

온라인 서비스 구현을 위한 전자정부 기술

김규태*, 김종원, 최종욱
(주) 마크애니, 상명대학교 소프트웨어 대학

e-Government Technologies for Implementing On-line Service

KaeKyu Kim, JongWon Kim, and Jong Uk CHOI
MarkAny Inc., Sangmyung University.

요 약

인터넷을 통한 전자정부의 활동은 시민들의 편의 제공과 업무의 효율성을 높일 수 있다는 측면 때문에 전세계적으로 활발한 서비스 계획이 이루어지고 있다. 그러나, 모든 서비스가 전자적으로 이루어지는 것이 아니기 때문에 온라인의 디지털 형태의 문서와 오프라인 상에서 존재하는 종이 문서 사이를 연결시키면서 대민 서비스의 편의성을 높일 수 있는 기술이 필요하다. 본 연구에서는 전자정부의 대민 서비스에서 온라인을 통한 증명서 같은 문서발급을 제공할 수 있는 기술과 구조에 대해서 연구하고, 서비스 사례를 통해서 응용 예를 알아보았다.

1. 서론

온라인 전자정부 서비스를 제공하기 위해서는 크게 두 가지 측면에서 검토해야 할 요구사항이 존재한다. 한 가지는 서비스의 편의성 측면이며, 다른 한 가지는 보안성 측면이다. 서비스의 편의성과 보안성은 상호 배타적인 관계를 갖고있기 때문에 한쪽의 기능을 강화하면 다른 한쪽의 기능이 약화될 수 있다. 서비스의 편의성을 위해서는 민원인이 공공기관에 방문하지 않고 온라인을 통해서 등록이나 증명발급과 같은 서비스를 제공받도록 하는 것이며, 보안성은 민원인의 개인정보가 유출되지 않도록 보호하거나 결재과정의 보호, 민원서류에 대한 위변조 방지 등을 고려할 수 있다.

온라인으로 제공되는 서비스는 네트워크나 PC에서의 개인정보 유출이나 민원서류의 cracking에 의한 불법행위가 일어날 수 있기 때문에 철저한 보안대책을 마련해서 서비스가 제공되어야 하지만, 보안대책

만을 강조하다 보면 대민 서비스가 제한적으로만 이루어지기 때문에 두 가지 측면의 trade-off가 필요한 것이다. 현재 온라인을 통해서 이루어지고 있는 전자정부의 대민 서비스는 대부분 행정정보의 열람서비스나, 온라인 신청, 신청에 대한 처리 상태를 파악하고 e-mail을 통해서 통보 받는 정도에 불과하다. 이러한 서비스는 보안적인 측면에서는 관리가 용이하지만 대민 서비스의 향상이라는 측면에서는 불만의 요소가 높다. 따라서, 이미 서비스되고 있는 시스템의 데이터를 안전하게 사용자에게 전달해주고, 증명서와 같은 민원서류를 온라인으로 발급해줄 수 있는 서비스를 제공하기 위해서는 기 구축된 시스템의 변경을 최소화 하면서 보안성을 높여줄 수 있는 기술들의 채택이 필요하다.

현재 한국 내에서 서비스되고 있거나 서비스를 계획하고 있는 온라인 대민 서비스에서 요구되는 공통적인 기능들은 크게 다음과 같이 열거할 수 있다.

- ① 기 구축 시스템의 변경 최소화
- ② 발급기관에 대한 증명 기능
- ③ 발급문서의 위변조에 대한 방지 기능
- ④ 온라인 상에서의 문서정보 보호 기능

온라인 민원 서비스를 준비하고 있는 대다수의 기관들은 이미 정보시스템 구축이 이루어져 있으며, 따라서, 기 구축된 정보시스템을 변경하지 않고 민원 발급 서비스 시스템을 구축할 필요성이 요구되고 있다. 이를 위해서는 민원 발급 서비스 시스템을 모듈화하여 기존 시스템으로의 이식성을 높여야 한다.

온라인 민원 발급 서비스가 제공되면 발급기관에 대하여 증명할 수 있는 방안이 필요하다. 오프라인에서의 민원 발급 시에는 발급기관을 확인시켜주기 위해서 발급기관 고유의 인장을 찍거나 특수용지에 발급기관을 명시함으로써 불법적인 발급기관 도용을 막을 수 있었으나 온라인 민원 발급에서는 일반 용지에 사용자가 프린트를 하기 때문에 발급기관을 증명할 수 있는 기능이 필요하다. 즉, 온라인으로 출력하면서 발급기관에 대해서 공인해 줄 수 있는 기능의 추가가 필요하다.

온라인 민원 발급 서비스에서 가장 중요한 사항은 발급된 문서내용의 위변조를 방지할 수 있는 기능이다. 온라인으로 민원 발급이 가능하다는 것은 악의적인 사용자에 의해서 해당 발급문서를 위조하거나 변조하는 것이 용이할 수 있기 때문에 발급 문서에 대한 위변조 방지기능은 필수적이다.

마지막으로 발급기관으로부터 해당 사용자에게 이르기 까지 다양한 개인 정보들이 전달되며, 프린터로 해당 문서를 출력하기 위해서 컴퓨터에 문서와 관련된 정보들이 저장될 수 있기 때문에 각 단계에서 불법 사용자의 접근을 방지할 수 있는 기능이 필요하다. 이러한 기능들로서는 프린터 spool의 제어나 temporary file의 접근제어 등을 들 수 있다.

2. High Density 2D Barcode

온라인으로 발급된 공문서를 오프라인으로 출력하

게 되면 민원인은 공공기관을 찾는 수고로움을 덜 수 있는 장점이 있다. 그러나 오프라인으로 출력된 공문서의 위변조를 확인할 수 없다면 다양한 사기사건이 발생할 수 있고 선의의 피해자가 생기게 마련이다. 따라서, 오프라인으로 출력된 문서에 민원인이 생성할 수 없는 방법으로 원문에 대한 정보를 가지고 있다면 이러한 문제를 해결할 수 있을 것이다. 따라서, 원문을 출력된 공문서에 기록할 수 있는 방법이 필요한데 2D barcode가 적합한 솔루션이다.

국제표준의 barcode는 기록밀도가 낮기 때문에 약 4KB의 공문서 한 장에 해당되는 정보를 기록하기에는 어려움이 많다. 따라서, 최소한 기록밀도가 200Byte/cm²를 가질 수 있는 고밀도 2D barcode 기술이 필요하다. 이를 위해서는 데이터의 기록을 위한 기본 배치와 스캐너를 통해서 입력할 때의 왜곡을 보정할 수 있는 제어코드를 감안하여 2D barcode를 설계해야 한다.

본 연구에서는 자체적으로 고밀도 2D barcode를 설계하였으며, 설계된 구조는 다음과 같다. Watercode로 명명된 이 2D barcode는 기록밀도가 436Byte/cm²로서 4KB의 공문서 기록을 위해서는 10개의 블록만 있으면 된다. 그러나 436Byte/cm²의 기록밀도에는 제어코드를 위해서 10%가 할당되며, error correction을 위해서 error correction code를 삽입한다. Error correction code는 훼손율에 따라서 결정되며, 본 연구에서는 20%의 error correction이 가능하도록 error correction code를 할당하였다. 결과적으로 순수한 데이터 기록밀도는 320Byte/cm²이다. 개발된 2D barcode는 기본 블록으로 이루어져 있으며, 기본 블록은 1 cm²으로 이루어져 있다. 그림 1의 (a)은 2D barcode의 기본 블록을 나타내는 것이며, (b)는 기본블록을 연결하여 6.8Kbyte의 데이터를 저장할 수 있도록 만들어진 블록을 나타내고 있다.



(a)



(b)

그림 1. 개발된 고밀도 2D barcode

2D barcode는 해당 페이지의 내용과 함께 발급기관의 PKI 인증서를 내장하고 있으며, 해당 페이지의 내용에 대한 무결성을 검증할 수 있도록 digital signature가 함께 들어간다.

3. Digital Signature Technology

Digital signature는 문서나 메시지를 만든 기관이나 사람의 신원 및 무결성을 확인하기 위해 사용되는 서명이다. 본 연구에서 digital signature를 사용하는 목적은 문서의 발급기관에 대한 확인과 원본 문서에 대한 무결성 확인이다. 따라서 PKI(public key infrastructure)를 이용함으로써 그 목적을 달성할 수 있다. PKI는 암호학에서 키 분배에 대한 안정성 확보를 목적으로 개발된 것으로서 암호화할 때와 복호화할 때의 키를 서로 다르게 배정할 수 있는 것이다. 따라서 private key와 public key 쌍을 가지고 있고 private key는 개인이나 기관만이 가지고 있으며, public key는 모두에게 공개되어 있기 때문에 송신자에 대한 확인이나 수신자를 지정해서 메시지를 전송하는데 활용할 수 있다. 그러나, private key나 public key가 위조될 가능성을 배제하기 위해서는 제3의 신뢰성 있는 기관이 필요하며, 이들 기관에서는 private key와 public key를 발급해주고 해당 키에 대한 인증서를 발급한다. 이들 기관을 certification agency라고 하며, 인증기관을 인증하기 위한 상위 인증기관들도 존재한다. 최상위 기관은 root CA라고 불리운다.

4. Digital Watermarking

발급기관을 나타내는 관인이나 로고의 경우 손쉽게 도용이 가능하기 때문에 오프라인으로 출력된 문서의 관인이나 로고가 도용된 것이 아닌 적절한 절차에 의해서 사용된 것인지를 확인할 필요가 있다. 이를 위해서는 관인이나 로고에 일반인이 확인할 수 없는 정보를 은닉하여 적법 사용여부를 결정하는 것이다. 특히, 출력된 문서에서도 그 정보를 파악할 수

있어야 하므로 digital watermarking 기술을 이용하여 관인이나 로고에 특정 정보를 은닉하여 도용을 방지할 수 있다.

본 연구에서 사용한 워터마킹 알고리즘은 spread spectrum 방식에 그 기반을 두고 있다. 대역확산 방식은 noise addition 및 데이터의 일부 훼손에 강인하다는 특징을 가지고 있다. 삽입되는 random number의 특징은 white noise이며 random number의 추출은 cross-correlation을 이용한다.

Off-Line상의 워터마킹 추출을 위해서는 3단계의 전처리 과정이 필요하다. 첫번째는 영상을 회전하는 단계와 두 번째로 스캔된 영상에서 관인 영상을 정확히 잘라내는 단계 그리고 세 번째로 영상의 크기를 조절하는 단계이다.

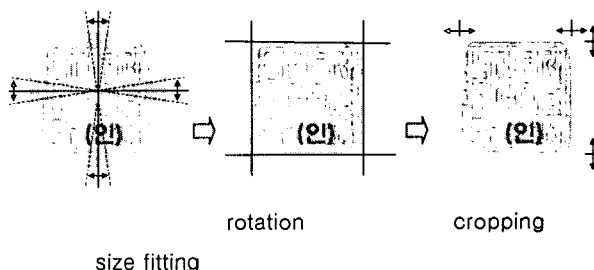


그림 2. 워터마크 추출을 위한 preprocessing

전처리 과정을 거친 후에 cross-correlation 값을 얻어내어 최대값의 위치가 동일한지 확인한다. 위치가 동일하면 워터마크가 검출된 것으로 일치하지 않으면 워터마크가 검출되지 않은 것으로 판단한다.

5. 화면 capture 방지기술

화면 capture 방지의 주된 목적은 웹을 통해서 제공되는 증명서류에 대한 source를 받아가거나 이미지 관인이나 로고를 capture하는 것을 방지하는 것이다. 윈도우 운영체제에서는 기본적으로 화면을 클립보드로 복사할 수 있는 기능이 제공되고 있으며, 특별히 화면을 capture할 수 있는 snag-it과 같은 프로그램들이 제공되고 있다. 본 연구에서는 화면 capture 방지와 웹 화면 보호를 위해서 비디오 메모리 호출을 제어하고, 마우스의 pop-up menu를 제어함으로써 이 목적을 달성할 수 있었다.

6. Print control and DRM technology

인터넷을 통한 증명서의 오프라인 발급을 위해서 중요한 것 중의 하나가 프린터를 제어하는 기술이다. 무료로 발급되는 증명서에서는 특별히 프린터를 제어할 필요는 없으나 유료로 발급되는 증명서는 발급 횟수를 제어해야 한다. 특히, 프린터를 사용하는 단계에서는 spool에 프린트될 문서가 이미지 파일 형태로 저장되기 때문에 임시파일 형성에 대한 제어가 필요하다. 따라서, DRM 기술에 의한 파일관리는 사용자의 불법적인 의도의 임시파일 사용을 억제할 수 있으며, 안전한 민원발급 서비스를 얻을 수 있는 기술이다.

DRM 기술은 멀티미디어 콘텐츠 서비스를 안전하게 하기 위해서 개발된 기술이지만, 오늘날은 내부 데이터 보안이나 컴퓨터 내에 존재하는 자체 파일보안 등 그 적용개념을 넓혀가고 있는 기술이다.

7. e-Government Service in Korea

여기에서는 가장 많은 민원인들에게 서비스를 제공하고 있는 대법원의 등기부등본 서비스 사례를 중심으로 위에서 소개된 기술의 활용을 설명한다.

대법원에서는 부동산 등기부등본과 법인 등기부등본에 대한 발급서비스를 하고 있다. 대법원 등기부등본 발급서비스의 편의를 위해서 온라인 열람이 가능하도록 시스템 구축이 되어있으며, 온라인 열람뿐 아니라 온라인으로 발급되는 등기부등본에 대해서 법적 효력을 제공하기 위한 시스템을 운영하고 있다.

현재 대법원에서는 등기부등본에 대한 열람 서비스를 제공하고 있으며, 이러한 구성은 그림 3에 나타내었다. 민원인은 대법원의 등기부등본 열람 서비스를 제공하는 웹사이트에 접속하여 자신의 ID와 password를 입력하고, 해당 등기부등본에 대한 정보를 입력함으로써 원하는 등기부 등본을 열람할 수 있다. 서비스 시스템에서는 사용자에게 대한 인증이 확인되면, 비용에 대한 결제 프로세스를 거쳐서 등기부등본 데이터베이스로부터 해당 자료를 가져와서 사용자의 화면에 표시해주며, 출력을 허용한다. 그러나 출력된 문서는 단순히 열람에 대한 확인용이며 증명

서로서의 효력은 갖지 못한다.

대법원의 등기부등본 열람 서비스를 발급 서비스로 전환하기 위해서는 앞에서 열거한 기술들을 채택하여 서비스 사용자와 기존 열람 서비스 시스템간을 연결해준다. 사용자가 최초로 발급서비스에 접속하게 되면 active-X를 통해서 client 모듈이 사용자의 컴퓨터에 설치된다. 사용자의 인증과정과 결제 프로세스까지는 기존 시스템과 동일하며, 데이터베이스로부터 해당 문서를 가지고 올 때는 HSM(hardware security module)을 이용하여 전자서명을 생성하고, 대법원의 PKI 인증서를 함께 발급 모듈로 전달한다. HSM 장비는 대법원의 private key와 PKI 인증서를 안전하게 보호하기 위한 하드웨어 모듈이다. 해당문서와 전자서명, PKI 인증서를 이용하여 2D 바코드 생성모듈이 하나의 2D 바코드를 생성하여, 원문과 함께 발급 웹 서버를 통해서 사용자의 컴퓨터로 전달한다. 이때 전달과정에서는 cracking 방지를 위해서 secure channel을 형성하여 전달한다.

전달된 문서와 2D barcode는 DRM에 의해서 보호되고 있으며, 사용자는 단순히 viewing과 printing만이 가능하게 된다. 사용자가 문서출력 버튼을 click하게 되면 인터넷을 통한 문서의 발급과정이 종료된다. 이와 같은 처리 서비스 시스템의 구조를 그림 4에 나타내었다.

이러한 시스템 구성을 통해서 민원인은 관공서에 방문하지 않아도 어느 곳에서든지 원하는 증명서의 발급이 가능하게 된다.

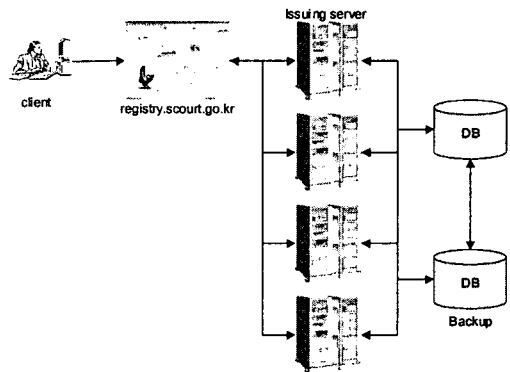


그림 3. 대법원 등기부등본 열람 서비스 구조

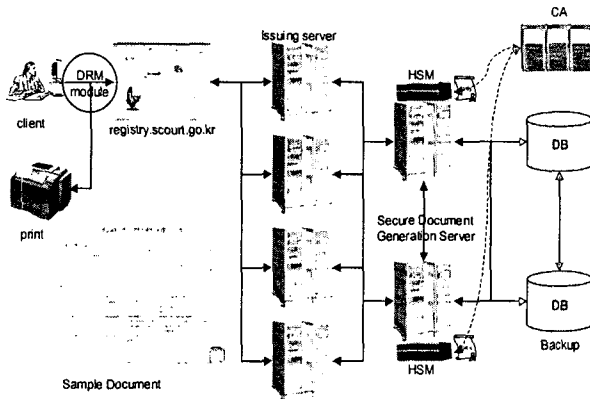


그림 4. 대법원 등기부등본 발급 서비스 구조

8. 결론

본 논문에서는 온라인 증명서 발급에 사용되는 보안기술과 위변조 방지기술을 소개하고, 아울러 현재 국내에서 진행되고 있는 온라인 증명서 발급 시스템 구축사례를 소개하였다. 향후 모든 증명발급이 온라인으로 이루어지고, 디지털 문서로 이루어지는 시스템으로 구축되기까지는 종이문서로 발급되는 증명서에 대한 필요성은 줄어들지 않을 것이다. 따라서 온라인으로 원하는 증명서를 종이문서로 출력할 수 있도록 하는 보안기술과 위변조 방지기술은 그 효용성이 매우 높다 할 수 있다.

향후, ubiquitous환경에 맞는 서비스 제공을 위해서 2D 바코드의 카메라를 통한 인식 등의 기술을 발전시킨다면 전자정부의 대민 서비스 질을 향상시킬 수 있을 것이다.

Reference

[1] KyungSup Kim, "Analysis of Structure Elements to Implement Successful e-Government", Information & Communication Policy Issue, vol.15, no.1, pp.1-51, Mar, 2003.

[2] <http://www.firstgov.gov/>