온라인 환경에서의 전자문서 안전배포 및 이용을 위한 인증방법 설계 및 구현

Design and Implementation of an Authentication Method for Secure Distribution and Use of E-documents in Online Environment

김 용(Yong Kim)*

초 록

개방형 네트워크인 인터넷의 확산과 웹(Web) 기술이 발전함에 따라 다양한 형태의 전자문서가 생산 및 유통되고 있다. 전자문서(e-Document)는 문서를 생산한 기관에서 일련의 행위를 유발하기 위한 정보 또는 내용을 포함하는 기록물의 일종이다. 본 연구에서는 이러한 전자문서의 안전한 이용 및 유통을 위하여 요구되는 보안 알고리즘을 제안하였다. 특히, 제안된 방법은 전자문서의 진본성(Authenticity), 신뢰성(Reliability), 무결성(Integrity)을 보장하기 위한 전자서명의 생성과 이용자의 정당성 확보를 위한 인증과정에 적용할 수 있다. 또한, 보안성과 저장성에 있어서 높은 신뢰도를 가지고 있는 스마트카드를 활용함으로써 기존의 방법에 비하여 높은 보안성을 확보할 수 있었다. 제안된 방법의 효율성 및 신뢰성에 대한 검증을 위하여 실험을 수행하였다.

ABSTRACT

With explosive growth in the area of the Internet and IT services, various types of e-documents are generated and circulated. An e-Document is a sort of electronic records which a organization performs works and goals. In this study, we propose a security algorithm for secure use and distribution of e-documents. Especially, the proposed method can be applied to generate digital signature which can guarantee authenticity, integrity, confidentiality of an e-document and authenticate authorized users. Also, we can get higher security level as using a smart card that provides highly storing capacity and security. We carried out an experiment to verify efficiency and security of the proposed method.

키워드: 인증, 전자문서, 무결성, 스마트카드, 디지털콘텐츠
authentication, e-document, security, integrity

* KT 인프라연구소 책임연구원(yongkim@kt.co.kr)

■ 논문접수일자 : 2008년 2월 13일 ■ 게재확정일자 : 2008년 3월 3일
■ 情報管理學會誌, 25(1): 75-98, 2008. [DOI:10.3743/KOSIM.2008.25.1.075]

1. 서 론

인류문명의 역사는 문자의 발명과 더불어 시작되었으며, 국가 또는 민족의 흥망성쇠는 문자의 발명과 활용에 의해 결정되었다고 해도 과언이 아닐 수 없다. 이러한 문자의 발명과 활용은 문자를 남길 수 있는 소재의 발달과 함께 한다. 초기의 암벽, 바위 등의 자연물에서 시작하여 중국의 대나무 고대 이집트의 파피루스와 같은 원시소재를 거쳐 중세 인쇄술 및 종이의 발명으로 인류문명은 비약적인 발전을 이룩하게 되었다. 이러한 문자문명은 인터넷과 정보기술의 발달과 함께, 새로운 발전의 전기를 맞게 되었다. 특히, 인터넷과 MS-Word, 한글, 아크로밧트(Acrobat) 등으로 대표되는 저작도구(Authoring tool)의 개발 및 발전은 전자문서라는 새로운 문서작성 및 보존방법을 만들어 내었다. 과거의 산업 및 농경사회에 있어서 새로운 발명이나 발견을 수용하는 방식과 시간은 단계적 적용 및 다양한 시행착오를 통하여 단계적인 발전과 수용이 이루어졌다. 그러나 현재에 있어서는 이러한 현상은 매우 빠른 속도로 사회 전반에 걸쳐 전방위적으로 동시에 수용되는 현상을 보여주고 있다. 이러한 현상은 인류문명의 생산 및 보존의 매체로서 대변되는 문서의 소재에도 적용되고 있다. 현재 문서의 생산에 있어서 종이문서는 급속한 속도로 전자문서로 전환 및 생산되고 있으며 기존의 종이문서 또한 변환과정을 통하여 이미지형태의 전자화문서로 변환되고 있는 상황이다. 이러한 현상은 정부, 공공 및 민간기관에서 생산되는 문서, 법령 등의 기록물에 있어서도 분명하게 나타나고 있다. 이는 문서의 관리 및 보존 등의 측면에 있어서 종이문서에 비하여 전자문서가 가지는 월등한 효용가치 및 효율성에 기반 한다. 이러한 현상의 주요한 원인은 종이문서와 전자문서의 존재형태에 기인한다. 즉 종이문서는 공간적으로 존재함에 반해 전자문서는 비공간적으로 존재한다는 것이다. 종이문서와 극명하게 대비되는 전자문서의 비공간적 존재의 특징은 전자문서 생산 및 활용을 더욱 활성화 하게 하는 요인이 되고 있다. 이를 위하여 정부에서는 전자문서가 종이문서와 같이 동일한 법적/제도적인 효력을 갖도록 하기 위하여 전자거래기본법을 제정하여 전자문서의 개념을 적극적으로 수용하고 있으며 최근 2005년에는 개정을 통하여 공인전자문서보관소에 관한 규정을 신설하고 정부기관 뿐만이 아니라 산업전반에 있어서 전자문서의 사용을 장려하고자 하였다(최학렬 2006). 이와 같은 법/제도의 정비에 따라 정부, 공공기관을 포함하여 은행, 통신사업자 등의 민간기관에서는 전자문서의 활용을 확대하거나 이를 계획 중에 있다. 현재 우리나라 기업 · 금융기관 등은 각종 문서 또는 서류의 유통 · 보관에 연간 1조 원 이상을 소요하고 있는 것으로 추정되며, 검색 · 참조 등 보관문서의 활용도 어려움이 있는 것이 현실이다. 예를 들어, 신용카드 매출전표의 경우 연간 15억 매가 발행되고 있는데, 이를 신용카드사가 수거하고 문서창고에 보관하는 데 약 1,200억 원 가량의 비용이 소요되는 것으로 추정된다(국회 산업자원부 2005). 또한 전표의 보관중 분실 · 훼손의 위험이 항상 존재하고 있을 뿐만 아니라 분쟁 발생시 해당 신용카드 매출전표를 찾아서 참조하는 데 있어서도 비효율성이 발생한다. 이와 같은 종이문서의 생산,

관리, 유지에 있어서의 비효율성에 대한 대안으로서 전자문서에 대한 선호 및 생산은 지속적으로 증가할 것으로 예상된다.

그러나 전자문서는 종이문서에 비하여 문서로서의 요구되는 정보전달적 기능(Informative function), 증거적 기능(Evidential function) 및 상징적 기능(Symbolic function) 측면(Walden and Savage, 1989)에 있어서 한번 표시된 내용을 그대로 보전해야 하는 증명적 기능과 물리적 존재 자체가 요구되는 상징적 기능에 있어서 문제점을 내포하고 있다(김진환 1999). 이와 관련하여 문서관리와 관련된 국제표준인 ISO 15489에서는 전자문서가 가져야 할 특성으로서 진본성(Authenticity), 신뢰성(Reliability), 무결성(Integrity) 및 가용성(Usability)의 관점에서 이에 대한 해결방안을 제시하고 있다.

한편, 전자문서의 상징적 기능의 확보는 법적/제도적 노력으로서 해결이 가능할 수 있으나 증거적 기능을 만족하기 위해서는 이러한 노력과 함께, 추가적으로 정보기술적인 해결방안이 요구된다. 즉, 종이문서의 경우에 있어서 문서가 갖추어야 할 증거적 요건을 만족하기 위하여 문서를 생산 또는 내용에 대하여 책임을 갖는 개인의 직접 수기(Handwriting)에 따른 서명(Signature)을 통하여 확보할 수 있다. 또한 종이문서는 소재자체의 특징으로 인하여 문서의 내용 및 서명의 매우 어려우며 이를 통하여 문서내용의 기밀성 및 신뢰성을 만족할 수 있다. 그러나 정보시스템과 저작도구를 통하여 생산된 전자문서의 경우에 있어서 종이문서와는 달리 간단한 조작만을 통하여 전자문서의 내용을 쉽게 수정 및 삭제할 수 있다. 정보시스템을 기반으로 저작도구 또는 콘텐츠 생성도구를 통하여 생산되는 관점에서 전자문서는 일종의 디지털콘텐츠라고 할 수 있으며 디지털콘텐츠의 대표적 특징인 수정, 삭제 및 복제의 용이성과 함께, 불법적 생산, 수정 및 복제가 가능한 양면적인 특성을 동시에 내포하고 있다. 이러한 내용의 수정 및 삭제의 용이성은 전자문서 활성화를 더디게 하는 직접적인 요인으로 작용하고 있다. 따라서 일종의 디지털콘텐츠로서의 부정적인 측면은 전자문서의 활성화에 있어서 반드시 해결해야 할 문제점이다.

특히, 정부, 공공기관 및 민간기관에서 내부적 또는 외부적으로 법적/제도적으로 효력을 갖는 문서, 법령, 사규, 증명서 등의 내용 또는 정보를 포함하는 전자문서는 네트워크를 통하여 생산기관에서 이용 또는 보존기관으로 전송된다(송병호 2004). 이와 같은 이용과 보존의 과정에서 전자문서는 위, 변조 및 삭제 등의 위험에 노출되어 있다. 따라서 정보보안의 관점에서 전자문서에 포함된 내용의 위, 변조 및 정당한 이용자에 대한 인증을 통한 전자문서의 기밀성(Confidentiality), 무결성(Integrity), 및 신뢰성(Reliability)을 확보하기 위한 방법이 요구된다. 이를 위한 방법으로서 공인인증서, 전자서명, 이용자식별 및 비밀번호(ID/Password) 등을 활용하는 다양한 방법들이 현재 일부 분야에서 적용되고 있다. 이와 관련하여 초기 Shamir (1984)에 의해 ID(Identification)정보에 기반한 서명 기술이 제안된 이후 ID정보에 기반한 많은 연구가 진행되고 있다.

한편, 정부문서, 증명서, 인증서, 법령 등과 같은 전자문서는 네트워크를 통하여 이용자 또는 요구기관의 단말로 1차 전송된 후, 전자문서

의 생산목적에 따라 1차 전송된 단말에서 전자문서의 보존을 위한 자료관 또는 이용을 위한 하위기관의 2차 단말로 전송되어 온라인 환경에서 이용되거나 또는 기록물로서 보존된다. 이와 같은 특징을 갖는 전자문서는 생성, 유통 및 보존의 과정에서 ISO 15489에서 규정하고 있는 문서로서 요구되는 특성을 만족하여야 한다. 특히, 정부기관 또는 민간기관에서 발급되는 전자증명서 또는 인증서 등의 이용을 위해서 이용자는 2차 단말 또는 저장장치로서 데스크탑 컴퓨터 및 하드디스크, 플로피 디스크, CD, 기타 메모리 장치 등이 필요하며 영구보존을 위해서는 대용량 저장장치 등이 요구된다. 이와 같은 전자문서의 이용 및 보안성을 고려한다면 스마트카드는 전자문서의 보안 및 이용자의 인증을 위한 도구로서 중요한 역할을 수행할 수 있다. 이러한 연구의 일환으로서 한편 스마트카드와 생체정보를 동시에 이용하여 이용자 인증프로토콜에 대한 연구도 진행되고 있다(Kim, Lee and Yoo 2003).

2. 연구의 내용 및 방법

전자문서의 유통 및 보존과 관련된 기술로는 일반적인 데이터 송수신 기술과 서버관리 기술, 로그 및 감사, 추적 기술 외에, 송수신 데이터의 무결성을 증명하기 위한 암호 기술, 데이터 수신자 확인을 위한 인증 기술, 전자문서의 권한 위임을 지원, 관리하는 접근제어 기술 및 암호화 기술, 전자문서 유통 증적 확인을 위한 시점확인 기술, 증명 기술, 공증관련 기술 등이다. 이와 관련하여 공인전자문서보관소 1차 사업자로 지정된 KT-NET에서는 공개키 기반구조(PKI)와 타임스탬프(TSA: Time Stamp Authority)의 활용을 적극 검토하고 있다(한국무역정보통신 2004). 공개키 기반구조는 공인인증기관에서 발급하는 공인인증서를 기반으로 이용자에 대한 검증을 위한 방법이며 타임스탬프 방법은 전자문서의 진본성에 대한 검증을 위한 방법이라고 할 수 있다. 그러나 이와 같은 방법은 전자문서의 이용을 위한 휴대성에 있어서는 문제점과 인프라 구축에 있어서 문제점을 내포하고 있다. 공인문서보관소에 있어서는 전자문서의 안전한 보존과 이용에 중점을 두고 있으나, 특정 목적의 정부, 공공 및 민간기관이 발급하는 전자증명서, 인증서를 포함한 전자문서는 온/오프라인을 통하여 유통 및 이용될 필요가 있다. 예를 들어 정부의 행정전산시스템에서 발급되는 주민등록등본 등의 전자증명서는 종이문서로 인쇄하고 이를 요구하는 기관에 제출하고 있으나 원칙적으로 인쇄를 금지하는 특정 목적의 전자문서의 경우에 있어서 전자문서 생산기관 또는 공인전자문서보관소로 부터 온라인상으로 전송을 받아서 이를 제출하게 된다. 그러나 이러한 방법은 반드시 온라인을 기반으로서 서비스가 제공되기 때문에 이용자의 입장에서 많은 불편함을 야기 할 수 있으며 네트워크를 통한 전자문서의 전송에 있어서 보안적인 문제가 발생할 수 있는 단점이 있다. 따라서 전자문서의 휴대성 및 안전성을 고려할 때 발급받은 전자문서의 안전한 저장 및 보안성을 만족할 수 있는 매체가 활용될 수 있다. 이러한 측면에서 스마트카드는 전자문서의 안전한 유통 이용을 위한 가장 적합한 저장 및 보안매체라고 할 수 있다. 이와 같은 스마

트카드는 저장성과 보안성에 탁월한 장점을 가지면서 연산기능을 수행할 수 있는 마이크로프로세서(microprocessor)와 데이터를 저장할 수 있는 메모리(memory)를 갖는 IC칩(IC Chip)을 내장함으로써 정당한 이용자에 대한 인증 및 저장된 내용에 대한 보안성을 보장할 수 있는 중요한 매체로서 역할을 수행한다(Rankl and Effing 2004).

초기 스마트카드는 주로 신용카드, 현금카드 등의 금융서비스 분야에 적용이 고려되었으나 저장성 및 보안성에 있어서의 탁월한 성능과 안전성에 따라 우리나라 정부를 포함하여 미국, 싱가포르, 영국 등의 국가에서 추진하고 있는 전자주민증, 전자여권, 전자운전면허증 등의 분야에 적용되고 있다(송영상, 신인철 2004; 디지털타임즈 2007). 따라서 스마트카드는 국가 및 사회적 인프라 구축에 용이하다는 장점을 가지고 있다.

따라서 본 연구에서는 이러한 스마트카드의 장점을 수용하면서 전자문서의 유통 및 이용을 위하여 온/오프라인 환경에서의 일정한 속성을 가진 전자문서 프레임워크(Framework)를 정의하며, 안전한 전자문서의 생성, 유통 및 보존을 위하여 1) 전자문서 생산시스템에서의 전자문서 생성, 2) 온라인 환경에서의 전자문서의 전달을 위한 이용자 및 스마트카드 인증, 3) 네트워크를 통하여 전달된 전자문서의 스마트카드 및 저장장치로의 저장 4) 오프라인 환경에서의 스마트카드 및 저장장치에 저장된 전자문서의 정당성 인증, 5) 전자문서의 수집 및 폐기 등을 위한 방법을 알아보고자 한다. 이를 위하여 이용자 인증 및 전자문서의 정당성을 인증하기 위한 프로토콜을 설계하고 이를 구현하였으며 실행속도에 대한 실험을 수행하였다.

3. 전자문서의 정의 및 특징

3.1 정의

전자문서(Electronic Document)은 전자문서를 생산한 목적, 성격 및 용도에 따라 다양한 정의가 가능하다. 송병호(2004)는 전자문서에 대해 "정보유통을 위하여 기계와 사람이 모두 이해할 수 있도록 표현된 이진(디지털) 기록물"이라고 정의하였다. 또한 2005년도에 제정된 전자거래기본법 제2조 제1호에서는 전자문서를 "정보처리시스템[1]에 의하여 전자적 형태로 작성, 송신/수신 또는 저장된 정보를 말한다"고 정의하고 있다. 이러한 관점에서 전자문서는 개인이 보편적으로 사용하는 워드프로세서로 작성된 텍스트 기반의 문서, 종이문서를 스캐닝을 통하여 전자화한 이미지 파일, MP3, AVI, JPG 등의 멀티미디어파일, 기계/건축 설계분야에서 사용하는 CAD 등의 도면문서 등을 포함하는 일반적인 의미의 전자문서와 전자상거래, 전자무역 등의 분야에 국한되어 사용되는 전자거래문서가 있으며 이러한 전자거래문서는 일반 전자문서에 비해 정형화 및 표준화된 규격에 의해 생산된다. <표 1>은 전자문서

1) 전자거래기본법에서 정의하는 정보처리시스템은 전자문서의 작성, 송/수신 도는 저장을 위하여 이용되는 정보처리능력을 가진 전자적 장치 또는 매체로 정의하고 있다.

〈표 1〉 전자문서의 파일 형식에 따른 종류 및 분류

	화일형식	종 류
일반 전자문서	텍스트	한글, MS 워드, 파워포인트, 엑셀 등 문서작성 소프트웨어를 사용하여 작성된 HWP, DOC, PPT, XLS, TXT, PDF 형식의 파일
	이미지	종이문서를 스캔하거나(tiff) 디지털카메라 등을 이용하여 만든 이미지
	도면	CAD/CAM 을 이용하여 작성된 도면 파일
	HTML	인터넷에서 사용되는 HTML 형식의 파일
	멀티미디어	JPG, MP3, AVI 등의 음악, 사진, 동영상 등의 멀티미디어 관련 파일
전자거래 문서	EDI[2]	전자문서교환방식(EDI: Electronic Data Interchange)을 사용하여 작성된 문서
	XML	확장형 표기 언어(XML: Extensible Markup Language)를 사용하여 작성한 문서

의 사용분야에 따른 분류에 따른 형식을 보여주고 있다.

3.2 특징

이와 같은 다양한 형식의 전자문서는 기존의 종이문서에 비하여 생산, 이용 및 보존의 관점에서 탁월한 장점을 보여준다. 종이문서는 공간적인 모습으로 존재하고 그에 담겨진 정보는 시각적인 방법으로 인식가능하다. 또한 종이문서는 항구적인 보존이 가능하며 문서내용에 대한 위변조의 어려움으로 인하여 무결성이 보장된다. 이에 대하여 전자문서는 비공간적인 모습으로 존재한다. 그러나 종이문서와는 달리 전자문서를 인식하기 위한 특정한 소프트웨어(Viewer)를 사용하여야 한다는 단점이 있으나 이를 통하여 종이문서와 차이가 없이 시각적으로 인식이 가능하다. 또한 정보처리기술의 발달로 종이문서에 비하여 오히려 보존의 완전성이 뛰어나다고 할 수 있다. 한편 전자문서는 소재가 고형물질이 아니고 전자적인 형태를 가지고 있기 때문에 생산, 수정 및 부분적인 삭제가 용이한 장점이자 단점으로서의 특성을 지닌다. 그러나 전자문서와 관련된 법제도의 제정과 정보기술의 발전은 전자문서가 효력이 있는 문서로서의 기능을 수행할 수 있는 기반을 제공하고 있다. 이러한 법적, 기술적 기반과 함께, 전자문서의 비공간성은 전자문서의 생산 및 이용의 활성화에 매우 중요한 특성이라고 할 수 있다. 이러한 특성에 따라 문서의 전자화를 통하여 얻을 수 있는 긍정적인 변화는 다음과 같다.

첫째, 사회 및 업무환경 변화에 따라 요구되는 폭증하는 문서의 보존 및 관리에 따른 비효율성을 개선할 수 있다.

둘째, 전자문서는 관리의 용이성으로 인하여 사무의 질과 효율을 높이며, 나아가 관련된 업무의 생산성을 제고한다.

셋째, 종이문서에 비해 검색 및 저장 등의 용이성으로 이용의 편의성을 확보할 수 있다.

넷째, 안전한 보안기술과 함께, 문서로서의

2) 기업간 거래에 관한 데이터와 문서를 표준화하여 컴퓨터 통신망으로 거래 당사자가 직접 송·수신하는 정보전달 시스템이다. 주문서·납품서·청구서 등 무역에 필요한 각종 서류를 표준화된 상거래서식 또는 공공서식을 통해 서로 합의된 전자신호로 바꾸어 컴퓨터 통신망을 이용하여 거래처에 전송한다. 전자문서교환에서 사용하는 국제적인 통신표준은 현재 국제연합이 중심이 되어 만든 UN/EDIFACT의 표준을 따르고 있다.

완벽한 진본성, 무결성, 기밀성 등의 특징을 확보할 수 있다.

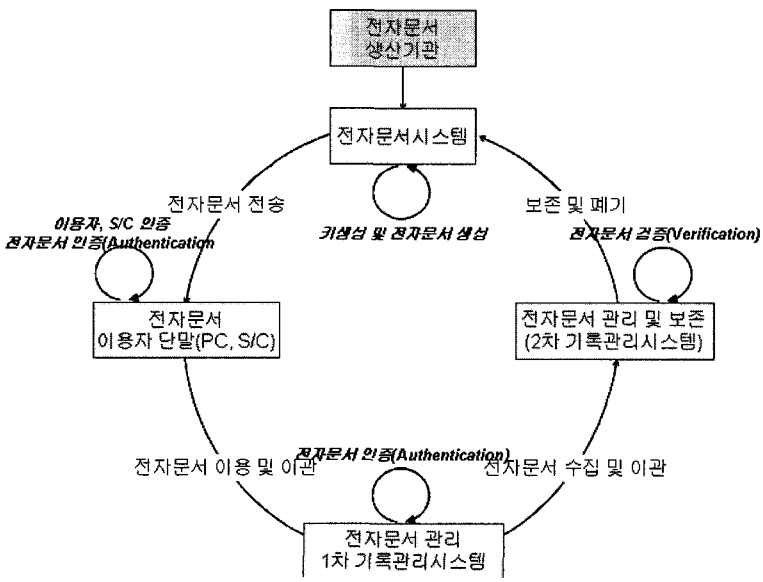
이와 같은 전자문서가 제공하는 장점은 전자문서가 ISO 15489에서 제시하는 특징을 완벽하게 만족함으로서 확보할 수 있다.

전자문서의 진본성, 기밀성, 무결성을 보장하기 위해서는 전자문서의 생산적인 측면 또는 보존 측면 등의 개별적인 영역에 대한 접근이 아니라 전자문서와 관련된 생산, 이용 및 보존이라는 전자문서의 전체 라이프사이클의 관점에서 접근하여야 한다. 즉, 전자문서가 생산되면 생산된 전자문서는 문서의 이용 및 수집을 위하여 네트워크를 통하여 전송되며 전송된 전자문서는 문서의 성격 및 내용에 따라 이용 또는 보관이 이루어진다. 이러한 과정에서 전자문서는 정당하지 않은 개인 또는 시스템에 의하여 위·변조 및 삭제가 가능하다. 또한 이용 또는 1차 관리를 위하여 보관된 전자문서는 중요도에 따라 영구보존 또는 폐기를 위하여 국가기록원과 같은 전문보존기관으로 전송된다. 이러한 과정에서도 1차 전송이 이루어진 과정에서 발생될 수 있는 동일한 위험성이 존재한다. 〈그림 1〉에서는 전자문서의 라이프사이클에 있어서 단계별 요구되는 위험성과 요구되는 보안성을 표현하고 있다.

4. 제안된 인증 및 보안 프로토콜

4.1 전자문서 구성요소

국내의 전자문서에 대한 기술규격에서 규정하고 있는 전자문서의 등록, 이관, 보존, 및 배포에 있어서는 실제 문서의 내용과 문서에 대한 메타데이터로 구성되는 전자문서 정보패키지라는 개념적 형태로서 관리된다. 여기에서 메타데



〈그림 1〉 일반적인 전자문서 라이프사이클

이터는 전자문서의 생산, 등록, 내용, 환경 등에 관한 정보와 문서의 보존 및 활용 관리를 위한 정보를 포함하는 등록정보, 기준정보, 구조정보, 맥락정보, 내용정보, 환경정보, 이용 및 관리정보, 진본인증정보를 포함하는 총 124개의 항목으로 구성된다(전자거래진흥원 2006).

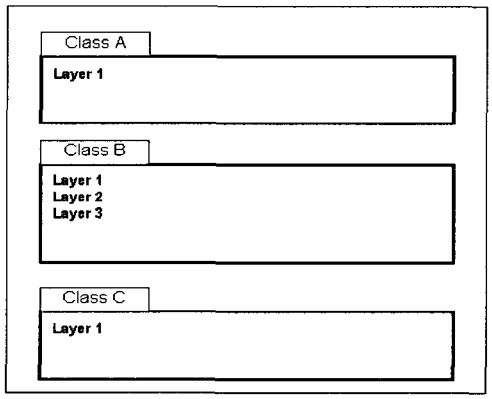
이러한 기술규격에 대한 고려와 함께, 본 연구에서는 전자문서의 특성에 기반하여 3장에서의 전자문서에 대한 정의와 함께, 본 연구에서는 구조적 관점에서 이용자 인증 및 전자문서의 검증을 위하여 전자문서를 다음과 같이 기술한다. 정당한 문서 이용자(Document User: U)와 스마트카드(Smart Card: SC)를 대상으로 문서가 가지는 속성과 가치를 전자문서 헤더(H_{ED}), 전자문서 본체(B_{ED}), 그리고 두 데이터(H_{ED}, B_{ED})를 전자문서 생산(발급)기관(Issuer: I)이 서명한(Signed) 전자서명(Digital Signature: DS_{ED})으로 구성 및 디지털 형태로 변환된 디지털 컨텐츠이다.

- 전자문서 헤더(H_{ED}): 전자문서 생산기관(발급기관), 전자문서의 유형코드, 전자문서 ID의 요소들로 구성된다.
- 전자문서 본체(B_{ED}): 각 서비스 어플리케이션에 따른 전자문서의 다양한 특성(Properties)을 정의하는 요소들로 구성된다.
- 전자서명(DS_{ED}): 상기 두 데이터 항목에 대한 전자문서의 정당성을 보장하는 전자문서 생산(발급)기관의(Issuer)의 전자서명 값이다.

4.2 전자문서 기반구조 및 기술

전자문서의 기반구조(framework)는 문서의 성격, 목적 및 속성에 따라 데이터 필드가 전자문서 기술규격에서 정의하고 있는 항목을 기준으로 필수 및 선택 항목을 기준으로 서로 상이하게 구성된다.

따라서 전자문서는 실제 문서의 생산 목적 및 성격에 따라 문서의 정보 속성을 디지털 정보로 변환하여 일정 형태의 문서구조를 가져야 한다. 본 연구에서는 전자문서를 연구의 목적 및 실험을 위하여 정보패키지 기술규격에서 정의하는 전자문서의 목록을 계층화 및 단순화하여 〈그림 2〉와 같이 표현하였다.



〈그림 2〉 전자문서 기본구조(Framework)

전자문서는 문서의 내용과 문서에 대한 기술정보(Description information)를 포함하는 메타데이터를 디지털 정보로 변환하고, 이를 네트워크를 통하여 유통(Circulation)하고 일정 기간의 경과에 따라 저장장치에 보존되기 위해서는 정형화된 형식의 데이터로 정의 및 기술되어져야 한다. 현재 이를 위한 적절한 정의/기술 언어(Language)로 주목을 받고있는 언어가 XML, RDF/XML 등이다. XML 형태의 변형된 형식의 ebXML 형식은 이중 메타 데이

터처리를 위한 기반 프레임워크로 웹(Web)상에서 컴퓨터가 인식 가능한 형태의 정보를 응용프로그램 간에 상호호환(interoperability)되도록 하는 XML이며 네임 스페이스(namespace) 기반의 RDF/XML은 전자문서의 특성을 표현함에 있어서는 뛰어난 언어로 인식되어있다. 그러나, 전자문서의 유통을 위한 조건 또는 문서유통을 제어하기 위한 특성을 기술함에 있어서 XML 자체만을 이용하는 것에 비해 다소 가중(重)한 점과 표현의 중복성(Redundancy)을 증가시키는 측면이 있어 XML를 이용한 전자문서 정의/기술이 보편성을 띄어가고 있다. 한편, 지난 몇 년 사이에 전 세계적으로 전자거래에 대한 관심이 높아짐에 따라 수많은 IT업체(MS, IBM, Sun, etc)가 전자거래를 위한 다양한 표준화 노력을 보였다. 특히, XML의 데이터 처리능력에 대한 장점이 부각되면서 여러 기구 및 단체에서 XML의 e-비즈니스 표준화를 시도하였고, 그 결과 1999년에는 수십가지의 표준화가 진행되어 혼란이 가중되었다. 이처럼 여러 표준들이 난립하여 전자거래는 오히려 퇴보할 수 있는 상황이었고, 이에 e-비즈니스 표준화에 있어 가장 권위 있는 UN/CEFACT와 OASIS 두 기관이 이러한 시장상황을 바로잡고, 표준을 둘러싼 과도한 경쟁을 막고자 전 세계적으로 단일한 전자거래 공통의미론 및 표준화작업을 공동 진행하였고, 그 결과 XML 기반의 개방형 표준인 ebXML이 탄생하게 되었다. 본 논문에서의 전자문서 기술을 위해 XML을 사용을 예시하고, 구현에 있어서는 특정 기술언어를 적용하지 않은 디지털 정보로 표현한다.

4.3 전자문서의 계층 및 구성

본 연구에서 고려하는 전자문서는 3개의 계층화된 구조로서 표현할 수 있다. 각 계층에 대한 설명은 다음과 같다.

〈표 2〉 전자문서 표현을 위한 기호

기 호	내 용
e	전자문서의 요소(Element)
x	전자문서 전자서명
{ }	집합(set)
( )	생략 가능한(omissible) 요소
+	구성

- Layer 1: 전자문서의 기본(basic) 특성에 대한 구조를 정의한다.
- Layer 2: 전자문서의 개별 특성에 대한 구조를 정의한다.
- Layer 3: 특정 기관 또는 이용자 집단에 특성화된 전자문서의 구조를 정의한다.

앞에서 정의하고 있는 전자문서의 계층적 구조와 함께, 전자문서는 〈표 2〉의 기호(notation)에 의하여 〈표 3〉과 같은 구조로 표현할 수 있다.

전자문서의 헤더정보는 전자문서에 대한 전자문서 기술규격에 있어서 정의하고 있는 전자문서에 대한 메타데이터를 포함하는 전자문서 헤더정보(H_{ED}), 전자문서 내용을 포함하는 전자문서 내용정보(B_{ED})와 전자문서에 대한 전자서명값을 포함하는 전자서명(DS_{ED})으로 구성된다.

각 분야별 구성요소에서 포함하고 있는 주요한 정보는 다음과 같다.

• 전자문서 헤더정보(H_{ED})

- 전자문서 분류코드(h_{clid}): 전자문서의 속성에 따른 분류 코드
- 전자문서 생산기관 또는 생산자(h_{orid}): 전자문서 생산기관 또는 생산자에 대한 식별자
- 전자문서 생산 또는 수정 일자(h_{date}): 전자문서가 생산 또는 수정된 시간으로서 전자문서의 위, 변조에 대한 검증에 있어서 중요한 정보
- 전자문서 식별자(h_{edid}): 전자문서 실체(Instance)로서 생산 또는 발급되는 전자문서의 유일성을 보장함과 동시에 검증이 가능한 전자문서 식별자

• 전자문서 본체정보(B_{ED}): 전자문서 내용 및 첨부화일 등의 실제 내용을 명시한다.

• 전자문서에 대한 전자서명(DS_{ED}): 전자문서를 생산한 기관에서 전자문서의 생산과 함께 생성한 전자서명

본 연구에서 정의하는 전자문서는 아래의 〈표 4〉와 같은 전자문서속성을 지원한다.

이를 보다 편의성과 보안성의 관점에서 종합하여 보면 다음과 같다.

• 효율성(Efficiency): 특정 어플리케이션 적합한 최적화된 전자문서 프레임워크를 구성함으로써 적은 메모리 용량과 제한된 연산(computation)기능을 수행하는 스마트 카드에 효율적으로 적용될 수 있다.

〈표 3〉 전자문서 구조화의 예

영 역	표 현
전자문서 정보패키지(ED)	$\{\langle H_{ED}\rangle + \langle B_{ED}\rangle + \langle DS_{ED}\rangle\}$
전자문서헤더(H_{ED})	$H_{ED} = \{\langle h_{e1}\rangle + \langle h_{e2}\rangle + \langle h_{e3}\rangle \cdots + \langle h_{en}\rangle\}$
문서본체(B_{ED}, B_{En})	$B_{ED} = \{(\langle b_{e1}\rangle) + (\langle b_{e2}\rangle) + \cdots + (\langle b_{en}\rangle)\}$ $B_{En} = \{(\langle bb_{e1}\rangle) + (\langle bb_{e2}\rangle) + \cdots + (\langle bb_{en}\rangle)\}$
전자서명(DS_{ED})	$DS_{ED} = \{\langle x\rangle\}$

〈표 4〉 안전한 배포 및 이용을 위한 전자문서 요구속성 및 제안된 전자문서 특징

특 성	제안된 전자문서
보안성(Secure)	Yes
휴대성(Portable)	Yes(Smart Card)
오프라인 이용성(Off-line Capability)	Yes(Smart Card)
분할성(Divisible)	No
견고성(Persistency)	Yes(Specified Period)
수납성(Wide Acceptance)	Yes
이용자 편의성(User-friendly)	Yes
기계가독성(Machine-understandable)	Yes
상태관리(State manageability)	Yes(Per-paid or unpaid)

- 보안성(Security): 3-DES 대칭키 암호방식(Symmetric-Key Cryptography) 과 단방향 해쉬방식(One-way hash function)을 기반으로 하여 시스템을 설계/구현함으로써 데이터의 무결성(Integrity), 기밀성(Confidentiality), 그리고 개체(Entity) 상호간의 정당성을 인증(Authentication) 가능하게 한다.
- 휴대성(Portability): 스마트카드 매체를 이용한 전자문서의 저장, 위/변조의 방지 그리고 카드 비밀번호(PIN)에 의한 카드 분실/도난에 대한 타인 사용의 불가능성을 제공하며, 개인이 휴대하며 실환경에서 사용이 가능하다.

5. 전자문서 인증 프로토콜

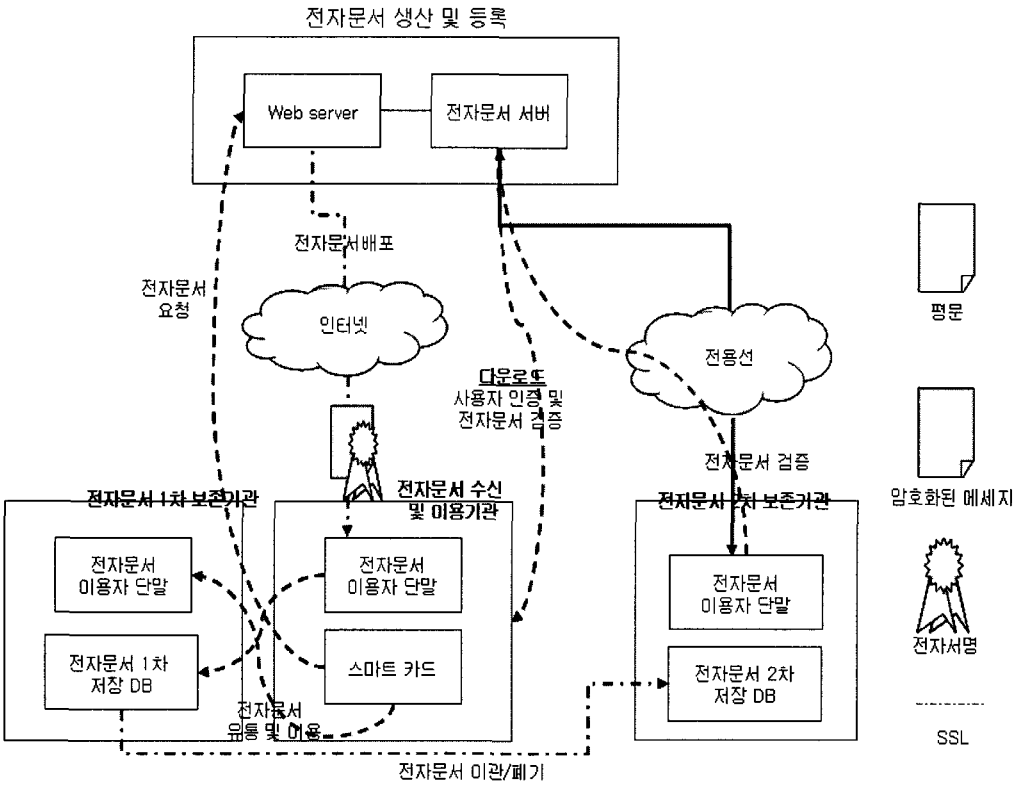
5.1 서비스 구성요소

본 연구에서의 전자문서 유통, 이용 및 보존 과정에 있어서 구성요소는 전자문서의 생산 및 등록업무를 수행하는 웹서버 및 전자문서 서버와 전자문서의 이용 및 유통과정에서 적용되는 이용자 클라이언트(Client) 시스템, 보관소 시스템으로 구분할 수 있다. 이용자 클라이언트 시스템에는 스마트카드, 이용자 전자지갑, 이용자 단말(PC) 및 스마트카드 리더 등이 포함되며 보관소 시스템은 전자문서의 보존을 위한 저장 시스템이 포함된다. 개별 구성요소의 기능 및 역할은 다음과 같다.

- 스마트카드(Smart Card): 스마트카드는 데이터의 연산, 저장 그리고 전송을 수행할 수 있는 집적회로(IC)를 내장한 카드이다. 본 시스템에서의 스마트카드는 이용자의 인증 및 전자문서의 저장/검증 기능을 가지며, 이를 위한 칩 운영체제(COS)와 보안 알고리즘(DES/3DES)을 가진다.
- 스마트카드리더(SmartCard Reader): 스마트카드와 PC와의 데이터 통신을 위해 PC/SC규격을 지원하는 스마트카드리더를 사용한다.
- 이용자 전자지갑(Wallet): 이용자의 컴퓨터에 설치된 전자지갑은 전자문서의 생성, 다운로딩 및 조회(View)를 위해 스마트카드 API를 제공하며, 전자문서 서버와 통신을 위한 보안프로토콜인 SSL v3.0과 데이터 암호용 보안API를 지원한다.
- 전자문서 이용자 단말(User Terminal): 전자문서의 이용 및 유통과정에 있어서 전자문서를 수신 및 저장하는 사이트에 설치된 이용자 단말은 이용자와의 상호작용을 통하여 스마트카드에 저장된 전자문서의 검증(Verification) 기능을 수행하며 독립된 형태의 키오스크 또는 유인 PC단말을 사용한다. 이때 전자문서의 검증을 위해서 SAM(Secure Application Module)카드를 이용한다.
- 전자문서 웹 서버(Web Server): 웹 브라우저(Web Browser)을 통해 이용자에게 전자문서에 대한 정보를 제공하며, 전자문서 다운로딩(downloading)을 위해 전자문서 서버와의 인터페이스 역할을 제공한다.
- 전자문서 서버(e-Document Generation Server): 전자문서의 실질적인 생산 및

관리를 수행하는 기관의 시스템으로서 전자문서의 생산, 등록, 취소 및 검증과 발급 및 배포된 전자문서를 관리하는 기능을 가진다. 전자문서 서버는 전자문서를 생산하는 기관 또는 생산 및 등록이 완료된 전자문서의 1차 저장기관이 될 수 있다.

- 전자문서 저장 서버(e-Document Storage Server): 전자문서 서버를 통하여 생산된 전자문서의 이용 및 유통과 함께, 보존이 요구되는 전자문서의 영구 보존을 위한 저장서버로서 정부문서의 경우에 있어서 국가기록원이 해당되며 본 연구에서는 전자문서의 2차 저장기관이 된다.
- 네트워크(Network)&통신(Communication)
  - 전자문서 웹 서버 ~ 웹 브라우저: 인터넷 기반의 HTTP
  - 전자문서 지갑(Wallet) ~ 전자문서 서버: TCP/IP & SSL v3.0
  - 이용자 단말 ~ 전자문서 서버: PSTN
  - 전자문서 웹 서버 ~ 전자문서 서버: TCP/IP



〈그림 3〉 전자문서의 생성, 이용 및 유통 흐름도

5.2 제안된 전자문서 인증 프로토콜

5.2.1 보안알고리즘

본 연구에서는 전자문서의 생산, 이용 및 유통의 흐름에 있어서 전자문서의 보안 및 안전성을 위하여 스마트카드를 기반으로 다음과 같은 보안 메커니즘을 사용한다.

- 암호화 알고리즘(Cipher Algorithm)
  전자문서 시스템의 효율성과 사업자의 비용 측면을 고려하여 대칭키(Symmetric) 기반의 암호화 알고리즘을 채택하여 구현한다. 이를 위해 3DES(Triple-Data Encryption Standard)알고리즘을 사용한다.
- 해쉬 알고리즘(Hash Algorithm)
  전자문서의 전자서명(Certificate)을 위해 메시지 다이제스트(Message Digest) 생성 알고리즘인 SHA-1을 사용한다.

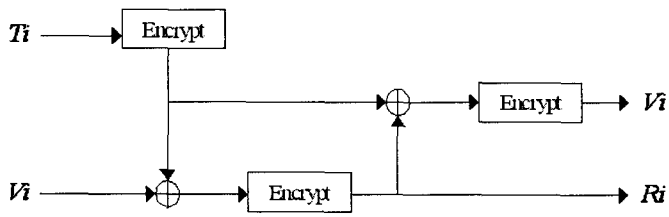
5.2.2 키 생성(Key Generation)

3-DES에 적용되는 이용자(User) 키(Key) 생성은 전자문서의 유통과정의 전체적인 보안성을 결정하는 중요한 부분이다. 3-DES의 이용자 키는 DES에서 가지는 보안성이 취약한 키(Weak Key, Semiweak Key, Possible Key)를 피해서 생성하며(Schneier 1996) ANSI X9.17 에서 정의하는 키 생성 방법을 적용한다. 〈그림 4〉는 ANSI X9.17에서 정의하고 있는 키 생성방법을 보여주고 있으며 이때 임의의 키(Random key) R_i를 생성하기 위한 방법은 다음과 같다.

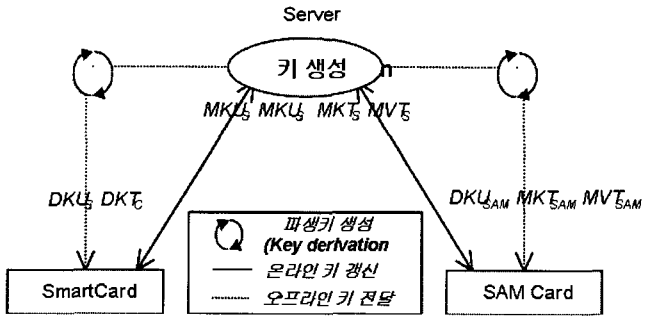
임의의 키 $R_i = E_k(E_k(T_i) \| V_i)$
V_{i+1} 의 생성은
$V_{i+1} = E_k(E_k(T_i) \| R_i)$
$E_k(X)$: $3DES\ Algorithm$, $V_i = Secret\ 64-bit\ seed$
$T_i = Time\ Stamp$, $R_i = Random\ Key$

5.2.3 키 분배(Key Distribution)

본 연구에서 사용되는 키의 분배는 중앙서버에서 집중 관리하는 방식을 사용하며, 이용자 카드 및 SAM카드용 키(Key)는 시스템 센터에서 생성 및 변형되어 카드 내에 저장되어 안전한 방법으로 이용자 및 보관소 시스템에 전달된다. 또한 이용자 카드 및 SAM카드는 시스템의 안전을 위하여 주기적 또는 필요에 의해서 온라인상으로 키를 갱신(update)한다. 〈그림 5〉에서는 본 연구에서 키의 분배를 위한 방법 및 흐름을 보여주고 있다.



〈그림 4〉 ANSI X 9.17의 키 생성 알고리즘



〈그림 5〉 보안키 배포 흐름

5.3 전자문서 생산 및 발급

5.3.1 전자문서 생산(e-Document Generation)

전자문서의 생성은 다음 2단계의 절차를 통해서 이루어진다.

Step 1: 전자문서 생산기관의 필요에 의하여 전자증명서와 같은 개인 또는 기관의 직접적 이용, 법령, 사규 등과 같은 보존용 문서 등을 전자문서(결제) 시스템을 이용하여 전자문서의 성격과 종류에 따라 정의된 형식과 내용에 대한 구조(framework)를 형성하고, 전자문서 서버의 데이터베이스에 등록 및 저장한다.

〈표 5〉 전자문서 생성 및 등록에 적용된 표기(Notation)

표기	설명	표기	설명
U	User	DKT	Derivation Key of MKT
C	Smart Card	DKV	Derivation Key of MKV
S	e-Document Server	DKU	Derivation Key of MKU
SAM	Secure application module	SK	Session Key
ED	Electronic Document	$E(m)$	Encryption Function
H_{ED}	e-Document Head-part	$D(m)$	Decryption Function
B_{ED}	e-Document Body-part	$H(m)$	Hash Function
DS_{ED}	e-Document Certificate	$RNG(m)$	Random number Generation Function
EID_{ED}	e-Document Identifier	m	Input Data
A_{ED}	e-Document Attribute Da Set	R	Random Data
AT_{ED}	A_{ED} Components	UD	Card Unique Data
NO_{ED}	e-Document Serial Number	MAC	Message Authentication Code
M_{ED}	EID's MAC	SI	Digital signature
MKT	Card Authentication Key	$\{\ \}$	Set
MKV	e-Document Authentication Key	$\|\|$	Concatenation
MKU	Key Update Key	$(\ )$	Omissible Element

Step 2: 이용자의 요청에 따라 전자문서 서버의 데이터베이스에 등록 및 저장된 전자문서를 해당 이용자 및 스마트카드별로 전자서명(Digital certificate)을 생성하여 이용자에게 전송한다.

5.3.2 전자문서 구조(framework) 형성

전자문서 구조는 전자문서의 성격 및 종류에 따라 전자문서 편집기(Editor)를 이용하여 정의된 형식에 준하여 형성한다.

전자문서의 식별자(EID_i)는 전자문서 속성(전자문서 생산기관, 전자문서 분류코드, 전자문서 생산일시 등)데이터(A_{ED}), 전자문서의 생산에 따른 일련번호(NO_{ED}), 그리고 전자문서 인증번호에 대한 인증코드 값(M_{ED})으로 구성된다.

전자문서 식별자(EID_i)는 다음과 같이 생성된다.

먼저 전자문서 식별자의 속성요소 집합인 A_{EDi}는 아래와 같이 정의할 수 있다.

$A_{EDi} = \{ae_1 \| ae_2 \| ae_2 \|, \cdots; ae_n\}$ 〈수식 1〉

$ae_j \in \{ED_i(e_1), ED_i(e_2), \cdots, ED_i(e_k),$

$(i = 1, 2, 3, \ldots, n)$, n은 생산 및 발급된 전자문서의 수

$(j = 1, 2, 3, \ldots, k)$, k는 전자문서의 총 요소개수

다음으로 인증코드 값(M_{EDi})의 생성을 위해 우선 전자문서의 해쉬값(H_{mi})을 아래와 같이 생성한다.

$H_{mi} = H(H_{EDi}' \| B_{EDi})$, $H_{EDi}' = (H_{EDi} - B_{EDi})$ 〈수식 2〉

〈수식 2〉를 통하여 얻은 결과값 해쉬값(H_{mi})를 암호화하여 인증코드 값(M_{EDi})을 〈수식 3〉을 통하여 구한다.

$M_{EDi} = E_K(h_{mi})$ 〈수식 3〉

또한 추가적으로 전자문서 일련번호(NO_{ED})를 구한다. 이러한 과정과 함께, 〈수식 1〉, 〈수식 3〉에서 추출한 결과값과 전자문서 일련번호(NO_{ED})를 연접연산(Concatenation)과정을 통하여 전자문서의 식별자는 아래의 〈수식 4〉를 통하여 구할 수 있다.

$EID_i = \{A_{EDi} \| NO_{EDi} \| M_{EDi}\}$ 〈수식 4〉

이러한 과정을 통하여 생성되는 전자문서 식별자는 다음의 특성(Property)을 만족하여야 한다.

- 유일성(Uniqueness): 전자문서 식별번호(e-document ID)는 전체 발급된 문서에서 유일하여야 한다.
- 검증성(Verification): 전자문서 ID 및 전자문서의 정당성을 검증한다.

5.4 이용자 및 스마트카드 인증

전자문서의 성격과 종류에 따라 전자문서는 생산에 따른 이용자의 직접적인 이용 및 생산, 배포의 과정을 통하여 보존을 위하여 2차 보존기관으로 이관되게 된다. 이러한 일련의 전자문서의 유통과정에서 아래와 같은 이용자 인증, 네트워크 보안 및 스마트카드 인증의 과정을 통하여 이용자에게 전자문서가 전달된다.

5.4.1 이용자 인증

전자문서에 대한 이용자 인증은 전자문서의 이용에 따른 정당한 이용자에 대한 인증 및 전자문서의 배포에 있어서 이를 수신하는 수신자에 대한 정당성을 검증하기 위한 과정으로서 현재 공인전자문서보관소에서는 공인 인증서 기반의 인증을 적용하고 있다. 그러나 본 연구에서는 스마트카드를 기반으로 하는 전자문서의 이용 및 거래를 위하여 스마트카드에서 적용되는 PIN 인증 방법을 추가적으로 적용한다.

- PIN(Personal Identification Number) 기반의 이용자 인증: 스마트카드 소지자가 자신이 소지한 스마트카드에 대한 정당한 소유권자임을 증명하는 방법으로 카드 내에 저장된 PIN과 소지자가 입력한 PIN과의 상호 일치 여부로 인증한다.
- 공인인증서(Public Certificate) 기반의 이용자 인증: 스마트카드 내에 저장된 자신의 전자문서 서비스용 인증서(Certificate)를 온라인상으로 전자문서 서버로 제출함으로써 이용자의 정당성을 인증 받는다.

5.4.2 스마트카드 인증

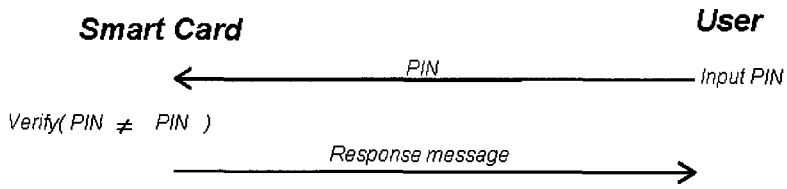
온/오프라인 환경에서의 전자문서를 저장하거나 저장된 스마트카드에 대한 인증은 네트워크를 통하여 스마트카드와 원격지(remote site)의 전자문서 서버간의 통신을 통하여 인증이 이루어진다. 이는 동일 시점의 상이한 공간에서 전자문서를 생산 및 배포하는 주체인 전자문서 서버와 이를 이용하는 전자문서 이용자 또는 1차 보존기관의 관리자가 비대면 방식에 의하여 전자문서의 송수신을 수행하는 인터넷 환경에서 전자문서를 제공하는 전자문서 생산 또는 배포기관은 단위 서비스 세션(Session)마다 원격에 위치하는 이용자의 스마트카드의 위/변조와 같은 정당성을 인증하여야 하기 때문이다(이원진, 김은주, 전일수 2005).

〈그림 7〉에서 보여주는 스마트카드에 대한 인증절차는 다음과 같다.

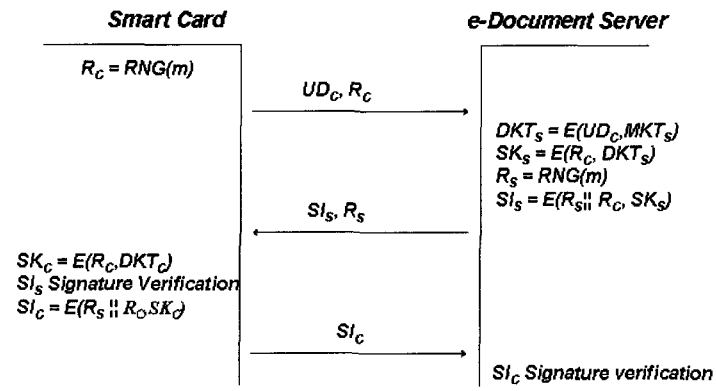
Step 1: 스마트카드(C)는 임의의 데이터(Random data: $R_c = RNG(m)$)를 생성하고 카드 고유 데이터(UD_c)와 함께 전자문서 서버(S)로 전송한다.

Step 2: 전자문서 서버(S)는 세션 키(Session Key: SK_s) 생성을 위한 파생키(DKT_s)를 생성한다.

$$DKT_s = E(UD_c, MKT_s) \qquad \langle \text{수식 } 5 \rangle$$



〈그림 6〉 스마트카드에 대한 이용자 인증



〈그림 7〉 스마트카드 인증 프로토콜

〈수식 5〉에서 생성된 DKT_s를 이용하여 〈수식 6〉의 과정을 통하여 세션 키(SK_s)를 생성한다. 그리고 전자문서 서버의 임의의 데이터(Random data: $R_s = RNG(m)$)를 생성한다.

$$SK_s = E(R_c, DKT_s) \qquad \text{〈수식 6〉}$$

〈수식 6〉에서 생성된 SK_s를 이용하여 서버의 서명(SI_s)를 생성하고 이를 스마트카드로 전송한다.

$$SI_s = E(R_s \| R_c, SK_s) \qquad \text{〈수식 7〉}$$

Step 3: 스마트카드는 카드의 세션 키(SK_c)를 생성하고 Step 2의 단계의 전자문서 서버에서 생성한 전자서명을 검증하기 위하여 〈수식 8〉에서 생성한 스마트카드의 세션키(SK_c)를 이용하여 〈수식 9〉과 같이 복호화과정을 수행한다.

$$SK_c = E(R_c, DKT_c) \qquad \text{〈수식 8〉}$$
$$Result = D(SI_s, SK_c) \qquad \text{〈수식 9〉}$$

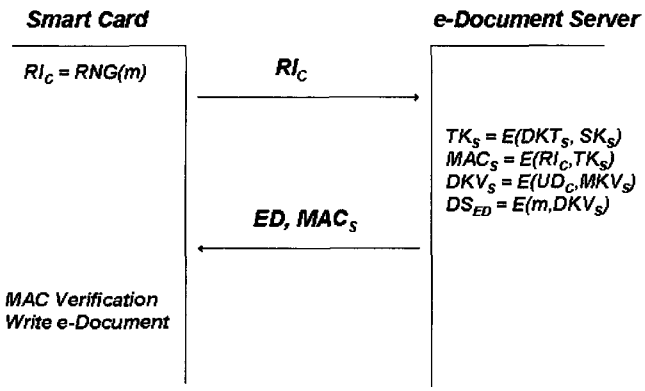
〈수식 9〉를 통하여 복호화된 결과값(Result)에서 추출된 R_s'와 R_c' 중에서 R_c'를 Step 1에서 생성한 R_c와 상호 비교하여 서버의 정당성을 인증한다. 그리고 〈수식 8〉에서 생성한 SK_c를 이용하여 스마트카드의 전자서명(SI_c)을 〈수식 10〉의 과정을 통하여 생성한다. 이렇게 생성된 스마트카드의 전자서명은 스마트카드에 대한 정당성에 대한 검증을 위하여 전자문서 서버로 전송한다.

$$SI_s = E(R_s \| R_c, SK_s) \qquad \text{〈수식 10〉}$$

Step 4: 전자문서 서버는 〈수식 8〉에서 생성한 세션키(SK_c)를 이용하여 스마트카드로 부터 수신된 전자서명(SI_c)을 복호한다.

$$Result = D(SI_c, SK_c) \qquad \text{〈수식 11〉}$$

〈수식 11〉을 통하여 복호화된 결과값(Result)에서 추출된 R_s'와 R_c' 중에서 R_s'를 Step 2에서 생성한 R_s와 상호 비교하여 스마트카드에 대한 정당성을 인증한다.



〈그림 8〉 전자문서 생성 및 배포를 위한 암호화

이와 같이 상기 Step 1~ Step 4까지의 과정을 통해서 스마트카드와 전자문서 서버는 인터넷 온라인 환경에서 상호간의 인증과정을 통하여 정당성을 인증한다. 이와 같은 상호인증은 온라인상에서 원격지에 위치하는 매체가 전자문서의 송수신에 있어서 서로에 대한 정당성여부를 판단하기 위한 중요한 과정이다.

5.4.3 전자문서 생성 및 배포

5.4.2 절에서의 스마트카드와 전자문서 서버와의 상호인증 절차가 완료되면 전자문서의 이용을 위하여 스마트카드는 전자문서 서버에 전자문서를 요청하게 되거나, 전자문서 서버는 필요에 의하여 생성한 전자문서를 적절한 관련기관 또는 1차 보존기관에 배포하기 위하여 다음과 같은 절차를 통하여 전자문서를 생성하게 된다. 본 연구에서 의미하는 전자문서의 생성 및 전달의 의미는 전자문서의 실제 내용에 대한 생성이 아닌 전자문서 내용에 대한 무결성 및 기밀성 등과 같은 전자문서의 정당성을 위하여 요구되는 인증코드 값 및 전자서명의 생성을 의미한다.

Step 1: 스마트카드(C)는 임의의 데이터 $R1_c = RNG(m)$을 생성하고 이를 전자문서 서버(S)로 전송한다.

Step 2: 전자문서 서버(S)는 MAC(Message Authentication Code)의 생성을 위하여 〈수식 6〉의 세션키(SK_s)를 이용하여 〈수식 5〉에서 생성한 DKT_s를 〈수식 12〉의 과정을 통하여 암호화함으로써 임시키(TK_s)를 생성한다.

$$TK_s = E(DKT_s, SK_s) \qquad \text{〈수식 12〉}$$

한편, 생성된 임시키(TK_s)와 함께 전자문서를 스마트카드에 전송 및 저장하기 위한 인증코드 값(MAC)을 〈수식 13〉의 과정을 통하여 생성한다.

$$MAC_s = E(R1_c, TK_s) \qquad \text{〈수식 13〉}$$

또한, 전자문서 서버는 생산 및 발급되어 배포되는 전자문서에 대한 인증서(DS_{ED})를 〈수식 14〉와 〈수식 15〉의 과정을 통하여 생성한다.

$$DKV_s = E(UD_c, MKVs) \quad \langle 수식\ 14 \rangle$$

$$DS_{ED} = E(m, DKV_s), m = \{H_{ED} + B_{ED}\} \quad \langle 수식\ 15 \rangle$$

한편, 전자문서의 내용의 중요성에 따라 문서내용에 대한 암호화가 요구된다. 따라서 암호화된 전자문서의 생성은 〈수식 15〉에서 생성된 전자문서 인증서와 구조화된 전자문서의 실제 내용을 조합하여 〈수식 16〉의 과정을 통하여 생성한다. 이렇게 생성된 전자문서는 전자문서 인증코드값(MAC)과 암호화된 전자문서를 스마트카드로 전송한다.

$$ED = \{H_{ED} \| B_{ED} \| DS_{ED}\} \quad \langle 수식\ 16 \rangle$$

Step 3: 스마트카드는 전자문서 서버로부터 전송된 전자문서를 스마트카드에 저장하기 전에 인증코드값(MAC)에 대한 검증을 수행한다. 이를 위하여 〈수식 8〉의 세션키(SK_c)를 이용하여 카드의 파생키(DKT_c)를 암호화하여 임시키(TK_c)와 카드의 인증코드값(MAC_c)을 생성한다.

$$TK_c = E(DKT_c, SK_c) \quad \langle 수식\ 17 \rangle$$
$$MAC_c = E(R1_c, TK_c)$$

스마트카드는 〈수식 17〉을 통하여 생성된 카드의 인증코드값(MAC_c)과 서버의 인증코드값(MAC_s)를 상호 비교하여 결과값이 일치하면 전자문서(e-Document)을 스마트카드에 저장한다.

5.5 전자문서 이용 및 인증

전자문서의 이용 및 보존의 과정에서는 스마트카드에 저장된 전자문서에 대한 인증이 요구된다. 이를 위하여 이용자 및 스마트카드에 대한 매체인증이 요구되며 이를 위한 방법은 4.4절에서 기술한 방법을 적용한다. 따라서 본 절에서는 전자문서 생산기관에서 생산 및 배포된 전자문서에 대한 기밀성 및 무결성을 검증하기 위한 방법에 대해서 알아본다.

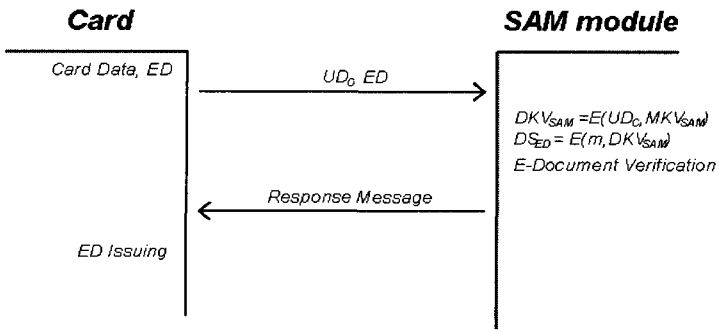
이용자 및 스마트카드에 대한 인증이 완료되면 다음과 같은 절차를 수행함으로써 전자문서의 유효성을 검증한다.

Step 1: 스마트카드(C)는 카드 고유 데이터(UD_c)와 전자문서(e-Document)를 서비스 단말을 통하여 SAM카드로 전송한다.

Step 2: SAM카드는 스마트카드(C)로부터 전송받은 데이터(UD_c)를 암호화하여 전자문서 인증키에서 파생된 파생키(DKV_{SAM})를 생성하며 이렇게 생성된 파생키를 이용하여 전자문서 인증서를 생성한다.

$$DKV_{SAM} = E(UD_c, MKV_{SAM}) \quad \langle 수식\ 18 \rangle$$
$$DS_{ED}' = E(m, DKV_{SAM})$$
$$m = \{H_{ED} \| B_{ED}\}$$

Step 3: 위의 과정에서 생성된 전자문서 인증서(DS_{ED}')와 스마트카드로부터 전송받은 전자문서 인증서(DS_{ED})를 비교함으로써 전자문서의 정당성을 인증한다.



〈그림 9〉 전자문서 검증 프로토콜

5.6 전자문서 검증

영구보존이 요구되거나 장시간의 보존을 위해서는 최초 생산된 전자문서와 최종 보존기관에 이관된 전자문서에 대한 검증작업이 요구된다. 따라서 영구보존기관은 전자문서 생산기관으로부터 전자문서 생산과정에서 이용된 데이터 및 암호화키를 전달받아야 한다. 이렇게 전달된 데이터를 이용하여 전자문서에 대한 실직적인 검증은 전자문서 식별자(EID)에 대한 검증을 통해서 이루어지며 수행절차는 다음과 같다.

Step 1: 이관된 전자문서의 헤더부분에서 전자문서 식별자를 추출한다.

$$EID_i = \{A_{EDi} \| NO_{EDi} \| M_{EDi}\} \quad \langle \text{수식 } 19 \rangle$$

Step 2: 이관된 전자문서(ED_i)로부터 초기입력 데이터(m_i)를 추출하고 이에 대한 해쉬값(hm)을 생성한다.

$$m_i = (H_{EDi}' \| B_{EDi}') \quad \langle \text{수식 } 20 \rangle$$
$$(H_{EDi}' = H_{EDi} - EID_{EDi})$$
$$hm_i = H(m)$$

Step 3: 〈수식 19〉에서 생성된 해쉬값(hm_i)을 암호화하여 인증코드(M_{EDi}')를 생성한다.

Step 4: 생성된 인증코드(M_{EDi}')와 이관된 전자문서의 인증코드(M_{EDi})와 상호 비교하여 전자문서의 정당성을 검증한다.

Step 5: 위의 과정의 검증처리가 완료되면 이관된 전자문서 식별자(EID_i)를 기본 키(Primary Key)로 사용하여 전자문서 서버의 데이터베이스에 이관된 전자문서(EID_i)의 라이프 사이클이 완료되었음을 전달한다.

6. 실험 및 분석

본 연구에서는 전자문서의 이용 및 유통에 있어서 보안성을 높이기 위한 방법으로서 이용자와 스마트카드에 대한 인증 및 전자문서 내용에 대한 진본성, 기밀성, 무결성을 만족하기 위한 보안 알고리즘을 제안하고 있다. 특히, 제안하고 있는 보안 알고리즘은 온/오프라인에서 적용되기 위한 요구조건으로서 실행속도 및 높

은 보안성을 요구한다. 따라서 제안된 알고리즘을 구현 및 실험을 수행한 결과는 다음과 같다. 실험에 사용된 스마트카드는 을 살펴보면 ST19RF08 Microprocessor를 탑재하고 3-DES 알고리즘을 지원하고 있으며 며 전자문서 서버의 기능을 수행을 위하여 Windows XP Professional운영 체제에서 Visual Studio .NET, C++/STL의 개발환경에서 Pentium 3.0GHz/800MHz/2MB 환경에서 수행 되었다

6.1 전자문서 식별자 및 전자서명 생성

〈표 6〉과 〈표 7〉에서는 제안된 방법의 구현을 통하여 실질적인 입력값을 통하여 추출된 결과값을 보여주고 있다.

〈표 6〉 전자문서 식별자 생성 및 실험 데이터

표 기	데이터
A_{ED}	전자문서 속성 데이터 집합
	4B545138 37313431 38373031
NO_{ED}	전자문서의 일련번호
	09 14 F9 60
M_{ED}	EID의 MAC
	A0 FA 0F 42
H_{ED}	전자문서 헤더 정보
	37 36 35 34 33 32 31 20
B_{ED}	전자문서 본체 정보
	4E 6F 77 20 69 73 20 74
H_m	해쉬 결과 값
	66 52 77 6E C7 E9 E5 84 8D BC 19 68 13 46 FA 35
$MKEID_s$	보안 키
	62C10CC9 EFBF15AA 15EEA1EE C4844293 772FAD27 2B3B5739
EID	전자문서 식별자(EID)
	4B545138 37313431 38373031 0914 F960 A0FA0F42

〈표 7〉 전자문서의 전자서명 생성 및 실험 데이터

표 기	추출 데이터
MK_s	마스터 키
	6E9D9456 E7818D5E F00BE768 73280B01 6E9D9456 E7818D5E
UD_c	카드 고유 데이터
	655272A4 F098C0B1 A318C7FE 4418234F DAE538C2
DK_s	$DK_s = E(UD_c, MK_s)$
	7E9FBD7C33EB5EAA BFBCF3D75B0E7EE5 7E9FBD7C33EB5EAA
m	전자문서 헤더 및 본체 정보 데이터
	F3DA1DD4378A881334A0ABEF30643172655272A4F098C0B1
DS_{ED}	$DS_{ED} = E(m, DK_s)$
	C9BA5ABB1E2BD653

6.2 전자문서 생성 및 검증시간

〈표 8〉에서는 전자문서의 생성에 따른 매체 인증 및 전자서명에 따른 연산시간과 전자문서 검증에 있어서 연산시간에 대한 실험 결과를 보여주고 있다.

본 연구에는 온/오프라인에서의 전자문서의 안전한 이용 및 유통을 위하여 이용자 인증 및 전자문서의 기밀서 및 무결성을 만족할 수 있는 보안 알고리즘을 제안 및 구현하였다. 특히, 전자문서의 임시 저장 및 이용을 위하여 높은 보안성을 제공하는 매체로서 스마트카드를 활용하였다. 이와 같은 방법을 통하여 다음과 같은 효과를 얻을 수 있었다.

- 임의의 전자문서 생성이 불가능: 블록 암호(block cipher) 알고리즘인 3-DES기반의 전자서명(DS_{ED}) 및 인증코드값(MAC)을 가지는 전자문서 식별자(EID)는 정당한 스마트카드 및 이용자에게만 전자문서가 발행되며 이는 부정 이용자의 전자문서 생성을 불가능하게 한다.
- 전자문서의 위, 변조에 대해서 안전: 3-DES와 충돌 회피형 해쉬 함수(Collision-free hash function) 기반의 전자서명(DS_{ED}) 및 인증코드값(MAC)은 전자문서의 위/변조에 대한 무결성(integrity)을 보장한다.
- 시스템에 사용된 비밀키의 노출에 대해서 안전하다.: 높은 보안성을 제공하는 스마트카드의 사용과 서비스 세션마다 생성되는 세션키(SK_c, SK_s)의 사용을 통한 키의 노출에 대해서 안전하다.
- 전자문서 부정사용에 대한 추적이 가능하다: 카드 고유의 데이터(UD_c)를 기반으로 생성된 전자서명과 전자문서 서버의 데이터베이스에 등록된 스마트카드 이용자 및 카드 일련번호에 의한 부정사용에 대해 추적이 가능하다.

〈표 8〉 연산시간에 대한 실험 결과

전자문서 생성 및 발급		전자문서 검증	
인증	Card: 10ms + 30ms x2 + 30ms = 100ms (m=8 bytes) Server: 0.18ms + 0.63ms x 3 + 0.63ms = 2.7ms(m=8 bytes)	인증	User Card: 10ms + 30ms x2 + 30ms = 100ms(m=8 bytes) SAM Card: 10ms + 30ms x 3 + 30ms = 130ms (m=8 bytes)
전자서명 생성	Card: 10ms Server: 0.63ms x 4 x 12= 156.25ms(m = 96bytes)	전자문서 검증	SAM Card: 30ms x 2 x 12 = 720ms(Here, m = 96 bytes)
데이터 전송	PC 〈-〉 Server: 80ms(baud rate=9600bps)	데이터 전송	120ms(m = 144bytes, baud rate=9600bps)

〈표 9〉 3-DES 연산시간

	스마트카드	서 버
CPU 속도	5MHz	Pentium 3.0GHz/800MHz/2MB
키 사이즈	196 bits	196 bits
데이터 사이즈	64 bits	64bits
암, 복호화 시간	30ms	0.63ms

7. 결 론

정부 및 공공기관에서의 업무효율성 및 비용 절감을 위한 전자문서 활용의 확대는 의심의 여지가 없다. 특히, 기록물로서 문서의 이용, 관리 및 보존에 따른 전자문서의 효율성은 전자문서의 활성화를 촉진시키고 있다. 그러나 전자문서의 유통에 있어서 가장 문제점으로 지적되고 있는 것은 전자문서의 위, 변조라고 할 수 있다. 광의적인 관점에서 전자문서는 0과 1로서 표현할 수 있는 디지털콘텐츠의 일종이라고 할 수 있다. 따라서 디지털콘텐츠가 갖는 장점과 단점을 동시에 포함한다는 것이다. 특히, 전자문서는 일반 디지털콘텐츠와는 달리 법적, 제도적인 효력을 갖는다는 것이다. 따라서 전자문서의 활성화를 위해서는 내용에 대한 위, 변조의 방지와 정당한 이용자에 대한 검증이 중요한 이슈가 된다. 본 연구에서는 이러한 관점에서 전자문서의 진본성, 기밀성, 무결성을 보장하고 정당한 이용자에 대한 인증 방법을 제시하고 있다. 특히, 본 연구에서는 전자문서를 단순히 보존적인 측면에서만 고려하지 않고 실생활에서의 이용 및 유통의 관점에서 고려하였다. 이를 위하여 국가 전자주민증 및 민간기관에서 신분증으로서 활용되고 있는 스마트카드를 기반으로 전자문서의 이용 및 유통을 위한 매체로서 활용하고 있다. 스마트카드는 높은 보안성과 저장성으로 인하여 현재 금융기관에서 기존의 마그네틱 카드를 대체하는 추세에 있다. 따라서 이러한 스마트카드는 국가 또는 민간기관에서 발급하는 전자증명서를 포함하는 다양한 전자문서의 실생활에서의 활용을 위한 저장수단으로서 활용될 수 있으며 또한 높은 보안성으로 인하여 전자문서 활성화에 많은 기여를 할 수 있는 도구가 될 수 있다.

비록 본 연구에서 제안하고 있는 방법이 전자문서의 이용 및 유통적인 측면을 고려하여 스마트카드를 활용하고 있으나 환경에 따라서는 전자문서의 생산기관과 수신기관의 서버/클라이언트 환경에 즉각적으로 적용할 수 있다. 즉, 스마트카드가 수행하는 역할과 기능을 전자문서 수신기관의 클라이언트 모듈에서 수행함으로써 수신단말로서 스마트카드가 아닌 저장서버 또는 일반 데스크탑 컴퓨터와 같은 매체가 가능하다.

현재 전자문서 활성화에 따른 보안에 대한 연구가 일부 수행되고 있으며 전자문서의 거래에 대한 국가적인 관심이 매우 높다. 그러나 이러한 연구들은 대부분 전자문서의 보존과 온라인을 통한 유통에만 집중되어져 있다. 따라서 온, 오프라인에 공통적으로 적용할 수 있는 보안방법이 요구된다. 이러한 관점에서 본 연구에서 제안하고 있는 스마트카드 기반의 전자문서 보안방법은 의미하는 바가 크다고 할 수 있다. 따라서 지속적으로 온라인 및 오프라인에서의 전자문서의 이용, 유통 및 보존을 위한 연구는 전자문서를 수신 또는 이용하는 기관과 이용자측 단말을 고려한 연구가 요구된다.

참 고 문 헌

국가기록원. 2006. 『기록 영구보존기술 적용을 위한 테스트베드 구축 최종보고회 자료, 2006. 9』.

국회산업자원위원회. 2005. 『전자거래기본법중 개정 법률안 검토보고서, 2005. 2』.

김진환. 1999. 전자거래에 있어서의 문서성과 서명성에 관한 고찰(I), 『법조』. 통권 515: 114-147.

디지털타임즈. "전자여권 도입 내년까지 본격추진." [cited on 2007.3.19]. 〈http://www.dt.co.kr/contents.html?article_no=2007022602010251650002〉.

송병호. 2004. 정보 전자문서유통의 발전방향에 관한 연구. 『한국정보관리학회지』, 21(3): 185-202.

송병호. 2005. 전자기록물을 위한 보존매체의 관리. 『2005 한국기록관리학회 학술발표논문집』, 2005. 10, pp.131-143.

송영상, 신인철. 2004. 서명을 이용한 스마트카드 이용자 인증을 위한 COS 설계. 『전자공학회논문지: CI 편』, 41(4): 421-430.

이원진, 김은주, 전일수. 2005. 스마트카드를 이용한 ID기반의 이용자 인증 프로토콜. 한국정보과학회, 『2005 한국컴퓨터종합학술대회 논문집(A)』, pp.166-168.

전자신문. 2007. "전자주민증 시험사업 시작." 〈http://www.etnews.co.kr/news/detail.html?id=200703070188〉.

최학렬. 2006. 전자문서 이용활성화를 위한 공인 전자문서보관소, 『주간기술동향』 1238호, 〈http://kidbs.itfind.or.kr/WZIN/jugidong/1238/123801.htm〉.

한국무역정보통신. 2004. 『공인전자문서보관소 인프라 개발을 위한 연구, 2004. 6』.

한국전자거래진흥원. 2006. 『전자문서 정보패키지 기술규격 V. 0.8. 2006. 8』.

Kim, H.S., S. W. Lee, and K. Y. Yoo, 2003. "ID-based Password Authentication Scheme using Smart Cards and Fingerprints", *ACM SIGOPS Operating Systems Review*, 37(4): 32-41.

Matonis, J.W. 1995. "Monetary Freedom", *Proceedings of INET95, Internet Society*, 〈http://info.isoc.org/HMP/PAPER/136/html/paper.html〉.

Rankl, Wolfgang and Wolfgang Effing. 2004. *Smartcard Handbook*. WILEY: New York.

Schneier, Bruce. 1996. *Applied Cryptography*. John Wiley & Sons: New York.

Shamir, A. 1984. "Identity-based cryptosystems and signature schemes." *Proceedings CRUPTO '84*, pp.47-53.

W3C. 2004. *RDF Vocabulary Description Language 1.0: RDF Schema W3C Recommendation*, 〈http://www.w3.org/TR/rdf-schema/〉.

W3C. *XML(Extensible Markup Language)*, 〈http://www.w3.org/XML/〉.

Walden, Ian and Nigel Savage. 1989. "The legal problems of paperless Transaction." *Journal of Business Law*. March, 1989. p.103.