제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

웹서비스 기술을 이용한 그리드 인증서 및 키관리 시스템 개발

김상완*, 박형우*, 이상산*, 김종**
*KISTI 슈퍼컴퓨팅센터, *포항공과대학교
e-mail:
{sangwan, hwpark, sslee}@hpcnet.ne.kr, jkim@postech.ac.kr

Development of Certificate and Key Management System Using Web Service Technology

Sang-Wan Kim, Hyung-Woo Park, Sang-San Lee
KISTI Supercomputing Center

요 약

현재 그리드 컴퓨팅 툴킷으로 사용되고 있는 Globus는 PKI (Public Key Infrastructure) 기반의 인증방식을 이용하고 있다. PKI 인증방식은 통합 인증 기능(Single Sign-On)을 구현하기에 적당하지만, 그리드에 참여하는 수많은 컴퓨터와 사용자들의 공개키 인증서(public key certificate)를 발급하고 관리해야하는 부담이 따른다. 본 연구에서는 인증기관이 사용자에게 인증서를 발급하고, 인증서를 관리하는 과정을 자동화 해 줄 수 있는 시스템을 개발하고, 다양한 클라이언트에 서비스 제공을 위해 웹서비스를 통한 인터페이스 기능을 새로 추가하였다.

1. 서론

그리드(Grid)[2]란 다양한 기관에 걸쳐 분산되어 있는 다양한 종류의 컴퓨팅 자원을 네트웍을 이용하여 보다 효율적으로 사용하는 컴퓨팅 방식이다. 그리드 서비스를 가능하게 해주는 그리드 미들웨어에 대한 연구가 활발하게 이루어지고 있으며 미국의 ANL에서 개발된 Globus[3]는 현재까지 개발되어 있는 그리드 미들웨어 중 가장 널리 이용되고 있다.

Globus에서는 계산 자원의 서비스 요청에 대한 인증을 PKI(Public Key Infrastructure)[4] 방식을 이용하고 있다. 따라서 사용자와 컴퓨터, 또는 컴퓨터와 컴퓨터간에 상호인증을 위해서 모든 사용자와 컴퓨터에 공개키 인증서를 발급하여야 한다. 따라서 인증기관은 인증서와 키를 체계적으로 발급, 관리, 갱신, 폐기할 수 있는 시스템을 가지는 것이 중요하다. [1]에서는 Globus 설치과정에서 컴퓨터 및 사용자의 인증서 발급 및 관리를 편리하게 할 수 있게 해 주는 웹기반 도구를 개발하였다. 본 연구에서는 이 기존 연구에서 개발된 웹기반 인증서 관리 시스템을 확장하여 사용자의 웹을 통한 인터페이스 뿐만 아니라, 다양한 클라이언트와 상호 작용할 수 있도록 웹서비스 모듈을 확장하여 보다 편리하게 인증서를 발급하고 갱신할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 제2절에서는 Globus의 설치시에 인증서를 발급받는 절차에 대해서 기존에 이용하던 방법에 대한 설명과 개선점에 대해서 이야기하고, 제3절에서는 본 연구에서 개발된 웹서비스 기술을 이용한 인증서 및 키관리 시스템에 대해서 설명한다. 마지막으로 제4절에서는 향후연구 방향과 결론으로 끝을 맺도록 한다.

2. 기존의 인증서 발급 절차

Globus를 개발한 ANL에서는 인증서 발급 및 신청을 이메일을 통해서 처리하고 있다. Globus 사용

자는 Globus 설치과정에서 grid-cert-request 라는 명령을 실행하여 자신의 홈 디렉토리아래에 인증요청서와 개인키를 생성시키고, 인증요청서를 이메일로 인증기관으로 보낸다. 인증기관에서는 사용자의 신원 확인을 하고, 인증서를 발급하여 다시 돌려주면, 사용자는 받은 인증서를 홈디렉토리에 복사하여 설치하는 과정을 거치게 된다. 인증기관에서는 사용자 신원 확인시에 CSR(Certificate Signing Request) subject의 도메인명과 이메일을 보낸 사람의 메일주소 도메인을 비교하여 일치될 경우에만 인증서를 발급해 주고 있다. 그림1은 이 과정을 그림으로 나타낸 것이다.

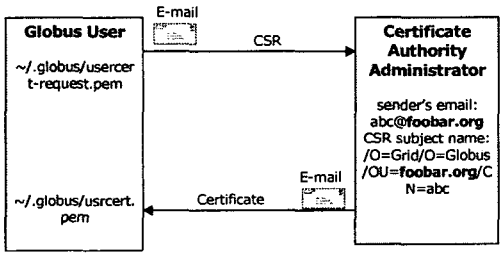

그림1. Globus 인증서 발급과정

웹기반 인증서 관리 시스템([1])을 이용할 때는 Globus 사용자나 인증기관이 CSR이나 인증서의 내용을 이메일로 보내지 않는다. 사용자는 웹사이트에 접속하여 자신의 CSR을 업로드하여 등록하고, 업로드된 CSR의 ID번호를 인증기관에게 알려주면 된다. 그러면 인증기관은 인증서를 만들고 데이터베이스에 저장한 다음 저장된 인증서의 ID만 다시 사용자에게 이메일로 보내준다. 사용자는 발행된 인증서를 다운로드하여 홈디렉토리에 설치하면 된다. 그림2는 이 과정을 그림으로 나타낸 것이다.

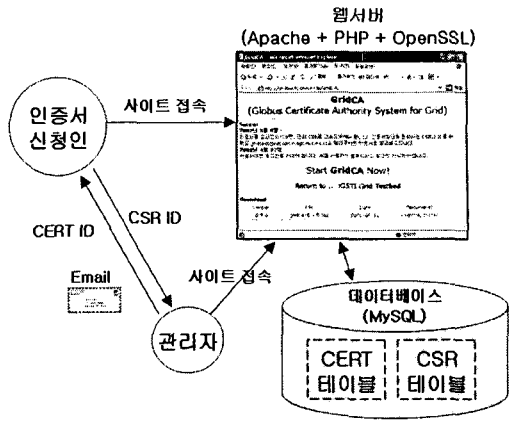

그림2. 웹기반 인증서 관리도구를 이용한 인증서 발급과정

그러나 이 시스템을 이용할 경우에도 인증서 발급 과정에서 사용자가 이메일을 보내고 받는 과정이 필요하고, 사용자가 직접 인증서 파일을 편집해야 하는 불편함이 따른다.

3. 웹서비스 기술을 이용한 인증서 관리도구

그리드의 Single Sign-On 기능을 구현하기 위해 Globus에서는 PKI를 이용하고 있고, 따라서 컴퓨터와 사용자의 인증서를 만들어 사용하고 있다. 이렇게 발행된 인증서를 체계적으로 관리하기 위해서 필요한 요구사항들을 정리 해보면 다음과 같다.

1) 인증기관은 자신이 발행한 인증서에 대한 정보를 계속 유지하고 있어야 한다.
2) 인증서의 유효기간이 만료되면 사용할 수 없기 때문에, 발행된 인증서를 갱신하여 유효기간을 연장할 수 있어야 한다.
3) 사용자가 인증기관과 정보를 주고받는 과정에서 이메일을 주고받는 등 발급과 갱신과정에서 사람이 개입되는 것을 최소한으로 막는다.
4) 인증기관은 발급된 인증서 중 사용기간 만료가 가까워온 인증서에 대해서 만료전에 사용자에게 통보를 해 주어야 한다.

이러한 요구사항에 비추어 볼 때 [1]에서 개발된 웹

기반 인증서 발급 시스템을 개선해야할 필요성이 있어 본 연구에서는 그 기능을 보강하고, 추가로 웹서비스 기술을 이용하여 사용자가 인증서를 따로 설치해 주어야 하는 불편함을 줄였다.

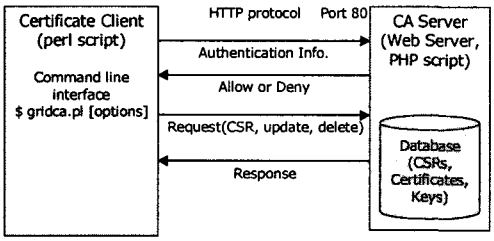

그림3. 웹서비스 기술을 이용한 인증서 및 키관리 시스템 구성도

그림3은 본 연구에서 개발된 시스템의 동작 과정을 그림으로 나타낸 것이다. CA 서버(CA Server)는 기존의 웹기반 인증서 관리 시스템으로써 웹서버와 CSR 및 인증서를 보관하기 위한 데이터베이스로 이루어져 있다. 인증서 클라이언트(Certificate Client)는 펄(perl) 언어로 작성된 스크립트 언어이며, HTTP 프로토콜을 이용하여 CA서버의 특정 페이지에 접근하여 인증서의 발급과 갱신 등에 대한 요청을 하고, 응답을 받도록 하고 있다. 그림4는 클라이언트에서 CA 서버 접속에 필요한 정보를 설정하기 위한 부분이다.

```
my $service = "http://gridtest.
 hpcnet.ne.kr/GridCA/GridCA/service.php";
```

그림4. 서비스 접속을 위한 서버의 정보 설정

위에서 알 수 있듯이 클라이언트는 HTTP프로토콜을 이용하여 http://gridtest.hpcnet.ne.kr/GridCA/GridCA/service.php 라는 URL로 접속하도록 되어 있다. 서버는 데이터베이스와 연동 등을 위하여 웹 프로그래밍 언어로 많이 사용되고 있는 PHP로 작성되어 있다. 클라이언트의 서버에 대한 요청은 HTTP프로토콜의 POST method를 통하여 이루어진다. 클라이언트의 요청은 사용자 인증을 필요로 하는데, 이때 기존의 웹기반 시스템에 사용자등록을 할 때 사용자 정보가 전달된다.

사용자는 클라이언트에 설치된 gridca.pl 이라는 명령어를 통하여 모든 서비스를 받을 수 있으며, 인증서 발급, 갱신, 삭제, 열람이 가능하다. 현재 제공되는 기능은 다음과 같다.

1) 인증요청서 생성기능 : 인증서 발급에 필요한 정보를 입력하여 인증요청서를 생성할 수 있다.
2) 인증요청서 업로드 기능 : 이미 만들어진 인증요청서를 인증기관의 데이터베이스에 등록시킬 수 있다.
3) 임시 인증서 자동 발급 기능 : 유효기간이 짧게 제한되어 있는 임시 인증서를 발급받을 수 있다. 임시 인증서의 유효기간은 1주일이다.
4) 정식 인증서 발급 신청기능 : 정식 인증서는 인증기관 관리자의 검토후에 발급된다. 정식 인증서로 발급을 신청하면 자동으로 관리자에게 이메일로 통보된다.
5) 발급된 인증서 다운로드 기능 : 데이터베이스에 저장된 발급된 인증서와 키를 다운로드 할 수 있다.
6) 인증기관의 인증서 다운로드 기능 : 인증기관의 인증서를 다운로드받을 수 있다.

4. 향후연구 방향 및 결론

향후 연구 방향으로 클라이언트와 서비스 제공자 사이에 보다 표준화된 통신 방법으로 XML형식을 사용될 것이다. XML은 유사한 서비스를 제공하는 다양한 인증기관과 다양한 클라이언트들이 통일된 방법으로 통신할 수 있게 할 것이다. 아직은 내부적으로 규격화된 방법을 사용하고 있지 않다.

두번째 향후연구 방향으로써 인증서의 상태에 대한 정보를 질의해 보기 위한 OCSP[5] 프로토콜이 IETF(Internet Engineering Task Force)에 의해서 표준화 되어있다. 본 연구에서 개발된 시스템을 조금 확장함으로써 이러한 OCSP 응답자(responser)로 동작하도록 만들 수 있을 것이다.

마지막으로 서버와 클라이언트 사이에 통신을

SSL(Secure Socket Layer)과 같은 프로토콜로 암호화시키는 연구가 필요하다. 현재는 사용자 인증에 필요한 사용자명과 비밀번호가 암호화 없이 그대로 전송된다.

결론으로, 본 연구에서는 그리드 환경에서 PKI를 사용하기 위해 필요한 인증서 및 키관리 시스템을 구현하고 확장하였다. 본 연구에서 만들어진 시스템은 그리드 환경 뿐만 아니라 일반적인 PKI 시스템에 사용이 가능하다. 또한 기존의 웹기반 시스템에 웹서비스 기능을 추가함으로써 다양한 클라이언트에서 인증서 발급등의 서비스를 이용할 수 있도록 하였다.

참고문헌

[1] 김상완, 박형우, 이상산, "웹기반 그리드 인증서 및 키관리 시스템의 개발", 한국정보처리학회 2002년 춘계학술발표대회, 2002년 4월

[2] I. Foster and C. Kesselman, "The Grid: Blueprint for a New Computing Infrastructure", Morgan Kaufmann, 1998

[3] The Globus Project, http://www.globus.org

[4] Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997

[5] Myers, et al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999