CCCA를 이용한 CORBA기반의 상호 인증 메커니즘

이 용 주† · 장 종 현†† · 이 동 길†††

요 약

인터넷의 이용증가와 전자상거래의 활성화 등으로 인해 급속도로 발전하는 공개키 기반구조에 능동적으로 대처하기 위해서는 확장성과 상호 운용성, 관리용이성, 타 공개키 기반구조 기관의 수용 등 여러 가지 문제를 고려한 인증 모델이 제시되어야 한다. 이 논문에서는 인터넷에서 이기종의 컴퓨터들이 서로 연결되어 자료를 공유하고 분산되어 실행할 수 있는 개방 분산 시스템인 CORBA 기반의 상호인증 모델을 설계한다. 공개키 기반 시스템(PKI)을 도입하되 CCCA(Cross Certification CA)를 이용하여 효율적으로 상호인증 할 수 있는 모듈과 인터페이스를 설계하고 기존 모델과 비교 분석하여 우수성을 증명한다.

CORBA Based Mutual Authentication Mechanism using CCCA

Yong-Ju Yi† · Jong-Hyeun Jang†† · Dong-Gil Lee†††

ABSTRACT

To cope dynamically with quickly changing PKI due to activation of electronic commerce and increase of Internet use, we must design the authentication model considering enlargement, mutual operation, management facility and accommodation of other PKI. In this paper, we propose a mutual authentication mechanism based on CORBA which is a open distributed system and enables different systems to share their information and be executed in distributed environment. We design interface modules using PKI and CCCA (Cross Certification CA), analysis this model by comparing it with existing one and prove superiority of our model.

키워드 : 코바(CORBA), 인증(Authentication), 보안(Security), 공개키 기반구조(PKI), 인증국(Certificate Authority)

1. 서 론

컴퓨터 성능의 향상과 소프트웨어 개발 기술의 발달로 인하여 기존의 중앙 집중식 시스템의 형태에서 이기종의 컴퓨터들이 서로 연결되어 자료를 공유하고, 분산되어 실행할 수 있는 개방 분산 시스템의 형태로 전환이 이루어지고 있다[1, 2]. 이에 관한 연구 활동도 증대되어, 1989년에는 객체지향 기술을 바탕으로 응용 프로그램들을 결합하기 위한 객체지향 표준을 제정하기 위해서 OMG(Object Management Group)가 탄생하게 되었으며, OMG는 이종의 분산된 환경 하에서 응용 프로그램들을 통합하고 상호연동 할 수 있는 표준 기술인 OMA(Object Management Architecture)를 제정하였다.

CORBA(Common Object Request Broker Architecture)는 OMG라는 컨소시움의 산출물이다. 또한 CORBA는 분산 컴퓨팅 환경과 이기종 분산 환경의 시스템 통합을 위한 표준이다. CORBA는 효과적인 시스템 통합을 위해 기술적인 이익을 제공하며, 이 기종 시스템들의 분산 의사소통 환경을 위한 하부구조를 제공한다[3]. 이러한 분산 객체 기술인 CORBA는 기존에 존재하는 모든 다른 형태의 클라이언트/서버 미들웨어를 포함할 수 있는 잠재력을 갖는 미들웨어를 정의하며, 객체의 위치와 구현에 상관없이 그들 사이의 통신을 가능하게 하여 주는데, 이러한 CORBA의 장점을 이용하여, 플랫폼에 독립적이면서 보안성을 강화시키기 위하여 상호 인증 기능을 갖는 인증 서비스를 CORBA에 적용할 수 있도록 모델을 제시하고 인터페이스를 설계한다. CORBA기술의 사용인 보안 서비스는 플랫폼에 상관없이 동일하며 안전한 서비스를 제공할 수 있을 뿐 아니라 분산된 객체 환경으로 제공될 수 있다[4]. 또한 이러한 분산객체 환경인 CORBA를 향후 차세대 인터넷에 적용할 수 있도록 차세대 인터넷에서 CORBA 기반의 보안 플랫폼은 절실히 요구된다.

2. 차세대 인터넷에서 CORBA 보안

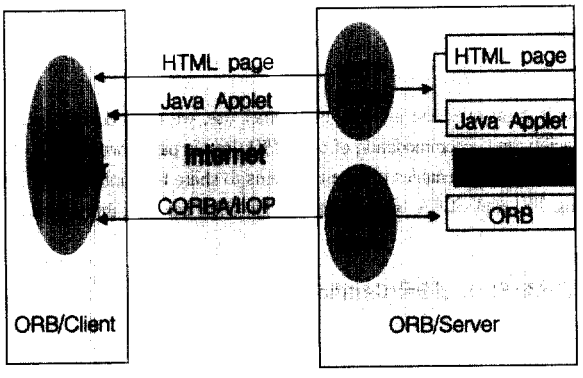
CORBA기반의 분산처리 응용들은 다양한 보안 위협들로부터 안전성이 보장될 수 있는 보안 서비스의 필요성이 요구되는데, 이를 위해 OMG는 CORBA 기반 응용의 보안성을 유지하는데 핵심적인 보안기능과 보안 인터페이스의 표

† 준 회 원 : 한국전자통신연구원 네트워크 기술연구소 연구원
†† 준 회 원 : 한국전자통신연구원 네트워크 기술연구소 선임연구원
††† 정 회 원 : 한국전자통신연구원 네트워크 기술연구소 책임연구원
논문접수 : 2001년 2월 21일, 심사완료 : 2001년 4월 30일

준안을 제시하였다[11]. 이 단원에서는 CORBA와 인터넷이 어떻게 협력하여 동작하는지 동작원리와 보안정책 모델에 대하여 기술한다.

2.1 CORBA와 인터넷

하이퍼 텍스트기반의 전송원리에서 웹 기술은 데이터 표현과 분산에 대한 표준 기술로 발전하였다. 웹이 신뢰성 있는 TCP/IP 프로토콜에 기반하고 있는데 반해 CORBA의 초기 버전은 ORB 내부 통신 프로토콜을 명세하지 않았다. 그러나 2.0버전에 IIOP가 정의되었으며 IIOP는 표준화된 통신 프로토콜로서 서로 다른 ORB 간의 통신을 허용한다. 또한 자바를 지원하는 CORBA의 영향으로 ORB 개념이 인터넷으로 흡수되는 상황에 이르렀다. 웹 브라우저는 IIOP를 통해 서버 측의 객체에 접근하고자 하는 클라이언트로서 작동한다. 전통적인 웹 프로토콜인 HTTP는 더 이상 사용되지 않으며 (그림 1)은 클라이언트 역할을 하는 웹 브라우저와 IIOP-server 사이에서 IIOP 연결을 설정하는 그림을 설명하고 있다.

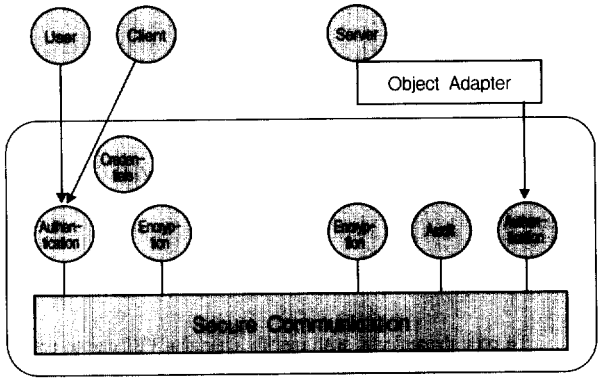


(그림 1) 인터넷에서 CORBA의 동작과정

(그림 1)에서 클라이언트는 HTTP-server에 있는 자바 클래스를 요청해야 하며 클라이언트 측에 다운로드 된 클래스는 브라우저가 CORBA 서버와 통신할 수 있도록 해준다. 이런 경우 브라우저는 IIOP 자바 파일을 가지고 있을 필요가 없지만 서버는 반드시 기본적인 IIOP 클래스를 가지고 다운로드 하여야 한다. 이런 방법은 오버헤드, 서버 함수의 반환 값, 데이터 타입 등이 적으며 언어에 독립적이라는 장점이 있다.

2.2 CORBA에서의 보안 정책 모델

분산환경에서 객체는 기존의 전통적인 환경에서와 다르게 클라이언트와 서버의 역할 모두를 수행할 수 있다. 서버는 신뢰하지만 서버의 자원을 허가 받지 않은 접근으로부터 보호하기 위해서는 네트워크상의 어떠한 클라이언트 운영체제도 신뢰할 수 없다. 분산환경에서의 네트워크 자체도 아주 쉽게 접근을 허용하며 스니퍼나 트로이 목마의 삽입 같은 침해를 당하기 쉽다. 또한 객체와 상호 작용할 때 런타임에 동적으로 구성될 수 있다. 이는 객체에 대한 구현이 계속해서 변화할 수 있다는 것을 의미한다. 또한 객체의 다형성으로 인해 유연해지는 장점이 있는 반면에 ORB 상에 있는 하나의 객체를 같은 인터페이스를 가진 다른 것으로 대체하는 것이 쉽다. 이와 같은 보안의 취약점들로부터 안전한 분산환경에서의 설계를 위해 CORBA 보안서비스가 제공하는 보안 특성들로는 사용자 인증, 사용자 권한 및 접근 제한, 객체간의 통신 보안, 부인봉쇄, 보안정보의 관리 등이 있으며, 이러한 보안 서비스들은 대칭키 혹은 비대칭키 암호와 같은 보안 메커니즘을 사용한다. 응용 객체는 ORB가 어떤 보안 메커니즘을 사용하였는가의 인터페이스에는 관여하지 않으며 CORBA 보안서비스는 분산 객체환경에서 메시지를 어떻게 보호할 것인가를 명세하고 방법들을 정의한다.



(그림 2) CORBA 보안 정책

(그림 2)에서 보듯 클라이언트는 인증 된 사용자 ID로 인증을 거쳐야 하고 모든 자원은 접근 통제 리스트에 의해서 보호되어야만 한다. 또한 감리 증적이 제공되어야만 하고, 접근 권한이 동일 아이템을 재 사용하는 다른 사용자에게 전달되지 않아야만 한다. 이는 ORB가 분산 객체를 위하여 제공하는 최상위 수준이며 ORB공급업체가 필요로 할 경우 더 낮은 보안 수준의 시스템 제공이 허용된다[5].

CORBA는 구조적 모델과 객체 모델을 기반으로 보안 구조를 제시하고, ORB에서 반드시 보안기능을 거치도록 하였으며 객체 단위로 교체가 가능토록 하여 외부 기능을 유연성 있게 활용할 수 있도록 하였다. 안전한 분산객체 모델을 설계하기 위해 모든 객체 호출에 대한 접근제어는 안전한 연계설정 정책 정보 등을 제공하는 보안 서비스에 의해 중재되며, 대부분의 응용 객체들은 보안 정책이 어떻게 적용되는가를 인식하지 않고도 하부에서 자동적으로 제공되는 보안서비스에 의해 안전하게 호출되도록 한다[6].

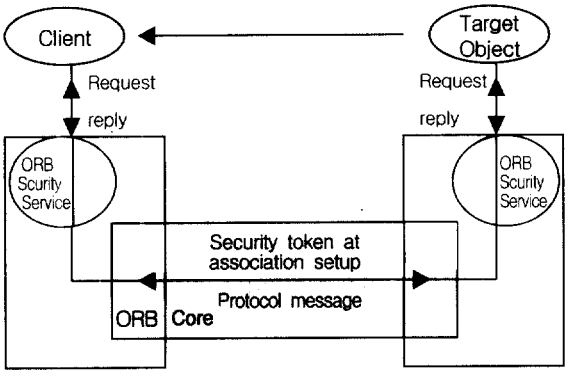
2.3 CORBA보안 서비스의 상호운용성

하나의 벤더에서 만든 동일한 ORB를 사용하는 두 객체간의 상호운용성은 보장된다. 그러나 한 ORB 벤더가 모든 컴퓨터의 다른 플랫폼에 동일한 ORB를 제공할 수 없을 뿐 아니라 그렇다 하더라도 모든 컴퓨터에 동일한 ORB가 설치될 가능성은 없다. 따라서 다른 ORB간에 상호운용성의 확장이

요구된다[7, 8].

IIOP(Inter-ORB Protocol)의 강점들 중 하나는 여러 공급업체 ORB간에 외부 영역 상호운용성을 제공한다는 것이다. 보안 측면에서의 IIOP 상호운용성은 메시지 암호화, 공개키, 비밀키, 특권 위임의 수준을 포함하며 기반 보안 메커니즘을 강제화 하는 프로파일의 집합을 통해 이루어진다[9]. 여러 ORB간에 보안공통 보안 기술들을 따를 수 있는 보안 서비스 상호운용의 기술들은 CORBA2에서 명세된 IOR(InterOperable Object Reference)을 이용하여 타겟 객체에 대한 보안정책을 전달하는 방법과 클라이언트와 타겟 객체간에 *"security association"*을 설정하여 지원하는 보안 상호운용성 프로토콜을 사용하는 방법, 그리고 DCE-CIOP 프로토콜을 이용하는 방법이 있다.

이중 클라이언트와 타겟 객체간에 보안연합을 설정하여 메시지를 보호하는 보안 상호운용성 인터페이스 구조에 대하여 살펴보겠다.



(그림 3) CORBA 보안서비스 상호운용성 모델

(그림 3)에서 ORB는 서비스 상호운용성 프로토콜을 공유하며, 같은 보안 메커니즘을 사용하여 클라이언트와 타겟 객체에게 지속적인 보안 정책을 지원한다. 타겟 객체가 객체 참조를 등록하면 안전하게 메시지를 송수신 할 수 있도록 보안정보를 포함한다. 이때 *"security association"*이 설정되어 있지 않으면 *"security token"*을 전송함으로서 설정이 가능하다[10]. 이와 같은 상호운용성 모델을 기반으로 하여, 차세대 인터넷에서 이용 가능한 CORBA 보안서비스 모델에 대해서 살펴보도록 하겠다.

2.4 차세대 인터넷에서 CORBA 보안 서비스

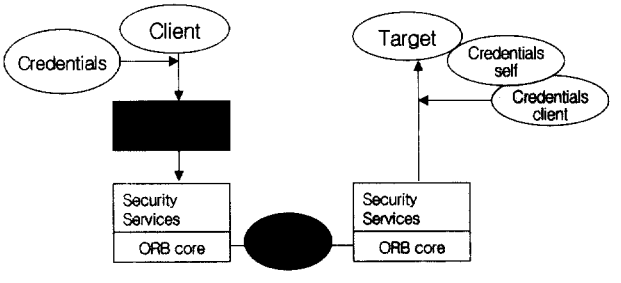
CORBA 보안 서비스 명세는 응용 프로그램 개발, 보안 관리, 보안 서비스 자체의 구현 등에 대한 보안 모델이나 인터페이스 등을 포함하기 때문에 보안 자체의 성질인 복잡성을 크게 감소시켜 준다. CORBA 보안 서비스는 다음의 인터페이스를 제공한다[12].

- 중간 개체에 대한 인증의 위임을 포함한 인증서의 발행이나 이에 대한 인증
- 객체들 사이의 안전한 거래를 수행
- 다음 이벤트에 대한 안전한 거래를 감사
- 거래의 증거물을 생성하고 이전의 행위를 부인하는 것으로부터 막기 위한 부인봉쇄 퍼실리티

이러한 모든 인터페이스는 독립적인 구현으로 명세되어 있으므로 보안 서비스의 인터페이스는 특정 인증 프로토콜의 사용에 독립적이다[13].

CORBA 보안 서비스 명세에 사용되는 모델은 인증 객체를 사용해 인증된 주체를 포함하며, 일단 인증되면 인증 받은 신분과 접근 권한에 대한 정보를 가지고 있는 인증서 객체를 가지고 서로 협상한다. 이러한 인증서 들은 부인봉쇄 모드에서 행해지거나 감사되는 행위에 대해 자신들의 신분을 등록하기 위한, 당사자들의 접근 권한을 검증하기 위한 안전한 거래에 사용된다.

클라이언트는 로컬 참조 값을 통해 원격 객체에게 요청한다. 클라이언트의 인증서는 이때 ORB에 명세된 보안 서비스에 의해 요청에 붙여지며 사용되는 전송 메커니즘을 통해 서버객체에게 전달된다. 원격객체는 자신의 ORB를 통해 클라이언트가 보낸 인증서와 함께 요청을 수신한다. 이때 서버 객체인 타겟 객체는 클라이언트가 인증서의 주인인지 아닌지를 확인하며 요청이 원격 객체로부터 수신이 되었을 경우 요청된 리소스의 접근에 대한 권한이 접근 결정 객체를 통해 검사되어 진다. 다음은 인터넷에서 CORBA 보안 서비스를 통해 인증 되어지는 절차를 나타낸 그림이다.



(그림 4) 차세대 인터넷에서 CORBA 보안 서비스 모델

3. 관련 연구

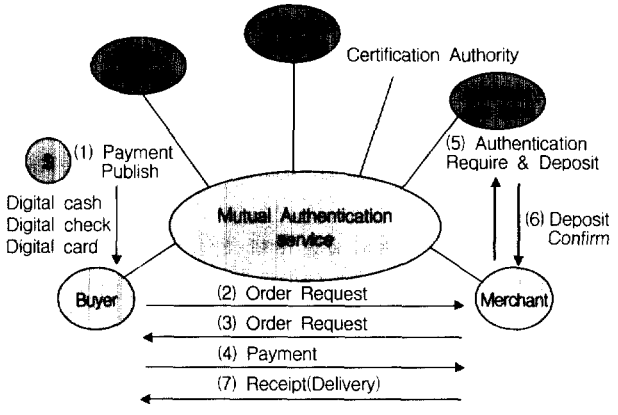
3.1 커버로스기법을 이용한 CORBA 기반의 상호인증

CORBA보안 명세를 기반으로 전자상거래 참여자들에 대한 객체 단위 인증 및 권한부여 기법을 제공하는 상호인증 서비스 구조를 제안하였다. 커버로스의 인증기법 및 인증 키 교환 기법으로 전자상거래 참여자간에 상대 주체의 신원 확인 뿐 아니라 거래 진행 중 취득한 정보의 근원을 파악할 수 있도록 하였다. 또한 커버로스 기법을 CORBA플랫폼 기반의 상호 인증 구조로서 분산 환경에 대해 확장하였다[6].

3.1.2 커버로스 기반의 상호 인증모델

(그림 5)은 커버로스 기반의 상호 인증을 나타내기 위해

상인과 소비자인 전자상거래 상의 두 개체간에 일반적인 모델을 나타내고 있다. 이 모델은 데이터의 전송과 교환에 기반한 시퀀스이며 실제로 수행되는 행동도 데이터의 전송과 교환이다. 전송과정에서 한 쪽이 다른 한 쪽에게 비즈니스 아이템을 전달한다. 이때 비즈니스 아이템은 암호화된 서류나 증명서 혹은 크레디트 카드 등의 돈이 될 수 있다. 또한 먼저 보내는 측에서는 비밀성, 익명성, 부인봉쇄 등의 보안 요구사항 들을 정의할 수 있게 된다.



(그림 5) CORBA기반의 전자상거래 주체간 상호 인증 서비스

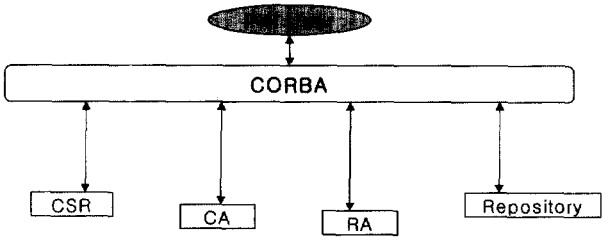
CORBA 보안 서비스가 제공하는 인터페이스로는 증명서를 발행하고 인증하며 객체들 사이에 안전한 거래를 수행하고 안전한 거래인가를 감사하는 것이다. 또한 거래의 증거를 생성하여 부인봉쇄 기능을 제공하여 이후에 부인을 하지 못하게 하는 역할도 한다.

3.2 PKI를 이용한 CORBA기반의 인증

OMG에 정의된 CORBA기반의 PKI(Public Key Infrastructure) 모델을 각각의 CORBA모델에 도입하여 신분에 대한 인증서 발급을 원하는 클라이언트에게 인증서를 발급해 주는 인증국의 형태를 도입하였으나, 서로 다른 분야 인증국과의 상호인증 등은 제공하지 못하고있다.

3.2.1 PKI를 이용한 CORBA기반의 인증모델

(그림 6)은 CORBA객체를 통해 PKI와 상호 작용하는 구조의 주요 인터페이스를 보여주고 있다. 기존에 정의된 명세에 기반하여 구현된 모든 시스템의 컴포넌트를 수용하는 모델이지만 여기에 제한된 것은 아니다.



(그림 6) PKI를 이용한 CORBA기반의 인증모델

PKI user는 인증서 발급을 원하는 클라이언트와 인증서를 검증하는 서버 모두를 뜻하며 클라이언트는 ORB를 통해 CA에게 인증서 발급을 신청한다. CA는 클라이언트의 신분을 확인하기 위하여 도전/응답 방식을 이용한다. 신분확인이 끝나면 인증서를 발급하고 저장소에 저장한다. 이와 같은 모델은 자체 인증국을 두어 PKI user들이 인증서 발급 및 확인 등을 할 수 있지만 상호인증의 기능이 없고 단지 미리 등록되어 인증가능한 클라이언트에게 인증서를 발급해 주는 정도의 간단한 인증만을 제공한다[16]. 이러한 단점을 극복하기 위하여 PKI를 이용한 CORBA기반의 인증모델을 상호인증으로 확대하고 유연한 인터페이스를 제공하기 위하여 CCCA(Cross Certification CA)를 도입하여 새로운 모델을 설계하고 인터페이스를 정의한다.

4. CCCA를 이용한 CORBA 기반의 상호인증

4.1 CCCA를 이용한 CORBA 기반의 상호인증 모델

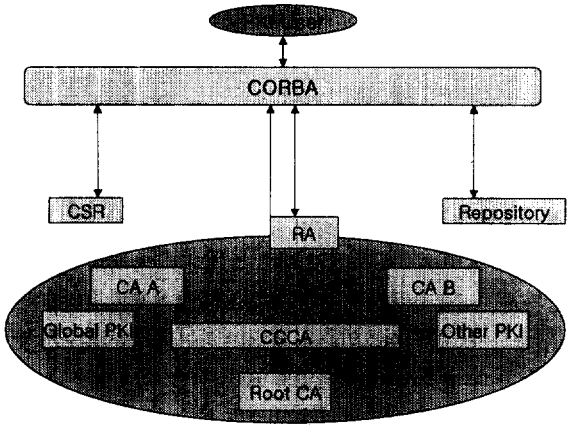
CORBA 기반의 CCCA(Cross Certification CA)를 이용한 상호인증 모델은 국내에 맞게 설계된 공개키 기반 구조로서 산업, 행정, 금융, 학계 등 여러 방면에서 공개키 기반구조를 이용하여 인증 과정을 거친다. 급속도로 발전하는 공개키 기반구조에 능동적으로 대처하기 위해서는 이러한 환경에서 확장성과 상호 운용성, 관리용이성, 타 공개키 기반구조 기관의 수용 등 여러 가지 문제를 고려한 모델이 제시되어야 한다[17]. 다음은 CORBA 기반의 CCCA를 이용한 상호인증 모델이다.

(그림 7)은 CORBA 객체를 통해 PKI와 상호 작용하는 구조도를 보인 것이다. 위의 그림에서 주목해야 할 부분은 CCCA를 이용해서 CA A과 CA B가 상호 인증하고 있다는 사실이며 여기에서 CA A과 CA B는 서로 다른 분야의 인증기관이 될 수 있다.

- PKI User : PKI를 이용하는 응용프로그램이나 사용자를 말함.
- Certificate : CA와 같이 신뢰받은 기관으로부터 서명 받은 디지털 문서로서 공개키 쌍에 대한 정보를 바인드한다.
- CRL(Certificate Revocation List) : CA에 의해 서명 받은 디지털 문서이며 CA에 의해 이전에 발행된 인증서가 포함된 리스트이다.
- Root CA : 최상위 인증기관으로 각분야 CA의 1차적인 인증을 수행한다. 인증 정책을 각 하위기관에 적용하고 감독한다. 또한, 외국 공개키 기반구조에 관한 접속과 정책의 상이성을 완충하는 역할을 수행한다.
- CCCA(Cross Certification CA) : 상호인증에 관련된 업무를 전담하게 된다. 분야 CA 수준의 상호인증을 수행하여 사용자의 실제 처리되는 업무의 양을 줄이며, 상호인증을 전담하여 상호인증의 안정성을 높인다. 또한 외국 공개키 기반구조의 다리 역할을 수행한다.
- CSR(Certificate Status Responder) : CRL을 사용하지 않고

인증서의 상태를 결정하기 위해 제공되는 서비스이다. CRL은 정기적으로 발행되며 이 기간 중에 어떤 취소는 CRL의 다음 발행때 까지 알려지지 않으므로 특정 인증서의 유효성을 확인하고 상태 정보를 얻는데 있어 가장 시간적으로 적절한 서비스이다.

- CA(Certificate Authority) : CA는 공개키 증명서 관리와 발행과 관련된 기능을 수행한다. 인증서에 관한 요청을 받고 검증하고 인증서와 CRL을 발행한다. 또한 인증서 상태 정보에 대한 요청을 서비스하고 키 관리도 함께 병행한다. (그림 7)에서 CA A와 CA B는 상호인증을 원하는 두 클라이언트에게 인증을 발행할 인증국을 의미한다.
- RA(Registration Authority) : CA 대신해서 클라이언트로부터 인증서에 대한 요청을 받고 공개키 쌍과 인증 받을 애트리뷰트 사이의 바인딩을 검증한다. 인증서에 대한 요청이 클라이언트로부터 들어왔을 때 비밀키의 소유 여부를 확인한 후 CCCA에게 상호인증을 요청한다.



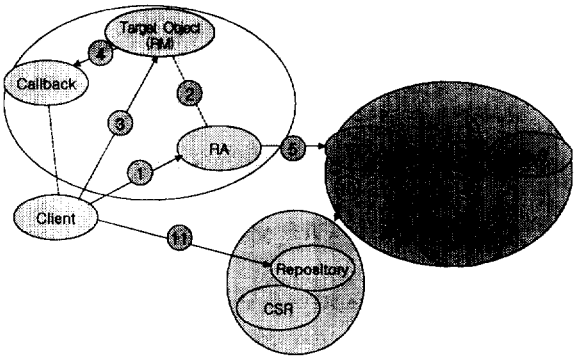
(그림 7) CCCA를 이용한 CORBA기반의 상호인증 구조도

4.2 상호 인증 모델을 위한 기본 요구사항

CORBA 환경에서 상호 인증을 제공하기 위해서는 참여하게 될 인증국의 수, 상호 인증을 위한 인증기관들간의 협약, 협약에 대한 조건, 국제 상호 인증, 인증기관들에 대한 제약조건, 인증서/인증서 취소목록(CRL) 형식, 인증 프로토콜, 동일 프로토콜에 있어서의 상호 인증, 다른 프로토콜에 있어서의 상호 인증, 인증 정책, 암호알고리즘 등에 대한 협약이다. 이와 같은 CORBA기반의 상호 인증을 제공하기 위해서 인증서 요구, 분배, 폐기, CRL 유지 등을 수행하기 위하여 인터페이스를 제공하여야 한다. 또한 저장소로부터 CRL을 꺼내오거나 인증 상태를 질의하기 위한 저장소와의 인터페이스를 정의하여야 하며 특정 인증서가 취소되었을 때 알림 기능을 하는 메커니즘 등을 제공하여야 하며 이러한 기능은 CORBA의 notification 서비스를 이용한다. 또한 키를 업데이트하고 관리하는데 필요한 인터페이스도 제공하여야 하며 이 또한 CORBA 보안서비스를 이용한다. 개체 사이의 정보 전송을 위해 CORBA 보안 서비스를 이용하며, 새로운 인증서, CRL, 키가 생성되었음을 알리기 위해 notification 서비스를 이용한다.

4.3 CCCA를 이용한 CORBA 기반의 상호인증 메커니즘

(그림 8)은 CCCA를 이용한 CORBA 기반의 상호인증 메커니즘에 대한 상세 구조도이다. 각각의 구성 요소들은 (그림 7)에서 설명한 바와 같으며 숫자는 행해지는 순서를 말한다.



RM : Request Manager

(그림 8) CCCA를 이용한 CORBA기반의 상호인증 메커니즘

1) 클라이언트가 RA에게 인증서 요청 오퍼레이션을 전달한다. RA는 클라이언트가 비밀키의 소유자인지 POP(Proof Of Possession)을 검증한다. 이것은 도전/응답의 형식을 갖는데 RA가 암호화된 메시지를 클라이언트에게 주면 클라이언트는 이것을 비밀키로 풀어서 반환한다.
2) RA는 클라이언트의 오퍼레이션의 결과로 Request manager 객체를 생성하고 참조 값을 클라이언트의 요청에 대한 응답으로 반환한다.
3) 클라이언트는 결과를 알아보기 위해 폴링(polling)을 사용한다.
4) 클라이언트는 콜백을 사용해서 타겟에 의해 호출되는 notify 오퍼레이션을 기다린다.
5) RA는 클라이언트의 요청에 따라 CCCA가 CA A와 CA B가 상호인증하여 인증서를 발행할 수 있도록 해당 CCCA에게 요청을 전달한다.
6) CCCA가 CA B에게 응답을 개시할 수 있는 응답개시요구코드 생성요청을 한다. CA B는 인증을 개시 할 수 있도록 인증개시 코드를 생성하여 CCCA에게 인터네트워크 이외의 구별수단(out-of-band)으로의 값과 요구 랜덤 값을 생성하여 함께 반환한다.
7) CCCA는 인증개시 코드를 CA A에게 전달한다. 요구 CA인 CA A는 온라인 순서의 개시를 기동하고 인증 개시코드에 기초하여 대칭키를 생성하고 생성된 키에 의해 온라인으로 전송되는 모든 메시지 인증코드(MAC : Message Authentication Code)을 생성한다. 또한 요구 랜덤 값을 생성하여 CCCA에게 반환한다.
8) CCCA는 CA의 프로토콜 버전을 확인 후 요구 랜덤 값을 보존 후 상호 인증 요구(CrossReq)를 응답 CA인 CA

B에게 전달하고 CA B는 응답 랜덤 값을 생성 후 반환 값으로 CCCA에게 전송한다.

9) CCCA는 CA A의 공개키를 포함하기 위해 CA A의 서명 비밀키로 서명한 새로운 요구 CA 인증서를 생성하고 요구 CA 인증서를 상호 인증 응답 CrossRep로 전송한다. CA A는 응답 랜덤 값을 체크한 후 불리언 값을 반환한다.
10) CCCA는 CA A에 대한 인증서와 CA B에 대한 인증서를 저장소에 저장하고 공개키 확인(PKI Confirm)을 CA A와 CA B에게 전송한다.
11) 클라이언트는 인증 정보를 얻기 위해 저장소와 CSR (certificateStatus Responder)에 접근한다.

4.4 CORBA 기반의 CCCA를 이용한 상호인증 메커니즘의 모듈 설계

IDL은 PKI, PKI 인증과 PKI 저장소 등의 3개의 Module로 구성되며 각각의 인터페이스는 아래와 같다.

```
Module PKI {
    type def;
}
Module PKIAuthority {
    Interface RegistrationAuthority_CAB;
    Interface CertificateAuthority_CAA;
    Interface RequestManager;
    Interface RequestCertificateManager;
    Interface RequestRevocationManager;
    Interface RequestKeyUpdateManager;
    Interface RequestKeyRecoveryManager;
    Interface CertificateCallback;
    Interface RevocationCallback;
    Interface KeyUpdateCallback;
    Interface KeyRecoveryCallback;
}
Module PKIRepository {
    Interface Repository;
}
```

PKI 모듈은 다른 모듈에 의해 사용되는 모든 타입을 정의하며 PKIAuthority는 인증서 관리를 담당하는 CA와 상호인증을 담당하는 CCCA사이의 인터페이스를 담당한다. PKI Repository는 CRL과 인증서를 저장하거나 꺼내오기 위한 인터페이스를 제공한다.

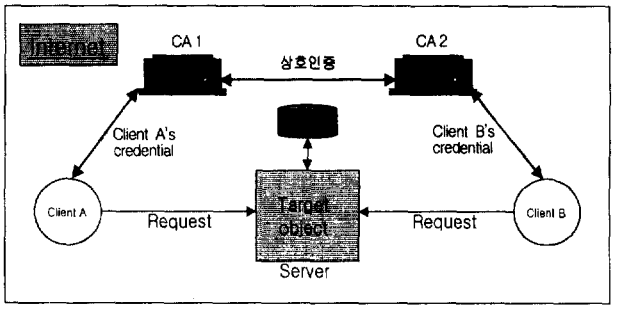
4.5 CORBA 기반의 CCCA를 이용한 상호인증 메커니즘의 특징

기존의 CORBA기반의 PKI를 이용한 인증은 클라이언트의 신분을 확인하고 인증서를 발급해주는 단순한 방식이었다. 그러나 제안하는 모델에서는 서로 다른 분야의 CA가 기존의 공개키 기반구조를 흡수하는 구조로서, CCCA를 이용해 상호 인증하는 방법을 채택하고 있다. 이때 CCCA는 논리적으로 분리된 하나의 독립된 요소로서 존재하여야 한다. CCCA의 안전성에 문제가 있다면 상호인증 업무는 루트 CA에게 전가하거나 일시 업무를 중단하여야 한다. 루트 CA와 논리적 물리적으로 같은 위치에 놓인다면 두 요소의 안전성에 문제가 발생하였을 때, 인증 서비스는 일시에 마비되게 된다. 따라서 CCCA는 여러 요소와 마찬가지로 분리하여 업무를 수행하고 각각의 요소마다 안전성의 문제를 각각 분리해 주어야 한다. 이러한 CCCA 상호인증 모델은 계층적 구조를 최대한 살리면서 상호인증 절차를 간소화하여 인증 경로를 대폭 줄일 수 있다. 또한 최상위 인증기관은 인증에 관련된 업무만 수행하게 되고 CCCA는 상호인증 업무만 맡게되어 효율적인 운영을 수행할 수 있다. 또한 계층적 구조로 인해 최상위 인증기관은 인증에 관련된 정책을 각 분야 CA와 CCCA에 전달함으로서 일관된 정책을 수행할 수 있고 각 분야를 쉽게 관리할 수 있는 관리 용이성이 증대된다. CCCA의 영역을 둠으로서 상호 인증의 절차를 단순화할 수 있으며 국내 타 공개키 기반구조 영역을 쉽게 수용 확장함으로서 각 부문의 특징을 그대로 살릴 수 있다. CORBA의 표준 서비스 중에서 개체간의 보안을 제공하기 위해 보안 서비스를 사용하고 클라이언트에게 알림을 위해 Notification 서비스를 사용한다.

5. 응용 분야

현재 제안된 CORBA의 인증 서비스를 이용하면 단지 인증된 내용을 확인하는 정도에 불과하다. 앞으로 차세대 인터넷에서 전자상거래 등을 하기 위해 미들웨어로 CORBA를 사용할 경우 공개키 기반구조와의 상호 연동이 필수적이라 할 수 있다. 전자 화폐와 전자 지불의 사용이 증대되는 차세대 인터넷 전자상거래 시장에서 물건을 사고 파는 전자상거래를 지원하는 CA가 금융분야 CA와 상호인증을 얻어야 하는 경우는 필수가 된다.

아래의 그림에서 클라이언트 A는 일반 소비자와 거래하는 상인일 수 있고 그렇다면 클라이언트 B는 은행이 될 수 있다. 이러한 클라이언트들이 CORBA 환경에서 상거래를 할 경우 서로 다른 영역에서 인증을 받아야 한다. Banker는 금융계의 인증을 받아야 하고 상인은 전자상거래 CA의 인증을 얻어야 한다. 이럴 경우 CCCA를 도입해 상호인증 모델을 도입한다면 효과적인 상호인증을 할 수 있다.



(그림 9) CCCA를 이용한 상호인증의 응용 모델

6. 기존연구와의 비교

이 장에서는 CORBA 기반의 메커니즘과 다른 미들웨어

의 특징을 비교하여 CORBA 기반의 제안 모델의 우수성을 입증한다. 이러한 모델에서 설계된 CCCA를 이용한 상호인증 모델과 앞서 소개한 기존연구들과 비교 분석한다.

6.1 다른 미들웨어와 비교한 CORBA 기반 메커니즘의 특징

가장 대표적인 미들웨어인 CORBA와 DCOM(Distributed Component Object Model)[15] 그리고 DCE(Distributed Computing Environment)[14]를 이미 정량화 된 평가 작업을 거쳐 발표된 특성을 기준으로, 여러 가지 기술적이고 전통적인 관점에서 비교하여 <표 1>로 구성하였다[6].

DCE는 미들웨어 부문에서 가장 뛰어난 기술을 보유하던 밴더의 소속이었으나 최근에는 CORBA와 DCOM이 강력한 경쟁상대로 떠오르게 되었다. 그러나 아직도 DCE는 많은 시스템과 플랫폼에 사용되는 미들웨어 중 하나이다. DCOM은 마이크로소프트사가 DCE와 CORBA에 대응하기 위해 내 놓은 미들웨어 기술이다. DCOM이 CORBA 보다 읽거나 생성하기에 좀 더 복잡하며 이것은 DCOM과 같은 미들웨어 기술이 널리 퍼지는데 걸림돌이 되고 있다. 위의 표에서 보여주듯이 CORBA는 비교대상인 DCE와 DCOM에 비해 훨씬 널리 우수성이 증명된 미들웨어 기술이라 할 수 있다[6].

〈표 1〉 미들웨어의 비교

비 교 항 목	DCE	DCOM	CORBA
프로그램의 용이성	△	X	O
상호운용성	O	△	O
마켓의 위치	X	O	O
네트웍의 투명성	O	X	O
개방성	△	X	O
플랫폼의 독립성	O	X	O
확장성	X	O	O
인터페이스와 구현의 독립	△	O	O
다중언어의 지원	△	O	O
다중 밴더에 대한 지원	O	X	O
기존 시스템에 대한 지원	O	X	O
서비스에 대한 지원	X	O	O

X : 전혀 지원되지 않음, △ : 부족함, O : 잘 지원됨

6.2 기존 모델과의 비교분석

현재 OMG에 정의되어 있는 PKI를 이용한 CORBA기반의 인증 모델과 이 논문에서 제안한 CCCA 상호인증 모델을 확장성, 관리 용이성, 인증경로길이, 상호인증 용이성, 처리 효율, 신뢰도 등의 기준으로 비교 평가하겠다[17].

〈표 2〉 CORBA 기반 인증모델의 비교

	일반적인 CORBA 기반의 인증 모델	CCCA를 이용한 CORBA 기반의 상호인증 모델
확장성	X	O
관리 용이성	O	△
인증경로 길이	△	△
상호인증 용이성	X	O
처리효율	△	O
신뢰도	△	△
복잡도	O	△

X : 전혀 지원되지 않음, △ : 부족함, O : 잘 지원됨

비교되는 일반적인 인증 모델에서는 확장성에 대한 고려가 전혀 없다. 단순한 인증 구조와 방식을 가지고 있으나 제안하는 모델에서는 타 인증기관이나 외국 인증 구조도 쉽게 흡수 및 통합이 가능하며 루트 CA와의 분담이 가능하다. 관리 용이성의 측면에서 제안하는 모델에서는 루트로부터 각각의 인증기관까지 정책 전달이 용이하며 외부의 기반 구조까지 적용할 수 있는 유연성을 갖는다. 또한 클라이언트에 속한 인증기관이 바로 CCCA를 거쳐 상호인증을 시행하므로 그 길이가 단축될 수 있고 상호인증을 전담하는 CCCA로 하부의 여러기관을 거치지 않고 직접 인증기관 대 인증기관의 상호인증이 용이하다. 각 구성요소마다 그 기능을 확실히 구분하여 업무를 분담하므로 처리효율 면에서도 우수하고 기본 계층구조를 살리면서 상호인증 구조를 별도의 기관으로 정의하여 각 기관의 신뢰도를 증가시킨다. 상호인증 절차를 간단히 하기 위하여 CCCA를 도입하였으나 기존의 일반적인 인증모델에 비하면 상호인증을 위한 부분의 패스가 추가되므로 복잡도의 측면에서는 약간의 단점을 가진다.

7. 결 론

CORBA에서 CA를 이용한 인증이라 하면 인증서를 발행하는 기관으로부터 인증국의 디지털 서명이 들어있는 인증서를 받는 것이 전부였다. 그러나 전자상거래 등이 활발해지는 차세대 인터넷에서 CORBA기반의 인증을 하고자 한다면 그것으로는 턱없이 부족하다. 즉 현재의 모든 분야에 있는 인증국과 상호 거래가 가능하여야 하며 이는 인증국 간의 신뢰도 포함된다. 이러한 요구조건들이 CORBA 기반이라는 제약 아래 부실하게 보완되어 있었다. 그러나 CCCA를 이용한 CORBA 기반의 PKI인증 모델은 이러한 문제점을 해결할 뿐만 아니라 앞으로 차세대 인터넷에서의 모든 거래에 대한 인증을 실행할 수 있게 된다. 즉 클라이언트는 인터넷을 통해 CORBA 기반의 서버를 통해 상거래 등을 할 경우 단 한번의 호출로 상대 CA와 상호인증을 통한 인증서를 받게 된다. 만일 CCCA의 안전성에 문제가 있다면 상호인증 업무는 루트 CA에게 전가하거나 일시 업무를 중단하여야 한다. 루트 CA와 논리적 물리적으로 같은 위치에 놓인다면 두 요소의 안전성에 문제가 발생할 경우 일시에 인증 서비스는 마비되게 된다. 따라서 CCCA는 여러 요소와 마찬가지로 분리하여 업무를 수행하고 각각의 요소마다 안전성의 문제를 각각 분리해 주어야 한다.

이 논문에서 설계한 모델은 계층적 구조를 최대한 살리면서 상호인증 절차를 간소화하여 인증 경로를 대폭 줄일 수 있다. 또한 최상위인증기관은 인증에 관련된 업무만 수행하게 되고 CCCA는 상호인증 업무만 맡게되어 효율적인 운영을 수행할 수 있다. 또한 계층적 구조로 인해 최상위 인증기관은 인증에 관련된 정책을 각 분야 CA와 CCCA에 전달함으로서 일관된 정책을 수행할 수 있고 각 분야를 쉽게 관리할 수

있는 관리 용이성이 증대된다. CCCA의 영역을 둠으로서 상호 인증의 절차를 단순화할 수 있으며 국내 타 공개키 기반구조 영역을 쉽게 수용 확장함으로서 각 부문의 특징을 그대로 살릴 수 있다. 또한 타 인증기관이나 외국 인증 구조도 쉽게 흡수 및 통합이 가능하며 루트 CA와의 분담이 가능하다. 관리 용이성의 측면에서 제안하는 모델은 루트로부터 각각의 인증기관까지 정책 전달이 용이하며 외부의 기반 구조까지 적용할 수 있는 유연성을 갖는다. 또한 클라이언트에 속한 인증기관이 바로 CCCA를 거쳐 상호인증을 시행하므로 그 길이가 단축될 수 있고 상호인증을 전담하는 CCCA로 하부의 여러기관을 거치지 않고 직접 인증기관 대 인증기관의 상호인증이 용이하다. 각 구성요소마다 그 기능을 확실히 구분하여 업무를 분담하므로 처리효율 면에서도 우수하고 기본 계층구조를 살리면서 상호인증 구조를 별도의 기관으로 정의하여 각 기관의 신뢰도를 증가시킨다. 이러한 모델을 실제 환경에 이용하기 위해서는 인터넷에 흡수된 PKI 환경이 필수적이다.

향후에는 다중 CA간의 다중 인증 프로토콜도 연구되어야 하며 이를 위해 새로운 개념이 도입되어야 한다. 또한 CCCA에 문제가 생긴 경우 발생할 수 있는 기능을 분담하지 않고도 해결 할 수 있는 고장감래의 기능도 필요하다. 이러한 구조가 인터넷 기반의 전자상거래 환경에 흡수되기 위해서는 대책마련이 필요하다.

참 고 문 헌

[1] 나중찬, 김영균, 김경범, 김명준, "CORBA 기반의 보안 플랫폼과 그 응용", 정보처리논문지, Vol.6, No.11S, pp.3278-3288, Nov, 1999.

[2] 박양수, 김현규, 이명준, 한상영, "CORBA 개방형 분산 환경을 위한 공유 객체 명세 언어 시스템", 정보처리논문지, Vol.5, No.2, pp.404-414, 1998.

[3] 김남용, 왕창종, "CORBA 기반 시스템 통합 모델", 정보처리논문지, Vol.5, No.1, pp.63-72, 1998.

[4] 신영미, 홍원기, "분산 멀티미디어 협동 작업 환경을 위한 CORBA 기반의 보안성 있는 세션 서비스", Vol.26, No.6, pp.670-682, JUNE, 1999.

[5] Robert Orfali, Dan Harkey, 클라이언트/server programming with Java and CORBA, pp.3-181, 1998.

[6] 장경아, 김태윤, "전자상거래 주체간 CORBA기반 상호 인증 서비스", Vol.26, No.10, 정보과학회논문지, pp.1237-1247 OCT, 1999.

[7] 금영욱, 윤민영, "CORBA-분산 객체 통합 기술", 한국정보과학회 소프트웨어공학회지, 제12권 제2호, pp.5-14, 1999.

[8] 신경민, 김명희, 주수종, "CORBA기반 실시간 응용 서비스 지원 객체그룹 플랫폼 설계", 한국정보과학회 추계학술발표대회, 제25권 제2호, pp.193-195, 1998.

[9] Object Management Group, CORBA 2.2/IIOP Specification, OMG, 1998.

[10] Object management Group, CORBA service : Common Object Security Specification, pp.15-1~15-382, 1997.

[11] OMG Security Working Group, "OMG White Paper on Security," OMG Doc. No.94.4.16, April, 1994.

[12] IONA Technologies, OrbixSecurity White Paper, December, 1998.

[13] Andreas Vogel, Keith Duddy, java Programming with CORBA, 2nd Ed, John Wiley & Sons, 1998.

[14] mannix, Frank, OSF/DCE : Introducrion to Open Software Foundations Distributed Computing Environment, Digital service, 1992.

[15] Mark Roy, Alan Ewald, Inside DCOM, DBMS Magazine, April 1997.

[16] 김지연, KISA Report, 한국정보보호센터, Aug, 1999.

[17] 이제호, "PKI를 이용한 효율적인 연동 메커니즘", 충북대학교 석사학위 논문지, Feb, 2000.

[18] 이상영 "전자서명 상호인증", 한국정보보호센터 월간리포트, July, 2000.

이 용 주

e-mail : silvia@etri.re.kr

1999년 청주대학교 정보통신공학과 졸업(학사)

2001년 충북대학교 전산학과 졸업(석사)

2001년~현재 한국전자통신연구원 네트워크 기술연구소 연구원

관심분야 : Network, Middle-ware

장 종 현

e-mail : jangjh@etri.re.kr

1988년 경북대학교 전자공학과(공학사)

2000년 충남대학교 전자공학과(공학석사)

현재 한국외국어대학교 전자공학과 박사과정

1988년~1994년 대우통신㈜ 종합연구소

1994년~현재 한국전자통신연구원 네트워크 기술연구소 선임연구원

관심분야 : 네트워크 보안, 이동통신, 미들웨어 등

이 동 길

e-mail : dglee@etri.re.kr

1983년 경북대학교 전자공학과(공학사)

1985년 한국과학기술원 전산학석사

1994년 한국과학기술원 전산학박사

1985년~현재 한국전자통신연구원 네트워크 기술연구소 책임연구원

관심분야 : 컴파일러 구성론, 프로그래밍 언어론, 미들웨어 등