Grid 환경에서 엔티티 인증과 권한부여에 관한 연구

국 중 옥[†] · 이 재 광[††]

요 약

기존의 그리드 사용자 인가 시스템은 해당 로컬 시스템에 접근하는 사용자가 많아지게 되고, 사용자 프록시 인증서의 subject DN(Distinguished Name)과 로컬 시스템의 ID를 일대일로 매핑할 경우, 계정 관리 문제와 메모리 자원, 디스크 자원의 관리에 있어 많은 어려움을 겪게 된다. 이러한 문제를 기존의 그리드에서는 여러 subject DN이 하나의 로컬 ID를 공유하는 형태로서 해결하고자 하고 있다. 하나의 로컬 ID를 공유할 경우에 발생하는 문제는 수많은 그리드 사용자의 모든 요구사항을 적용하는데 있어 더 많은 불편함을 초래하게 된다. 이에 본 논문에서는 ID 기반이 아닌 인증서 기반의 사용자 인가 시스템을 제안하였다. 앞서 설명한 기존의 ID 매핑 방식의 인가 시스템 대신에 인증서내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 하였다.

A Study on Authentication and Authorization on Entity in Grid

Joung-Ook Kug[†] · Jae-Kwang Lee[††]

ABSTRACT

When an existing user authorization systems in Grid access many user to local system and subject DN (Distinguished Name) in a user-proxy authenticate and ID in local system is one-to-one mapping, they have difficulties in ID management, memory resource management and resource management. At this, a variety of subject DN is shared of one local ID in an existing Grid. But this faces many difficulties in applying all requirements for many Grid users. Thus, we suppose user authorization system based on a certificate not them based on ID in this paper. That is, we add user's access level to extension field in a certificate, and make a supposed authorization system decide access limitation level on resources instead of an existing ID mapping methods.

키워드 : 그리드(Grid), 클라이언트 CA(Client Certificate Authority), 인증 서비스(Authentication Service), 인가 서비스(Authorization Service)

1. 서 론

그리드(Grid)는 네트워크로 연결된 가상의 슈퍼컴퓨터로 현재의 협업 업무부터, 컴퓨터를 이용한 정밀 실험, 원격 데이터세트의 검색, 원격 소프트웨어의 사용, 데이터 중심의 컴퓨팅, 대형 시뮬레이션 등의 연구에 사용될 수 있을 것으로 기대되고 있으며, 이미 많은 프로젝트가 시작된 상태다. 그리드는 각 자원이 지역적으로 떨어져 있기 때문에 이를 활용할 수 있도록 각 엔티티를 인증하는 것과 각 그룹의 활발한 커뮤니케이션 보호 등의 보안 서비스가 필요한데 이와 같은 서비스를 그리드 미들웨어를 통해서 제공하고 있다[1].

현재 그리드 보안 서비스를 제공하기 위해서 다양한 버전의 미들웨어가 개발되었지만, 컴퓨팅 자원에 대한 인증 서비스를 제공하기 위해서 X.509 기반의 인증서를 적극적으로 활용하고 있는 글로버스(Globus)가 가장 대표적이다. 글로버스에서는 엔티티에 대한 인증 및 인가 서비스를 인증서를 통해 제공하고 있기 때문에 기존 시스템의 큰 변경 없이 손쉽고 효율적으로 인증 서비스를 제공할 수 있지만, 현재까지 글로버스에서 제공하고 있는 인증서를 통한 엔티티 인증 및 인가 서비스는 각각의 엔티티에 대한 인증만을 제공하고 있을 뿐, 인증된 주체에 대하여 서로 다른 권한을 부여하는 것에 대한 연구가 미흡한 실정이며, 발행된 인증서를 엔티티 측면에서 효율적으로 관리하고, 활용할 수 있는 관리 클라이언트에 대한 연구가 전무한 실정이다.

본 논문에서는 표준문서[2-4]를 바탕으로 그리드에서 요구하고 있는 엔티티 인증 및 인가에 대한 요구사항과 메커니즘을 분석하고, 글로버스에서 적용하고 있는 ID 기반이 아닌 인증서 기반의 사용자 인가 시스템을 제안하였다.

앞서 설명한 기존의 ID 매핑 방식의 인가 시스템 대신에 인증서내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 하였다. 또한, 인증서를 효율적으로 관리할 수 있는 그리드 CA 클라이언트에 대해서 연구하였다.

2. 관련 연구

그리드는 지리학적으로 분산되어 있는 고성능 컴퓨팅 자

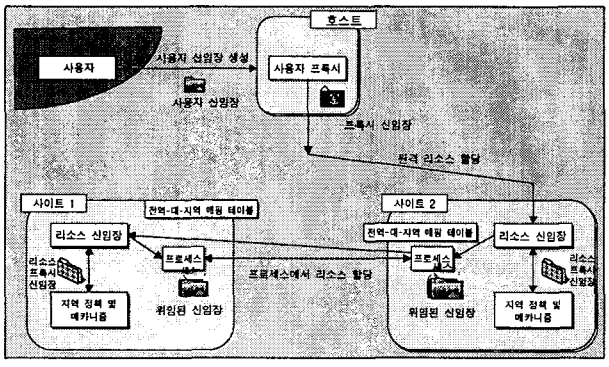
† 종신회원 : 한남대학교 대학원 컴퓨터공학과
†† 종신회원 : 한남대학교 컴퓨터공학과 교수
논문접수 : 2003년 3월 5일, 심사완료 : 2003년 4월 18일

원을 네트워크로 상호 연동하여 조직과 지역에 관계없이 슈퍼컴퓨터처럼 사용할 수 있는 환경을 말한다. 그리드라는 용어는 1990년대 중반 미국의 슈퍼 컴퓨팅 센터를 중심으로 고성능의 분산 컴퓨팅 인프라를 구축하는데서 비롯되었으며, 고성능 자원, 대용량 정보 및 혁신적인 애플리케이션에 초점이 맞추어진 것이 일반적인 분산 컴퓨팅과 구별된다[5].

그리드를 구축하는데 있어서 가장 중요한 미들웨어(Middleware)는 그리드 응용 서비스와 이를 위한 네트워킹 서비스를 제공하기 위한 컴포넌트들로 구성되며, 대표적인 서비스 기능으로는 보안 기능, 자원관리 기능, 자원할당 기능, 통신 기능 등이 있다. 또한, 그리드는 다양한 형태의 애플리케이션과 프로그래밍 패러다임을 지원하며, 사용자가 원하는 서비스를 쉽게 지원 받을 수 있도록 툴(Tool) 서비스 형태로 지원한다[6].

2.1 그리드 보안 기반구조(GSI : Grid Security Infrastructure)

그리드의 발전은 분산 시스템 보안에 많은 영향을 주었다. 전통적인 분산 시스템에서 보안 메커니즘의 초점은 사용자로부터 시스템을 보호하는 것이었다. 그리드 애플리케이션에서도 시스템의 보호가 여전히 중요한 부분으로 남아있지만, 그리드는 애플리케이션과 계산에 사용될 사용자의 데이터를 보호하기 위한 특수한 요구사항을 가지고 있으며, 실행 코드가 네트워크 상의 여러 곳에서 시작될 수 있기 때문에, 악의적인 코드가 실행될 수 있는 잠재성, 출처를 검증하기 위한 강력한 방법의 요구, 코드의 인증과 그것의 실행확인 수단이 요구된다. 또한, 그리드 자원들이 서로 다른 기관에 의해 관리되기 때문에, 각 기관의 보안 요구사항과 보안정책의 충돌 가능성을 가지고 있다. 이러한 이유로 그리드 환경에서의 보안 관리는 많은 어려움을 주고 있다[7].



(그림 1) 그리드 보안 기반구조에서 사용자 인증 기본 동작

이와 같은 문제점을 해결하기 위해서 그리드 보안에 관하여 연구하는 워킹그룹에서는 GSI 솔루션에 대해 논의하고 이에 대한 표준화 과정을 진행하고 있다. GSI 솔루션은 가능한 현존하는 표준들의 개정을 통하여, 앞에서 설명한 사용자 인증과 통신 보안 요구사항을 만족하도록 조합되고 개발되며, 그리드 환경의 구성원 사이트들의 서로 다른 지역 보안 솔루션들 간의 차이를 연결해 주는 도메인 상호 보안 프로토콜을 제공한다[8]. (그림 1)은 그리드 보안 기반 구조에서 사용자를 인증하기 위한 기본 동작에 대한 시나리오를 보여주고 있다.

2.2 그리드 환경에서 필요한 인증

2.2.1 단일 인증(Single Sign On)

그리드 사용자는 각 지역의 그리드 자원에 접근하여 활용하기 위해서 단 한번만 "로그인(Log In)"한다. 로그인 후에는 어떠한 그리드 자원에 접근하더라도 추가적인 인증을 받기 위해서 다시 로그인 하는 경우가 없어야 한다.

2.2.2 위임(Delegation)

사용자는 그리드 자원을 활용하기 위해서 획득한 권한을 사용자가 실행하는 애플리케이션이나 프로세스에 부여할 수 있어야 한다. 사용자 애플리케이션은 부여받은 권한을 가지고 해당 자원들에 접근할 수 있어야 하며, 또한 사용자 애플리케이션은 다른 애플리케이션에 부여받은 권한을 다시 위임할 수 있어야 한다.

2.2.3 사용자 기반 신뢰 관계(User-based Trust Relationships)

사용자가 다양한 그리드 자원 제공자(Provider)의 자원을 사용하기 위해서는, 보안 시스템이 각각의 자원 제공자들과 서로 협력하는 것을 강요하거나, 보안 환경 설정시에 상호 작용하도록 해서는 안된다. 다시 말하면, 어떤 사용자가 사이트 A와 B를 사용할 권한이 있다면, 그 사용자는 사이트 A와 B의 보안 관리자들에게 상호 작용하는 것을 요구하지 않고도 사용자 자신이 인증 받은 권한을 가지고 사이트 A와 B를 함께 사용할 수 있어야 한다.

2.2.4 다양한 지역 보안 솔루션의 통합

그리드 자원이 존재하는 각 시스템은 서로 다른 보안 요구사항과 이를 만족하는 솔류션을 가지고 있다.

그리드상의 각 사이트 또는 자원 제공자는 커버러스, 유닉스 보안 등과 같은 다양한 지역 보안 솔루션 중에서 하나를 채택할지도 모르기 때문에, 그리드에서 지원하는 보안 솔루션은 다양한 지역 보안 솔루션과 호환되어야 한다.

2.3 그리드 환경에서 필요한 권한부여

2.3.1 제 3자에 의한 인증(Authorization by Stakeholders)

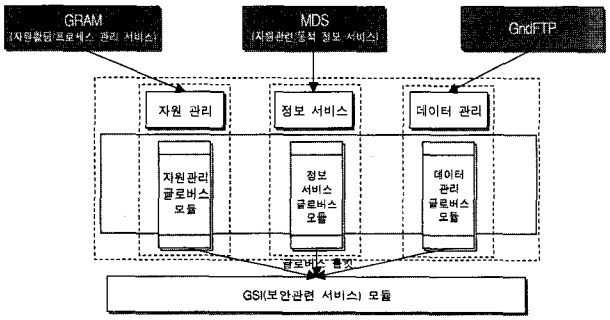
자원 소유자 또는 제 3자들은 적당한 조건이 되면 자원에 접근할 수 있는 주체(대상)를 조정 할 수 있어야 한다.

2.3.2 제한된 위임(Restricted Delegation)

손상되거나 오용된 위임된 인증서로 인하여 발생할 수 있는 취약성을 최소로 하기 위해, 위임되는 인증 권한을 제한하기 위해 많은 정책을 가지고 있는 것이 바람직하다.

2.4 그리드 미들웨어(Grid Middleware)

그리드 미들웨어는 지리적 또는 환경적으로 분산되어 있는 자원을 단일 컴퓨터에 속해있는 자원처럼 활용할 수 있도록 하는 연동시키는 소프트웨어이다. 현재 주로 사용되는 미들웨어로는 글로버스(Globus), Legion, Condor 등이 있다[9]. 특히, 글로버스는 지리적으로 분산된 서로 다른 자원을 하나의 가상 컴퓨터에 속한 자원처럼 사용할 수 있도록 하는 소프트웨어 기반 구조를 제공한다. 글로버스의 가장 큰 특징은 고정된 프로그래밍 기법을 취하는 것이 아니라 객체 지향 모델과 같이 보안, 통신 및 자원 관리 등의 기본적인 핵심 서비스만을 제공하고 응용 프로그래머 자신의 목적에 필요한 서비스를 선택·조합함으로써 다양한 형태의 응용 프로그램을 지원하도록 하고 있다는 점이다. 현재 글로버스는 GRAM(Grid Resource Allocation Management : 자원할당 및 프로세스 관리 서비스), GSI(Generic Security Interface : 보안관련 서비스), MDS(Monitoring and Discovering Service : 자원관련 동적 정보 서비스), 데이터 관리 서비스 등으로 이루어져 있다[10]. (그림 2)는 글로버스 내의 각 서비스들의 관계를 표현한 것이다.



(그림 2) 글로버스에서 제공하는 각 서비스의 관계

2.4.1 GRAM

글로버스에서 자원 관리를 담당하는 부분으로 GRAM은 글로버스의 가장 중심이 되는 요소이다. GRAM은 원격지 자원을 사용할 수 있게 하고 분산 자원들을 동시에 사용하게 하며 자원들의 관리의 상이함을 처리한다. 사용자는 자신의 작업을 그리드 환경에서 처리할 때 원하는 요구사항을 RSL이라는 스크립트를 이용하여 표현한다. GRAM은 리소스 브로커(resource broker)를 이용하여 RSL 스크립트를 저급의 스크립트로 변환하고, 각 자원에 있는 스케쥴러가 처리할 수 있는 형태의 스크립트로 변환한다. 이 변환 과정에서 리소스 브로커는 현재 또는 추후 사용 가능한 자원을 검색하기 위해 MDS를 이용하게 된다. 분산 환경에 할당되는 각 작업의 협업을 위해 GRAM은 DUROC이라는 요소를 사용한다.

2.4.2 GSI

그리드 보안은 분산 자원들을 공유하면서 발생하게 되는 필요악이다. 글로버스에서는 보안을 담당하는 부분을 GSS (Generic Security Service)라고 부른다. 사용자의 입장에서는 안전하면서도 사용의 편리성을 요구할 것이고, 각 자원을 소유하고 관리하는 관리자의 입장에서는 자원이 그리드 환경에 노출되는 것이기 때문에 사용의 편리성보다는 더 안전한 보안을 원할 것이다. 이를 위해 GSI는 단일인증을 제공하며 글로버스 프록시(Globus Proxy)를 이용한다. 사용자는 그리드 환경에 한번의 인증과정을 거침으로써 사용이 허가된 자원들을 사용할 수 있고 분산된 각 자원에 대한 사용자 인증은 프록시가 대신 수행한다. 그렇지만 각 자원 내에서 자원의 사용에 대한 허용범위는 각 자원이 제시하는 보안정책을 따른다.

2.4.3 MDS

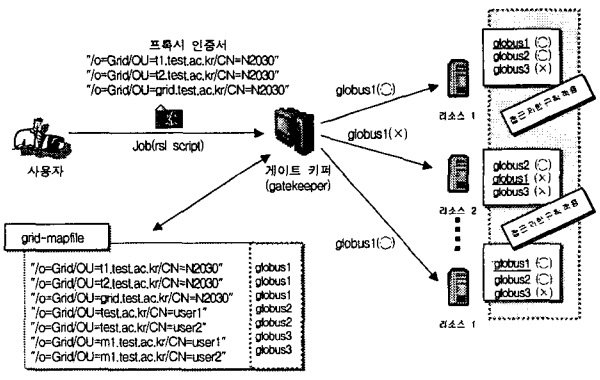
글로버스에서 정보 서비스를 수행하는 요소인 MDS는 그리드 내에 존재하는 자원들의 상태정보를 공유하고 사용자들에게 제공하기 위한 요소로서 인터넷의 DNS와 비슷한 것이다. 정보를 저장하고 사용자들에게 제공하기 위해 MDS는 LDAP을 이용한다. 정보 서비스를 위해 글로버스에서는 두 개의 서버를 제공하는데, 각 자원의 정보를 수집하는 GRIS와 수집된 정보를 통합하는 GIIS이다. 이들이 수집하여 제공하는 정보는 각 자원의 구조, 노드 수, 부하 정보, 배치작업 스케쥴러, 네트워크 상태 등이다. 이들 정보는 애플리케이션 개발자나 리소스 브로커 등에 의해서 제공된다.

3. 새로운 글로버스 보안 서비스

3.1 사용자 등급 기반의 보안 서비스 모델 설계

3.1.1 단순 ID 기반의 인가 서비스

현재 글로버스에서는 (그림 3)과 같이 그리드 사용자들의 인증서에서 subject DN(Distinguished Name)을 추출하여 로컬 시스템의 ID와 매핑하여 사용자에게 권한을 부여하고 있다. 사용자가 작업을 그리드 상에서 수행하기 위해서는 작업 파일과 프록시 인증서를 해당 시스템에 전달하게 되는데 해당 시스템에서는 프록시 인증서의 subject DN을 로컬 시스템의 /etc/grid-security/grid-map에서 검색하여, 일치하는 ID를 추출하고 로컬 시스템의 ID에 따라서 로컬 시스템에 대한 자원 접근을 인가한다.

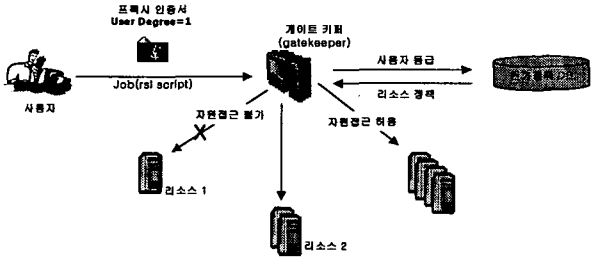


(그림 3) 단순한 ID 기반의 인가 서비스

이러한 자원에 대한 접근은 OS 차원에서의 접근 제한뿐만 아니라 LSF, PBS, LoadLeveler와 같은 작업 관리 프로그램에 의해서도 적용될 수 있다. 작업관리 프로그램에서는 사용자 ID를 기반으로 하여 사용가능한 CPU의 개수, 메모리 용량, 실행 시간 등을 제한할 수 있다.

3.1.2 엔티티별 등급 기반의 인가 서비스

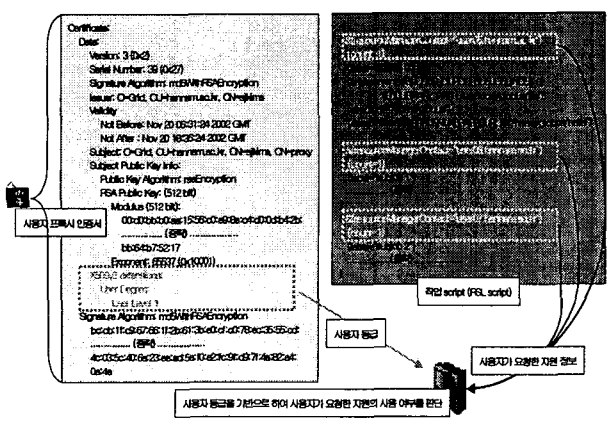
기존 글로버스의 사용자 인가 시스템은 해당 로컬 시스템에 접근하는 사용자가 많아지게 되면, 사용자 프록시 인증서의 subject DN과 로컬 시스템의 ID를 1 : 1로 매핑 할 경우, 계정 관리 문제와 메모리 자원, 디스크 자원의 관리에 있어 많은 어려움을 겪게 된다. 이러한 이유로, 기존의 글로버스에서는 여러 subject DN이 하나의 로컬 ID를 공유하는 형태를 띠고 있다. 하나의 로컬 ID를 공유할 경우에 발생하는 문제는 수많은 그리드 사용자의 모든 요구사항을 적용하는데 있어서 불합리한 면을 지닌다. 이에 본 논문에서는 ID 기반이 아니라, (그림 4)에서 보는 바와 같이 인증서 기반의 사용자 인가 시스템을 제안하였다. 앞서 설명한 기존의 ID 매핑 방식의 인가 시스템 대신에 인증서내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 하였다.



(그림 4) 인증서를 이용한 사용자 등급 기반의 인가 서비스

3.1.3 엔티티 등급별 필드 적용

본 논문에서 제안된 인증서 기반의 사용자 인가 시스템은 사용자의 프록시 인증서 내에 사용자 등급을 표시 할 수 있는 필드를 인증서 확장영역에 추가하였다. 사용자가 작업을 실행하기 위해서 로컬 시스템으로 작업파일과 프록시 인증서를 전송하게 되면 로컬 시스템에서는 프록시 인증서에서 사용자 등급을 추출해낸다. 이를 미리 정의된 로컬의 인가 정책 데이터베이스를 검색하여 사용자가 접근 가능한 자원과 정책에 의해서 정의된 각종 시스템 자원 사용량을 검사하여 제출한 작업파일이 실행할 수 있는지를 검사하고 작업의 실행여부를 결정하게 된다. (그림 5)는 인증서의 확장 필드에 사용자의 등급과 관련된 사항을 추가한 것이다.



(그림 5) 인증서내의 사용자 등급 사항

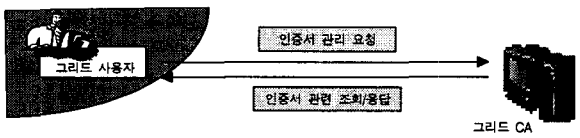
또한, 인증서내의 사용자 등급을 포함하고 있는 확장 필드를 추가하기 위해서는 글로버스에서 인증서버로 사용하고 있는 OpenSSL의 openssl.conf 파일에 다음과 같은 항목과 값을 추가한다.

```
.....(중략).....
[user_ext]
UserDegree = "User Level 1"

[user_ext2]
UserDegree = "User Level 2"
```

3.2 그리드 CA 클라이언트

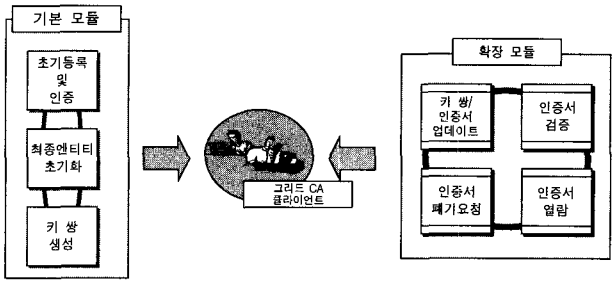
그리드 CA 클라이언트는 글로버스를 통하여 그리드 상의 자원을 사용하고자 할 경우, 각 엔티티의 신원을 증명해주는 인증서 관리 업무를 수행하는데 목적이 있으며, 그리드 자원을 사용하고자 하는 사용자가 인증서를 효율적으로 이용하고 관리할 수 있는 인증서 관리 도구를 구축하는데 그 목적이 있다. (그림 6)은 기본적인 클라이언트와 그리드 CA 사이의 관계 모델이다.



(그림 6) 그리드 CA 클라이언트 동작 관계 모델

3.2.1 인증 모델

그리드 CA 클라이언트의 인증 기능과 관련한 모듈은 크게 인증서 생성과 관리를 위한 기본 모듈과 인증서 활용을 위한 확장 모듈로 나누어 볼 수 있다.

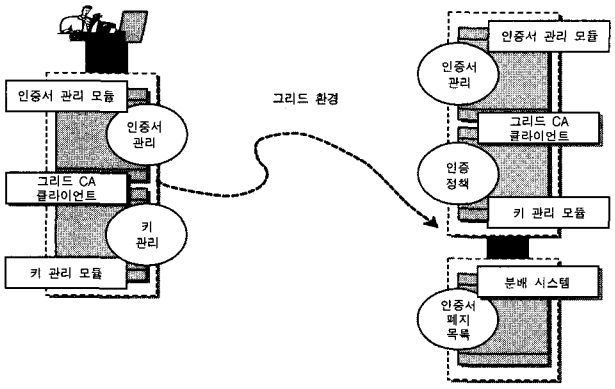


(그림 7) 그리드 CA 클라이언트 인증 기능 모듈

기본 모듈은 인증서의 초기 생성을 위한 초기등록/인증 모듈, EE 초기화 모듈, 키 쌍 생성 모듈로 나누어 볼 수 있으며, 확장 모듈은 인증서의 유효성을 검증하기 위한 모듈과, 키 쌍 업데이트를 통한 인증서 업데이트 모듈, 인증서 폐지 요청 모듈, 인증서 열람 모듈 등이 있다. (그림 7)은 그리드 CA 클라이언트에서 요구되는 각각의 인증 기능 모듈이다.

3.2.2 그리드 CA 클라이언트의 인증서비스 모델

그리드 CA 클라이언트는 그리드 CA와의 연동을 통해서 사용자의 인증서 요청을 받아들여, 요청 메시지를 생성한 후에 그리드 CA에 전송하여 처리하는 것과, 그리드 CA의 응답 메시지를 받아들여, 사용자에게 전달하는 역할을 담당한다. 그리드 CA 클라이언트는 (그림 8)과 같이 크게 인증서 관리 모듈, 키 관리 모듈로 구성되며, 그리드 CA 클라이언트와 그리드 CA간의 메시지 교환은 안전한 통신 채널 환경에서 이루어지게 된다.

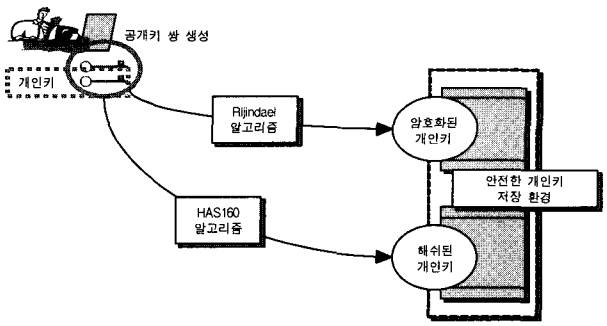


(그림 8) 그리드 CA 클라이언트 구조

위와 같은 그리드 CA 클라이언트는 인증 시스템 구축에 있어서 현재 글로버스에서 사용하고 있는 그리드 CA와 비교하여, 기존에 없었던 인증서 관리 클라이언트를 확장함으로써, 그리드 사용자가 자신이 소유하고 있는 인증서의 관리를 보다 편안히 수행하고, 전체적인 인증서 관련 업무를 간소화시킬 수 있는 장점이 있다.

① 암호화 저장 모델

인증 시스템에서 전자서명 및 수신된 문서에 대한 암·복호화에 사용되는 개인키를 보관하는 것은 매우 중요한 문제이다. 개인키가 유출된다면 인증 시스템에 근본적인 신뢰도가 붕괴되므로 해당 인증서를 사용할 수 없으며, 추후 발생할 문제의 여지가 남아 있다. 본 논문에서는 개인키 보관에 대한 취약한 보안 강도를 높이기 위해, 최근에 가장 안전하다고 알려진 Rijindael 알고리즘을 이용하여 암·복호화를 수행하고, PKCS #5 v2.0 표준에 정의되어 있는 해쉬 알고리즘인 SHA-1을 이용하여 해쉬 값을 출력하게 된다. 이러한 개인키 저장 모듈에 대한 모델은 (그림 9)와 같다.

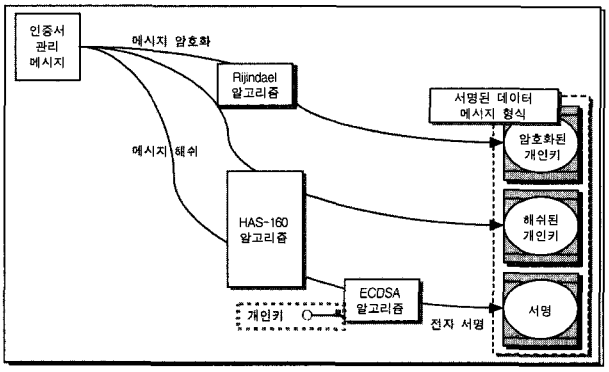


(그림 9) Rijindael을 이용한 개인키 저장

개인키를 전자서명 및 수신된 암호화 메시지를 복호화하는데 사용하기 위해서는 암호화되어 저장되어 있는 개인키를 복호화해서 사용한다. 개인키의 복호화는 암호화 모델의 역순으로 진행된다.

② 암호 메시지 교환 모델

그리드 CA 클라이언트와 그리드 CA가 공개된 네트워크 상에서 메시지를 교환할 경우 발생하는 제 3자의 도청에 의한 메시지 유출 및 변경과 같은 보안 위협 요소에 대처하기 위해서 인증서 관리 메시지를 암호화하여 교환한다. 인증서 관리 메시지 암호화는 그리드 CA 클라이언트 또는 그리드 CA에서 생성하는 인증서 관리 메시지를 암호화하여 전송하는 과정을 포함하며, (그림 10)과 같이 암호화된 요청·응답 메시지 부분과 서명 부분으로 구성된다.

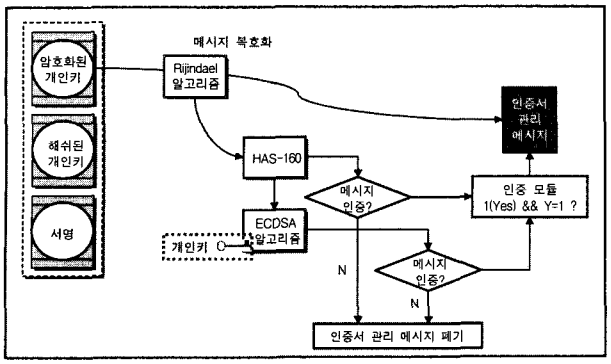


(그림 10) Rijindael을 적용한 인증서 관리 메시지 암호화

인증서 관리에 대한 요청·응답 메시지는 다음과 같은 순서로 암호화되어 진다.

㉠ 메시지를 Rijindael 알고리즘을 사용하여 인증서 관리 메시지를 암호화한다.
㉡ HAS160 알고리즘을 이용하여 메시지를 해싱한다.
㉢ ECDSA 알고리즘을 이용하여 메시지 전송자의 개인키로 해쉬 값을 서명한다.

그리드 CA 클라이언트 또는 그리드 CA에 수신된 인증서 관리 메시지는 각 부분별로 복호화 및 서명을 검증한다. (그림 11)은 이러한 과정을 보여준다.



(그림 11) Rijindeal을 적용한 인증서 관리 메시지 복호화

㉠ 수신된 메시지를 Rijindael 알고리즘을 사용하여 인증서 관리 메시지를 복호화 한다.

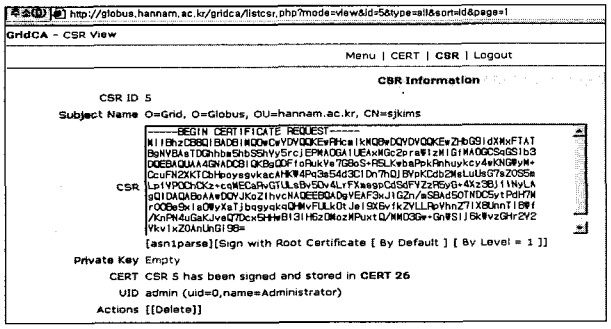
㉡ HAS160 알고리즘을 이용하여 복원된 메시지를 해싱한다.

㉢ ECDSA 알고리즘을 이용하여 메시지 전송자의 공개키로 서명을 검증한다.

4. 새로운 보안 서비스 적용

4.1 인증서 기반의 인가 서비스 구현

본 논문에서 구현된 인증서 기반의 인가 시스템의 핵심은 그리드 사용자의 인증서 내에 각 자원에 대한 접근 권한을 표시하는 확장 필드를 추가하고, 이를 데이터베이스에 저장하고, 해당 인증서의 등급에 맞춰 그리드 사용자와 프로세스에게 서로 다른 권한을 부여하는 것이다.

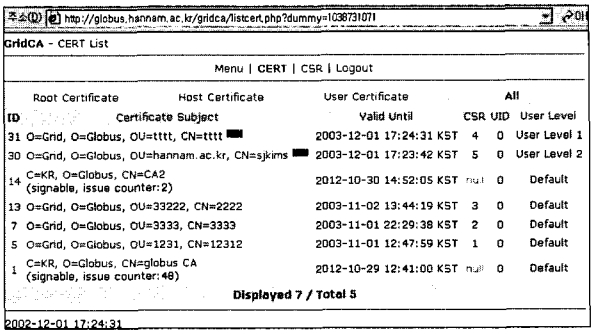


(그림 12) 새로운 인가 서비스를 적용한 인터페이스 화면

(그림 12)는 슈퍼컴퓨터연구실에서 개발·배포한 인증서 발급 시스템(GridCA V1.0)을 제안된 시스템에 맞게 변경한 화면이다. 위의 화면은 사용자의 인증서 발급 요청에 대하여 실제 인증서를 생성해주는 화면이며, 인증서 발급자(관리자)가 사용자의 인증서 요청을 확인한 후에 미리 정의한 정책에 따라 등급이 부여된 인증서를 사용자에게 발급할 수 있다.

본 논문에서 구현된 현재까지의 사용자 등급은 간단히 Default와 Level = 1로 구분하고 있으나 이것은 인증서 발급 정책에 의해서 보다 세분화가 가능하다.

(그림 13)은 수정된 인증서 발급 시스템을 통하여 등급을 부여하여 발급한 인증서들의 목록을 표시하는 화면이다. 인증서에 등급에 대한 확장 필드가 있다면 등급을 표시하며, 만일 정의하지 않았다면 Default로 표시하도록 구성되어져 있다.



(그림 13) 사용자 등급 부여 인증서 목록

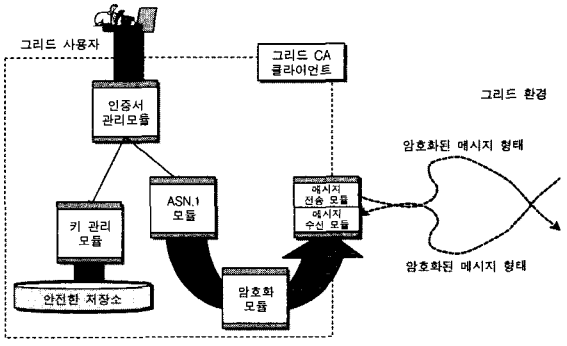
인증서 내에 추가된 사용자 등급 정보를 확인하기 위해서 openssl의 소스코드를 수정하여 policy라는 파라미터를 추가하였다. 이를 이용하여 다음과 같이 명령어 라인 상에서도 인증서내의 사용자 등급을 확인할 수 있다.

```
$openssl x509 -in userlevel1.pem -policy -text -noout
User Degree = User Level 1
$openssl x509 -in LevelNotDefine.pem -policy -text -noout
User Degree is Not Define.!
```

위의 예는 사용자 레벨이 1인 인증서(userlevel1.pem)와 등급이 정의되지 않은 인증서(LevelNotDe -fine.pem)에 대한 사용자 등급 표시 명령어를 실행한 예이다.

4.2 CA 클라이언트의 인증 서비스 구현

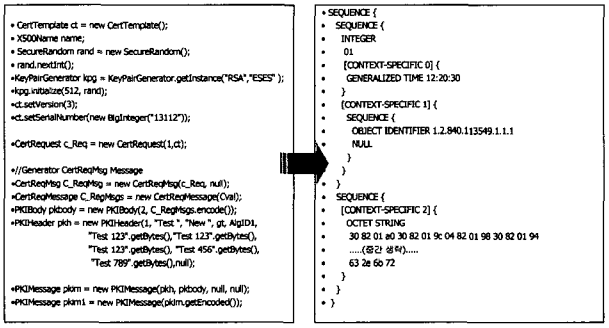
본 논문에서 구현된 인증서 기반의 인가 시스템과 그리드 CA 클라이언트의 핵심은 인증서 관리 프로토콜(Certificate Management Protocol ; CMP)을 준수하는 인증서의 관리 모듈, 개인키 저장 모듈, 그리고 안전한 메시지 교환을 위한 암호화 및 메시지 전송 모듈이다. (그림 14)는 클라이언트를 구성하고 있는 각 모듈의 구성도이다.



(그림 14) 그리드 CA 클라이언트의 인증서 관리 모듈

4.2.1 인증서 관리 클래스에 의한 ASN.1 모듈

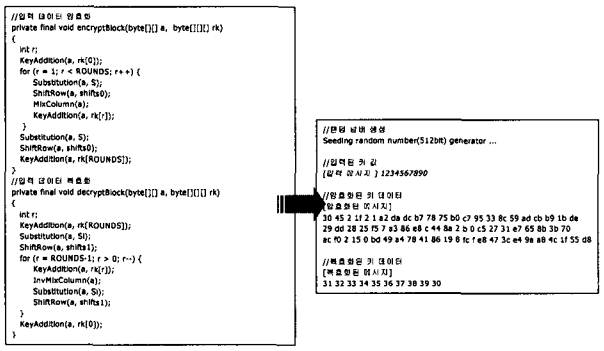
그리드 CA 클라이언트에서 그리드 CA로 인증서 관리와 관련한 메시지를 전송하고, 이를 처리하기 위해서는 국제 표준규약에 맞추어진 인증서 요청 메시지 형식을 생성해야 한다. (그림 15)는 클라이언트에서 초기 인증서를 요청하기 위한 ASN.1 구문으로, 클라이언트에서 전송되는 모든 메시지는 이와 같은 형태를 지니고 있다.



(그림 15) 인증서 요청 메시지의 ASN.1 형식

4.2.2 암호화 모듈

문서에 대한 서명 또는 수신된 문서를 복호화하기 위해서 사용되는 개인키는 안전하게 보관되어야 한다. 개인키의 저장은 일반적으로 안전한 이동 저장 매체 또는 디렉토리와 데이터베이스를 지정하여 저장하게 된다. 또한, 그리드 CA 클라이언트와 그리드 CA 사이에 교환되는 관리 메시지도 암호화되어 외부의 보안 위협으로부터 보호되어야 한다. (그림 16)은 Rijindael 알고리즘을 사용하여 개인키의 암호화 저장과 메시지 암호화이다.



(그림 16) 개인키 및 메시지의 암호화 예

5. 비교분석 및 성능평가

그리드에 대한 연구가 활발히 진행되고, 실용화하려는 노력이 산·학·연에서 활발히 진행됨에 따라 그리드 자원을 활용할 수 있는 그리드 미들웨어도 많은 발전을 하였다.

본 논문에서는 그리드를 위한 다양한 미들웨어 중에서 현재 가장 많이 활용되고 있으며, 표준화의 가능성이 높은 글로버스를 기반으로 그리드 CA 인증 서비스 모듈을 구현하였다. <표 1>은 기존의 글로버스 내에 포함되어 있는 인증 모듈과 본 논문에서 구현된 모듈과의 비교이다.

〈표 1〉 기존의 인증 서비스 모듈과의 비교

시스템 / 기 능	기존의 인증 서비스 모듈	제안된 인증 서비스 모듈
미들웨어 기반	Globus 2.0	Globus 2.0
그리드 CA	OpenSSL	OpenSSL
사용자 인증 서비스	인증서에 의한 인증	인증서에 의한 인증
사용자 인가 서비스	로컬 ID 기반	인증서 기반
서버 클라이언트	지원하지 않음	지원함

또한, 공개키 기반의 인증서버 클라이언트는 네트워크 상에서 다양한 사용자의 신분을 인증하기 위한 시스템의 확장 시스템으로 현재까지 많은 업체에서 다양한 제품들이 개발되어 왔다.

본 논문에서 설계하고 구현한 그리드 CA 클라이언트는 기존의 상용화 업체에서 제공하는 클라이언트 시스템들과 같이 인증서를 관리하기 위한, 인증서 신청, 인증서 갱신, 인증서 검증, 개인키 저장 기능을 제공하며, 더불어 각 요청을 전달하는 메시지를 암호화하고 검증하는 모듈에 보안강도가 높은 타원곡선을 적용한 알고리즘을 적용함으로써 높은 보안 요구사항을 달성할 수 있다. <표 2>는 본 논문에서 구현한 그리드 CA 클라이언트 시스템과 다른 상용제품의 클라이언트의 기능과 적용 알고리즘을 비교·분석하였다.

〈표 2〉 제안된 그리드 CA 클라이언트와 상용 소프트웨어와의 비교

비교대상 / 제품군		제안된 시스템	B사	V사	E사	M대학
인증서 관리 기능	신청	제공함	제공함	제공함	제공함	제공하지 않음
	갱신	제공함	제공함	제공함	제공함	제공하지 않음
	검증	제공함	제공함	제공함	제공함	제공함
	보관	제공함	제공함	제공함	제공함	제공함
	열람	제공함	제공함	제공함	제공함	제공함
알고리즘	키 저장	Rijndael	3-DES	3-DES	3-DES	DES
	메시지 암호화	Rijndael	RSA	RSA	RSA	RSA
	메시지 해쉬	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
	메시지 서명	ECDSA	ECDSA	ECDSA	DSA	DSA
프로토콜	인증	ID/PW	ID/PW	ID/PW	ID/PW	ID/PW
	통신 암호화	GSI MPI	SSL	SSL	SSL	SSL

또한, 기존에 개인키 저장 알고리즘으로 사용되고 있는 3-DES와 Rijindeal 및 다른 비밀키 알고리즘과의 차이점을 비교해 보면 <표 3>과 같다[11].

〈표 3〉 블록 암호 알고리즘 비교

알고리즘	블록 크기	키 길이	라운드 수	공 격
3-DES	64	168	48	K : 2/112/56
RC2	64	8~1024	18	C : 64/64/.(16)
RC5	128	8s, s < 256	16	C : 83/./., C : 123/./.(24)
IDEA	64	128	8, 5	C : /56/67/32(3, 5)
Rijindeal	128	128, 192, 256	10, 12, 14	?

● 공격방법 설명
- K : a/b/c : Known Plaintext Attack에서 2^a의 평문/암호문이 필요하고, 2^b의 암호화 작업을 해야 하고, 2^c의 메모리가 필요하다.
- C : a/b/c : Chosen Plaintext Attack에서 2^a의 평문/암호문이 필요하고, 2^b의 암호화 작업을 해야 하고, 2^c의 메모리가 필요하다.
- (r) : 공격 라운드 수, 만일 공백이면 알고리즘의 라운드 수
- ? : 공격법이 알려지지 않은 경우

Rijindeal 알고리즘은 DES를 대체하기 위하여 AES(Advanced Encryption Standard) 알고리즘 표준으로 개발되었으며, 3-DES보다 더 효율적이며 안전해야 한다는 설계기준이 제시된 상태에서 개발되었다[12].

위의 도표에서 살펴보듯이 Rijindeal은 3-DES 보다 더 작은 라운드 수를 지니며, 현재까지 알려진 뚜렷한 공격방법이 없기 때문에 기존의 알고리즘보다 수행 속도 측면이나 안전성 면에서 우수한 점을 보이고 있다.

6. 결론 및 향후 연구

그리드는 지역적으로 분산되어 있는 고성능의 컴퓨터 자원을 네트워크를 연결하여 마치 단일 컴퓨터처럼 자원과 데이터를 공유하여 사용할 수 있는 시스템으로, 각 자원을 연결하기 위해서 다양한 보안 요구사항을 가지게 된다. 하지만, 현재까지 다양한 그리드 보안 요구 사항을 만족하는 메커니즘이 제안되지 않았기 때문에 현재 표준으로 제정되어 운영되고 있는 기술을 바탕으로 이들을 통합하고 새로운 프로토콜을 확장하고 그리드 보안 요구사항을 만족하도록 구성하고 있다.

본 논문에서는 그리드의 보안 요구사항과 인증과 권한 부여를 연구하고, 이를 바탕으로 그리드 보안에서 발생할 수 있는 인증 및 인가 서비스에 대한 문제를 해결할 수 있는 방안을 연구하고, 이를 설계 및 구현하였다. 또한, 기존의 그리드 미들웨어인 글로버스의 인증 시스템에서 사용자의 권한을 부여해주는 모듈을 ID 기반에서 인증서 기반으로 확장함으로써 추후 발생할 수 있는 자원에 대한 권한 부여 문제를 해결하였다.

추후 본 논문에서 연구된 내용은 추가적인 보안 모듈 및 기능의 확장을 통하여, 실제 국내에 구축되는 국가 그리드(N*Grid)에서 활용 할 수 있는 통합 인증서 관리 도구를 개발하고, 이를 실제 그리드 CA와 연동하여 사용자의 요청을 처리할 수 있는 통합 모듈의 개발의 개발에 대안 방안을 연구하는 것이 향후 연구과제이다.

참 고 문 헌

[1] Randy Butler Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Garl Kesselman, "A National-Scale Authentication Infrastructure," IEEE, pp.60-66, December, 2000.

[2] IETF, "GSS-API EXtensions," Internet Draft, February, 2002.

[3] IETF, "Internet X.509 Public Key Infrastructure Proxy Certificate Profile," RFC 2459, August, 2001.

[4] IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocol," RFC 2510, March, 1999.

[5] Czajkowski, K., Fitzgerald, S., Foster, I. and Kesselman, C., "Grid Information Services for Distributed Resource Sharing," 2001.

[6] 강 경우, 박형우, "그리드 연구개발 동향", 한국정보과학회지, 제20권 제2호, p.27, 2002.

[7] Foster, I., C. Kesselman and S. Tuecke, "The Anatomy of the Grid : Enabling Scalable Virtual Organizations," International Journal of Supercomputer Applications, 2001.

[8] http://www.gridforum.org/2_SEC/SEC.htm.

[9] 윤찬현, 심은보, "그리드 구조 및 연구동향", 한국정보과학회지, 제20권 제2호, p.13, 2002.

[10] 김학두, 김진석, "그리드 미들웨어 : 자원 관리 및 원격 데이터 접근 기술 동향", 한국정보과학회지, 제20권 제2호, pp.35-39, 2002.

[11] http://www.kisa.or.kr/technology/sub1/current_bca.htm.

[12] http://csrc.nist.gov/CryptoToolkit/aes/.

국 중 옥

e-mail : jokug@netian.com

1998년 숭실대학교 대학원 전기공학과 (공학석사)

2003년 한남대학교 대학원 컴퓨터공학과 (박사과정)

1994년~현재 호서전산전문학교 컴퓨터 응용제어과 교수

관심분야 : 컴퓨터 네트워크, 정보통신 정보보호, 의료정보

이 재 광

e-mail : jklee@netwk.hannam.ac.kr

1984년 광운대학교 전자계산학과(이학사)

1986년 광운대학교 대학원 전자계산학과 (이학석사)

1993년 광운대학교 대학원 전자계산학과 (이학박사)

1986년~1993년 군산전문대학 전자계산학과 부교수

1997년~1998년 University of Alabama 객원교수

1993년~현재 한남대학교 컴퓨터공학과 정교수

관심분야 : 컴퓨터 네트워크, 정보통신 정보보호