국가자격 인증기반 구축을 위한 인증서 발급모델 연구

박배효*, 윤재호*, 이석래*
*한국정보보호진흥원(KISA) 인프라보호단
e-mail : parkbh@kisa.or.kr

A Study on Accredited certificate issuance on authentication infrastructure of national licence

Bae-Hyo Park*, Jae-Ho Yoon*, Seok-Lae Lee*
*Information Infrastructure Security Division,
Korea Information Security Agency(KISA)

요 약

디지털홈 서비스는 기존 PC에서 제공하던 서비스와 차별화된 서비스를 실용화 하지 못하고 있는 이유 중에 하나는 오프라인에서 제공하던 의료, 법률, 교육 등의 서비스를 가정에 맞게 직접 제공하고 있지 못하기 때문이다. 이를 위하여 본 논문에서는 온라인에서 의사, 변호사와 안전하게 거래할 수 있도록 국가자격 인증기반을 구축하고자 이에 필수적인 검증 가능한 온라인 자격증 발급을 위하여 기존 공인인증서에 자격필드를 추가하거나, 기존 공인인증서를 그대로 사용하거나, 별도의 자격인증서를 발급하는 등 세 가지 발급모델을 제시한다. 또한 이러한 세 가지 발급모델의 장단점을 비교 분석하여 향후 자격인증기반 구축할 때 선택할 수 있는 기준을 제시한다. 마지막으로 기 제시된 세 가지 발급 모델 중에 자격필드가 추가된 공인인증서를 이용하여 의료서비스(E-Health)를 받는 서비스 모델 시나리오를 제안하고자 한다.

1. 서 론

국내 디지털홈 서비스의 경우 정보통신부에서 초고속 인터넷 가입자를 바탕으로 향후 천만 가구의 디지털 홈을 구축하려는 계획을 세우고 관련 연구과제와 시범사업을 실시하여 기술적으로는 본격적인 서비스를 눈앞에 두고 있다. 하지만, 응용 어플리케이션 측면에서는 가정방범, 가스 잠금 등의 몇 가지 홈시큐리티 서비스를 제외하고는 기존 PC에서 제공하던 서비스와 크게 달라진 서비스를 실용화 하지 못하고 있다. 이러한 원인에는 여러 가지가 존재하겠지만, 그 중 하나는 오프라인에서 제공하던 의료, 법률, 교육 등의 서비스를 가정에 맞게 직접 제공하고 있지 못하기 때문이다. 디지털홈 서비스는 기존 PC와 달리 서비스 사용자 층이 한층 넓어짐에 따라 요구하는 서비스의 종류도 다양해진다. 기존과 차별화된 서비스에 대한 욕구는 더욱 커지고 있으며 특히 의료, 법률 서비스 같이 개인화된 서비스가 대표적인 예라 할 수 있다. 이에 따라 국가 차원의 자격인증 기반 구축으로 오프라인으로만 가능했던 대다수의 서비스를 가정에서 쉽게 처리할 수 있도록 해야 한다. 즉, 자격인증 기반이 구축된다면 서비스 제공자는 자신의 자격을 충분히 활용하여 차별화 된 서비스를 제공할 수 있으며, 서비스 이용 고객은 이러한 자격인증을 바탕으로 믿을 수 있는 개인화 서비스를 받을 수 있을 것이다. 본 논문에서는 국가자격 인증기반 구축을 위하여 자격인증서 발급모델을 제시하고 이를 자격인증 서비스 모델 시나리오에 적용하고자 한다. 자격인증서 발급 모델은 현재 온라인 신원확인에 이용되는 전자서명인증체계와 연계하여 기술적으로나 법적으로 최소화된 변경으로 자격인증기반을 현실에 구축 가능토록 하고자 한다.

2. 인증서 기반 홈네트워크 국가 자격인증

2.1 국가자격(National Licence)

국가자격이란 일정한 신분, 지위를 가지거나, 어떤 행동을 하는데 필요한 조건을 뜻하는 것으로 의사, 교사, 회계사 등 일정 시험이나 근무기간을 기준으로 해당 자격을 국가가 인정해 주는 것이다. 이러한 국가자격은 현재 오프라인 관점에서만 개인에게 주어지며 누군가에게 자신의 자격을 부여하는 것은 원

칙적으로 배제되어 있다. 예를 들어, 의사만이 환자를 진료하여 약국에 처방전을 발행할 수 있으며, 약사만이 처방전의 유효성을 검증하여 처방전에 있는 약을 조제하여 환자에게 제공할 수 있다.

본 논문에서 오프라인을 동일한 형태로 국가자격을 온라인에 적용하고자 한다. 다만, 자격을 국가에서 인정하는 국가자격으로 제한하고자 하는 까닭은 전자서명인증체계와 자격을 연계하기 위해서는 법적으로 국가에서 인정하는 자격만이 국가적인 자격인증기반 구축이 가능하기 때문이다.

2.2 국가자격 인증기관

국내 국가자격 인증기관으로는 한국산업인력공단, 교육인적자원부, 한국보건의료인국가시험원 등 정부기관이나 정부 산하기관을 중심으로 구성되어 있다. 국가자격 인증기관은 일정 경력이나 시험을 통하여 자격을 가지는 개인을 선별하고 이들을 인정하여 해당 증표를 나누어준다. 또한 부여된 증표를 데이터베이스 등의 저장소를 이용하여 특별 관리 등록하여 언제라도 자격을 가진 개인을 인증할 수 있어야 하다.

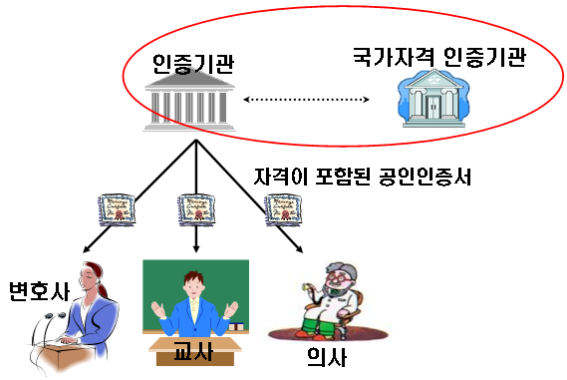
국가자격 인증기관은 인터넷 상에서 자격인증기반 구축을 위해서 가장 핵심적인 역할을 하게 될 것이다. 국가자격 인증기관은 해당 증표 역할을 하게 될 전자적 자격인증서를 직접 발급하는 자격 인증서 발급기관으로 운영되거나, 자격이 직접 포함된 공인인증서를 발급하는 인증기관(Certification Authority)과 협력하여 해당 자격이 올바른지 확인하고 검증하는 기관이 될 것이다.

2.3 자격인증 모델

국가자격인증기반 구축의 핵심은 자격인증에 필요한 자격정보를 어떻게 표현하며 어떤 과정을 통하여 발급받을 수 있으며 이를 검증할 수 있는가이다. 이에 기존 전자서명인증체계를 활용하여 최소한의 변경으로 국가자격 인증체계를 제공할 수 있는 모델을 제시한다. 이러한 모델은 기존의 속성인증에서 제시되었던 속성인증서 발급모델을 바탕으로 현재 인증기관(CA)에서 발급한 공인인증서에 자격필드를 추가하거나 공인인증서와 별도의 자격인증서를 구분하여 발급하거나 현재 공인인증서를 그대로 사용하는 것 등 세 가지 모델로 나누어 설명한다.[1]

2.3.1 공인인증서에 자격 필드 추가 모델

자격인증에 필요한 자격정보를 제공하는 첫 번째 방안으로 전자서명인증체계에서 사용되고 있는 공개키 인증서(이하 인증서)를 이용하여 자격 필드를 추가할 수 있다. 국내 인증서의 표준은 한국정보통신기술협회의 [TTAS.KO-12.0012]에서 정의하고 있으며, 자격을 공개키 인증서에 포함하는 방법에는 인증서의 필드로서 subject나 extensions를 사용할 수 있다. 인증서에 포함된 자격을 검증하는 방안은 사용자가 있는 자격을 가지고 있는 것을 검증한다. 검증 속도에 있어서 별도의 자격인증서를 검증하지 않고 인증서 검증만으로 자격을 구분할 수 있기 때문에 기존의 시스템 변경이 최소화할 수 있으며 빠른 검증결과를 가져올 수 있다. 인증서 발행 시에 자격 정보를 확인하는 것이 중요한데, 현존하는 공인인증기관과 국가자격 인증기관의 협조를 통해서 이를 구현할 수 있다. 다만, 자격필드 추가 오류에 따른 사고 발생시 책임 소재에 있어 문제가 야기될 수 있으므로 국가자격 인증기관에서 직접 CA를 구축할 수 있을 것으로 보인다. 현재 관련 국제표준으로 ISO/TS 17090-2이 있으며 이 표준에서는 안전한 의료정보 교환을 위해서 필요한 인증서 프로파일을 정의하고 있다. 특히, hcRole 속성을 이용하여 의료 종사자의 역할을 나타내고 있으며 인증서 내 Subject directory attributes extension로 설정하여 사용한다.[2]

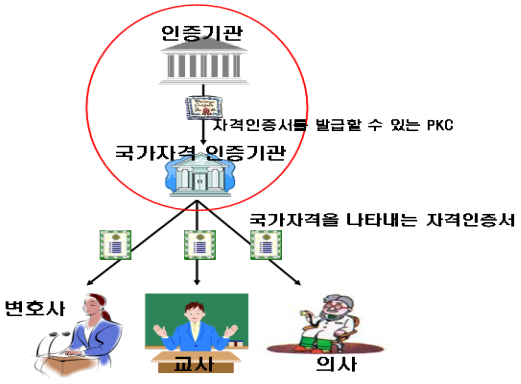


[그림 1] 공인인증서에 자격필드 추가 모델

인증서를 이용한 자격 인증에는 다음과 같은 특징이 있다. 첫째, 자격을 인증서에 포함시킴으로써 공개키 인증서가 가지는 안전성을 그대로 유지할 수 있으며 현재 사용 중인 PKI 응용 어플리케이션에서 최소화된 변경을 통하여 쉽게 적용시킬 수 있다. 둘째, 국가 전체 단위의 자격인증기반을 구축을 위해서는 사용자의 국가자격에 대응하는 표준화된 자격 ID를 결정해야 한다. 셋째, 자격의 변경이 있을 경우는 공인인증서를 다시 발행해야 하는 수고가 존재한다. 특히 인증서를 자격에 따라 여러 장의 인증서를 가질 수 있으나 여러 장임에 사용자가 관리해야 하는 부담이 더욱 커진다.

2.3.2 자격 인증서 발행 모델

자격정보를 제공하기 위한 두 번째 방법으로 공인인증서와는 별도의 국가자격인증서를 이용하는 방법이 있다. 자격인증서를 이용하는 시스템의 경우 공인인증서를 보유하는 사용자에 대해서 국가자격을 포함한 별도의 자격인증서를 발급한다. 이러한 자격 인증서의 발급은 [RFC3281]에서 정의한 속성인증서와 동일하며 속성인증서가 가지는 동일한 장단점을 가진다.[3]



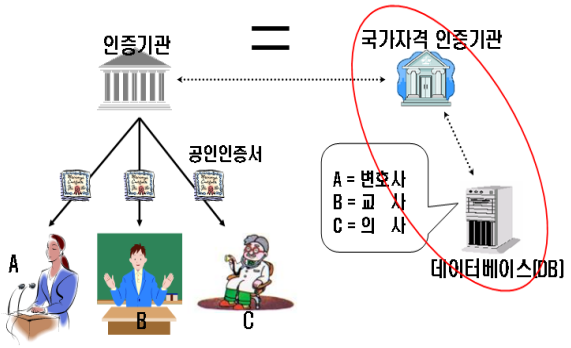
[그림 2] 자격인증서 발급 모델

본 논문에서는 [그림2]에서와 같이 자격인증서 발급 모델을 설정하기 위해서 기본적으로 [RFC 3281]에서 제시한 속성기관 모델을 따른다. [RFC 3281]을 따르는 자격인증서 발급 모델은 [X.509]와는 달리 PKI의 루트 인증기관에 상당하는 SOA(source of authority)라는 루트 속성 인증기관이 없으며 속성 인증기관간의 권한의 위임(delegation)이 존재하지 않는 심플한 모델을 제공하고 있다. 또한, 인증기관과 자격 인증기관이 서로 다른 기관으로 규정하고 있으므로, 현재 전자서명인증체계에서 현존하는 공인인증기관을 그대로 유지한 채 국가자격 인증기관이 속성 인증기관이 될 수 있다.

이러한 자격 인증서 발급모델이 가지는 특징은 다음과 같다. 첫째, 공개키 인증서의 유효기간과 상관없이 유효기간을 설정할 수 있으며 복수의 자격을 하나의 인증서에 포함하거나 여러 장의 인증서에 자격을 나누어 넣을 수 있다. 둘째, 현존하는 공인인증기관과 별도로 국가자격 인증기관에서 자격인증서를 발행해야 하므로 별도 인증시스템 구축이 필요하다. 셋째, 자격인증기관의 전자서명에 의해 자격이 인증되며 자격을 암호화하여 숨길 수도 있다. 넷째, 3.1.1 방식과 동일하게 국가 전체 단위의 자격인증기반을 구축을 위해서는 사용자의 국가자격에 대응하는 표준화된 자격 ID를 결정해야 한다. 자격이 변경되거나 폐지되었을 경우, 이를 검증할 수 있도록 자격 폐지목록이나 온라인 자격 유효성 확인시스템 등을 통하여 자격인증서의 유효성을 확인할 수 있는 검증 메커니즘 표준화도 필요하다. 이 때문에 다른 방식보다 검증시간이 많이 필요하다.

2.3.3 공개키 인증서 발행 대상자 제한 모델

자격정보를 제공하기 위한 마지막 발급모델은 공인인증서에 어떤 자격정보도 포함시키지 않고 통합 자격인증기관에서 공인인증서를 발급하도록 한다. 이는 국가자격 인증기관이 공인인증서를 직접 발급할 수 있어야 하기 때문에 통합 국가자격 인증기관이 공인인증기관으로 지정되어야 하는 문제점이 생긴다. 다만, 본 논문에서는 이러한 문제점도 해결 가능하다는 과정에서 하나의 발급모델을 제시함을 밝힌다. 이러한 인증서 발급으로 개인은 통합 인증자격기관의 공인인증서를 가졌다는 것만으로 국가자격을 가졌다고 판단한다. 이는 현재 이용 중인 PKI 관련 소프트웨어를 이용할 수 있을 가능성이 높고 시스템 구축이 비교적 용이하다. 통합 국가자격인증기관은 개별 국가자격 인증기관으로부터 개인의 자격에 대한 검증을 마친 뒤 인증서를 발급한다. 하지만, 공인인증서와 동일한 자격인증서를 이용하여 서비스를 제공한다면 어떤 자격을 가진 인증서인지 검증 자체가 어려워진다. 이를 위하여 통합 자격인증기관은 사용자의 공인인증서로와 해당 자격을 연결하고 있는 데이터베이스를 관리하여 데이터베스 상의 사용자의 레코드로부터 사용자의 자격을 꺼내어 이를 확인하여 사용자가 해당 자격이 있음을 최종 확인한다.



[그림 3] 공개키 인증서 발행기관 제한 모델

이 방안의 주요 특징은 다음과 같다. 첫째, 통합 자격인증기관이 인증기관(CA) 역할을 해야 한다. 둘째, 현재 전자서명인증체계에서 사용 중인 PKI 모듈을 사용할 수 있기 때문에 추가적인 표준화나 추가 기술이 필요 없다. 셋째, 통합 자격인증기관은 자격을 가진 사람의 공인인증서 발급시 자격을 철저히 검증하고 공인인증서와 자격을 연계하여 데이터베이스에 보관한다. 넷째, 고객은 자격을 가진 사람의 공인인증서를 검증하여 이를 식별하고 이후 식별된 사용자가 가지는 자격을 자격인증기관에서 보관하고 있는 데이터베이스를 통해 확인한다. 이 때, 데이터베이스 보안은 무엇보다 중요하게 보장되어야 한다.

2.4 장단점 비교

이상에서 제시된 세 가지 모델을 기존 어플리케이션 활용 여부, 검증방안 등을 중심으로 장단점을 분석하면 [표1]과 같다. 이를 통해 알 수 있듯이 국가 자격인증기반 구축을 위하여 기존 공인인증서를 사용할 때는 현재 전자서명인증관리체계에서 사용하고 있는 응용 PKI 어플리케이션을 그대로 사용할 수 있어 비용을 줄일 수 있다. 하지만, 데이터베이스 보안, 자격 변경에 따른 인증서의 변경 및 추가 발급의 단점이 존재한다. 이에 반해 자격인증서를 사용할 때에는 별도의 자격인증서 발급 및 검증 툴을 개발해야 하지만 복수 개의 자격 처리가 용이할 수 있다는 장점이 있다. 이렇듯, 앞서 제시한 세 가지 방안은 모두 각각

장단점을 가지고 있기 때문에 현재 전자서명인증체계에 수용하기 위해서는 향후 전자거래 환경에 맞추어 비용과 성과 측면에서 선택해야 한다.

[표 1] 장단점 비교

구분	장점	단점
인증서 내 자격필드 추가	- 기존 시스템 변경 최소화 - 속도 성능 향상	- 자격 변경에 따른 인증서 추가 발급 - 타 시스템과 상호 운용 어려움
자격인증서 사용	- 복수 개의 자격 처리 가능 - 자격 은닉 가능 (암호화)	- 자격인증 기관에 대한 신뢰성 확인 - 자격 변경에 따른 갱신 발급 - 속도 저하
기존 인증서 사용	- 기존 시스템 변경 불필요 - 인증서 추가 발급없이 자격변경 가능	- 데이터베이스 보안 강화 필요 - 타 시스템과 상호 운용 어려움

3. 전자서명인증체계에서의 홈네트워크 자격인증 서비스 모델 시나리오

디지털홈 서비스에서 킬러 어플리케이션으로 부각되고 있는 의료 서비스(E-Health) 모델을 구현하기 위하여 2장에서 제시된「인증서 내 필드추가」모델을 적요하기로 한다. 본 서비스 모델은 전자서명인증체계와 연동될 수 있도록 공인인증기관을 포함시켰으며 세부적인 서비스 모델 시나리오는 다음과 같다.

1) 의사, 약사 본인의 자격인증서 취득
2) 메일이나 광고를 통하여 의료 서비스 마케팅
3) 의사의 고객 진료
4) 처방전 내리기, 처방전 검증하기
5) 약사 자격 검증, 고객 검증, 약사에게 처방전 전달
6) 처방전으로 약 구입, 약 구입에 따른 영수증 취득
6) 전자 진료기록카드 서버에 보관된 전자 진료기록카드의 접근제어

먼저 의사나 약사 자격을 가진 사람은 공인인증기관에 의해 신원을 확인하고 자격검증기관에 의해 의나 약사 자격을 검증받은 뒤 해당 자격이 포함된 공인인증서를 발급받는다. 이에 대한 자세한 내용은 2.3.1절을 참조하도록 한다. 이후 의료서비스를 선전하기 위해서 메일이나 광고에 발급받은 자격인증서를 이용하여 전자서명한 뒤 고객에게 송부한다. 고객은 메일이나 광고를 받은 뒤 첨부된 송신자의 전자서명을 검증하고 이를 신뢰한다. 특히 의료 서비스를 받기를 원하는 고객은 광고나 다른 루트를 통해 얻은 정보를 가지고 의료서비스 사이트를 접속하고 자신이 받을 의료과목과 의사를 선택한다. 의사는 자신의 공인인증서를 웹에 게시하는데, 사용자는 자신이 선택한 의사의 인증서를 검증하고 검증이 성공되면 선택된 의사를 통해 진료를 받고 의사로부터 전자 서명된 처방전을 발급받는다. 이 후 처방전은 온라인 약국으로 전송되는데 고객은 해당 약국의 약사 자격을 검증하고 약사는 해당 고객이 약을 받기로 되어 있는 고객인지 검증한다. 이러한 검증과정이 모두 성공한다면, 고객은 비로소 약을 구입하게 되며 본 의료서비스는 끝이 난다. 의료서비스를 통하여 고객의 의료정보는 전자 진료기록 시스템에 저장되어 관리되는데 각각의 공인인증서를 통하여 의사나 약사가 접속할 수 있는 자격을 가질 수 있다.

의사나 약사의 공인인증서는 인증서 폐지목록(CRL)이나 온라인 유효성 확인 시스템(OCSP)에 의해서 처리한다. 인증서 폐지목록은 국가자격 인증기관에서 실시간 관리하여 인증기관에 자격의 유효성에 대한 정보를 통보하여 관리되어야 한다. CRL과 OCSP에 대한 설명은 [RFC3280],[RFC2560]을 참조한다.[4],[5]

4. 결론

지금까지 전자서명인증체계에서 적용 가능한 세 가지 모델을 분석하였으며, 이를 토대로 서비스 모델 시나리오를 제안하였다. 현재 전자서명인증체계 공인인증서를 활용하는 방안은 기존 시스템을 이용할 수 있기 때문에 비용 측면에서 활용도가 높으며 별도의 자격인증서를 발급할 때에는 다양한 자격을 처리할 수 있는 장점이 있다. 이러한 장단점을 잘 분석하여 실제 서비스 모델 구현에 적용해야 할 것이다. 또한, 서비스 모델을 현실에 실현하기 위해서는 기술 마련뿐만 아니라 법・제도가 뒷받침되어야 한다. 현재 자격과 관련된 서비스는 오프라인에서 온라인으로 넘어가기 위해서는 법 개정이 반드시 필요한 사항이며, PC 인터넷 환경에서 누릴 수 없었던 다양한 개인화 서비스를 디지털홈에서 받을 수 있기 위해서는 온라인 병원, 온라인 법률사무소, 온라인 회계사무소 등의 자격인증기반 구축이 반드시 필요하다. 또한, 국가 전체가 자격인증기반이 정착되기 위해서는 자격에 대한 분류와 이의 전자적 식별체계(ID)가 표준화 되어야 하며 전자서명된 처방전이나 약국 영수증에 대한 장기검증 기술 개발도 필요할 것이다.

참고문헌

[1] ECOM, "Attribute Authentication Handbook", http://www.ecom.jp/en/results/results2004/2004_08.pdf
[2] ISO/TS, "Health informatics-Public key infrastructure - Part2:Certificate Profile, ISO/TS 17090-2, 2002
[3] S. Farrel, Housley, R., "An Internet Attribute Certificate Profile for Authorization", RFC3281, 2002
[4] Housley, R., Polk, W., Ford, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC3280, 2002
[5] M. Myers, R. A., A. M., S. G., C. A., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP", RFC2560, 1999