韓國 컴퓨터情報學會 論文誌
第13卷 第6號, 2008. 11.

2008-13-6-3-1

전자문서의 안전한 보관 및 발급 서비스 확보를 위한 시스템 설계

성 경 상*, 김 정 재**, 오 해 석***

System Design for the Safe store and Issue Service Assurance of the E-Document

Kyung-Sang Sung*, Jung Jae Kim**, Hae-Seok Oh***

요 약

공인전자문서보관소는 전자기록의 진본성을 확인하고 보장하는 제도로서 법적인 보호 아래 보관되며, 전자기록 사항을 진정한 것으로 추정하고 전자기록의 내용이 변경되지 않았음을 입증한다. 그러나, 전자기록은 매체의존도가 높고 정보의 유실위험이 매우 높은 문제점을 가진다. 또한, 정보의 첨삭(첨부와 삭제)과 수정이 용이하기 때문에 전자기록의 진본성과 무결성에 대한 문제가 야기되고 있다. 현존하는 시스템에서는 다음과 같은 비효율성을 드러내고 있다. 원본성 보장을 위한 기존의 전자문서 암호화 방법은 하나의 대칭키로 전체 문서의 암호화 과정을 수행하며, 중간에 수정되어지는 정보가 발생시에는 해당 문서 전체 내용을 재스캔 및 재암호화 과정을 수행해야 한다. 이러한 비효율성을 극복하기 위해, 본 논문에서는 등록 요청된 전자문서에 대해 페이지의 연관성을 기반으로 하는 Link 정보를 이용하여 암호화하고 관리함으로써 해당 문서의 부분 정보 수정 요청시 발생하는 비용적 효율성을 극대화시켰으며, 키 관리의 복잡도를 증가시켜 정보 노출에 따른 문제점을 최소화함으로써 보안성을 향상시켰다.

Abstract

Certified e-Document Authority keep it with protection legal as a system a guarantee and identifies originality of an e-Record, It presume to be authenticity e-Records and contents of an e-Record prove what was not changed. But, e-Records has high medium degree of dependence and loss danger of information has very high problems. In addition, Because correction(attachment and deletion) and a revision of information are easy, a problem for integrity and the originality of an e-Record is caused. Existing system show the following inefficient. For the originality guarantee, an existing e-Documents encryption method accomplishes a encrypted process of a whole document with a symmetric key, if the information revised midway, the whole documents content must accomplish re-scanning and re-encryption process again. To get over such inefficient, this paper maximize efficiency which occurred at the time of partial information revision request by encryption and managing using the link information based on the linkage characteristics of the each page on the registered requested e-Documents, It was able to increase security configuration by minimizing problems on an information exposure through increasing complicated of the key management.

▸ Keyword : certified electronic Document Authority(공인전자문서보관소), authenticity(진본성), originality(원본성), integrity(무결성), security(보안성)

• 제1저자 : 성경상
• 접수일 : 2008. 8. 7, 심사일 : 2008. 10. 6, 심사완료일 : 2008. 11. 26.
* 경원대학교 전자계산학과 박사과정 ** 숭실대학교 컴퓨터공학과 연구원 *** 경원대학교 IT대학 교수

Ⅰ. 서 론

최근 산업전반에 확산되고 있는 디지털화와 전자거래의 활성화는 기업 운영에 많은 순 기능적인 역할과 함께 적지않은 역기능적인 역할을 하여왔다[1]. 정보통신 인프라의 질적 향상에 따라 전자거래의 비약적이고 양적인 팽창을 이루게 되었고, 전자문서에 의한 종이문서의 대체가 가속화 되고 있다. 또한, 전자기록의 활성화로 종이문서 보관에 필요한 비용을 점진적으로 감축할 수 있게 됨은 물론 검색·활용 그리고 그 보관방안에 있어 시간과 비용을 획기적으로 관리할 수 있으며, 재해복구시스템을 이용한 다중보관 방식으로 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 전자문서의 이용이 확대되어야 함에도 불구하고 종이문서와 같은 원본성 확보가 어려움과 원본 전자문서의 보관 및 증명 업무의 필요성이 절실하다.

이러한 이유로 현재, 법률로 전자문서의 생성·유통은 전자서명으로 안정성을 보장하고 있다. 그러나, 보관단계에서는 위·변조, 멸실 방지에 대한 방안이 미비한 상태에 머무르고 있다.

따라서 위와 같은 문제를 해결하기 위해서는 전자문서의 신뢰성·안전성 확보와 신원확인, 전자문서의 위·변조방지, 개인정보의 보호 등을 선결과제로 활성화되어야 한다. 따라서 법률을 통해 원본성 문제를 해결하기 위한 방안으로 공인전자문서보관소(전자거래기본법 제 5장 2, 이하 공전소)를 통해 보관중인 전자문서는 그 내용이 변하지 않았음을 법적으로 보장하고 있다.

공인전자문서보관소의 주요기능인 문서보관기능, 송수신의 기능은 전자기록의 진본성 유지를 위한 방안의 관리방안과도 직접적인 연관성이 있다. 문서작성, 문서배달과 관련해서는 전자기록의 정체성과 관련되고, 문서변환, 문서관리, 문서검색, 보존연한, 이관·폐기, 보존매체, 백업, 복구, 암호화, 위조 변조등은 전자기록의 무결성을 유지시키기 위한 방안으로 마련하고 있다.

전자기록의 업무활동 과정을 통해 관리되는 정보를 통제하고 생산단계에서부터 보존되어 폐기될 때까지 감사 추적을 가능하게 하여 진본임을 유지 관리할 수 있게 한다. 또한 기록과 관련된 업무과정을 파악할 수 있는 모든 사항들에 대한 프로파일을 상세히 기록 관리해야 한다. 또한, 전자기록의 송·수신시 위·변조의 위험성으로부터 보호하기 위해 전자기록에 포함된 전자서명으로 신원확인과 무결성을 입증하도록 관리한다. 따라서, 전자기록의 특성상 기록자체가 변경될 수 있기 때문에 보존 통제로서 관리되어야 한다. 보존통제는 매체 이전 시 기록이 변하지 않도록 하는 시스템적 통제와 기록의 정체성과 무결성을 보존하는데 많은 영향을 주는 여러 기술적 조치들이 발생함에도 기록이 진본으로 남겨지도록 유지하는 통제로서 진본성 유지를 위해 갖추어야 할 필요조건이다.

전자문서의 신뢰성과 안정성을 보장하는 공전소를 구축·운영하는데 있어 담당자의 책임하에 종이문서원본을 확인하고 스캔한 후 디지털화하는 일련의 작업을 수행한다. 이 후, 등록된 전자문서는 향후 제 3자의 요청에 의해 정보를 제공하는 과정에서 다음과 같은 문제점들을 가진다.

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, 등록된 전자문서의 수정 사항이 발생시 제안하는 키 방식을 통해 등록된 전체 정보가 아닌 요청된 정보만 수정함으로써 불필요한 정보의 노출을 최소화를 꾀함으로써 공전소 운영 방식의 효율화를 가져올 수 있으며 이를 통해 정보유출에 대한 신뢰성을 향상할 수 있다.

Ⅱ. 관련 기술 및 서비스

2.1 공인전자문서보관소 서비스

공전소는 크게 보관, 송·수신, 증명서비스 등을 〈그림 1〉과 같이 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 증명서비스를 위해 시점확인서비스도 할 수 있다[2].

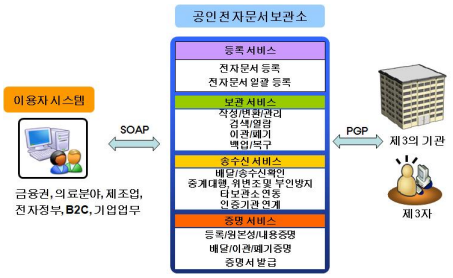

그림 1. 공인전자문서보관소 구성 및 서비스
Fig 1. CEDA Composition and Service

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.

2.2 전자서명 생성 및 검증 절차

전자서명이란 현실 세계에서 인감도장을 날인하여 거래하는 것처럼 공개키 암호화 방식을 이용하여 디지털 데이터에 서명을 행하는 것으로 전문성과 공신력이 있는 인증기관이 확인 및 증명하는 것을 말한다. 즉, 신뢰성이 검증된 개인·단체 등에 전자서명이 첨부된 인증서를 발급, 인터넷 등 가상공간에서 거래 당사자 간의 신뢰성을 보증해 주는 역할을 하게 된다[3].

인증기관의 인증서를 발급 받은 이용자가 행하는 전자서명의 생성 및 검증 절차는 〈그림 2〉와 같다.

그림에서 보듯이 ① 서명하고자 하는 전자문서를 해쉬 알고리즘을 통해 전자문서 해쉬 값인 축약문서를 생성한다. ② 전자문서 해쉬 값인 축약문서에 자신이 소유하고 있는 전자서명 생성키와 전자서명 알고리즘을 적용하여 전자서명을 생성한 후 ③ 전자서명+전자문서+검증키를 함께 수신자에게 전송한다.

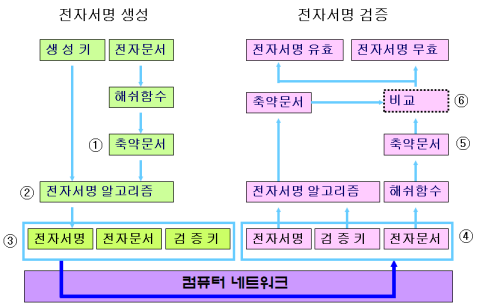

그림 2. 전자서명 생성 및 검증 절차
Fig 2. E-Signature creation and verification process

④ 전자서명을 생성한 사람의 전자서명 검증키의 정당성에 대해서는 인증서를 통해 검증하며, ⑤ 수신된 전자문서의 해쉬 값인 축약문서를 생성한다. 마지막으로 ⑥ 전자문서 해쉬 값인 축약문서에 서명한 사람의 전자서명 검증키와 알고리즘을 적용하여 전자서명을 검증한다.

2.3 OTP를 통한 인증 과정 서술

일회용비밀번호(One Time Password : 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[4].

OTP 인증 방식은 암호 알고리즘의 일종인 해쉬 함수(Hash function)을 이용하는 방식으로 사용하기에 간단하고 어떤 비밀 정보도 호스트에 남지 않기 때문에 안전한 시스템이다.

〈그림 3〉에서와 같이 사용자의 입력값에 해쉬 함수를 정해진 회수 'n'번만큼 적용해서 1회용 패스워드를 'n'개 생성한 후 맨 마지막에 생성된 패스워드 값을 인증서버와 사용자(또는 사용자 S/W)가 나눠 갖게 된다. 그 후 사용자는 미리 생성된 패스워드 중에서 'n-1'번째 패스워드를 사용해서 사용자 인증을 시도하면, 인증서버는 사용자로부터 받은 패스워드에 해쉬함수를 1회 적용해서 나온 값이 인증서버에 있는 패스워드값(n번째 패스워드값)과 같은지 비교한 후 인증 성공/실패를 판단하게 된다. 인증에 성공하게 되면 인증서버는 'n-1'번째를 새로운 패스워드로 저장하고 두 번째 패스워드부터는 해

쉬 함수 적용 회수를 순차적으로 한번씩 적게 적용한 값을 패스워드로 사용하게 된다.

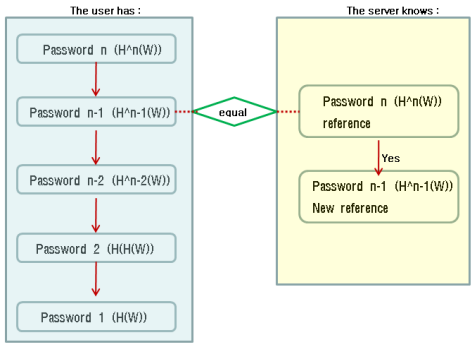

그림 3. OTP를 통한 인증 과정
Fig 3. Certification process using OTP

인증을 여러 번 수행하게 되면 해쉬 함수 적용 가능 횟수가 하나씩 줄어들게 되므로 어느 시점에 다다르면 패스워드를 재초기화 시켜 줘야 하는 불편이 있으나, PC 등에서 저장해 놓거나 미리 계산해 놓은 후에 사용할 수 있다는 장점을 가지고 있다.

2.4 OOXML 구조와 개념 정의

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 OOXML(Office Open XML)이 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[5].

OOXML은 다음 〈그림 4〉와 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 컨테이너 구조를 제공하며 이를 OPC(Open Packaging Convention)로 표기한다.

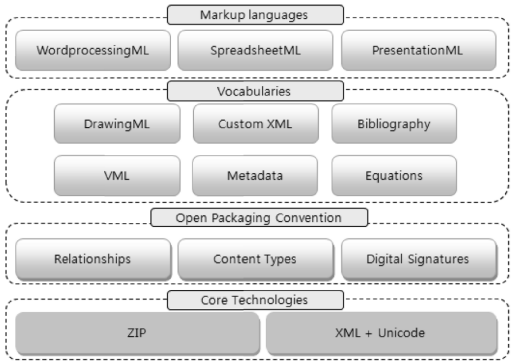

그림 4. OOXML의 주요 구조
Fig 4. The Essential Scheme of the OXML

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[6].

III. 효율적 키 정보 활용을 통한 공전소 시스템 설계

3.1 제안시스템 개요

공전소의 효율적 보관 관리 방안을 위해 제안하는 방법과 같이 이용자시스템에서 등록 요청된 문서를 이용자가 정하는 기준에 따라 세분화하고 리스트화한다. 각각 서로 다른 방식의 키를 생성 후 이용하여 암호화 과정을 거친 다음 메타데이터 정보와 함께 보관소에 정해진 규칙에 따라 보관한다. 향후 이용자의 요청에 의한 문서의 수정 또는 업데이트가 요청되어지면, 제안하는 시스템의 특성상 개별적으로 관리되는 문서의 해당 정보에만 허가되고 관리됨으로써, 보안적 측면과 더불어 비용적 부분에 있어서 효율화를 이끌어 낼 수 있다[7]. 등록 요청된 문서의 부분 관리 방안에 관한 제안시스템의 흐름은 〈그림 5〉와 같다.

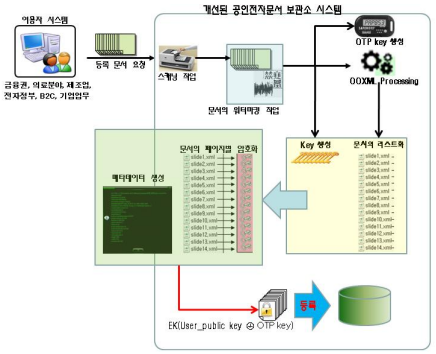

그림 5. 전자문서 등록 업무 처리 흐름도
Fig 5. E-Document Registration operation process

본 논문에서 제안하는 개선된 공인전자문서 보관소 시스템에 접근하기 위하여 이용자시스템에서 공전소 시스템에 문서 등록을 요청한다. 전자문서의 전송은 SOAP(Symbolic Optimal Assembly Program)을 통해 이루어지며, 등록 요청된 문서는 공전소 내의 인가된 관리자에 의해 인가된 장비를 통해 전자문서화한다. 이후 문서에 저작권을 부여하기 위한 워터마킹 작업이 이루어지며, 문서에 대한 암호화 키(OTP key, 문서에 대한 key)를 생성한다. 워터마크 처리된 문서를 OOXML 처리 과정을 통해 문서를 리스트화한 후, 관리 목록에 추가한다. 리스트화 되어진 개별 문서들은 생성된 문서 키와의 개별적 암호화를 통해 관리된다. 페이지별 암호화 문서 리스트와 해당 키와의 연관성을 두며, 인증을 위한 메타데이터를 생성한다. 이와 같은 과정을 마친 후, 사용자의 공개키와 생성된 OTP key를 통해 암호화 한 후, 보관소에 보관하는 과정을 거친다. 향후, 문서를 제 3자에게 발급할때 대칭키, OTP값과 같이 2개의 복호화용 키가 해당 암호화된 문서와 함께 전달됨으로써 보안이 강화된 문서가 전달된다.

3.2. 상호인증 절차와 문서 등록 및 암호화 과정

〈그림 6〉은 상호인증 처리절차와 문서 등록과 암호화 과정에 따른 처리 절차를 보여준다.

상호 인증 과정은 사용자 인증과 공전소 인증으로 구분된다. 사용자 인증은 공인인증기관을 통해 정당한 이용자인지 공전소 입장에서 검증하는 단계로서 실시된다. 먼저, 사용자는 공인인증서를 통해 정당한 이용자인지 검증한 후, 요청 메시지를 전송한다. 공전소는 이용자 인증정보 내의 인증서와 공전소가 관리하는 이용자의 인증서가 동일한 지를 확인한 후, 공인인증기관과 연계하여 추출한 공인인증서가 유효한지를 확인 후, 요청 메시지의 전자서명을 검증한다[8].

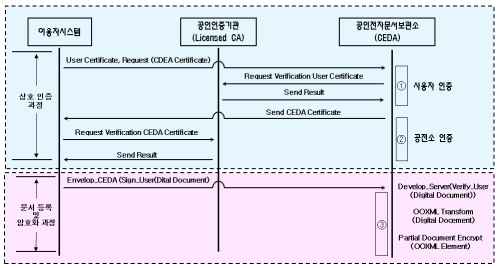

그림 6. 상호인증 절차와 문서 등록 및 암호화 과정
Fig 6. Mutuality Certification procedures and Document Registration and cryptograph process

이와 같은 과정을 통해 공전소와 이용자간에 인증이 정상적으로 이루어지면, 서로간의 인증이 완료되었으므로 상호간에 세션 아이디(Session ID)를 저장하고 통신하게 된다. 이렇게 교환된 인증서는 상호인증에 사용될 뿐만 아니라 인증서에 포함된 서로의 공개키를 이용하여 전자문서의 암호화에 사용하게 된다.

3.3. OOXML 기반의 처리 절차

이용자로부터 암호화된 원본 파일을 수신 받으면 공전소 시스템은 개인키와 이용자의 공개키를 통해 원본 파일을 복호화한 후 〈그림 7〉의 ①과 같이 OOXML 처리를 통해 실제 문서의 내용과 메타데이터를 분리한다. 메타데이터가 분리된 후 실제 전자문서는 ②와 같이 이용자가 분류한 기준에 따라 OOXML 처리과정을 통해 세분화되고, ③과 같이 각각 서로 다른 대칭키에 의해 암호화되어 보관된다.

등록 요청된 전자문서의 압축을 풀게 되면 해당 지정 폴더에 각 페이지 내용 정보가 포함되어 있으며, 서로 다른 대칭키에 의해 암호화되고 리스트화되어 관리된다.

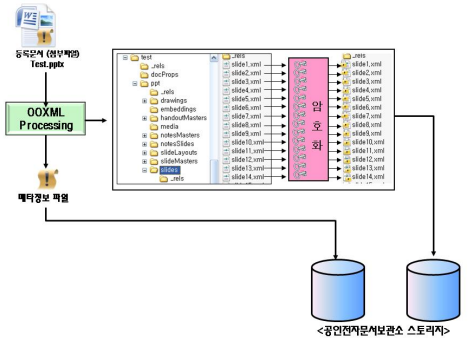

그림 7. OOXML 기반의 처리 절차
Fig 7. operation process on the based OOXML

3.4 암·복호화 방안을 이용한 전자문서 발급

이용자로부터 공전소에 전자문서 등록을 요청받으면, 공전소 서버는 향후 등록 된 문서 중 일부 즉 부분문서 발급을 위하여 OOXML 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 사용되어지는데, 제안시스템에서는 Link 정보를 이용하여 복수개의 키가 전송되는 것을 방지하고, 키 유출에 대비하여 문서 발급시 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.

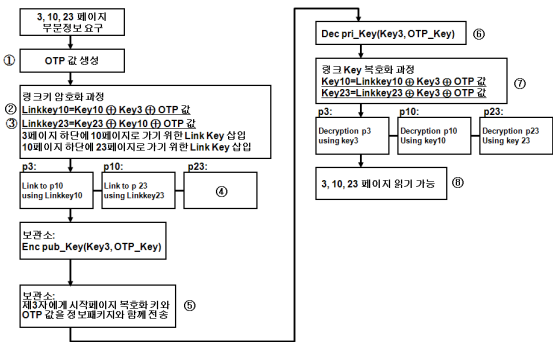

그림 8. Link 정보와 OTP key를 이용한 처리 흐름도
Fig 8. Operation process using Link Information and OTP Key

제 3자가 등록된 문서 중 3, 10, 23 페이지의 부분문서 발급을 요청한다면, 발급된 전자문서 하단에 다음 발급될 페이지에 대한 Link 정보가 기록되므로, 〈그림 8〉의 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 8〉의 ②와 같이 3페이지 하단의 링크정보 계산한 방식과 동일하게 계산하여 저장한다.

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 9〉와 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
Fig 9. CA_Server web Service Interface

제안시스템은 인증서를 통한 암호화를 위해 공개키 및 개인키를 생성한다. 키 사이즈는 1024bit를 기본으로 유지하며, 공개키 방식을 통해 키를 관리하는 일반적인 CA 기능과

같이 운용된다.

4.2 구현 결과 및 성능 평가

4.2.1 암·복호화 속도 평가

본 논문에서 실험 평가를 위해 5MB 크기의 전자문서 Test.pptx를 각각 기존 공인전자문서보관소 시스템과 제안하는 시스템을 통해 비교평가 하였다. 암호화에 대한 시간을 비교 분석한 결과는 〈그림 10〉과 같이 기존시스템보다 훨씬 빠른 성능을 보여주고 있으며, 〈표 1〉에서 보듯이 복호화 속도 측면에서도 속도적 우수성을 보인다.

암호화 속도에 따른 수행시간 비교를 위해 데이터(수표 이미지) 1,000장 분량을 기준으로 실험 평가하였으며, 650장을 기준으로 속도에 따른 성능 교차점이 발생됨을 알 수 있었다. 이는 암호화에 따른 데이터를 개별적으로 운용함에 따른 시스템적 성능 차이로 볼 수 있다.

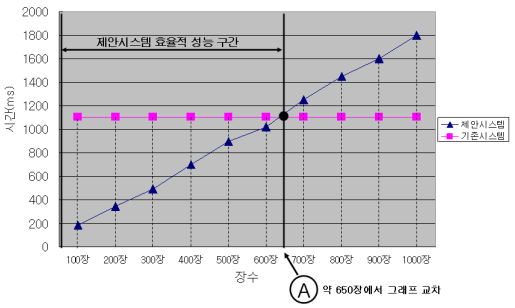

그림 10. 제안시스템의 암호화 비교
Fig 10. Cryptography comparison of proposed system

제안시스템은 오히려 연속된 전체 페이지 암호화에 대해서는 비효율적일 수 있으며 전체 페이지 60~70% 분량의 부분정보 발급시에는 효율성이 높은 것으로 평가되었다.

표 1. 문서 복호화 속도 비교
Fig 1. Document Decryption Speed comparison

	1회	2회	3회	●●●●	100회	평균
기존 시스템	1초 203ms	1초 211ms	1초 199ms	●●●●	1초 211ms	1초 201.3ms
제안 시스템	15ms	13ms	12ms	●●●●	14ms	14.02ms

그러나, 제안시스템은 오히려 연속된 전체 페이지의 수가 증가할수록 키 생성과 관리에 대해서는 비효율적일 수 있으며, 암복호화에 따른 속도 또한 증가함으로써 효율성이 떨어지는 것으로 평가되었다. 하지만, 속도적 문제점은 시스템의 성능 향상을 기반으로 극복할 수 있을 것으로 사료된다.

4.2.2 보안성에 대한 평가

전자문서 시스템에서 가장 중요한 것은 강한 보안성을 바탕으로 무결성을 유지 하는 것이다. 제안시스템에서는 부분정보 발급을 위해 문서 암·복호화에 대한 시간이 기존시스템에 비해 증가할 수 있지만, 이에 반해 보안성은 증가한다. 제안시스템은 기존시스템과는 다르게 전자문서를 대칭키를 이용하여 페이지별로 암호화하였고, Link 정보를 이용한 복호화 키 은닉방법을 제안하였다. 등록 요청받은 전자문서를 이용자의 요청으로 세분화 한 후 서로 다른 대칭키를 이용하여 암호화를 수행한 후 하므로, 공개키 암호화 기법을 사용하여 전체의 내용을 암·복호화 하는 기법보다는 빠르다.

제안하는 시스템은 전자문서를 페이지별로 암호화하고 Link 정보를 이용하여 복호화 키들을 은닉하였고, 이중 암호화 방식을 이용하였으므로 복호화에 따른 복잡도를 증가시킴으로써 보안성을 증가시켰다.

V. 결론 및 향후 연구방향

기존 서류거래와는 달리 전자거래는 비대면 거래라는 특징 때문에 신뢰성 확보에 따른 문제점을 동반하게 되었으며, 제3자를 통한 전자서명 인증 방식을 활용함으로써 위와 같은 문제를 해결할 수 있게 되었다. 이러한 현대적 기술을 활용하여 폭주하는 막대한 양의 문서를 처리하고 기록 관리에 대한 요구를 만족하기 위한 방안으로 전자문서보관에 대한 요구 수요가 증대하고 있다. 전자문서에 대한 신뢰성 부여를 위한 방안으로 암호화 방법을 활용하고 있다.

본 논문에서는 이용자의 해당 대칭키가 노출되었을때 더 이상 전자문서에 대한 안전을 보장받지 못한다는 문제점을 해결하기 위해, 여러 개의 대칭키를 생성하여 요소별로 추출하여 암호화하고 OTP값을 통해 관리하는 방법을 제안하였다. 만약 해당 키가 노출되는 문제가 발생해도 정보 노출의 최소화를 통해 최대한의 정보 보호를 이끌어낼 수 있다.

그러나, 제안시스템은 오히려 연속된 전체 페이지의 수가 증가할수록 키 생성 복잡도와 관리에 대해서는 비효율적일 수 있으며, 암·복호화에 따른 속도 또한 증가함으로써 효율성이 떨어지는 것으로 평가되었다. 하지만, 속도적 문제점은 시스

템의 성능 향상을 기반으로 극복할 수 있을 것으로 사료되지만, 향후 지속적인 연구를 통해 키 관리 방안을 향상시키도록 계속 진행할 예정이다.

참고문헌

〔1〕 장덕성, "누출차단과 식별을 위한 다큐먼트 보안 디자인", 한국 컴퓨터정보학회 학회지, 제 10권 제 2호, pp.16-24, 2003. 6

〔2〕 최학열, "전자문서 이용 활성화를 위한 공인전자문서보관소", 정보통신진흥원, 주간기술동향 1238호, 2006.3

〔3〕 천재용, "전자거래 기록의 진본성 유지를 위한 방안", 명지대학교 기록과학대학원 석사학위 논문, 2005.

〔4〕 김기환, 박대우, "Tokenless OTP를 활용한 인증 모델", 한국컴퓨터정보학회지, 제 14권, 제 2호, pp. 205-214, 2006, 12

〔5〕 ZDNet Korea 뉴스, "MS OOXML 마침내 ISO 표준 승인" 2008. 4.

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

〔7〕 명유진, "전자문서의 보관 및 유통 활성화 방안에 관한 연구, 호서대학교 벤처전문대학원 석사논문, 2005.

〔8〕 박재표, 이광형, 김정재, 전문석, "라이센스 에이전트를 이용한 디지털 저작권 보호 및 감시 시스템의 설계," 한국산업정보보안학회 논문지, 제4권, 제1호, pp.15-24, 2004.

〔9〕 Australian Government e-Authenticaiton Framework Implementation Guide for Government, AGIMO, 2005. 3

〔10〕 Barbara L. Fox Brian A. LaMacchia, "Encouraging Recognition of Fair uses in DRM Systems," Communications of The ACM, VOL. 46 NO. 04 pp. 61 ~ 63 2003. 04

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

저 자 소 개

성 경 상

2003년 : 숭실대학교 대학원 컴퓨터학과졸업(공학석사)

2004~현재 : 경원대학교 대학원 컴퓨터 공학과 박사수료

관심분야 : 전자거래, 센서네트워크, 보안, 정보통신

김 정 재

2001년 : 숭실대학교 컴퓨터공학과 (공학석사)

2005년 : 숭실대학교 컴퓨터공학과 (공학박사)

2006년 ~ 2008 : (주)리테일테크 기술연구소 수석연구원

관심분야 : DRM, 암호학, RFID

오 해 석

1981 : 서울대학교 대학원 컴퓨터과학과 졸업(이학박사)

1982~2003 : 숭실대학교 컴퓨터학부 교수/부총장 (역임)

2003~현재 : 경원대학교 소프트웨어 대학 교수

관심분야 : Multimedia, Database, 지식경영