별로 사용되는 서명 및 검증

단계	CA 서명문	ACA 서명문	PKC 유효성	AC 유효성	사용자 서명문
PKC 발급단계	서 명 (2)	-	-	-	-
AC 발급단계	검 증 (5)	서 명 (6)	검 증 (4)	-	-
서버 접속단계		검 증 (8)	검 증 (9)	검 증 (9)	서명/검증 (10)

① PKC 서명문 : 사용자 PKC에 첨부된 서명문 사용자 PKC 발급단계에서 CA가 서명하고, ACA에서 사용자 인증으로 사용된다.

② AC 서명문 : 사용자 AC에 첨부된 서명문 사용자 AC 발급단계에서 ACA가 서명하고, 서버측에서 권한확인을 위해 사용된다.

③ PKC 유효성 : PKC에 대한 유효성 PKC 유효성 검증은 AC 발급단계와 서버 접속단계에서 필요로 하며, CRL 혹은 OCSP 등의 검증방법이 사용된다.

④ AC 유효성 : ACC에 대한 유효성 push 방식인 경우에는 수신된 AC에 대한 유효성 검증 CRL 등의 검증방법이 사용된다. pull 방식인 경우에는 ACA로부터 AC를 가져와야 하므로, ACA에게 유효성 검증을 문의한다.

⑤ 사용자 서명문 : 서비스 요구패킷의 서명문 서버에서 사용자의 서비스 요구패킷에 날인된 서명문 확인을 위해 사용자의 공개키를 사용한다.

2. 응용서버 접근시의 문제점

가. 동일 도메인 내의 사용자에게 발급된 AC

그림 3은 한 개의 인증기관에 의해 관할되는 인증 도메인 내에서, 권한제어를 필요로 하는 모든 사용자와 시스템, 그리고 AC를 발행하는 ACA 들이 모두 동일 도메인 내에 위치하는 경우를 말한다.

이와 같은 경우는 가장 일반적으로 사용되는 접근제어 형태 구조로서, 도메인1 내의 CA에 의해 모든 사용자, 시스템 및 ACA에 대한 인증서 및 CRL에 대한 처리를 동일 도메인내의 CA에서 관리한다.

ACA는 사용자에 대한 AC를 발급하기 위해서, 도메인내의 CA에서 발급된 사용자의 PKC를 이용

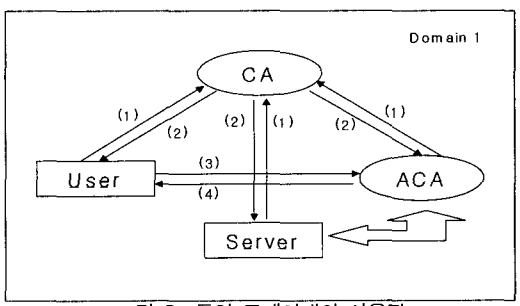


그림 3. 동일 도메인내의 사용자

하여 사용자를 확인하고, 또한 사용자도 CA에서 발급받은 PKC를 이용하여 서버에 접속할 때, 암호, 서명 등의 암호화서비스를 제공받을 수 있다.

그림 3에서 (1)과 (2)의 과정은 각각의 개체(사용자, ACA, 서버)들이 CA에 PKC를 요청하고, 신원확인작업을 거쳐 PKC를 발급하는 과정을 표시하고, (3)과 (4)의 과정은 동일 도메인내의 사용자가 ACA에게 AC를 요청하고, 이를 발급받는 과정이다. ACA와 서버간의 굵은 화살표는 ACA에서 AC를 발급하기 위하여 필요로 하는 사용자의 접근권한정보를 서버의 ACL(Access Control List) 정책에 의해 수행됨을 의미하는 종속성(dependency)를 나타낸다.

나. 타 도메인 사용자에게 발급된 AC

타 도메인 사용자에 대한 접근제어는 주로 웹 서비스를 필요로 하는 경우와 같은 응용에 적용된다. 예를 들어 그림 4 와 같이 도메인2 사용자가 도메인 1의 서버에 접근하기 위하여 서버의 접근권한정보를 관리하는 도메인 1의 ACA에게 AC 발급을 요청하는 경우에 해당되며, 이와 같이 타 도메인의 ACA에게 AC를 요청하는 경우에 자신의 도메인으로부터 발급받은 PKC1을 사용할 수 있다.

이와 같은 경우에는 도메인1의 ACA는 사용자의 AC 발급요청에 대하여 PKI 구조의 인증서 신뢰체인방식에 의해 도메인2 사용자의 PKC를 확인할 수 있다. 그러므로 도메인2 사용자의 PKC에 대한 인증서 및 CRL 상태정보는 도메인2의 CA2에서 관리되며, ACA의 PKC에 대한 인증서 및 CRL 상태정보는 도메인 1의 CA1에서, AC에 대한 속성인증서 및 CRL 상태정보는 ACA 저장소에서 관리하게 된다.

그림 4에서 도메인2의 사용자가 도메인1의 서버에서 상급수준의 접근 권한을 필요로 하는 경우에는 도메인1의 CA1에 접속하여 PKC를 발급받고, ACA에 AC를 요청하는 절차를 취하는 경우에는 전절의 동일 도메인내의 사용자의 경우에 해당된다.

사용자가 실제로 서버에 접근하는 단계에서는 서버에서 사용자 권한확인 작업과 함께, 사용자의 AC와 PKC에 대한 유효성 검증작업도 함께 이루어져야 하며, 사용자 서명문 확인은 인증기능과 서비스 요구 메세지에 대한 무결성 기능을 보장할 수 있다.

동일 도메인인 경우에는 사용자와 ACA의 PKC에 대한 관리와 사용자 AC에 대한 관리가 모두 동일 도메인 내에서 이루어지므로, 인증서 관리를 집중화 시킬 수 있다. 타 도메인으로 구성되는 경우에는

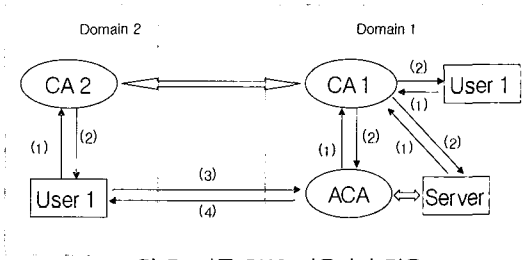


그림 5. 다중 PKC 사용자의 경우

웹서비스 등에 응용될 수 있다는 장점을 가진 반면에, 사용자와 ACA의 PKC가 별도의 도메인 저장소에서 관리되어야 하므로 인증서 관리에 다소 비용이 들며, PKC에 대한 인증서 상태검증과 AC에 대한 인증서 상태정보간의 동기성 등의 문제가 발생될 수 있다.

다. 다중인증서로 인한 문제

PKI 기반구조에서는 사용자가 여러 도메인으로부터 각각 인증서를 발급받을 수 있는 다중인증서 정책을 지원한다. 그림 5는 그림 4와 유사하지만, 사용자 1은 도메인1으로부터 발급받은 PKC1과 도메인2로부터 발급받은 PKC2를 소지하고 있는 다중인증서를 보유한 경우이다. 그러나 AC의 사용자 이름 항목에 지정된 PKC ID가 아닌 사용자의 이름, 사용자의 이메일, 사용자의 공개키 등이 사용되는 경우, 도메인 1의 CA1으로 부터 발급받은 PKC1으로 지정되어 있는 상태에서 도메인 2에서 발급받은 PKC2를 이용하여 접속하는 경우가 발생할 수 있다.

특히 도메인1의 CA1으로부터 발급받은 PKC1이 취소(revoked) 혹은 정지(hold) 상태에서, 사용자가 고의로 도메인2의 CA2로 부터 발급받은 PKC2를 이용하여 접속한 경우에는 도메인2의 CA2로부터 발급받은 PKC2가 유효한 상태이기 때문에 PKC 유효성은 검증되지만, 서버에 접속하기 위해 사용된 사용자의 각종 서명문은 실제로 AC와 결합된 도메인 1의 PKC1의 공개키를 이용하여야 하기 때문에 서버측에서는 서명문을 확인할 수 없다. 즉, AC 발급시의 "사용자 이름" 항목에 명시된 PKC는 도메인 1의 PKC1이기 때문에 사실상 CA1으로부터 발급받은 PKC1에 대한 상태검증을 통하여야만 주어진 권한이 허용될 수 있다.

일반적으로 시스템에 접근하기 위해서는 인증(authentication) 단계와 권한확인(authorization) 단계로 구분된다. 초기에는 사용자 인증기능을 통하여

시스템에 접근 여부를 확인하고, 사용자 인증이 통과된 경우에 한해서는 권한확인 단계를 거쳐야만 시스템의 자원에 대하여 접근할 수 있다.

다중 PKC 사용자인 경우에는 사용자인증, 권한확인 이후의 사용자의 서비스요구패킷에 사용된 서명문이 어느 PKC와 결합되었는지 확인할 필요가 있으며, 다음 절에서는 이와 같은 문제점을 지적한다.

라. AC와 PKC 검증방법의 문제점

AC는 사용자에 대한 공개키 정보를 가지고 있지 않기 때문에 암호 및 인증서비스를 사용하기 위해서는 PKC와 병행하여 사용하여야 한다. 또한 실제로 접근제어를 원하는 서버에서는 인증서 검증절차를 두 번해야 된다는 단점이 있다. 즉, AC에 대한 CRL 검증과 PKC에 대한 CRL 검증이 수행되어야 한다. 이와같은 이유로 최근의 많은 연구에서는 인증서 형식에 중점을 두고, AC와 PKC를 결합시키는 방안이 제시되고 있다[2,3]. 그러나 이와같이 AC와 PKC를 결합하는 방법은 인증기관(CA, ACA)이 별도로 구성된 형태에서는 인증서 유효성 검증에서의 동시성(concurrency)을 만족시킬 수 없다는 문제점이 제기된다[1]. 예로서 AC는 유효하지만, PKC가 취소된 상태이면 AC를 사용할 수 없다.

인증서의 유효성을 검증하는 방법으로는 인증서 취소목록(CRL) 방법과 OCSP(Online Certificate Status Protocol) 방법이 있다. OCSP 방식[8]은 실시간 인증서 상태를 조회하기 위한 클라이언트의 요청을 수용하기 위하여 별도의 OCSP 서버를 사용하는 방법이다. 또한 클라이언트와 OCSP 서버간에 동작되는 OCSP 프로토콜은 인증서 상태정보 요청패킷과 인증서 상태정보 응답패킷으로 구분되며, 응답패킷에는 인증서의 상태정보가 클라이언트에게 제공된다.

본 논문에서는 전 장에서 지적된 문제점을 해결하기 위하여, 기존의 OCSP 서버에 추가적인 기능을 부가한 서버를 ICVS(Integrated Certificate Verification Server) 서버라고 명명하였다. 또한 AC와 PKC(AC의 사용자이름 항목에서 지정하는 PKC)에 대한 인증서 상태정보는 표 3과 같이 분류될 수 있다.

일반적으로 OCSP 응답으로 제공되는 상태정보는 Good, Unknown, Revoked로 분류된다[8]. Good 상태는 인증서가 유효함을 의미하고, Revoked 상태는 인증서가 취소되어 무효화됨을 의미하며, Unknown 상태는 요구된 인증서에 대한 상태정보를 가지고 있지 않아, 확인할 수 없음을 의미한다.

표 3. 사용자의 PKC와 AC의 상태정보

종류	PKC	AC	사용가능 여부	상태정보
1	유효	유효	사용자인증, 서명기능	Good
2	유효	무효	사용자인증, 접근불가	Partial Good
3	무효	유효	사용자인증 및 접근불가	Revoked
4	무효	무효	사용자인증 및 접근불가	Revoked
5	확인 불가		PKC 혹은 AC 확인불가	Unknown

표 3에서는 AC 및 이와 결합된 PKC에 대한 인증서상태를 구분하여 정리하였다. 먼저 PKC는 유효하지만, AC가 취소된 상태를 Partial Good 상태로 정의하고, 사용자 인증은 가능하지만 특정 서비스를 사용할 권리가 없음을 의미한다. 또한 AC가 유효하더라도, PKC가 무효화되면 AC를 사용할 수 없기 때문에 이를 Revoked 상태로 정의한다. Partial Good 상태는 본 논문에서 정의한 상태로서, 응용에 따라 Revoked 상태로 처리할 수 있다.

3. 제안 방식

본 논문에서는 2장에서 제시된 PKC와 AC 간의 결합과 관련된 문제점을 해결하기 위한 방법으로서, OCSP 서버에 몇 가지 추가적인 기능을 부가하여 실시간으로 동시에 두개의 인증서(PKC, AC)에 대한 상태정보를 제공하는 ICVS 서버 방식을 제안하였다.

그림 6은 기존의 pull 방식의 AC 접근제어모델에 PKI 기반구조를 적용한 모델로서, AC 기반으로 PKC와 AC 검증을 동시에 수행할 수 있는 구조이다.

그림 6에서 ICVS 서버는 AC 사용시에 필요한 PKC에 대한 정보를 실시간으로 보관하고 있으며, 서버의 요구에 따라 실시간으로 인증서 유효성 정보를 제공하는 서버이다. ICVS는 동일 도메인(PKI_1)내의 사용자에 대한 PKC 정보 및 웹 서비스 사용자들을 위한 타 도메인(PKC_2) 사용자에 대한 PKC 정보를 AC 정보를 기반으로 실시간으로 취합하여, 서버의 AC 및 PKC 정보에 대한 인증서 유효성 검증요구를 수용한다.

이에 대한 절차는 3장의 서버접속절차에서의 인증서 유효성을 검증하기 위한 절차인 CA 및 ACA에 대한 각각의 저장소에 대한 접속 절차를 ICVS

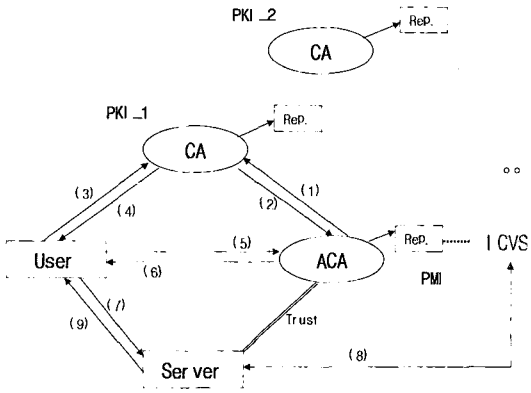


그림 6. AC 기반의 인증서 검증방식

서버에 접속하여 한번의 검증요구로 처리할 수 있도록 하였다. 다만 ICVS 서버는 PMI의 ACA와의 교류을 통하여 AC 사용자들에 대한 PKC 정보를 PKI의 CA들로 부터 인증서 취소정보를 실시간으로 취합하여야 하며, 서버 시스템과의 통신방식은 기존의 OCSP 프로토콜과 동일한 방식을 사용한다.

이와 같이 Pull 방식의 접근제어 모델을 적용함으로서, 사용자가 서버에 접근시에 AC를 제출할 필요가 없으며, ICVS 서버를 이용하여 ACA의 저장소로부터 사용자들의 속성인증서 정보를 취합하고, 이와 결합되는 PKC를 통합하여 인증서 검증정보를 제공할 수 있다.

그림 7은 ICVS 서버에서의 동작방법으로서 다음과 같은 절차로 수행된다.

(AC 발급절차)

① 사용자가 ACA에 접속하여 AC 발급을 요청한다. 이때, 사용자는 AC를 작성하고, 자신의 PKC와 함께 ACA로 보낸다.

② ACA는 서버시스템에 설정된 사용자의 권한을 확인하고, ICVS 서버로 사용자의 PKC 검증을 위해 AC와 PKC를 보낸다.

③ ICVS는 AC 와 결합된 PKC에 대한 검증을 거치고, 이에 대한 상태정보를 ICVS의 데이터베이스에 저장한다.

④ 또한 ICVS는 결과를 ACA로 보낸다.

⑤ ACA는 사용자에게 AC가 발급되었음을 알리고, AC를 ACA 저장소에 보관한다.

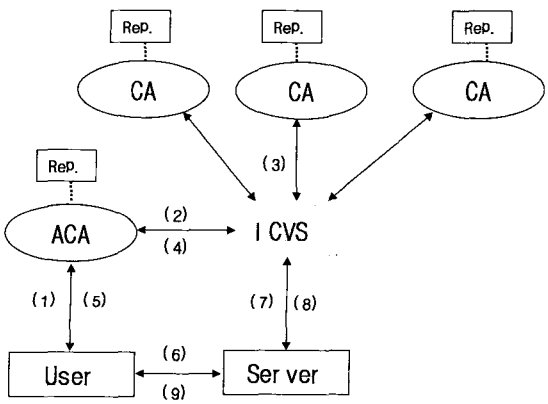


그림 7. ICVS 서버에서의 동작방법

이후 ICVS 서버는 ACA와 CA들로부터 인증서(AC, PKC)에 대한 상태정보를 실시간으로 취합한다.

(서버 접속절차)

⑥ 사용자는 서버로 접속요청을 한다.

⑦ 서버는 사용자의 접속요청에 대하여, 인증 및 권한확인을 위하여 ICVS 서버로 요청한다.

⑧ ICVS 서버는 실시간으로 기록된 사용자의 AC 및 PKC에 대한 상태확인 결과정보(good, revoked, uncertain)을 서버에게 전송한다.

⑨ 서버는 사용자에게 접속허용여부를 알려준다.

ICVS 서버에 저장되어 있는 AC를 기준으로 구성된 데이터구조는 다음과 같다.

표 4는 ICVS 서버에 저장된 AC 및 PKC에 대한 인증서 검증정보를 보인다. AC의 SN(Serial Number)를 기준으로 하여, 발급자인 ACA의 DN (Distinguished Name), Holder, AC의 유효기간 및 취소여부 정보를 실시간으로 보관한다. 또한 AC의 Holder 필드에는 AC와 결합되는 PKC에 대한 일련번호(PKC의 일련번호와 동일)가 기록되며, 이를 이용하여 PKC에 대한 CA DN, 유효기간 및 취소여부 정보를 실시간으로 수집할 수 있다.

표 4. ICVS 서버에 저장된 AC 및 PKC 정보

속성인증서					공개키인증서				적합성
SN	ACA DN	Hol-der	유효기간	취소여부	CA DN	일련번호	유효기간	취소여부	

ICVS 서버에서는 이러한 정보들을 취합하여 종합적인 적합성에 대한 저장하는 방식이다.

종합적인 적합성 여부에 따라 OCSP 프로토콜로 표 3과 같이 good, revoked, uncertain 으로 판정한다.

4. 제안된 방식의 특징

OCSP 프로토콜은 CA의 CRL 기능을 위임받아 사용자에게 인증서의 상태정보를 실시간으로 전달해 주는 시스템이다. 본 논문에서는 기존의 PKI 구조에서 인증서 유효성 검증기능을 제공하는 OCSP 프로토콜을 AC에 대한 유효성 정보와 함께, 결합되는 PKC에 대한 정보를 함께 보관함으로서, PKC와 AC 간의 동시성 문제를 해결하였다. 이를 위하여 기존의 PKI 구조에서의 OCSP 서버가 CA로 부터 PKC 상태정보를 수신하는 것과 마찬가지 방법으로, ICVS 서버를 이용하여 ACA로부터 AC 상태정보를 수신하고, 이에 따른 PKC 정보를 실시간으로 취합하는 방법을 사용한다.

따라서 ACA는 사용자로부터 AC 발급요청을 받고 사용자의 PKC를 확인하기 위하여, ICVS 서버에 요청하면, ICVS 서버는 사용자의 AC 정보와 함께, PKC 정보를 수신하여 인증서 검증을 한다. 검증결과 유효성이 입증되면, ICVS 서버내에 등록하고, 검증결과를 ACA로 보낸다. ACA는 사용자에게 AC가 발급됨을 알려주게 된다.

이후, 서버는 사용자로 부터의 서비스 접근요구를 받고, ICVS 서버에 인증서 검증요청을 한다. ICVS 서버는 실시간 인증서 검증 정보를 서버에게 알려줌으로서, 사용자의 접속허용여부를 결정하게 된다.

또한 PKI 구조의 CA처럼 PMI 구조의 ACA는 인증서 취소사유가 발생되면, 이를 ICVS 서버에 전달함으로서, ICVS 서버는 실시간으로 사용자 인증서(PKC 및 AC)에 대한 상태정보를 제공한다. 이와 같이 ICVS 서버는 CA 저장소로부터 상태정보와 ACA 저장소로부터 받은 상태정보를 취합하여 사용자의 인증서 상태정보요구에 대하여 통합적인 상태정보 응답을 제공한다.

이와 같이 본 논문에서 제안된 ICVS 서버는 기존의 OCSP 프로토콜을 이용하여 클라이언트와 동작되며, PMI 구조 및 PMI 구조의 CA와 ACA로부터 PKC와 AC에 대한 상태정보를 실시간으로 전달받아, 사용자별 인증서 상태정보에 대한 데이터베이스를 구축함으로서, 사용자의 인증서 상태정보 요구에 대하여 PKC와 AC의 상태정보를 통합 처리할 수 있다.

Ⅲ. 결 론

PKC를 이용한 인증기반구조와는 별도로, 응용서버에 대한 접근권한을 허용하기 위한 AC에 대한 내용을 검토하였다. AC는 사용자의 공개키 정보를 포함하지 않고 있기 때문에, 접근제어를 위한 응용시스템에 사용하기 위해서는 공개키 정보를 포함하고 있는 PKC와 함께 사용되어야 한다. 그러므로 두 개의 인증서를 사용하기 위해서는 PKC에 대한 검증과정과 AC에 대한 검증과정이 병행되어야 한다.

본 논문에서는 기존 OCSP 프로토콜을 변환하지 않고, 단지 OCSP 서버의 기능을 보완하여 PKC에 대한 상태정보와 함께, 권한기반구조에서 사용되고 있는 AC에 대한 상태정보를 제공할 수 있는 ICVS 서버방식을 제안하였고, 이를 이용하여 PKC와 AC 간의 동기문제를 해결하였다. 또한 ICVS서버에서 AC와 PKC를 결합하여 보관하는 데이터구조를 제안하였다. 또한 이와같은 과정을 통하여 인증서 검증과정을 단일화하여 속도를 향상시키고, 비용을 절감시키는 효과를 발생시킬 수 있다.

또한 PKI 구조에서의 OCSP는 PKC에 대한 인증서 유효성검증을 수행하는 반면에, 본 논문에서 제안된 ICVS 서버는 접근통제를 우선으로 필요로 하는 인터넷 기반의 대규모 접근통제 시스템에 적합할 것으로 기대된다.

마지막으로 본 연구 결과는 보다 섬세한 프로토콜 제안을 통하여 보완되어야 할 것으로 생각되며, 기존의 사용자 인증과 권한 인증을 동시에 필요로 하는 응용시스템에 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 Tel., Buchartest, Romania, pp. 293-298, June 2001.

[2] Joon S. Park and Sandhu, "Smart Certificates : Extending X.509 for Se-

cure 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, "X.509_4th Edition Draft V8 - Draft ISO/IEC 594-8", May 3. 2001.

[5] RFC 2693, "SPKI Certification Theory", C. Ellison.

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

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

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

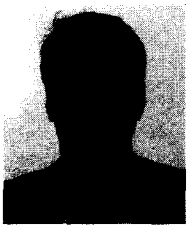
[9] Risa pretty, "Attribute Certificate", NIST, TWG-99-67, 1999.

[10] 윤이중, 류재철, "속성인증서 프로화일 연구", 한국정보보호학회 논문지 제11권, 제5호, pp. 75-83, 2001. 10.

〈著者紹介〉

박 종 화(Chong-hwa Park) 정회원
1974년 2월 : 숭실대학교 전자 공학과 졸업
1990년 1월 : 미국 Syracuse University 컴퓨터공학과 석사
1976년~1978년 : (주)CDC
1979년~1981년 : 전자통신 연구원
2002년 : 아주대학교 컴퓨터공학과 박사수료
1994년 3월~현재 : 세명대학교 소프트웨어학과 교수
〈관심분야〉 정보보호, 시스템 소프트웨어 보안, 네트워크 보안

김 지 홍 (Jihong Kim) 종신회원
1982년 2월 : 한양대학교 전자공학과 졸업,
1984년 2월 : 한양대학교 전자통신공학 석사,
1996년 2월 : 한양대학교 전자통신공학 박사
1982년~1991년 : 엘지전선 연구소 근무
1995년 : 정보통신기술사
1991년~2002년 : 세명대학교 전자공학과 교수
2002년~현재 : 세명대학교 정보보호학과 교수
〈관심분야〉 공개키기반구조, 접근제어, 네트워크보안



이 철 수 (Lee Chul Soo) 정회원
1975년~1977년 : KAIST 전산과 석사
1977년~1981년 : KAIST 전산과 박사
1982년~1993년 : (주) 데이콤
1993년~1998년 : 한국전산원장
1999년~2000년 : 한국 정보보호진흥원장
2000년~2002년 : 정보통신대학교 교수
2003년~현재 : 경원대학교 소프트웨어 대학 교수

김 동 규 (Dong-Kyoo Kim) 정회원
1973년 2월 : 서울대학교 공과 대학 응용수학과 졸업
1979년 2월 : 서울대학교 자연과학대학원 전자계산학과 석사
1984년 : 미국 Kansas State University 전자계산학과 박사
1986년 : IEEE 802.4, 802.6, 802.10 Working Group Member
1979년~현재 : 아주대학교 정보 및 컴퓨터공학부교수, Asiacrypt '96 조직위원장, 건설교통부 항공 교통관제소 신공항 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국정보보호학회 부회장 역임
〈관심분야〉 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링