XML 정보보호 기술을 활용한 자동화된 그리드 VO 인증 시스템 연구

이성현*, 이원구*, 이재광*
한남대학교 컴퓨터공학과*

A Study of Automatically Grid VO Authentication Using XML Security

Seoung-Hyeon Lee*, Won-Goo Lee*, Jae-Kwang Lee*
Dept. of Computer Engineering, Hannam University*

요 약

그리드 VO(Virtual Organization)는 내부 규정과 정책의 집합에 의하여 제어되는 기존의 VO 개념에서 벗어나 임시적, 동적 기반의 자원 공유와 협업을 하기 위해 개인 또는 기관, 시스템 자원이 모인 임시적인 VO이다. 이것은 개인 또는 기관, 시스템 자원들이 동시에 몇 개의 VO의 일원이 되는 경우나 변화하는 시스템 자원의 상황에 따라 VO 구성을 위한 결합, 형성된 그리드 VO에 대한 인증에서 많은 문제가 발생하게 된다. 본 논문에서는 그리드 VO 구성에서 발생할 수 있는 보안 문제 중 자원에 대한 인증과 관련된 문제를 해결하고자 XML 정보보호기술을 토대로 경량화된 그리드 VO에 대한 자원 인증 시스템을 제안하였다.

1. 서론

그리드는 시스템 자원을 네트워크를 통해 연결한 가상의 슈퍼컴퓨터로 실험, 원격 데이터베이스 검색, 원격 소프트웨어 사용, 대형 시뮬레이션 등의 연구에 사용될 수 있으며, 이미 가시적인 성과가 이루어지고 있다[1][2][3].

그리드 환경을 구축하기 위해 사용되는 각 시스템 자원(CPU, 메모리, 디스크 등)은 매우 동적인 특성을 지니게 된다. 이러한 시스템 자원을 묶어 하나의 그리드 VO를 형성할 경우에는 단순히 사용자와 기관, 시스템을 묶은 기존의 시스템에 비해서 많은 보안 문제점들을 가지게 된다. 이러한 보안 문제점으로는 자원의 통합, 상호호환성, 신뢰 관계, 위임 및 정책 구성, 그리드 VO 인증 등이 있으며, 이것을 해결하기 위하여 OGSA(Open Grid Service Architecture) Security Roadmap을 통하여 다양한 컴포넌트들과 웹 서비스 보안(WS-Security) 기반의 보안 서비스 프로토콜을 제안하고 있다[4]. 하지만, OGSA와 OGSA Security Roadmap은 그리드 보안 요구사항과 적용 기술, 각 기술과의 관계만을 정의하고 있을 뿐 이를 구체적으로 적용한 서비스 모델을 제안하고 있지 않으며, 실제 구축된 사례도 찾아보기 어렵다.

본 논문에서는 표준문서를 바탕으로 그리드에서 요구하고 있는 그리드 VO 인증과 관련한 요구사항과 메커니즘을 분석하고, XML 정보보호기술을 활용한 그리드 VO 인증 시스템의 구축방안에 대하여 연구하였다.

본 연구는 산업자원부에서 시행한 산업기술개발사업 (2003-61-10009504)에 의해 지원되었음

본 논문의 구성은 다음과 같다. 2장에서는 그리드 VO 인증 시스템을 구축하기 위한 OGSA 보안 기반 구조와 요구사항, 보안 프로토콜을 살펴본다. 3장에서는 XML 정보보호기술을 활용한 그리드 VO 인증 시스템 구성을 위한 세부 모듈 구조를 정의하고, 4장에서 본 논문에서 제안된 연구사항을 적용한 시스템의 일부를 살펴본 후 결과를 분석한다. 마지막으로 5장에서 결론을 맺고 향후 연구방향을 제시한다.

2. 관련연구

2.1 OGSA(Open Grid Service Architecture)

OGSA는 그리드 환경에서 VO를 구축할 때 발생하는 문제들을 해결하는 프로토콜, 서비스, 도구(tool)들에 대한 규정과 메커니즘을 포함하고 있다.

기존의 조직과 그리드 VO의 구별에서 조직은 구성원의 내부 규정과 정책의 집합에 의해 제어되는 실제 조직에 속해 있는 반면, 그리드 VO는 임시적, 동적 기반의 시스템 자원을 공유하고 다른 협업을 하기 위해 합의된 개인 또는 기관들의 모임이다. 이것은 보안 측면에서 하나의 도메인이 수많은 다른 방법으로 다른 도메인과 중첩, 불규칙, 교차 도메인과 직면하게 되며, 이를 해결하기 위하여 보안 정책과 메커니즘의 분리와 도메인 상호간의 호환성을 요구하게 된다[5].

OGSA는 이러한 문제를 해결하기 위해, 이전의 기술을 통합하는 보안 추상화의 집합에 기반을 둔 안전하고, 통합되었으며, 상호호환이 가능한 그리드 보안 서비스를 제공하기 위한 방안을 제안하고 있다.

2.2 OGSA Security Roadmap

OGSA Security Roadmap은 OGSA에서 제안하고 있는 보안 컴포넌트들을 소개하고, 이들이 WS 보안 명세서와 어떤 연관이 있는지 보여주고 있다[6]. 컴포넌트들의 그룹에서 보안 기술과 표준화 계층은 동일하거나 유사한 다른 특성들과의 교환으로 다른 레벨에서 구현될 수 있다.

(1) 웹 서비스 보안 명세서

OGSA Security Roadmap은 웹 서비스 보안 구조에서 기술된 OGSA 보안 명세서들의 집합을 제안하고 있다. 웹 서비스 보안 구조는 계층화된 프레임워크를 기술한다. 이러한 모듈에서 작성된 명세서들은 이 로드맵에서 제안된 OGSA 보안 명세서에 대한 블록을 구축함으로써 사용자들에게 편의를 제공할 것이다. OGSA 보안 그룹에서 관심을 가지고 있는 명세서들은 XKMS, SAML, XACML, XML-Signature, XML-Encryption이다.

(2) OGSA 보안 명세서

OGSA 보안 명세서들은 OGSA의 특정 보안 요구사항을 만족하기 위해 필요하므로 다른 보안 표준들을 확장하고 수정하는 것에 대해 제한된 목적을 가진다. 전체적인 OGSA Security Roadmap의 임계 경로에서 OGSA 보안 명세서들이 있다고 예상되지만, 아직 알려지지 않은 다른 명세서들에 의존하는 상황에서, 적절한 명세서들이 후에 조정될 것이라는 의도를 가지고 제안되었다. 이 로드맵에서 제안된 다수의 OGSA 보안 명세서들은 한 OGSA 보안 서비스들을 정의할 것이다.

2.3 XML 정보보호기술

XML 정보보호 기술은 인터넷 상에서 발생할 수 있는 메시지 도청, 메시지 변조, 메시지 송신 및 수신 부인, 메시지 위조, 불법적인 서비스 이용 등의 보안 위협 요소를 해결하기 위한 XML 기반의 보안 서비스 기술이다. 표 1은 웹 상에서 발생할 수 있는 보안 위협 요소와 대응 기법을 정리한 것이다[7].

표 1. 보안 위협 요소와 대응 기법

범주	보안 요소	대응 기법
비인가된 거래 및 사기	인증, 무결성, 전자서명, 부인봉쇄	XML 전자서명
메시지 도청	기밀성	XML Encryption
비 인가된 거래 및 사기	인증, 인가 정보 교환	SAML
관리 및 감사 결과의 손실	효율적인 키 관리	XKMS
메시지 도청	통신 메시지 보안	WS-Security
비 인가된 거래 및 사기	인가 규칙	XACML
각종 에러 탐지	바이러스, 침입탐지, 서비스 거부, 시스템 설정 부정확	백신 S/W, 관리 툴, 감사 정책
법적 책임	공통 적용 법률의 부재	

위 표에 정리된 보안 위협 요소에 대하여 XML 기반의 정보보호 기술을 통하여 대응할 수 있는 요소들이 존재한다. XML 기반의 정보보호 기술은 XML Encryption, XML Signature, XML Key Management System 등으로 나누어 볼 수 있다.

3. 그리드 VO 인증 시스템 모듈

3.1 그리드 VO 인증을 위한 시스템 구조

그리드 VO는 그리드 환경을 구성하고 있는 이 기종의 시스템 자원들 중에서 사용자의 작업 요청에 대해서 이용 가능한 이기종의 시스템 자원을 묶어 하나의 도메인으로 제공하기 위한 가상 시스템으로 볼 수 있다.

이러한 그리드 VO를 구성하기 위한 자원으로는 CPU, 메인 메모리, 보조 기억장치, 데이터베이스, 고가의 연구장비 등을 들 수 있다. 이러한 시스템 자원들은 이 기종으로 구성될 가능성이 매우 높으며, 서로 다른 인증 정책, 보안 프로토콜, 보안 정책 등의 보안 메커니즘을 가지게 된다. 이러한 특성을 지니고 있는 그리드 VO의 구성에 있어서 가장 중요한 점은 재구성된 그리드 자원들을 마치 하나의 시스템 자원처럼 사용자가 활용할 수 있는 방안을 제공하는 것이 중요하다.

그리드 VO 인증은 VO 활용을 위한 여러 가지 방안 중에서 인증 서비스를 제공하기 위한 목적으로 사용된다. 별개의 독립접인 자원들의 집합에 대하여 공통의 인증서를 부여함으로써 그리드 VO에 대한 사용자 인증 서비스를 제공하고, 자원들 간에 오가는 데이터와 사용자의 작업 요구에 대하여 안전한 보안 서비스를 제공할 수 있다.

(1) 그리드 VO 시스템의 전체 구조

그리드 VO 인증 시스템은 그리드 사용자의 요청에 의하여 VO를 구성할 경우에 VO에 대한 인증 서비스를 제공하기 위한 시스템으로 사용자의 작업 요청에 의해 구성된 그리드 VO, 그리드 CA, 각 구성요소 사이의 중간 모듈로 그리드 VO 인증 모듈 등의 세부 구성 요소를 통하여 구성되며, 그림 1과 같은 전체 구조를 가지게 된다.

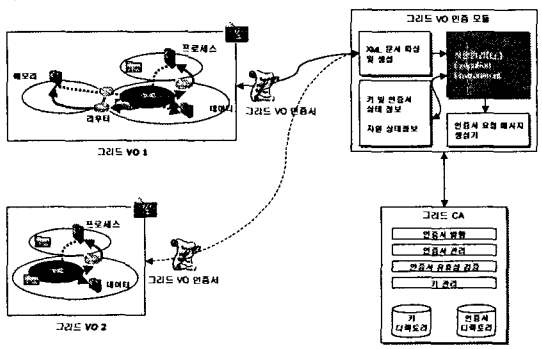

그림 1. 그리드 VO 인증 시스템의 전체 구조

위 그림에서는 각 그리드 VO 도메인과 인증서를 발급하기 위한 그리드 CA 사이의 메시지 흐름에 대한 간략한 흐름을 보여주고 있다. 그리드 VO를 구성하기 위한 일반 절차는 다음과 같이 요약할 수 있다.

첫째, 그리드 환경에서 작업을 수행하려는 사용자는 자신이 부여받은 인증서를 통하여 각 자원에 접근 한다.

둘째, 사용자의 작업 요청을 받은 그리드 자원 정보 시스템은 현재 유효한 자원의 규모를 파악하고, 이를 묶어 하나의 그리드 VO를 형성한다.

셋째, 구성된 그리드 VO는 자신에 대한 인증서를 발급받기 위하여 VO를 구성하고 있는 자원에 대한 정보, VO 구성을 요청한 사용자의 인증서를 포함한 XML 문서를 생성하여 그리드 VO 인증 모듈에 전송한다.

넷째, 서명된 XML 문서를 수신한 그리드 VO 인증 모듈은 요청된 그리드 VO 정보를 추출하여 이에 대한 인증서를 그리드 CA에 요청하게 된다.

다섯째, 발급된 임시 그리드 VO 인증서와 키에 대한 정보를 해당 VO에 전송하게 된다.

3.2 그리드 VO 인증 모듈 구조

그리드 VO 인증 모듈은 VO 인증을 위한 중요한 모듈로서 XML 문서의 파싱 및 생성을 담당하는 모듈, 키 및 인증서의 상태 검증을 위한 모듈, 인증서 요청 메시지 생성을 위한 모듈 등으로 구성되며, 이들 모듈의 동작을 실행환경에서 제어하게 된다. 그림 2는 그리드 VO 인증 모듈의 전체 구조도이다.

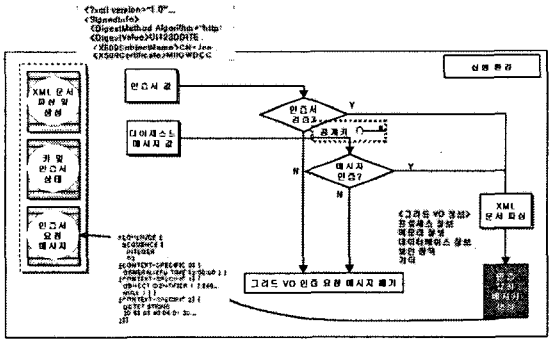

그림 2. 그리드 VO 인증 모듈의 전체적인 구조 및 동작

(1) XML 문서 생성 모듈

XML 문서 생성 모듈은 그리드 VO를 구성하기 위한 정보와 VO 구성 요청자의 인증서를 통한 키 값을 통하여 XML 서명 문서를 생성하기 위한 모듈로 그림 3과 같은 과정을 거쳐 그리드 VO 인증을 위한 XML 서명 문서를 생성하게 된다.

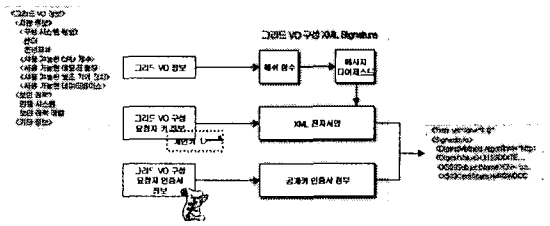

그림 3. 그리드 VO 인증을 위한 XML 서명 문서 생성

그리드 VO 인증서를 요청하기 위한 VO 구성 정보는 다음 표 2와 같은 정보로 구성되어 있다.

그리드 VO 구성을 위한 자원 정보는 해쉬와 메시지 다이제스트 과정을 거쳐 검증을 위한 값을 생성한다. XML 정자 서명과정에서는 자원 정보를 VO 구성을 위한 요청자의 개인키로 암호화하여 전자서명을 생성하고, 검증을 위한 요청자 인증서를 <KeyInfo>로 포함한 XML 서명 문서를 생성한다.

표 2. 그리드 VO를 구성하기 위한 자원 정보

<그리드 VO 정보>	: 그리드 VO를 구성하기 위한 자원 정보
<자원 정보>	: 구성 자원의 개요
<구성 시스템 정보>	
벤더	: VO 구성 시스템의 기종 및 제조업체
운영체제	: 각 자원이 속한 시스템의 운영체제
<CPU 개수>	: 그리드 VO를 구성하고 있는 CPU의 총 개수
<메모리 총량>	: 그리드 VO를 구성하고 있는 메모리의 총량
<보조기억 장치>	: 그리드 VO를 구성하고 있는 보조기억장치의 총량
<데이터베이스>	: 그리드 VO에서 접근할 수 있는 데이터베이스 목록
<보안 정책>	
인증 시스템	: 그리드 VO를 위한 인증 메커니즘
보안 정책 레벨	: 그리드 VO를 위한 보안 정책 레벨
<기타 정보>	: 기타 필요 정보

이와 같은 과정을 통하여 그리드 VO 인증을 요청하기 위한 XML 서명 문서를 생성하기 위한 과정은 다음과 같이 요약할 수 있다.

① 그리드 VO 구성을 위한 자원 정보를 수집하여 문서를 생성한다.
② 작업 요청자의 개인키로 서명하고 검증을 위한 다이제스트 값을 첨부한다.
③ 서명 검증을 위한 공개키 정보는 작업 요청자의 인증서를 포함한 <KeyInfo>를 생성한다.
④ 전체 과정 값을 포함한 XML 서명 문서를 생성한다.

(2) XML 서명 검증 모듈

XML 서명 검증 모듈은 VO 인증서 요청을 위해 전송되어진 XML 문서를 검증하고 요청된 그리드 VO 자원 정보를 추출하기 위한 모듈로 그림 4와 같은 과정을 거쳐 인증서 생성을 위한 자원 정보를 취득하게 된다.

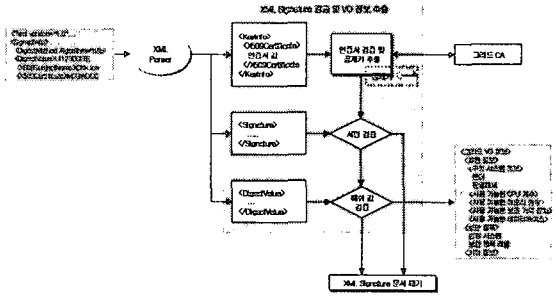

그림 4. XML 서명 검증을 통한 그리드 VO 자원정보 획득

그리드 VO 구성을 위한 도메인에서 전송되어진 XML 서명 문서는 XML 파서를 거쳐 각부분의 태그 정보로 분리한 후 각각의 검증 과정을 거쳐 VO 구성을 위한 자

원 정보를 추출하게 된다. 그리드 VO 정보를 취득하기 위한 과정은 다음과 같이 요약할 수 있다.

① XML 서명 문서를 XML 파서를 통하여 각 정보부분 태그로 분리한다.

② <KeyInfo> 태그에 포함되어 있는 인증서의 유효성 여부를 그리드 CA를 통하여 확인하고 공개키 값을 획득한다.

③ XML 서명 문서에 포함되어 있는 서명값을 복호화하여 서명을 검증한다.

④ XML 서명 문서에 포함되어 있는 다이제스트 값과 서명 검증을 통해 생성된 값의 해쉬값을 비교하여 무결성 여부를 검증한다.

⑤ 그리드 VO 자원 정보를 획득한다.

(3) 인증서 요청 메시지 생성 모듈

인증서 요청 메시지 생성 모듈은 그리드 CA에 그리드 VO 도메인에 대한 인증서를 요청하고, 생성된 인증서를 획득하기 위한 모듈로 그리드 VO 인증 모듈과 그리드 CA 사이의 통신을 담당하게 되며, 그림 5와 같은 세부 모듈로 구성되어 있다.

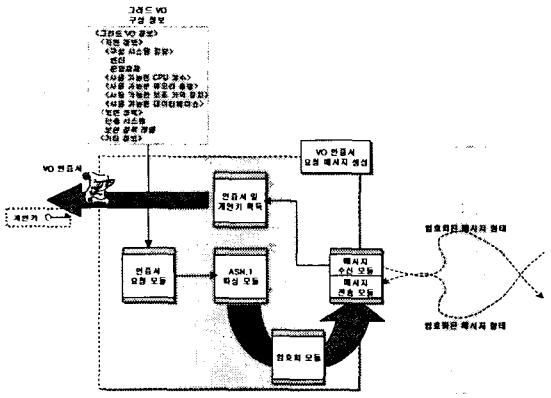

그림 5. 인증서 요청 메시지 생성 모듈의 동작

위 그림에서 VO 인증서 요청 메시지 생성 모듈을 구성하고 있는 각 세부 모듈에 대한 설명은 다음과 같다.

① ASN.1 파싱 모듈 : 인증서를 생성하기 위한 정보를 국제 표준규약인 인증서 요청 메시지 형식으로 구성하기 위한 데이터 구조 생성 모듈

② 암호화 모듈 : 생성된 인증서 요청 정보에 대한 보안 서비스를 위하여 암호화 된 데이터를 생성하기 위한 모듈

③ 메시지 송/수신 모듈 : 그리드 CA와의 데이터 교환 창구의 역할을 수행하는 모듈

④ 인증서 및 개인키 획득 모듈 : 그리드 CA에서 그리드 VO 도메인에 대해 생성한 인증서와 개인키 값을 획득하여 이를 VO 도메인에게 전송하기 위한 모듈

4. 그리드 VO 인증 시스템 적용 사항 및 비교 분석

4.1 그리드 VO 인증 시스템 적용

(1) 그리드 VO 인증 요청을 위한 XML 서명 파일 생성

그림 6은 본 논문에서 제안한 시스템을 적용하여 생성한 그리드 VO 인증 요청을 위한 XML 서명 문서의 생성 예제이다. XML 서명 문서의 태그 중에서 <DigetValue>는 그리드 VO 구성을 위한 자원 정보에 대한 무결성을 검증하기 위한 메시지다이제스트 값을 포함하며, <SigatureValue>는 자원 정보를 VO 구성 요청자의 개인키로 암호화한 서명값을 포함하여 실제 그리드 VO 자원 정보를 획득할 수 있는 값을 포함한다. 마지막으로 <KeyInro>에서는 서명 검증을 위한 요청자 인증서 정보를 포함하여 전체적인 XML 서명 문서를 생성하게 된다.

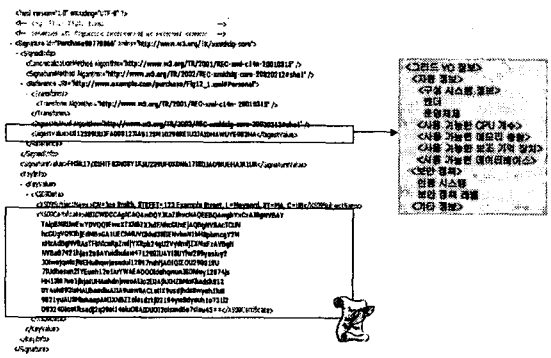

그림 6. 그리드 VO 인증 요청을 위한 XML 서명 문서 예

(2) 그리드 VO 인증서 생성

본 논문에서 제안한 그리드 VO 인증 시스템의 최종 결과는 VO에 대해 발행된 인증서이다. 발행된 인증서는 그리드 VO를 통한 작업이 종료되면 폐기되는 임시적인 인증서로 그리드 미들웨어에서 사용자 인증서를 통하여 생성한 프록시 인증서(사용자 인증을 위한 임시 인증서)와 동일한 성격을 지니게 된다.

그리드 VO 인증서는 그림 7과 같이 X.509 v3 형식으로 발행되며, 유효기간이 짧게 발행된다. 또한, 그리드 VO 자원 정보를 위한 확장 필드를 둠으로써 구성된 그리드 VO 도메인에 대한 자원 정보, 보안 정보 등을 포함하게 된다.

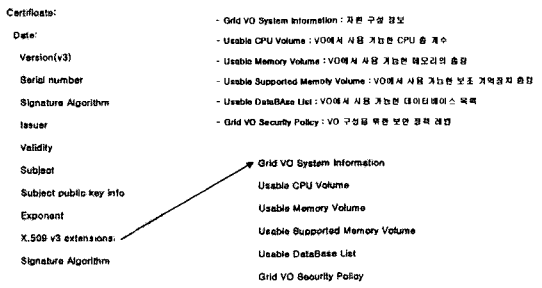

그림 7. 그리드 VO 인증서의 필드 형식

4.2 비교 분석 및 평가

본 논문에서 제안한 그리드 VO 인증 시스템은 수행 속도, 알고리즘 등의 계량적인 비교 할 수 있는 시스템이 구축되어 있지 않다. 현재 그리드 포럼에서 논의되고 있는 그리드 VO는 구성을 위한 자원 정보의 유무, OGSA 기반의 구성 측면 등에서 기초적인 논의만 진행되고 있으며, 실제 국내에서 구축되고 있는 K*Grid에서도 VO 구성을 위한 세부 사항을 독자적으로 추진하고 있는 상황이다.

따라서, 본 논문에서 제안한 시스템은 기존 그리드를 구성하기 위한 기본 인증 시스템과의 지원 기능 및 사용 알고리즘, 제공 서비스 등의 기능을 중심으로 비교 분석하고 이를 평가한 후 <표 3>과 같은 결과를 산출하였다.

표 3. 기존의 그리드 인증 서비스와의 비교 분석 결과

시스템 / 지원 기능	기존의 그리드 인증 시스템	제안된 그리드 인증 시스템
미들웨어 기반	Globus 3.0	Globus 3.0
암호 라이브러리	OpenSSL	Bouncycastle, OpenSSL
사용자 인증 서비스	인증서에 의한 인증	인증서에 의한 인증 프록시 인증서 생성에 의한 임시 인증
그리드 VO 인증 서비스	지원하지 않음	VO 인증서 생성에 의한 임시 인증
OGSA 지원 여부	지원하지 않음	웹 서비스 지원 XML Signature 문서 생성 그리드 VO 구성
보안 메커니즘	PKI	PKI, XML 정보보호기술 WS-Security
서버 클라이언트	지원하지 않음	지원함

5. 결론

그리드 VO는 동적으로 변화되는 시스템 자원에 대한 정보를 모아 하나의 자원 그룹으로 묶어 사용자에게 제공하는 개념적인 도메인 그룹으로 볼 수 있다. 그리드에서 부각하고 있는 이 기종 시스템간의 자원을 하나의 구성 요소로 묶어 제공하는 그리드 VO는 기존 시스템에서 발생할 수 있는 보안 문제와 다르게 상호호환성, 신뢰관계, 자원 통합 및 인증, 보안 정책 등에서 많은 문제를 일으키게 되는데, 그리드 보안 그룹에서는 이것을 OGSA Securtiy Roadmap의 제안을 통하여 해결하고자 하는 연구를 진행하고 있다.

본 논문에서는 OGSA에서 요구하고 있는 보안 요구사항을 살펴보고, XML 정보보호기술의 적용을 통하여 OGSA Security Roadmap의 인증 서비스의 한 방안을 구체적으로 제안하였으며, 이를 모델링 하였다. 본 논문에서 제안하고 있는 VO 인증 시스템은 동적으로 변하는 자원의 상황에 맞추어 VO 자체에 대한 인증 서비스를 수행할 수 있으며, 사용자에게 자원에 대한 VO를 효과적으로 제공할 수 있다.

추후 본 논문은 제안된 시스템을 바탕으로 추가적인 서비스 모델링과 실제 구축을 통하여, 실제 국내에 구축되고 있는 K*Grid에 VO 인증 서비스를 적용하는 것이 향후 연구과제이다.

[참고문헌]

[1] 강 경우, 박형우, "그리드 연구개발 동향", 한국정보과학회지, 제 20권 제2호 pp.27, 2002.2

[2] 윤찬현, 심은보, "그리드 구조 및 연구동향", 한국정보과학회지, 제 20권 제2호 pp.13, 2002.2

[3] 김학두, 김진석, "그리드 미들웨어 : 자원 관리 및 원격 데이터 접근 기술 동향", 한국정보과학회지, 제20권 제2호 pp.35~39, 2002.2

[4] "Grid Security Infrastructure Working Group", http://www.grid- forum.org/2_SEC/GSI.htm

[5] GGF. "OGSA Security Roadmap", Draft 1.3, July 2002

[6] GGF. "The Security Architecture for Open Grid Services", Draft 1. July 2002

[7] 문기영외 1명, "XML 정보보호 개요", 2003. 정보처리학회 학회지, vol.10, No.2.