전자문서 보관 서비스의 정보유출 최소화를 위한 효율적 시스템 설계에 관한 연구

정회원 성 경 상*, 오 동 열**, 김 정 재***, 나 원 식****, 오 해 석*****

Study on the Efficiency System Design for Minimize the Information Leak of the E-Document Store Service

Kyung Sang Sung*, Dong Yeol Oh**, Jung Jae Kim***, Won Shik Na****,
Hae Seok Oh***** ***Regular Members***

요 약

공인전자문서보관소는 전자기록의 진본성을 확인하고 보장하는 제도로서 법적인 보호 아래 보관되며, 전자기록 사항을 진정한 것으로 추정하고 전자기록의 내용이 변경되지 않았음을 입증한다. 그러나 원본성 보장을 위한 기존의 전자문서 암호화 방법은 하나의 대칭키로 전체 문서의 암호화 과정을 거치고 있으며, 이용자가 해당 대칭키를 노출시킨다면 해당 전자문서에 대한 안전은 보장받지 못하게 된다. 또한, 전체 문서의 암호화 과정을 통한다면 이용자는 상대방에게 불필요한(원치 않는) 정보까지도 노출되는 문제점이 발생된다. 이와 같은 문제점을 해결하기 위해 본 논문에서는 이용자가 전자문서를 등록한 후 향후 제 3자에게 발급하는 과정에서 등록된 전체의 정보가 아닌 부분정보 발급을 통해 불필요한 정보유출을 방지하고, 문서의 가독성을 향상시키며, 문서 암·복호화 키 분실 시에도 OTP 인증원리를 추가하여 정보유출을 최소화함으로써 공전소에 등록된 문서의 정보보호를 강화할 수 있는 방안을 제안하였다.

Key Words : 공인전자문서보관소전소(Certified Electronic Document Authority), 원본성(originality), 무결성(Integrity), 가독성(Readability), OTP(One Time Password)

ABSTRACT

Certified e-Document Authority keep it with protection legal as a system a guarantee and identifies originality of an e-Record, But, encryption method of the existing E-Documents for the original guarantee use a encryption process of a whole documents with the symmetric key, if user exposed concerned the symmetric, safety of the concerned E-Documents cannot guarantee. But, encryption method of the existing E-Documents for the original guarantee use a encryption process of a whole documents with the symmetric key, if user exposed concerned the symmetric, safety of the concerned E-Documents cannot guarantee. In addition, if encryption processing the whole Documents by the public electronic documentary depository rule, it is occurred the problems that your unnecessary(I do not pray) information exposed to a partner. So, if you used the proposed method in this paper, when registered E-document process issuing to the third party, prevent an unnecessary information outflow through the partial information issuance that is not whole information, and improvement in document's readability. In addition, added an OTP certification principle, if you lost the encryption key or decryption key, this method can minimizing an information outflow. though strengthen information protection of the document registered with the public electronic documentary depository.

* 경원대학교 전자계산학과 인텔리전트 연구실(actofgod@ku.kyungwon.ac.kr), ** 숭실대학교 컴퓨터공학과 멀티미디어 연구실(javarian99@empal.com),
*** 숭실대학교 컴퓨터공학과 정보보안 연구실(argniss@yahoo.co.kr), **** 남서울대학교 교양과정부(wsna@mic.khu.ac.kr),
***** 경원대학교 전자계산학과 IT(oh@kyungwon.ac.kr)
논문번호 : 08051-0730, 접수일자 : 2008년 7월 30일

Ⅰ. 서 론

최근 정보통신 인프라의 질적 향상에 따라 전자거래의 비약적이고 양적인 팽창을 이루게 되었고, 전자문서에 의한 종이문서의 대체가 가속화 되고 있다. 그러나 전자문서의 이용이 확대되어야 함에도 불구하고 아직도 여전히 많은 양의 종이문서가 생산되고 있다.

우리나라의 경우, 기업·금융기관 등은 각종 문서 또는 서류의 유통·보관에 연간 1조원 이상을 소요하고 있는 것으로 추정되며, 보관 문서의 활용에도 어려움이 따르고 있다. 예를 들어, 신용카드 매출전표의 경우 연간 15억 매가 발행되고 있는데, 이를 신용카드사가 수거하고 문서 창고에 보관하는데 약 1,200억원 가량의 비용이 소요되는 것으로 추정된다. 또한 세무자료 등 중요 자료는 5~10년간 보관되는 과정에서 화재나 도난 등으로 인한 유실·훼손의 위험이 항상 존재하고 있을 뿐 아니라 분쟁 발생 시 해당 신용카드 매출전표를 찾아서 참조하는데 있어서도 많은 어려움을 가지고 있다.

종이문서는 기업 활동이 확대되면서 지속적으로 보관량이 증가하고 있고, 조직개편 및 담당자 이동에 따라 분류·검색·참조가 시간이 지남에 따라 어려워진다. 이러한 시간·비용·노력의 투입에도 불구하고 분쟁해결과 자료제출에 활용되는 비율은 매우 낮다.

이러한 종이문서를 전자문서로 대체하면 종이문서 보관에 필요한 문서 창고를 점진적으로 감축할 수 있게 됨은 물론 검색·활용이 온라인상에서 가능하게 되어 시간과 비용을 획기적으로 절약할 수 있다. 또한 전자문서는 그 보관에 있어 재해복구시스템을 이용한 원격지 이중보관을 통해서 화재·수재·테러 등 재해에 따른 유실 및 훼손의 위험도 방지할 수 있다. 따라서 전자문서 활용은 기업 등의 업무처리의 효율성·신속성 등을 제고함으로써 경쟁력 향상을 위한 핵심요인으로 자리잡을 수 있다.

그러나, 비즈니스 효율화를 위해 전자문서의 도입과 이에 대한 원본 전자문서의 보관 및 증명 업무의 필요성이 절실하다. 즉, 전자문서의 효율성에도 불구하고 전자문서 이용을 저해하는 법·제도로 인해, 종이문서의 생산·유통·보관은 지속되고 있는 상태이다. 기업의 전자문서 활용에 있어서는 기술적인 문제점보다 신뢰성 부족이 더 큰 제약사항으로 작용하고 있는 실정이다.

이러한 전자문서 이용의 문제점을 해소하기 위한 방안의 하나로서 착안한 것이 "신뢰할 수 있는 제3자(Trusted Third Party)"에 의한 보관이며, 그 결실이 바로 공인전자문서보관소(이하 "공전소" 라 한다)라는 제 3자를 탄생시킨 2005년 3월에 개정된 전자거래기본법이다. 본 제도의 핵심은 전자문서 보관을 목적으로 제 3자를 개입시켜 법적 추정력을 부여하며 이를 통한 미래 안정성을 꾀함으로써 전자문서의 장점을 충분히 살리는 것이다.[1]

그러나, 등록된 전자문서를 요청자에게 발급하는 과정에서 증명력을 강조하기 위해 암호화된 문서 전체를 전달하는 도중에 문서의 불필요한 정보유출이 부득이하게 발생된다. 또한, 등록된 전자문서의 수정 요청이 발생된 경우 문서 전체의 디지털화하는 작업이 반복됨으로써 시간과 비용의 낭비가 발생된다. 마지막으로 관리자의 실수로 키가 노출되거나 분실되는 경우 발생되는 정보 유출 문제는 극히 심각해 질 수 밖에 없다.

따라서 본 논문에서는 전자문서의 신뢰성과 안정성을 보장하는 공전소를 구축·운영하는데 있어 핵심 서비스 중의 하나인 전자문서 보관 및 발급 서비스를 이용 시, 이용자가 전자문서를 등록한 후 향후 제 3자에게 발급하는 과정에서 등록된 전체의 정보가 아닌 부분정보 발급을 통해 불필요한 정보유출을 방지하고, 문서의 가독성을 향상시키며, 문서 암·복호화 키 분실 시에도 정보유출을 최소화함으로써 공전소에 등록된 문서의 정보보호를 강화할 수 있는 방안을 제공한다.

본 논문의 구성은 다음과 같다. 2장은 선행연구 및 관련 기술로서 공개키 기반구조(Public Key Infrastructure, PKI), OTP(One Time Password), M사의 오피스 문서 포맷 표준으로 국제표준화기구 ISO(International Organization for Standardization)의 표준으로 승인받은 OOXML(Office Open XML)에 대해 기술하고, 본 연구의 대상인 기존 공전소 현황, 관련 기술, 제공되는 서비스의 문제점을 파악하고, 개선안을 제시한다. 3장은 기존 공전소 서비스의 문제점을 해결하기위한 전자문서의 안전한 저장과 OTP를 활용한 등록된 문서의 부분정보 발급 방법을 통한 발급된 전자문서의 정보보호 방안 등에 대하여 연구하였다. 4장은 기존시스템과 비교하여 제안시스템의 성능을 평가하고 보안성에 대하여 비교 분석하였으며 마지막 5장으로 결론을 맺는다.

Ⅱ. 관련 기술 및 서비스

2.1 공개키 기반구조

공개키 기반구조는 개방형 네트워크에서 안전한

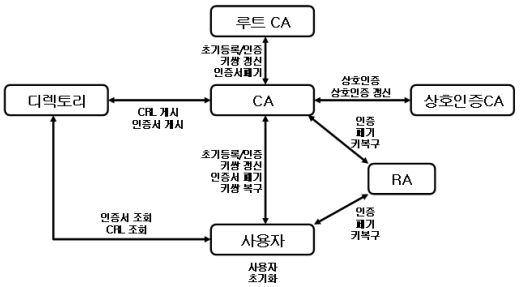


그림 1. PKI 구성요소

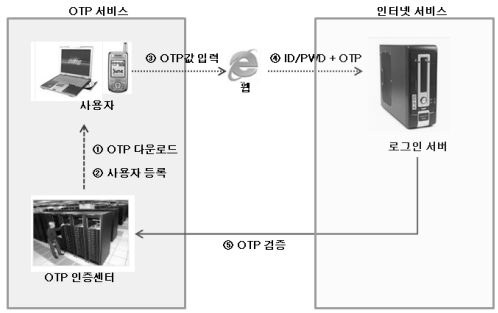


그림 2. OTP 운용 개념도

서비스가 이루어질 수 있도록 통신 정보의 비밀성, 인증, 무결성, 부인방지 등의 기본적인 보안 서비스를 가장 효과적으로 제공하는 기반구조이다. PKI는 공개키 암호기술이 안전하게 적용될 수 있는 기반 구조로써 공개키와 그 소유자를 연결해 주는 전자 증명서, 키와 인증서를 안전하게 관리해주는 서비스, 그리고 인증서의 유효성 여부를 확인할 수 있는 구조라고 정의한다. PKI는 그림 1과 같이 정책승인기관(Policy Approving Authority, PAA), 정책 인증기관(Policy Certification Authority, PCA), 인증기관(CA), 등록 기관(Registration Authority, RA), 디렉토리(Directory), 사용자 등으로 구성된다.[2]

정책승인기관(PAA)은 공인인증 서비스 전반의 정책과 절차를 수립하는 역할을 수행하며, 정책인증기관(PCA)은 정책승인기관(PAA) 아래 계층으로 자신의 도메인내의 사용자와 인증기관이 따라야 할 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서폐기목록(CRL) 등을 관리한다. 인증기관은 정책인증기관의 아래 계층으로 인증서의 생성이나 CRL의 관리 등의 기능을 수행한다.

2.2 OTP(One Time Password)

일회용비밀번호(OTP)는 1회에 한해 사용할 수 있는 비밀번호 시스템으로 매번 다른 비밀번호를 이용하여 사용자를 인증하는 방식이다. 일정 시간마다 전용 단말기 등에 새로운 비밀번호가 생성되어 시스템에 접근할 때마다 새로운 비밀번호를 입력해야 하기 때문에 해킹이나 사용자의 관리소홀 등으로 비밀번호가 노출되는 것을 방지할 수 있다. 35개의 정해진 범위에서 비밀번호를 입력하는 기존의 인쇄된 보안카드에 비해 OTP는 사용자 비밀번호가 노출되더라도 새로 생성된 비밀번호를 입력해야 하기 때문에 훨씬 강력한 보안성을 제공할 수 있다.[3]

대부분의 모든 OTP 생성 알고리즘은 일방향 함수(출력 값을 통해 입력 값을 유추할 수 없는 함수)에 기반을 두고 있으며, 거의 모든 유닉스(UNIX) 운영체제에 구현되어 있는 S/Key 시스템(RFC1760)이 좋은 예다.

또 날이 갈수록 전자금융거래가 증가하고 있어 OTP의 도입은 현재의 수요 이상으로 크게 늘어날 것으로 예상되며, 정부에서도 더욱 강화된 보안을 제공하는 OTP의 필요성을 공감하고 있어 전자금융거래 안전성 강화 대책을 통해 장기적으로 OTP 도입을 권장하고 있다. 또한, 모바일 OTP(MOTP)는 휴대전화에 탑재 가능한 일회용 비밀번호 생성 SW로 OTP SW가 매번 다른 비밀번호를 생성해 주기 때문에 강력한 보안성을 제공받을 수 있다. 인터넷 서비스 업체는 MOTP를 이용하여 사용자에게 편리하고 강력한 사용자 인증 서비스를 제공함으로써 서비스 품질을 한 단계 높일 수 있도록 하고 있다.

2.3 OOXML(Office Open XML)

일반적으로 문서편집기에서 생성된 전자문서 포맷은 특정 업체에 종속된 바이너리 형식을 따르게 된다. 최근 웹의 활용성 측면에서 바이너리 문서의 한계가 지적되면서 XML에 기반을 둔 문서 포맷에 대한 요구가 높아졌으며, 2008년 4월 ISO 표준 승인이 되어 ISO/IEC 29500으로 결정된 OOXML이 등장하게 되었다. XML 기반의 포맷을 이용하명 구조화된 문서의 표현이 가능하므로 특정 APP나 플랫폼에 종속적이지 않으며, 차별화된 서비스와 기술력 중심의 경쟁 가속화를 가져오는 특징을 가지고 있다[4]. OOXML은 다음 그림 4와 같이 3개의 주요 마크업으로 구성되어 있다.

워드문서와 엑셀, 파워포인트 기능을 담당하는 WordprocessingML,SpreadsheetML, PresentationML을 포함한다. 부가적으로 주요 기능을 담당하는 별도의 마크업을 포함하며 DrawingML의 경우 그래픽, 챠트, 테이블 및 도형 등을 표현할 수 있다. 한편 OOXML도 ODF와 같이 ZIP 파일 형식의 컨테

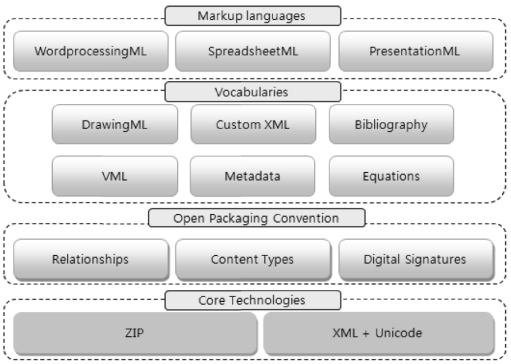


그림 3. OOXML의 주요 구조

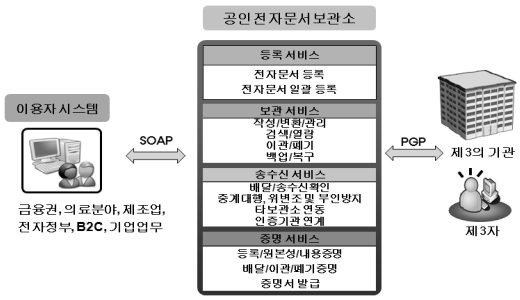


그림 4. 공인전자문서보관소 구성 및 서비스

이너 구조를 제공하며 이를 OPC(Open Packaging Convention)로 표기한다.

또한, OOXML은 문서 내에 "사용자 정의 스키마"의 사용을 통해 Office와 같은 생산성 향상 어플리케이션과 비즈니스 프로세스를 관리하는 정보시스템과의 통합관리를 가능하게 한다. 이것은 문서에 불투명하게 묻혀 있어 비즈니스 어플리케이션이 조회하거나 변경할 수 없었던 비즈니스 정보를 재사용하거나 자동으로 처리할 수 있는 가능성을 제공한다. 이와 같이, 기존 바이너리 문서포맷에 대한 높은 호환성과 다양한 기능성을 제공하는 OOXML은 단순히 읽고 쓰던 기존의 문서편집기 시장을 넘어서 문서교환이 필요한 다양한 분야의 어플리케이션이 등장하게 될 것이다.[5]

3.4 공인전자문서보관소 서비스

공전소는 크게 보관, 송·수신, 증명서비스 등을 제공하며, 이러한 세 가지 기본 서비스에 더하여 기존 종이문서의 전자화를 위한 스캔 서비스와 이용자가 공전소를 이용할 수 있도록 하는 웹 인터페이스도 제공한다. 또한 공인인증기관과 TSA(Time Stamping Authority)와 연계되어 이용자 인증과 증

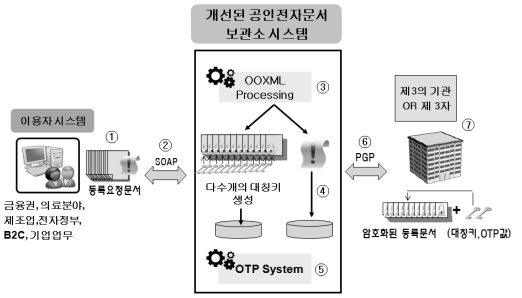


그림 5. 전자문서 등록 및 발급업무 처리 흐름도

명서비스를 위해 시점확인서비스도 할 수 있다[6].

공인전자문서보관소의 주요기능인 문서보관기능, 송수신의 기능은 전자기록의 진본성 유지를 위한 방안의 관리방안과도 직접적인 연관성이 있다. 문서작성, 문서배달과 관련해서는 전자기록의 정체성과 관련되고, 문서변환, 문서관리, 문서검색, 문서열람, 보존연한, 이관·폐기, 보존매체, 백업, 복구, 암호화, 위변조등은 전자기록의 무결성을 유지시키기 위한 방안과 직접적인 연관성을 가진다고 볼 수 있다. 그리고 공인전자문서보관소에서 보관되고 있는 전자기록이 진본임을 증명서기능으로서 표현되는 것이다[7].

Ⅲ. OTP를 활용한 공전소 시스템 설계

3.1 제안시스템 개요

제안시스템은 그림 5와 같이 공전소의 기능 강화를 통하여 이용자시스템에서 등록 요청된 문서를 이용자가 정하는 기준에 따라 세분화하고, 각각 서로 다른 대칭키를 이용하여 암호화한 후 보관하여, 향후 제 3의 기관 혹은 제 3자에게 발급될 시 이용자가 원하는 정보만 공개될 수 있도록 함으로써, 문서 등록자의 정보보호를 강화하는데 목적이 있다. 등록 요청된 문서의 저장 및 발급과 관련된 제안시스템의 업무처리 흐름은 다음과 같다.

본 논문에서 제안하는 개선된 공인전자문서 보관소 시스템에 접근하기 위하여 ①이용자시스템에서 문서 등록을 요청 한다. ②전자문서의 전송은 SOAP을 통해 이루어지며, ③등록 요청된 문서는 OOXML 처리 과정을 거쳐서 이용자의 분류 기준에 따라 세분화 된다. ④세분화된 문서는 각각 서로 다른 대칭키에 의해 각각 암호화 된 후 저장되며, ⑤이용자로부터 문서발급 요청 시 생성된 OTP 값을 복호화용 대칭키와 함께 전송함으로써 키가 안정성을 보호하며, 발급된 문서의 정보보호를 강화한다. ⑥문서를 메일로 발급할때에는 PGP(Pretty Good Privacy)를 통해

이루어지며, ⑦문서를 제 3자에게 발급할때 대칭키, OTP값과 같이 2개의 복호화용 키가 암호화된 문서와 함께 전달됨으로써 보안이 강화된 문서가 전달되는 과정을 거치게 된다.

3.2 전자문서 등록 및 보관

이용자와 공전소 간에 상호인증 과정이 끝나면 이용자는 공전소에 전자문서의 등록을 요청한다. 이용자는 원본 문서를 공전소에 등록하기 위해 먼저 원본문서에 자신의 개인키 및 인증서를 사용하여 전자서명을 하고, 전자서명을 한 데이터를 공전소의 공개키로 암호화하여 그림 6의 ①과 같이 서로 간에 맺어진 통로(session)로 SOAP을 통해 전송하게 되며, 이렇게 전송된 메시지는 공전소 서버의 개인키로 복호화하고, 해쉬 값을 통해 위·변조의 유무를 판단하게 된다[8].

수신된 원본 파일은 그림 6의 ②와 같이 OOXML 처리 과정을 통해 향후 제 3자에게 부분정보 발급을 위해 세분화되며, 그림 6의 ③과 같이 서로 다른 대칭키에 의해서 각각 암호화 된다. 이때 세분화되어 등록된 전자문서 중 향후 전자문서 등록자에게 어떤 부분의 전자문서 발급을 원하는 가를 묻기 위해 문서 보관시 세분화된 문서에 대한 목차(index)를 그림 6의 ④와 같이 생성하여 동시에 보관한다.

3.3 부분정보 발급 방안

공전소에는 이용자의 요청에 의하여 금융권의 대출문서, 병원의 환자 진료 기록, 기업체의 사무용 서류 등 다양한 많은 전자문서들이 보관되어 있다. 보관된 이 문서들 중에는 제 3자에게 발급될 경우, 등록자의 개인 프라이버시에 상당한 피해를 줄 수 있는 경우가 많다.

예를 들면, 병원에 진료를 받은 환자가 보험처리를 위하여, 병원에 진단서 및 입원확인서를 요청했을 경우, 이 병원은 진료기록을 공전소에 맡겨놓은 상태이므로 이 환자가 원하는 정보를 보험회사에 발급하라는 요청을 공전소에 할 것이다. 이 경우 만일 공전소에서 이 환자에 대한 모든 진료 기록을 보험회사에 발급한다면, 이 환자는 보험처리를 위한 정보 이외에 불필요한 정보까지 외부에 있는 보험회사에 알려지게 되므로, 개인의 정보보호 혹은 사생활에 막대한 타격을 입을 수 도 있을 것이다.

이와 같은 이유로 인해서 공전소 문서 발급시스템은 이용자가 등록한 전체 문서가 아닌, 이용자가 제시한 기준에 의해서 세부적으로 분류되어 저장되고, 향후 문서가 발급될 시 등록된 전체 문서가 아닌 이용자가 원하는 정보만 선별하여 발급될 수 있는 시스템 구축이 필요하다.

제안시스템의 부분정보 발급 처리절차는 그림 7과 같으며, 흐름도에 대한 세부내용은 다음과 같다.

① 공인전자문서보관소에 대출관련 서류를 등록해 놓은 금융기관이 대출업무를 실시 중 고객과 마찰이 발생하여 법원으로부터 대출관련 서류를 제출하란 통보를 받는다.

② 이 금융기관은 대출관련 서류를 공전소에 등록시켜 놓은 상태이므로, 공전소에 제 3의 기관인 법원으로 해당문서 발급을 요청함.

③ 공전소는 등록된 문서 중 어떤 문서의 발급을 원하는지, 보관된 문서의 목록(Index)을 이용자인 금융기관에 전송함.

④ 이용자는 공전소로부터 온 등록문서 목록 중 발급되기를 원하는 항목을 정하여 발급을 요청함.

⑤ 암호화되어 등록된 전체 문서와 발급 요청된 문서를 복호화 하는데 필요한OTP 값을 생성한 후, 이용자가 발급을 요청한 첫 번째 페이지의 복호화용대칭키와 문서 발급시 생성된 OTP값과 암호화된 발급 문서를 전송한다.

⑥ 이용자 요청에 의해 제 3의 기관을 대상으로

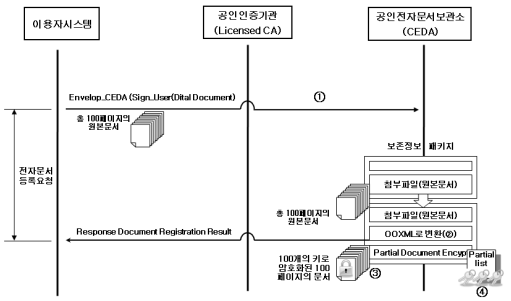


그림 6. 전자문서 등록 및 보관 처리 흐름도

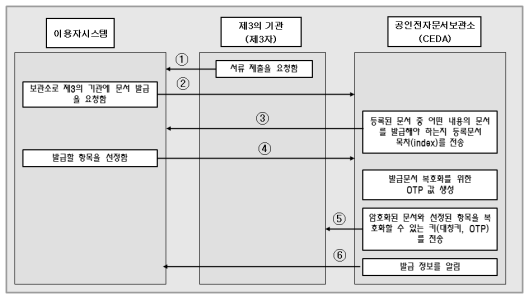


그림 7. 부분정보 발급 처리 흐름도

전자문서의 발급이 완료되었으므로 해당 발급 내역을 이용자에게 알린다.

3.4 OTP를 활용한 제안시스템의 전자문서 발급

이용자로부터 공전소에 전자문서 등록을 요청받으면, 공전소 서버는 향후 등록 된 문서 중 일부 즉 부분문서 발급을 위하여 OOXML(Office Open XML) 처리과정을 통해 문서를 세분화하여 분리하고, 각각 서로 다른 대칭키를 이용하여 암호화 한 후 보관한다. 문서 등록 시 이용자의 요청에 의해 100개의 세부 문서로 분리된다면, 이 문서 전체를 암호화 하는데 서로 다른 100개의 대칭키가 사용된다.

향후 이용자가 이 문서의 부분발급을 요청할 때 60개의 분리된 문서의 발급을 요청한다면, 60개의 문서를 발급함과 동시에 이용자에게 복호화 키 60개를 전달해 야 암호화된 문서를 복호화 할 수 있을 것이다. 이 경우 복호화 키 분배의 어려움, 복호화 속도의 증가 및 다수의 키 전송에 따른 Network Overhead 등과 같은 문제점이 예상된다.

따라서 제안시스템에서는 Link를 이용하여 복수개의 키가 전송되는 것을 방지하고, 키 유출에 대비하여 문서 발급 시 실시간으로 OTP 값을 생성하여 이를 다음 키 습득을 위한 Link 정보(Index) 생성 및 복호화에 참여시킴으로써 발급문서의 보안을 강화하였다. 실시간 OTP를 사용하는 이유는 부당한 이용자가 암호화된 원본파일에서 특정페이지에 대한 Key 값을 습득해도, 다음 링크페이지에 대한 정보를 복호화 하지 못하도록 하기 위한 것이며, 만약 실시간 OTP 값이 없다면 부당한 이용자가 현재페이지에 대한 Key 값을 알아도 다음 페이지를 복호화하지 못하게 됨으로써, 발급된 문서의 정보를 보호하기 위함이다.

제 3자가 등록된 문서 중 3, 10, 23 페이지의 부분문서 발급을 요청한다면, 발급된 전자문서 하단에 다음 발급될 페이지에 대한 Link 정보가 기록되므로, 그림 8의 ①과 같이 3페이지 하단에는 3페이지를 복호화 할 대칭키, 다음 발급 페이지인 10페이지 복호화키, 마지막으로 OTP 값, 이상 3개의 값을 "exclusive OR(⊕)"하여 생성된 값을 다음 페이지(10페이지) 링크 정보 키로 사용하기 위하여 3페이지 하단에 삽입하여 저장한다. 10페이지 하단의 23페이지에 대한 링크 정보 키도 그림 8의 ②와 같이 3페이지 하단의 링크정보 계산한 방식과 동일하게 계산하여 저장한다.

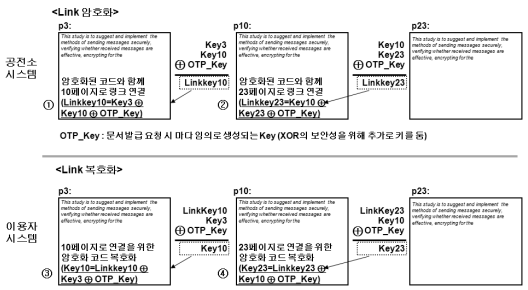


그림 8. Key 보호 및 문서보안 처리 흐름도

Ⅳ. 성능 평가 및 보안성 비교 분석

4.1 구현 환경

공전소 시스템과 유사한 환경하에 본 논문에서 제안하는 시스템의 성능 평가를 하였다. Visual C# 2005, ASP.NET을 통해 인증서 발급을 위한 웹 서버 구축과 메시지 전송을 위해 SOAP 방식의 통신 프로토콜을 이용하였다. 이용자시스템은 Intel(R) Core2 CPU 1.87GHz와 1GB의 RAM, MS-Windows XP Professional의 환경으로 테스트를 진행하였다.

이용자시스템에는 제안시스템으로 접속을 한 다음, 제 3자가 이용자시스템으로 전자문서 발급을 요청하면 제안시스템으로부터 전자문서를 발송해 줄 수 있도록 구성하였고, 암·복호화 과정이 수행되면서 문서를 열람 할 수 있도록 구성하였다.

인증서 발급을 위해 그림 9와 같이 웹서비스 기반의 인증기관(CA) 인터페이스를 제공하기 위한 CA_Server를 기반으로 구성하였으며, 이용자의 공개키를 전송받는 PublicKey_In_n_Cert_Issue를 통해 CA_Server의 인증서 및 개인키를 사용하여 이용자의 인증서를 발급한다. 또한 Cert_Verify메뉴는 인증서의 유효상태를 검사하여 유효한 이용자인지를 판단하도록 하였다.

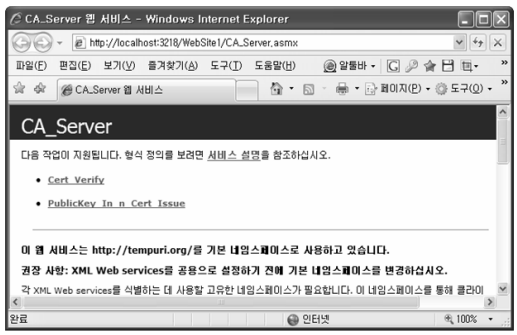


그림 9. CA_Server 웹서비스 인터페이스

제안시스템은 인증서를 통한 암호화를 위해 공개키 및 개인키를 생성한다. 키 사이즈는 1024bit를 기본으로 유지하며, 공개키 방식을 통해 키를 관리하는 일반적인 CA 기능과 같이 운용된다. 제안시스템에는 4가지 웹서비스 기능이 있으며, 각각의 기능은 다음과 같다.

- Receive_Cert : 이용자 인증서 획득 기능
- Receive_Document_Registration : 이용자 문서 등록 기능
- Document_Verify : 문서 검증 기능
- Request_User_Document : 제 3자가 이용자의 문서를 요청할 때 사용되는 기능이며, 이때 BeforeDeserialize 과정을 거쳐 보내주게 된다.
- Send_Document_Key : 제 3자에게 키 전송 기능

4.2 구현 결과 및 성능 평가

본 논문에서 실험 평가를 위해 63Kbytes 크기의 실제 사용되는 전표 스캔 문서 1000장을 데이터로 사용하였고, 기존시스템에서의 암호화 방법은 1024 Bit의 공개키 및 개인키를 사용하였다. 제안시스템 역시 1024 Bit의 공개키 및 개인키를 사용하였으며, 문서를 암호화할 대칭키 암호화는 AES 암호화 방법을 사용하여 평가를 수행하였다.

다음은 암호화에 대한 시간을 비교 분석한 결과는 그림 10과 같이 기존시스템의 1,000장 전체 암호화를 기준으로, 제안시스템은 그림 10의 Ⓐ와 같이 약 650장을 초과하면서 암호화 시간이 제안시스템보다 증가하기 시작했으며, 다른 데이터인 수표 이미지 데이터를 사용하여 다시 측정한 결과 기존시스템 1,000장 암호화를 기준으로 평균 600~700장 사이에서 기존시스템보다 제안시스템 암호화 시간이 증가하기 시작했다.

제안시스템은 오히려 연속된 전체 페이지 암호화에 대해서는 비효율적일 수 있으며 전체 페이지 6

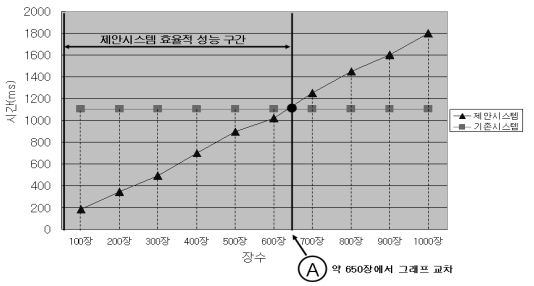


그림 10. 암호화 시간 비교

0~70% 분량의 부분정보 발급 시에 효율성이 높은 것으로 평가되었다.

또한 본 논문에서 제안하는 방식의 보안 강직도는 전자문서를 페이지별로 암호화하고 Link를 이용하여 복호화 키들을 은닉하는 방식을 취하며, 두 개 중 하나의 키는 OTP 값을 이용하기 때문에 키 노출시 재사용이 불가능하며, 두 개의 키를 이용해야 복호화가 가능하므로 보안 강도는 기존 시스템에 비해 강해졌음을 알 수 있다.

기존 전자문서 복호화 방식에 있어서는 전체 파일을 대상으로 하므로 많은 시간이 소요된다. 그러나 본 논문에서 제안하는 방식에서는 그림 11에서와 같이 이중 복호화 방식을 통해 부분 정보별 또는 페이지별 복호화 과정이 진행되면서 문서 열람이 가능하므로 많은 시간적 소요를 단축할 수 있다.

V. 결론 및 향후 연구방향

막대한 양의 계약서와 거래기록을 처리하는 금융업계와 보험업계, 하루에도 수백만 건의 인터넷 트레이딩이 발생하는 증권업계, 지적재산권 문제로 인해 복잡한 기록 관리를 요구하는 제약업계 등에서

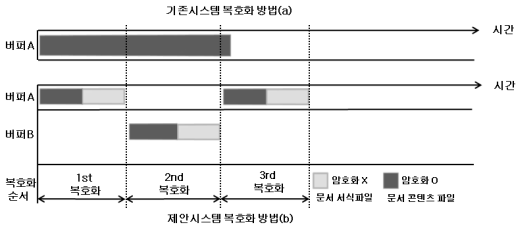


그림 11. 기존시스템과 제안시스템의 복호화 방법

표 7. 암호화에 대한 시간 비교

구분 / 장수	제안시스템 암호화 시간(ms)		기존시스템 암호화 시간(ms) (1000장 기준 평균)
	장수에 따른 계산 값	1,000장 기준 산출값	
100	180	1,800	1102
200	345	1,725	
300	492	1,640	
400	701	1,752	
500	895	1,790	
600	1070	1,783	
700	1250	1,785	
800	1450	1,812	
900	1600	1,777	
1000	1800	1,800	
평 균		1,766	1102

비즈니스 효율화를 위해 전자문서의 도입과 이에 대한 원본 전자문서의 보관 및 증명 업무의 필요성이 절실하다. 이에 따라 전자문서의 원본성 보장 및 증명 외에 유통과정에서의 전자문서 무결성 보장 및 유통 경로 추적, 유통 증적의 확인 및 증명에 관한 요구 수요도 증대하고 있다.

향후 공전소가 점점 활성화되고, 각종 비즈니스가 생성되면서 부분정보 발급에 대한 서비스가 필요하게 될 것이다. 따라서 본 논문에서 제안시스템의 필요성이 더욱 두각 될 것이며, 이에 따라 법적 제도 정비가 이루어짐과 동시에 휴대폰 및 PDA와 같은 다양한 방식의 개인 이동식 휴대 단말기에서도 활용도가 증가할 것이다.

본 연구에 이어 전자문서 등록시 부분적인 일부 문서만의 등록, 삭제, 수정 그리고 인증 서비스를 위한 연구를 계속 진행할 예정이다.

참 고 문 헌

〔1〕 최학열, “전자문서 이용 활성화를 위한 공인전자문서보관소”, 정보통신진흥원, 주간기술동향 1238호, 2006. 3.

〔2〕 박상현, “PKI상에서 효율적인 인증서 관리를 위한 시스템 설계 및 구현”, 인천대 대학원 석사 논문, 2004. 12.

〔3〕 OTP-EKE : 원-타임-패스워드 기반의 키 교환 프로토콜, 한국정보과학회 논문지 A, VOL.29 NO.05 pp.0291~0298, 2002. 06.

〔4〕 ZDNet Korea 뉴스, “MS OOXML 마침내 ISO 표준 승인” 2008. 4.

〔5〕 정제호, 손원성, 임순범, “ODF와 OOXM을 중심으로 한 사무용 전자문서 국제표준화 동향”, 정보과학회지, 제 26권, 제 6호, pp.20-28, 2008. 6.

〔6〕 산자부고시2006-48호, “공인전자문서보관소 전자문서 보관 등 표준업무 준칙”, 2006.

〔7〕 최학열, “전자문서 이용 활성화를 위한 공인전자문서보관소”, 정보통신진흥원, 주간기술동향 1238호, 2006. 3.

〔8〕 한국전자거래진흥원,“전자화문서의 생성 방법 및 절차에 관한 지침 소개”, 2006. 8

〔9〕 Andre Arnes, Mike Just, Svein Knapskog, Steve Lloyd, and Henk Meijer, “Selecting Revocation Solutions for PKI,” Proceedings of The Fifth Nordic Workshop on Secure IT Systems (NORDSEC), 2000.

〔10〕 Booz-Allen & Hamilton INC, Federal Public Key Infrastructure (PKI) Version 1 Technical Specifications: Part E - X.509 Certificate and CRL Extensions Profile.

〔11〕 Peter Hesse and David Lemire, “Managing Interoperability in Non-Hierarchical Public Key Infrastructures,” Network and Distributed System Security Symposium Conference Proceedings, 2002.

성 경 상(Kyung-Sang Sung) 정회원

2001년 호원대학교 전자계산학과 졸업(이학사)

2003년 숭실대학교 대학원 컴퓨터 학과졸업(공학석사)

2004~현재 경원대학교 대학원 컴퓨터 학과 박사수료

<관심분야> 전자거래, 센서네트 워크, 보안, 정보통신

오 동 열(Dong-Yeol Oh) 정회원

1999년 경희대학교 전자계산학과 졸업(이학사)

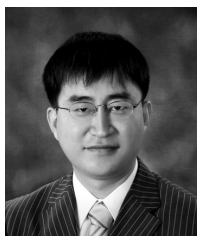
2002년 숭실대학교 대학원 컴퓨터 학과 졸업(공학석사)

2004년 숭실대학교 컴퓨터학과 박사 수료

2007년~현재 인젠트(주) 연구 개발 본부 차장

<관심분야> 유비쿼터스 컴퓨팅, P2P, 멀티미디어

김 정 재(Jung-Jae Kim) 정회원



1999년 영동대학교 컴퓨터공학과(공학사)

2001년 숭실대학교 컴퓨터공학과(공학석사)

2005년 숭실대학교 컴퓨터공학과(공학박사)

2006년 7월~현재 (주)리테일테크 기술연구소 수석연구원

<관심분야> DRM, 암호학, RFID

나 원 식(Won-shik Na) 정회원

2005년 8월 경희대학교 대학원 컴퓨터공학과 박사

2001년 3월~2003년 2월 (주)성신섬유 전산실장

2006년 3월~현재 남서울대학교 교양과정부 교수 (컴퓨터)

<관심분야> 네트워크 보안, 무선 LAN, 의료정보, 전자제어

오 해 석(Hae-Seok Oh) 정회원

서울대학교 대학원 계산통계학과 졸업(석사, 박사)

미국 스탠퍼드대학교 객원 교수

한국 정보처리학회 회장(역임)

1982년~2003년 숭실대학교 컴퓨터학부 교수/부총장(역임)

2003년~현재 경원대학교 소프트웨어대학 교수

<관심분야> Multimedia, Database, 지식경영