

인증서 기반 전자도서관 인증과 인가

원형석⁰, 김태성, 조영섭, 진승현

한국전자통신연구원

(moho⁰, taesung, yscho, jinsh)@etri.re.kr

Certificate-based Digital Library Authentication and Authorization Architecture

Hyung Suk Won⁰, Taesung Kim, Yeongsub Cho, Seunghun Jin

Electronics and Telecommunications Research Institute

요약

전자도서관은 기존의 자료 및 새로운 디지털 자료들을 웹을 통해 사용자에게 제공하고 있다. 하지만 웹을 통해 디지털 자료에 대한 서비스를 제공하고자 할 때 기존의 오프라인 도서관 서비스와는 달리, 많은 계약조건과 사용자의 접근 제어 방법을 도입하지 않아 대부분의 디지털 자료들에 대한 서비스가 매우 제한적으로 이루어지고 있다. 이것은 기존의 오프라인 도서관에서 사용하는 인증인가 방식을 전자도서관에 그대로 사용하고 있기 때문에 발생하는 문제이다. 이에 본 논문은 전자도서관에서 웹을 통해 디지털 자료를 서비스 할 때, 인증서를 통한 강화된 인증인가가 필요한 이유를 설명하고, 이를 해결하기 위하여 기존에 제안된 인증서 기반 인증 인가 모델을 살펴본다. 그리고 기존 모델의 문제점들을 보완한 인증서 기반의 인증인가 구조를 제시하고 향후 전자도서관 인증인가 모델 개발에 필요한 과제들을 제시한다.

1. 서론

이용자에게 보다 나은 자료와 정보를 제공하기 위해 전자도서관 구축 사업이 정부, 연구기관, 대학을 중심으로 활발하게 진행되었다. 하지만 이렇게 구축된 디지털 자료를 사용자에게 제공할 때 서비스가 매우 제한적으로 이루어지고 있다. 이러한 문제는 기존의 오프라인 도서관에서 사용하던 인증 인가 방식을 그대로 사용하고 기관간의 자료 이용을 고려하지 않은 결과이다. 외국에서는 이러한 문제를 해결하기 위해 다양한 연구가 진행되고 있지만 국내에서는 미흡하다. 따라서 본 논문에서는 전자도서관에서 인증서 기반의 인증인가가 필요한 이유를 설명하고 기존 연구결과를 바탕으로 현재 국내 전자도서관에 적용 가능한 모델을 제시하고자 한다.

2. 전자도서관의 인증인가 필요성

현재 이용자가 전자도서관에서 웹으로 디지털 자료를 이용하고자 할 때 여러 가지 제한 사항이 있다[1]. 예를 들어, 전자도서관에서 제공하는 전자저널과 같이 외부의 자료 제공 사이트에 접속해서 이용자가 자료를 얻고자 할 때 자신이 서비스 대상에 소속된 기관의 소속자라 하더라도 사용자가 물리적으로 기관 내부에 있지 않을 때는 이용이 불가능하다. 자체 구축한 디지털화된 자료에 대해서도 마찬가지 상황이다. 또한 자신이 소속된 기관 외의 디지털 자료에 접근하는 것은 원천적으로 불가능하다. 외부 기관의 자료에 접근하기 위해서는 기존 오프라인 방식처럼 사용자가 외부기관을 방문하여 신분을 확인 받은 후, 그 기관에서 아이디와 패스워드를 발급 받아야 사용이 가능해진다. 하지만 앞서의

자신이 소속된 기관의 경우와 마찬가지로 이용자가 물리적으로 사용하고자 하는 기관 외부에 있을 경우, 자료에 접근 할 수 없다.

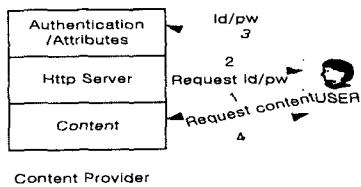
이것은 원격이용이 가능하고 이용시간의 제한을 받지 않고 여러 사람이 동시에 이용하도록 한다는 전자도서관 구축의 기본 취지에 어긋나는 것이다[2]. 이러한 제한 사항은 앞서 언급한 바와 같이 자료의 라이선스나 저작권 등의 이유와 자료제공자가 접속하는 기관 소속의 사용자의 인증인가를 제어할 수 없기 때문에 비롯된 것으로 모든 전자도서관에 해당되는 사항이다. 이러한 전자도서관의 서비스나 자료에 대한 적절한 이용을 가능하게 하기 위해서는 디지털 자료에 대한 인증인가 모델이 필요하다. 또한, 한 기관의 자료는 한정되어 있으므로 보다 나은 서비스를 위해서 그리고 기관별로 구축된 디지털 자료를 효율적으로 이용하기 위해서는 타 기관과의 연계 서비스가 필요하다. 이를 위해서 전자도서관 간의 인증인가가 필수적이다.

3. 기존의 인증인가 방식

기존의 인증인가 방식은 아이디/패스워드 방식, IP 방식, Proxy 방식 등으로 분류할 수 있다[3][4]. 각각의 방식들은 장단점을 가지고 있다. [그림 1]은 현재 전자도서관의 일반적인 인증인가 과정이다.

사용자가 필요한 자료에 접근시 기관에 부여된 아이디와 패스워드를 제시하거나 별도의 아이디 패스워드 제시 없이도 사용자의 IP주소만을 확인한 후 제공여부가 결정된다. 대부분의 현재 전자도서관의 제공형태가 여기에 속한다. 또한 인증과 인가가 특별한 구분 없이 혼재되어 있는 형태이다.

이처럼 자료에 대한 사용자의 접근시 인증인가에 대한 매커니즘이 전혀 존재하지 않기 때문에 자료제공자는 기관 밖에서나 이용자에 따른 맞춤 서비스를 사용자에게 제대로 서비스 하지 못하고 있는 것이다. 자료 제공자간과 자료제공자와 이용자 사이에 서로 신뢰하는 인증과 인가에 대한 과정이 제공될 때 이러한 서비스가 가능하게 된다.



[그림 1] 기존 전자도서관 인증인가 모델

4. 인증서 기반 인증인가 모델

4.1 인증서

인증서(certificate)란, 오프라인에서 운전면허증과 같이, 인터넷 상에서 공개키와 비밀키를 통한 암호화를 이용하여 개인이나 기관의 신분을 확인하는 데 이용되는 전자 보증서이다. 인증서를 이용하는 방식은 최근에 많이 연구되고 있는 방식이다. 인증서 방식은 가장 최근의 기술로서 모든 웹 브라우저에서 지원되고 지금까지 가장 보안이 뛰어난 방식으로 인정받고 있다.

하지만 아직까지 인증서 발급과 관리가 복잡하고, 도서관에서 아직까지는 널리 사용되지 않고 있고, 도서관의 공용 컴퓨터에 인증서가 남아있게 되면 문제가 있고, 폐기된 인증서를 다루는데 취약하고, 일반적으로 긴 유효기간을 가지는 등의 문제점을 가지고 있다.

4.2 기본조건

일반적으로 기관간 전자도서관의 인증인가 모델에서 다음의 내용들을 고려사항으로 제시하고 있다[3].

- (1) Privacy : 소속기관 외에 아이디를 포함한 어떤 개인정보도 서비스를 제공하는 사이트에 제공되지 않아야 한다.
- (2) Partitioning of information : 만약 정보의 공유가 필요할 때라도 그 중복을 최소화해야 한다. 아이디 대신 pseudo anonymous identity를 사용해야 한다.
- (3) Separation of authentication and authorization : 개인의 신분과 권한이 계속 변화하기 때문에 변화에 맞게 인증과 인가가 따로 분리되어 운영되어야 한다.

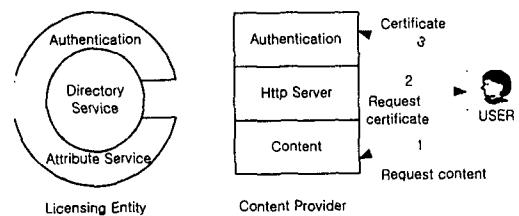
4.3 기존 인증서 기반 인증인가 모델

현재까지 행해진 기존 연구들에서 인증서를 사용하는 모델로 제시된 것들을 살펴보자 한다.

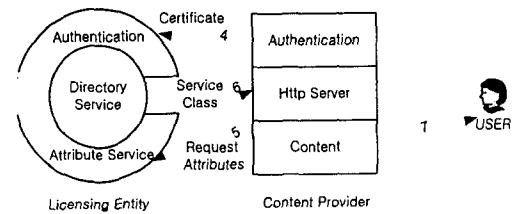
첫째 모델은, 사용자가 자료에 접근시, 웹서버는 개인의 인증서를 이용하여 개인을 인증하고 개인의 권한을 권한내용이 저장되어 있는 디렉토리에서 확인하여 자료 접근권한을 웹서버에 다시 알려주면 권한에 따라 웹서버는 자료에 접근을 시도한 사용자에게 가능한 서비스를 하는 과정을

거친다[5][6]. 그 절차는 [그림 2] [그림 3]의 번호 순서대로 진행되고, 각각의 과정의 자세한 설명은 다음과 같다.

1. 사용자가 웹을 통해서 원하는 자료에 접근을 시도한다.
2. 웹서버가 사용자에게 인증서를 요구한다.
3. 사용자가 인증서를 제공한다.
4. 인가에 필요한 정보를 인증서에서 추출한다.
5. 웹서버가 Attribute server에 연결하고 서버의 인증서를 제시하면 attribute server는 요청 서버를 확인하고 요청한 서버의 자료에 대한 사용자의 권한을 결정한다.
6. 접근 권한이 요청 서버에게 리턴된다.
7. 웹서버는 사용자에게 부여된 권한을 가지고 접근을 허가한다.



[그림 2] 인증서 이용 모델 (1)

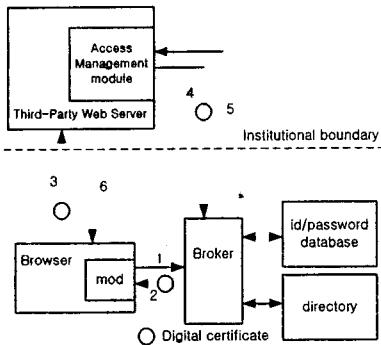


[그림 3] 인증서 이용 모델 (2)

하지만 이 모델은 접근하고자 하는 곳에 인증서를 사용자가 제공함으로써 사용자의 익명성이 보장되지 않으므로 모델 기본 조건 (1), (2)를 만족시키지 못한다.

둘째 모델은 소속기관에서 아이디/패스워드 확인 후 일시적인 인증서를 발급 받은 후 접근하고자 하는 곳에 인증서를 제시한다. 그러면 인증서를 발급한 곳에 인증을 요구하면 인증한 뒤 사용자가 가진 attribute를 들려주게 된다. 그 인증 결과와 attribute에 따라 자료 접근 유무를 판단하여 서비스하게 된다[7]. 이 과정은 [그림4]에 나타나 있다.

앞에서 살펴본 바와 같이 인증서는 여러 장점이 있는 반면, 인증서 방식을 도입할 때 폐기목록 관리, 실시간 인증 등의 여러 문제가 존재하고 있다. [그림4]의 모델은 일시적인 인증서를 사용하여 이러한 문제를 해결하고자 한다. 또한 이 방식은 기존의 아이디/패스워드 방식에 도입하기가 가장 간편한 방법이다. 기존의 시스템에 인증서를 발급하고 확인하는 기능만 추가하면 된다. 하지만 일시적인 인증서의 경우, 그 유효기간에 대한 적절한 연구가 필요하고, 자료를 접근하기 전에 반드시 자신이 속한 기관의 아이디/패스워드를 이용한 인증을 통해 인증서를 받은 후 외부 자료 접근이



[그림 4] 인증서 기반 인증인가 모델

가능하다. 이 방식은 여전히 기관 내부의 인증을 기존의 문제점을 그대로 가지는 아이디/패스워드 방식으로 한 후에 인증서를 발급하는 것이므로 인증서의 강한 인증을 제대로 사용한다고 볼 수 없다. 이러한 문제를 해결하기 위해 다음의 수정된 인증서 기반 모델을 제시하고자 한다.

4.4 수정된 인증서 기반 인증인가 모델

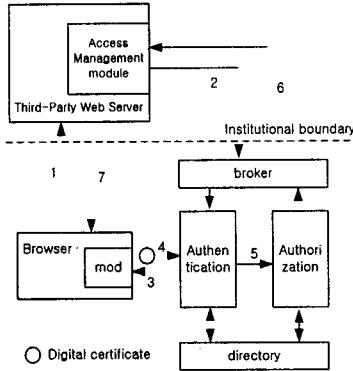
본 논문에서 제안하는 인증서를 기반으로 하는 인증인가의 모델은 [그림5]와 같고 다음과 같은 과정으로 진행된다.

0. 사용자가 등록기관을 통해 인증서를 발급 받는다.
1. 사용자가 웹을 통해서 원하는 자료에 접근을 시도한다.
2. 웹서버가 사용자가 속한 기관의 인증서버에게 인증을 요구한다.
3. 인증서버가 사용자에게 인증서를 요구한다.
4. 사용자는 자신의 인증서로 검증 받는다.
5. 인가 서버가 사용자의 attribute를 제공한다.
6. 브로커가 인증 결과와 사용자의 attribute를 인증을 요청한 서버에게 돌려준다.
7. 인증결과와 attribute를 기반으로 한 인가과정을 통해 사용자에게 자료에 대한 접근 권한을 부여한다.

여기서 제시한 모델과 앞서 살펴본 두 모델과의 차이는 인증서를 사용하는 원래 목적인 강한 인증을 위해 일시적인 인증서는 사용하지 않았고 인증과 인가를 분리하고 인증과 인가를 자신이 소속된 기관에서 하게 함으로써 익명성과 privacy를 강화한 것이다.

제시될 모델은 [그림4]의 모델처럼 일시적인 인증서를 사용하는 것이 아니므로 인증서 관리와 운용에 문제가 있을 수 있다. 하지만 현재 이와 같은 문제점을 해결하기 위한 방안들이 활발히 제안되거나 적용되고 있으며 인증서를 이용하게 되면 강한 인증을 통한 시스템 보안 강화 외에도 아이디 관리 업무 효율성 증가, 강한 인증을 통한 외부 기관과 연결 서비스의 용이성 증가 등의 이점을 얻을 수 있다. 기존의 경우, 타 기관 이용을 위해서 직접 사용자가 타 기관 방문 후 신분과 소속기관 확인 후 아이디 패스워드를 발급 받았지만, 자신이 속한 기관의 인증 후 타 기관의 자료를 웹으로 이용할 수 있게 된다. 이러한 점들이 PKI(Public Key Infrastructure: 공개키 기반구조) 기반의 인증서를 전자도서관의 인증인가에

적극적으로 도입하려는 이유이기도 하다.



[그림 5] 수정된 인증서 기반 인증인가 모델

5. 향후 과제 및 결론

본 논문에서는 전자도서관에서 디지털 자료를 서비스하기 위해 인증인가가 필요한 이유를 설명하고 이 문제를 해결하기 위해 기존의 연구결과를 바탕으로 인증서를 기반으로 한 기존 인가인가 모델들을 살펴보고 기존 모델들의 문제점들을 보완한 수정된 인증인가 모델을 제시하였다. 앞에서 살펴본 바와 같이 현재까지 여러 인증 방법이 있으나 자료제공자나 이용자 양쪽이 모두 동의할 만한 방식은 PKI(Public Key Infrastructure: 공개키 기반구조)를 기반으로 하는 인증서 방식이다. 또한 국내에서도 인증서를 기반으로 하는 안전한 정보보호 기반 구축과 이에 따른 연구가 활발하다. 따라서 웹을 기반으로 하는 전자도서관의 인증인가 시스템도 인증서를 기반으로 하는 것이 향후 발전될 기술을 적극적으로 도입할 수 있는 토대가 될 것이다. 또한 체계적인 서비스와 관리를 위해서는 인가에 대한 기술도 연구 및 적용이 시도되어야 한다.

참고문헌

- [1] 원형석, 김태성, 조상래, 진승현, “전자도서관 인증과 인가에 대한 연구”, 한국정보처리학회 추계학술발표대회 논문집, 제 9 권, 제 2 호, 2002.
- [2] http://www.lg.or.kr/lg_docs/index330.html
- [3] David Millman, “Cross-Organizational Access Management: A digital library authentication and authorization architecture”, D-Lib magazine, vol.5, no.11, 1999.
- [4] Clifford Lynch, “A White paper on authentication and access management issues in cross-organizational use of networked information resources”, Coalition for Networked Information, Apr. 1998.
- [5] Digital Library Federation (DLF) and Corporation for Research and Educational Networking (CERN), “Digital certificate infrastructure (FAQ)”.
- [6] Digital Library Federation (DLF), “A digital library authentication and authorization architecture”, 2000.
- [7] Ariel Glenn and David Millman, “Access management of web-based services: An incremental approach to cross-organizational authentication and authorization”, D-Lib Magazine, Sep. 1998.