情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

전자문서 소프트웨어의 전자서명 기능에 대한 안전성 분석*

박 선 우,[1†] 이 창 빈,[1] 이 광 우,[1] 김 지 연,[1] 이 영 숙,[2] 원 동 호[1‡]
[1]성균관대학교, [2]호원대학교

Security Analysis on Digital Signature Function Implemented in Electronic Documents Software*

Sunwoo Park,[1†] Changbin Lee,[1] Kwangwoo Lee,[1] Jeeyeon Kim,[1]
Youngsook Lee,[2] Dongho Won[1‡]
[1]Sungkyunkwan University, [2]Howon University

요 약

전자문서는 문서가 변경 및 수정되어도 이를 확인하기 어렵다는 특성을 가지고 있기 때문에 문서의 진본성을 확인하는 것이 전자문서 이용에 중요한 역할을 한다. 이에 따라 다양한 전자문서 소프트웨어들은 전자문서의 신뢰성을 보장하기 위해 전자서명 생성 및 검증 기능을 제공하고 있다. 하지만 이러한 소프트웨어들이 전자서명 생성 및 검증을 정상적으로 수행하는지에 대한 연구가 미비하여 이를 완전하게 신뢰하기 어렵다. 이에 본 논문에서는 Adobe PDF, MS Word, 훈글의 전자서명 기능과 법무부의 전자공증서비스, 국세청의 연말정산 간소화 서비스에서 제공되는 전자서명 기능의 안전성에 대해 분석해보고 이를 기반으로 전자문서 소프트웨어 개발자가 전자서명 생성 및 검증 기능을 올바르게 구현하기 위해 고려해야 할 사항을 제시하고자 한다.

ABSTRACT

Electronic documents have characteristics that detecting whether an electronic document is modified or not is not an easy process. Thus verifying integrity of documents is very important for using electronic documents. To facilitate this process, various electronic document software provide digital signature capabilities on themselves. However, there were not much research on the security of digital signature function of software. Therefore, in this paper, we analyze the security of Adobe PDF, MS Word, Hancom Hangul, digital notary service and digital year-end-settlement service, and propose recommendations for implementation of digital signature funcion.

Keywords: Electronic Documents, Electronic Document Software, Digital Signature, PDF, MS Word, Hancom Hangul

I. 서 론

세계적으로 이슈가 되고 있는 Green IT의 일환으로 종이문서 대신 전자문서를 사용하는 것이 장려되고 있다. 국내에서도 '민사소송 등에서의 전자문서 이용 등에 관한 법률', '약식절차에서의 전자문서 이용 등에 관한 법률', '독촉절차에서의 전자문서 이용 등에 관한

접수일(2012년 2월 6일), 수정일(1차: 2012년 5월 30일, 2차: 2012년 7월 25일), 게재확정일(2012년 8월 6일)
* 본 연구는 행정안전부의 출연금으로 수행한 전자서명 인증관리 사업의 결과입니다.
† 주저자, swpark@security.re.kr
‡ 교신저자, dhwon@security.re.kr

법률'과 같은 전자문서 이용을 촉진하는 법률을 제정하는 등 정부 주도하에 전자문서 이용을 활성화하기 위한 사업들이 추진되고 있으며 행정, 세무, 금융, 의료 등 다양한 분야에서 업무의 전산화 및 종이문서의 전자문서화가 진행되고 있다[1]. 하지만 문서가 변경되거나 수정되어도 이를 확인하기 어렵다는 전자문서의 특성 때문에 전자문서의 위·변조 및 이에 따른 피해가 매년 끊임없이 발생하고 있으며 이는 사회적으로 심각한 문제가 되고 있다. 따라서 전자문서의 무결성을 확인하고 신뢰성을 확보하는 것이 전자문서 이용 활성화에 중요한 역할을 하고 있으며, 전자문서의 위·변조를 확인할 수 있는 전자서명 기술에 대한 수요도 증가하고 있다. 이러한 수요에 맞춰 전자문서의 신뢰성을 확보하고자 Adobe PDF, MS Word, 훈글과 같은 몇몇 워드프로세서들은 전자서명 기능을 제공하고 있으며, 정부에서도 전자서명이 첨부된 전자문서를 활용한 전자공증 및 증명서 발급 서비스 등을 제공하고 있다. 하지만 워드프로세서 및 정부 서비스에서 제공되는 전자서명 기능의 안전성과 신뢰성에 대한 연구가 미비하기 때문에 이를 완전하게 신뢰하기에는 어려움이 있다.

이에 본 논문에서는 대표적인 워드프로세서인 Adobe PDF, MS Word, 훈글의 전자서명 기능과 법무부의 전자공증서비스, 국세청의 연말정산 간소화 서비스에서 제공되는 전자서명의 생성 및 검증 절차와 방법의 안전성에 대해 분석해보고 이를 기반으로 전자서명 기능 구현에 대한 권고사항을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 각 전자문서 소프트웨어들에 구현된 전자서명 기능의 안전성 분석을 위한 테스트 방법을 기술한다. 3장에서는 앞장에서 설명한 안전성 분석 방법을 토대로 PDF 소프트웨어들의 전자서명 기능에 대한 안전성을 분석하며, 4장에서는 MS Word의 전자서명 기능을, 5장에서는 훈글의 전자서명 기능에 대한 안전성을 분석한다. 6장에서는 법무부의 전자공증서비스와 국세청의 연말정산 간소화 서비스에서 제공되는 전자서명 기능의 안전성에 대해 분석한다. 7장에서는 전자문서 소프트웨어에서 신뢰할 수 있는 전자서명 기능을 구현하기 위한 개발자들의 고려사항들을 제시하며, 마지막으로 8장에서 결론을 맺는다.

II. 안전성 분석 방법

본 절에서는 전자문서 소프트웨어의 전자서명 기능에 대한 안전성 분석 방법을 기술한다. 본 논문의 전자서명 기능에 대한 안전성 분석은 전자문서 소프트웨어에서 전자서명을 생성하고 검증하는 방법과 절차가 안전하게 제공되고 있는지에 대한 분석을 뜻하며, 크게 전자서명의 표시 기능에 대한 분석, 전자서명 대상의 원문 범위 설정에 대한 분석, 서명 데이터 영역에 대한 분석, 전자서명 검증 및 인증서 검증에 대한 분석으로 나누어 진행한다.

전자서명 표시 기능에 대한 분석에서는 사용자가 전자서명의 존재 여부를 확인할 수 있는지와 검증 결과에 대한 정보를 정확하게 보여주고 있는지를 확인한다. 원문 범위 설정에 대한 분석에서는 서명값 영역을 제외한 문서 전체영역을 원문범위에 포함시키고 있는지를 확인한다. 전자서명의 대상이 되는 원문의 범위에 포함되지 않은 부분은 무결성을 보장받을 수 없기 때문에 원문의 범위는 서명데이터 영역을 제외한 문서 전체로 설정되어야 한다. PDF 국제 표준인 ISO-32000-1에서도 문서 전체를 원문의 범위로 설정하기를 강하게 권고하고 있으며 여기서 문서 전체란 Contents 엔트리(실제 서명값이 들어있는 영역)만을 제외한 모든 영역을 뜻한다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어에서 원문의 범위를 문서 전체로 설정하고 있는지에 대한 확인이 필요하다. 또한 전자서명의 원문 범위를 올바르게 설정하였다 해도, 서명데이터 영역에 서명값 이외의 데이터가 존재한다면 그 데이터의 무결성을 보장할 수 없을 뿐만 아니라 해당 데이터의 변조가 가능하다는 점을 이용해 악의적인 코드가 삽입될 수도 있다. 따라서 무결성을 보장받을 수 없는 서명데이터 영역에 전자서명 값 이외의 데이터가 존재하지 않는지도 확인해야 한다.

전자문서 소프트웨어는 전자문서에 포함된 전자서명의 유효성을 검증하기 위하여 전자서명의 서명검증 뿐만 아니라 전자서명에 사용된 인증서의 검증도 함께 수행해야 한다[2][3]. 인증서 검증은 인증 경로를 구축하는 과정과 인증 경로에 포함된 인증서들에 대한 기본 검증 과정으로 나누어 생각해 볼 수 있으며, 인증 경로에 포함된 모든 인증서들이 기본 검증을 통과한 경우에만 전자서명 검증에 사용된 인증서가 유효하다고 판단할 수 있다[4][5]. 인증서 기본 검증은 인증서에 적용된 전자서명 검증, 인증서 상태 검증, 유효기간 검증, 정책 검증의 네 가지로 구분할 수 있으나, 일반적으로 전자문서 소프트웨어에서 전자서명에 사용하는 인증서의 정책에 제한을 두지 않으므로 정책

〔표 1〕 안전성 분석에 대한 테스트 방법

분석 내용			분석 방법
전자서명 표시 기능 제공			- 사용자가 전자서명의 존재여부를 확인할 수 있는 기능이 제공되는지 확인한다. - 전자서명의 검증 결과, 서명자 정보, 서명 시간을 정확하게 표시하고 있는지 확인한다.
전체 문서에 대한 전자서명			- 서명의 대상이 되는 원문의 범위를 확인할 수 있는 문서 포맷의 경우, 원문의 범위가 전자서명 값 영역을 제외한 문서 전체로 설정되어 있는지를 확인한다. - 원문의 범위 확인이 불가능한 경우 서명데이터 이외의 영역을 변경한 뒤 검증을 시도한다. 전자서명 검증을 성공하면 원문의 범위를 문서 전체로 설정하고 있지 않다고 판단할 수 있다.
서명데이터 영역 확인			- 전자서명 값이 저장되는 영역에 전자서명 값 이외의 불필요한 데이터가 존재하지 않는지 확인한다.
전자서명 검증			- 전자서명 수행 후 서명을 검증해본다. - 전자문서에 포함된 서명값을 임의로 변경하여 전자서명을 생성한 뒤, 검증을 시도한다. 전자서명 검증을 실패하면 전자서명 검증을 정상적으로 수행하고 있다고 판단할 수 있다.
인증서 검증	인증서 경로 구축		- 최상위인증기관의 인증서 등록 기능이 있는지 확인한다. - 전자서명에 사용된 인증서의 구축 경로 확인 기능이 있는지 확인한다.
	기본 검증	서명검증	- 인증서의 signature value 필드 값을 임의로 변경하여 전자서명을 생성한 뒤, 검증을 시도한다. 전자서명 검증을 실패하면 인증서에 적용된 서명 검증을 정상적으로 수행하고 있다고 판단할 수 있다.
		상태검증	- 폐지된 인증서로 전자서명을 생성한다. 전자서명을 생성할 수 없으면 폐지된 인증서의 사용방지 기능이 존재한다고 판단한다. - 폐지된 인증서로 전자서명을 검증한다. 전자서명 검증을 실패하면 인증서 상태 검증을 정상적으로 수행하고 있다고 판단할 수 있다.
		유효기간 검증	- 유효기간이 만료된 인증서로 전자서명을 생성한다. 전자서명을 생성할 수 없으면 유효기간이 만료된 인증서의 사용방지 기능이 존재한다고 판단한다. - 유효기간이 만료된 인증서로 전자서명을 검증한다. 전자서명 검증을 실패하면 인증서의 유효기간 검증을 정상적으로 수행하고 있다고 판단할 수 있다. - 컴퓨터 시간을 인증서의 유효기간이 만료되기 이전의 시간으로 조작한 뒤 동일한 테스트를 수행한다. 테스트 결과가 유효기간이 만료된 시점의 테스트와 동일하다면 신뢰할 수 있는 시간 정보를 사용하여 유효기간 검증을 수행하고 있다고 판단할 수 있다.

검증을 제외한 세 가지 기본 검증에 대해서만 안전성을 분석하도록 한다. 각각의 안전성 분석에 대한 테스트 방법은 아래 〔표 1〕과 같다.

III. PDF 소프트웨어의 전자서명 기능 안전성 분석

3.1 PDF 개요 및 전자서명 표준 분석

PDF는 Portable Document Format의 약자로 하드웨어, 운영체제, 시스템 등에 구속되지 않고 문서를 생성하고 읽고 출력 가능하도록 지원해주는 Postscript 언어 기반의 문서 포맷 형식이다〔6〕.

PDF는 다양한 환경에서 생성된 문서간의 호환성을 제공한다는 장점 때문에 대중화되었으며, Adobe사에서 개발한 PDF 표준은 2008년 7월에 ISO 32000-1 국제 표준으로 지정되어 현재는 ISO (International Organization for Standar-dization)에서 유지 관리되고 있다. ISO 32000-1에는 전체 PDF 사양이 포함되어 있으며 이중 Interactive Features 항목에 전자서명과 관련된 표준이 포함되어 있다〔7〕.

ISO 32000-1의 '12.8 Digital Signatures'에서는 Signature Dictionary에 대해 명시하고 있으며, Signature Dictionary에는 전자서명 검증을 위해 필요한 정보들(예, 서명값, 원문의 범위, 인증서 등)에 대한 엔트리가 정의되어 있다. 따라서 PDF 소프트웨어에서 전자서명 생성 시에는 Signature Dictionary 형태로 데이터를 생성하여야 하며, 전자서명 검증 시에는 Signature Dictionary를 읽어 들여 필요한 데이터를 추출해내야 한다. Signature Dictionary의 주요 엔트리에 대한 정보는 아래 〔표 2〕와 같다.

〔표 2〕 Signature Dictionary의 주요 엔트리

엔트리	설명
Type	dictionary의 종류를 기술하며, 값은 Sig로 고정하여 사용한다.
Filter	서명값을 검증할 때 사용할 Handler의 이름을 기술한다. SubFilter를 지원하는 Filter를 사용하는 경우 SubFilter 엔트리에 값을 기술해야 한다.
SubFilter	Signature Dictionary에 존재하는 서명값과 키를 인코딩하는 방식에 대해 기술한다. Adobe Filter를 사용하는 경우 adbe.x509.rsa_sha1, adbe.pkcs7.detached, adbe.pkcs7.sha1을 사용할 수 있다.
Contents	실제 서명값이 들어간다.
Cert	서명값을 생성하거나 검증할 때 사용되는 X.509 인증서 체인이 들어간다.
ByteRange	서명에 대한 원문의 범위를 기술한다.
M	서명이 이뤄진 시점을 기술한다.

본 논문의 분석 대상 소프트웨어에서는 Adobe Filter를 사용하며, SubFilter로 adbe.pkcs7.detached와 adbe.pkcs7.sha1이 사용된다. 따라서 서명값은 PKCS#7 형태로 인코딩되어 저장되며 이때 인증서도 함께 인코딩되어 들어간다[8]. 일반적으로 PKCS#7의 SignedData 형식에는 원문이 함께 인코딩되어 들어가지만 PDF의 경우 전자서명이 전자문서에 첨부되는 방식으로 원문 사이에 서명값이 들어가야 하기 때문에, PKCS#7의 SignedData에 원문이 직접 들어가지 않고 ByteRange를 통해 원문의 범위만을 지정한다. 따라서 SubFilter로 adbe.pkcs7.detached가 사용되는 경우에는 PKCS#7의 SignedData에 원문이 생략되며, adbe.pkcs7.sha1이 사용되는 경우에는 원문 대신 원문의 해쉬 값이 인코딩되어 들어간다.

3.2 PDF 소프트웨어의 전자서명 기능 안전성 분석

PDF는 공개되어있는 국제 표준이기 때문에, Adobe사에서 제작된 Acrobat 외에도 다양한 종류의 PDF 소프트웨어가 존재하며 사용되고 있다. 본 논문에서는 안전성 분석 대상 소프트웨어로 CEOWORLD News에서 선정한 Top Best PDF Software 중 세 회사의 제품을 선택하였으며, 안전성 분석 대상 소프트웨어의 정보는 아래 〔표 3〕과 같다[9].

〔표 3〕 PDF 안전성 분석 대상 소프트웨어

회사명	제품명	버전
Adobe	Acrobat X Pro	10
Foxit	Phantom	2.2.4
Nuance	PDF Converter	7.0

Adobe Acrobat X Pro, Foxit Phantom, Nuance PDF Converter 세 제품을 대상으로 진행한 분석 결과는 아래 〔표 4〕와 같다.

분석 결과에서 볼 수 있듯이 세 제품 모두 전자서명 검증은 정상적으로 수행하고 있으나 Adobe Acrobat X Pro를 제외한 두 제품은 인증서의 기본 검증조차 제대로 수행하지 않고 있다. 이것은 악의적인 사용자가 인증서를 임의로 조작하거나 생성한 뒤 전자서명을 수행할 수 있다는 것을 의미하며, 결국 소프트웨어를 통해 생성한 전자서명을 신뢰할 수 없음을 뜻한다. Adobe Acrobat의 경우에도 전자서명 검증 시에는 인증서 기본 검증을 제대로 수행하였지만 전자서명 생성 시에 인증서의 상태검증을 수행하지 않아 서명자의 전자서명부인을 방지할 수 없다는 문제점이 존재한다. 또한 세 제품 모두 인증서의 유효기간 검증 수행에 있어 쉽게 변경이 가능한 사용자의 컴퓨터 시

〔표 4〕 PDF 소프트웨어의 전자서명 기능에 대한 안전성 분석 결과

분석 내용			Adobe Acrobat X Pro	Foxit Phantom	Nuance PDF Converter
전자서명 표시 기능 제공			O	O	O
전체 문서에 대한 전자서명			O	O	O
서명데이터 영역 확인			O	O	O
전자서명 검증			O	O	O
인증서 검증	인증서 경로 구축		O	?	?
	기본 검증	서명검증	O	X	X
		상태검증	◐	X	X
		유효기간 검증	△	△	△

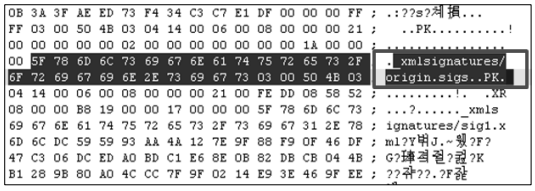
O: 정상적으로 검증을 수행함/안전하게 기능을 수행함
X: 검증을 수행하지 않음
△: 검증을 수행하지만 취약점이 존재함
◐: 전자서명 검증 시에만 인증서 상태 검증을 수행함
? : 최상위인증기관의 인증서 등록 기능이 없으며, 인증서 구축 경로를 보여주지 않음

간을 사용하기 때문에 사용된 인증서의 안전성을 신뢰할 수 없으며, 서명자의 서명부인을 방지할 수 없다는 문제점이 존재한다[10].

IV. 4.2 MS Word의 전자서명 기능 안전성 분석

4.1 MS Word 개요 및 전자서명 기능 분석

MS Word는 마이크로소프트(Microsoft)사에서 개발한 워드 프로세서이다. 현재 가장 널리 사용되는 워드프로세서 중 하나로, 여러 문서를 작성하는데 필요한 다양한 기능들을 포함하고 있다[11]. MS Word의 경우 전자서명 기능을 '문서에 표시되는 전자서명'과 '문서에 표시되지 않는 전자서명'의 두 가지 형태로 제공하고 있으며, '문서에 표시되는 전자서명'의 경우 서명자는 서명 이미지를 선택하거나 Tablet PC의 잉크 기능을 사용하여 서명할 수 있다. MS Word로 생성한 전자서명은 '문서에 표시되는 전자서명'과 '문서에 표시되지 않는 전자서명' 모두 [그림 1]과 같은 특정한 형태를 띤다. 하지만 MS Word의 경우 전자서명과 관련된 공개된 표준이 존재하지 않아 포맷을 분석할 수는 없다.



[그림 1] MS Word의 전자서명 관련 정보

4.2 MS Word의 전자서명 기능 안전성 분석

MS Word의 전자서명 기능 안전성 분석 결과는 아래 [표 5]와 같다. 분석 결과에서 볼 수 있듯이 MS Word는 전자서명 기능이 대부분 안전하게 구현되어 있었다. MS Word의 경우 포맷 분석이 불가능했기 때문에, 전체 문서에 대한 전자서명 분석과 서명데이터 영역의 불필요한 데이터 확인 분석은 생략되었다. 인증서 경로 구축은 사용자의 최상위인증기관 인증서 등록 기능이 존재하지는 않았지만, 운영체제에 등록된 신뢰된 루트 인증기관 정보를 통해 최상위인증기관의 인증서를 신뢰하는 방식을 사용하고 있었다. MS Word의 경우 인증서 기본검증 중 서명 검증과 상태

[표 5] MS Word의 전자서명 기능에 대한 안전성 분석 결과

분석 내용			분석 결과
전자서명 표시 기능 제공			O
전자서명 검증			O
인증서 검증	인증서 경로 구축		O
	기본 검증	서명검증	O
		상태검증	O
		유효기간검증	△

O: 정상적으로 검증을 수행함/안전하게 기능을 수행함
△: 검증을 수행하지만 취약점이 존재함

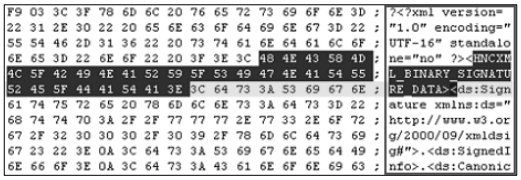
검증 또한 정상적으로 수행하고 있었다. 인증서의 유효기간 검증의 경우, 서명 생성 시에는 유효기간이 만료된 인증서를 보여주지 않음으로써 유효기간이 만료된 인증서의 사용을 방지하였고 서명 검증 시에도 인증서의 유효기간이 지난 경우 서명에 사용된 인증서가 유효하지 않음을 표시해 사용자가 이를 확인할 수 있도록 하였다. 하지만 인증서의 유효기간 검증 수행에 있어 쉽게 변경이 가능한 사용자의 컴퓨터 시간을 사용하기 때문에 사용된 인증서의 안전성을 완전하게 신뢰할 수 없다는 문제점이 존재한다[12].

V. 훈글의 전자서명 기능 안전성 분석

5.1 훈글 개요 및 전자서명 기능 분석

훈글은 한글과컴퓨터사에서 개발된 한글 워드프로세서로, 국내에 가장 널리 보급된 한글 문서작성 프로그램이며 문서 작성에 필요한 다양한 기능들을 포함하고 있다. 훈글은 훈글2007 버전부터 전자서명 생성 기능이 추가되었으며, 공인인증서를 사용한 전자서명 생성 및 검증 기능을 지원한다[13]. 훈글의 경우 전자서명을 문서에 표시하는 기능은 지원하지 않지만 전자서명이 포함된 문서를 불러올 때 훈글2007은 '전자서명이 포함된 문서입니다.'라는 메시지를 띄움으로써 수신자에게 전자서명이 포함된 전자문서임을 알려주고, 훈글2010은 전자서명 유효성 검증 결과 메시지를 띄움으로써 전자서명이 포함되었다는 사실과 함께 전자서명의 유효성 검증 결과를 보여준다. 훈글은 [그림 2]와 같이 전자서명 정보 저장을 위해 XML Signature 포맷을 사용하고 있다.

XML Signature의 내용을 분석해보면 전자서명 알고리즘으로 RSA-SHA1을 사용하였고, 해쉬 알고리즘으로 SHA1을 사용하였음을 알 수 있다. 또한,



〔그림 2〕 호글의 전자서명 관련 정보

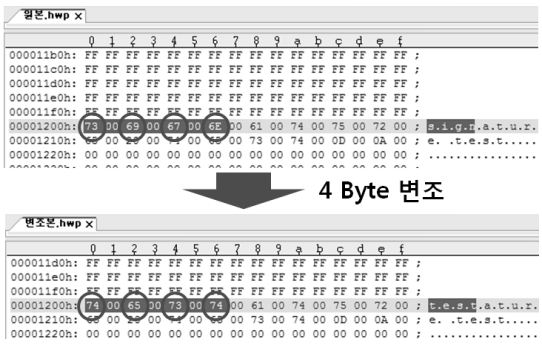
Digest Value 즉, 메시지의 해쉬 값과 전자서명 값을 확인할 수 있다. 전자서명 값은 Base64 인코딩되어 저장되고 있으며, 디코딩을 해보면 128bit의 전자서명 값이 들어가는 것을 확인할 수 있다.

5.2 호글 개요 및 전자서명 기능 분석

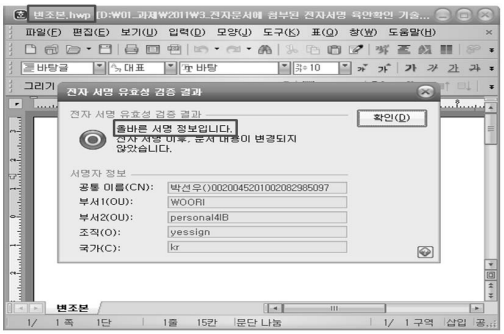
호글의 전자서명 기능 안전성 분석 결과는 아래 〔표 6〕과 같다. 전체 문서에 대한 전자서명 분석의 경우 호글에서는 원문의 범위 확인이 불가능하였지만, 서명데이터 영역을 명확하게 알 수 있었기 때문에 〔그림 3〕과 같이 서명데이터 이외의 영역에 대한 데이터 변조 테스를 수행하였다.

테스트 결과 호글에서는 〔그림 4〕와 같이 서명데이터 이외의 영역 중 일부 내용이 변경되었음에도 불구하고 서명정보가 올바르다는 메시지를 출력하였다. 즉 호글에서는 전자서명의 대상이 되는 원문의 범위를 전체 문서로 설정하지 않고 있음을 확인할 수 있었다.

호글의 경우 국산 소프트웨어이기 때문에 전자서명 생성 시 공인인증서만을 사용할 수 있도록 개발되었으며, 국내 공인인증체계에서는 신뢰할 수 있는 최상위 인증기관이 한국인터넷진흥원(KISA)으로 지정되어 있기 때문에 별도의 최상위인증기관 인증서 등록 기능



〔그림 3〕 호글의 서명데이터 이외 영역의 변조 테스트



〔그림 4〕 호글의 서명데이터 이외 영역의 변조 테스트 결과

은 필요로 하지 않는다. 또한 호글은 인증서 기본검증 중 서명 검증과 상태 검증을 정상적으로 수행하고는 있으나, 검증이 실패하는 경우 그 사유를 명확히 표시하지 않아 검증 실패의 원인 파악이 어렵다는 단점이 존재한다. 인증서 유효기간 검증의 경우, 서명 생성 시 유효기간이 만료된 인증서의 사용 방지 기능은 존재하지만 서명 검증 시에는 인증서의 유효기간 검증을 수행하지 않는다. 호글 담당자와의 토의 결과 이는 호글이 최초 설계 단계에서 전자서명 생성 시 검증된 인증서 유효기간은 전자서명 검증 시에 의미가 적다고 판단하였기 때문임을 알 수 있었다. 현재 호글에서는 이 부분에 대한 설계 수정을 검토하고 있다. 또한 호글 역시 인증서의 유효기간 검증 수행에 있어 쉽게 변경이 가능한 사용자의 컴퓨터 시간을 사용하기 때문에 사용된 인증서의 안전성을 완전하게 신뢰할 수 없다는 문제점이 존재한다.

〔표 6〕 호글의 전자서명 기능에 대한 안전성 분석 결과

분석내용			분석결과
전자서명 표시 기능 제공			O
전체 문서에 대한 전자서명			X
서명데이터 영역 확인			O
전자서명 검증			O
인증서 검증	인증서 경로 구축		O
	기본 검증	서명검증	O
		상태검증	O
		유효기간검증	◑

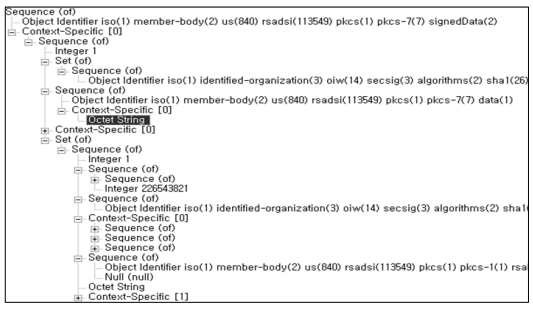
O: 정상적으로 검증을 수행함/안전하게 기능을 수행함
X: 안전하게 기능을 수행하지 않음
◑: 전자서명 생성 시에만 인증서 유효기간 검증을 수행함

VI. 정부서비스의 전자서명 기능 분석

6.1 법무부 전자공증 서비스의 전자서명 기능 안전성 분석

법무부 전자공증 서비스는 기존 오프라인 기반의 공증 서비스를 온라인상에서 서비스 받을 수 있도록 구현된 시스템이다. 법무부 전자공증 시스템을 이용하면 전자화 문서를 공증하고 공증 받은 문서를 보관할 수 있으며, 발급된 문서의 동일성을 검증할 수 있다[14]. 법무부에서는 이러한 전자공증 서비스를 제공하기 위해 자체적으로 전자공증용 PDF 소프트웨어를 제공하고 있으며, 전자공증용 PDF 소프트웨어에서는 다양한 포맷의 전자문서를 PDF 문서로 변환하고 전자서명을 첨부하는 기능을 제공한다. 또한 전자서명 생성 시 타임스탬프도 함께 생성해 준다. 전자공증 서비스는 adbe.pkcs7.sha1 Subfilter를 사용하여 생성되며, 서명값은 [그림 5]와 같이 확인해 볼 수 있다.

전자공증 서비스의 전자서명 기능 안전성 분석 결과는 아래 [표 7]과 같다. 분석 결과에서 볼 수 있듯이 전자공증 서비스는 전자서명 기능이 안전하게 구현되어 있었다. 인증서 경로 구축은 한글과 마찬가지로 공인인증서만을 사용하도록 개발되었기 때문에, 별도의 최상위인증기관 인증서 등록 기능은 필요로 하지 않는다. 전자공증 서비스의 경우 인증서 기본검증 중 서명 검증과 상태 검증 또한 정상적으로 수행하고 있었다. 인증서의 유효기간 검증의 경우, 서명 생성 시 유효기간이 만료된 인증서의 사용 방지 기능이 있었으며 서명 검증 시에도 인증서의 유효기간이 지난 경우 서명에 사용된 인증서가 유효하지 않음을 표시해 사용자가 이를 확인할 수 있도록 하였다. 또한 인증서 유효기간 검증에 사용되는 시간으로 사용자의 컴퓨터 시간정보를 사용하지 않기 때문에 컴퓨터 시간 조작에 대한 취약점이 존재하지 않았다.



[그림 5] 전자공증 서비스의 전자서명 관련 정보

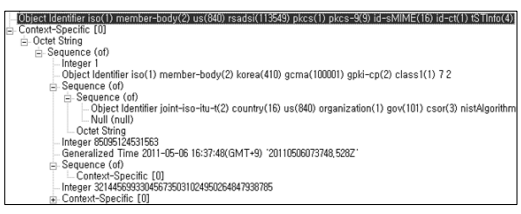
[표 7] 전자공증 서비스의 전자서명 기능에 대한 안전성 분석 결과

분석내용			분석결과
전자서명 표시 기능 제공			O
전체 문서에 대한 전자서명			O
서명데이터 영역 확인			O
전자서명 검증			O
인증서 검증	인증서 경로 구축		O
	기본 검증	서명검증	O
		상태검증	O
		유효기간검증	O

O: 정상적으로 검증을 수행함/안전하게 기능을 수행함

6.2 국세청 연말정산 간소화 서비스의 전자서명 기능 안전성 분석

국세청 연말정산 간소화 서비스는 근로소득세 연말정산에 필요한 각종 소득공제 증명 자료를 국세청이 은행, 학교, 병의원 등 영수증 발급기관으로부터 수집하여 이를 인터넷 홈페이지에서 제공하는 서비스이다[15]. 근로소득자는 국세청 연말정산 간소화 서비스를 통해 소득공제신고서를 출력할 수 있으며, 전자문서의 형태로 저장 및 제출할 수도 있다. 전자문서의 형태로 저장되는 경우 문서 포맷은 PDF 파일로 저장되며 문서의 변조를 방지하고자 정부 시점 확인센터로부터 타임스탬프를 발급받아 전자문서에 첨부한다[16]. 타임스탬프란 신뢰할 수 있는 제3의 기관이 전자문서에 대해 시각정보를 부여하고 전자서명을 수행함으로써, 전자문서가 어느 특정 시각에 존재하고 있었다는 것을 증명하는 것과 동시에, 그 시각 이후에 데이터가 변경되지 않았음을 증명하는 기술이다[17]. 연말정산 간소화 서비스의 경우 타임스탬프를 통한 문서의 변조 여부를 확인하기 위해 별도의 플러그인을 제공하고 있으며, 타임스탬프 값은 [그림 6]과 같이 확인해 볼 수 있다.



[그림 6] 연말정산 간소화 서비스의 전자서명 관련 정보

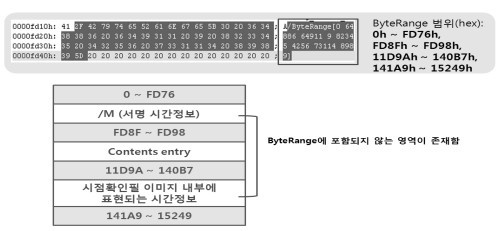
국세청의 연말정산 간소화 서비스의 경우 전자서명을 수행하는 주체가 일반 개인이 아닌 정부시점 확인센터 이기 때문에 전자서명 생성을 위한 별도의 소프트웨어는 제공되지 않는다. 다시 말해 앞서 수행했던 전자서명 구현에 대한 안전성 분석 방법을 그대로 적용하기에는 어려움이 따른다. 따라서 본 논문에서는 국세청 연말정산 간소화 서비스를 통해 생성된 전자서명의 안전성에 대한 분석만을 수행하였다.

ISO32000-1에서는 ByteRange 영역에 포함되지 않은 부분은 무결성을 보장받을 수 없기 때문에, 문서 전체를 ByteRange 영역으로 설정하기를 강하게 권고하고 있으며 여기서 문서 전체란 Contents 엔트리(실제 서명값이 들어있는 영역)만을 제외한 모든 영역을 뜻한다. 따라서 Contents 엔트리를 제외한 signature dictionary 영역도 ByteRange에 포함되어야 한다. 하지만 국세청 연말정산 시스템에서 전자서명을 수행한 PDF 문서를 확인해보면 〔그림 7〕과 같이 ByteRange의 영역이 4개의 영역으로 분할되어 있으며, ByteRange에 포함되지 않는 영역이 존재함을 알 수 있다.

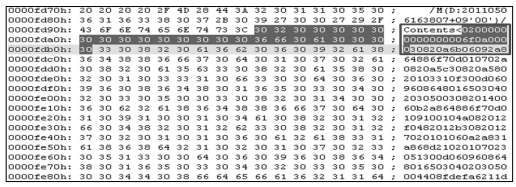
국세청 연말정산 시스템의 경우 타임스탬프 서비스를 제공하는데 발생하는 문제를 해결하기 위해 전체 문서에 대해 전자서명을 수행할 수 없었다. 하지만 다행히 원문의 범위에 포함되지 않는 영역의 무결성을 보장받을 수 있게 하기 위해 별도의 메커니즘을 제공하고는 있다.

국세청 연말정산 시스템과 같이 개발상의 이유로 ByteRange에 문서 전체 영역을 포함시킬 수 없다면, 개발자는 포함되지 않은 부분의 무결성을 보장하기 위해 별도의 메커니즘을 반드시 제공해야 한다. 만약 개발자가 이러한 부분을 고려하지 못했다면 해당문서는 전자서명이 적용되었음에도 불구하고 무결성을 보장 받을 수 없다.

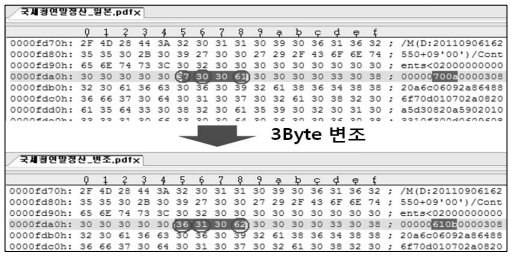
서명데이터 영역의 불필요한 데이터 확인 분석을 위해 국세청 연말정산 시스템에서 전자서명을 수행한



〔그림 7〕 국세청 연말정산 시스템의 ByteRange 설정



〔그림 8〕 국세청 연말정산 시스템의 Contents 엔트리



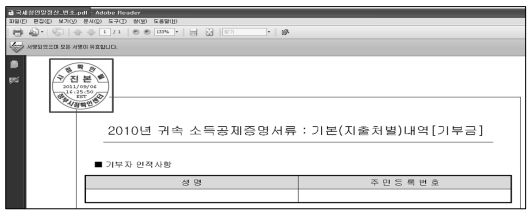
〔그림 9〕 Contents 엔트리 내부 데이터 변조 테스트

PDF 문서를 확인해보면 〔그림 8〕과 같이 Contents 엔트리에 서명값 이외의 데이터가 존재함을 확인할 수 있다.

Contents 엔트리에 존재하는 서명값 이외의 데이터가 무결성을 보장받을 수 없음을 확인하기 위해 〔그림 9〕와 같이 데이터를 1Byte 변경한 뒤 서명 검증을 시도해 보았다.

테스트 결과 〔그림 10〕과 같이 변조가 있었음에도 서명 검증이 성공하는 것을 확인할 수 있다. 즉 국세청 연말정산 시스템에서는 Contents 엔트리에 존재하는 서명값 이외의 데이터에 대한 무결성을 완전하게 제공하지 못하고 있음을 확인할 수 있다.

국세청 연말정산 간소화 서비스를 통해 생성된 전자서명의 안전성을 분석한 결과를 정리하면 아래 〔표 8〕과 같다. 분석 결과에서 볼 수 있듯이 국세청 연말정산 간소화 서비스에서는 전자서명 대상을 문서 전체로 설정하고 있지는 않지만, 전자서명 대상에서 제외된 부분의 무결성을 보장하기 위한 별도의 메커니즘을



〔그림 10〕 Contents 엔트리 내부 데이터 변조 테스트 결과

〔표 8〕 국세청 연말정산 간소화 서비스의 전자서명 기능에 대한 안전성 분석 결과

분석내용	분석결과
전자서명 표시 기능 제공	전자서명 표시 기능을 제공함
전체 문서에 대한 전자서명	전자서명의 대상을 문서 전체로 설정하지는 않으나, 전자서명 대상에서 제외된 부분의 무결성을 보장하기 위한 별도의 메커니즘이 제공됨
서명데이터 영역 확인	서명값 이외의 데이터가 저장되어 있으며,해당 데이터에 대한 변조가 가능함

제공하고 있다. 또한 전자서명의 서명값 영역에 서명값 이외의 데이터가 저장되어 있으며, 해당 데이터에 대한 변조가 가능하다. 물론, 이 부분이 원문의 무결성에 직접적으로 영향을 미치는 것은 아니지만, Contents 엔트리에 개발자가 의도한 값이 아닌 중간에 변조된 값이 들어가도 이를 검증 시 검출하지 못한다는 점은 위협요소가 될 수 있다.

VII. 전자서명 기능 구현에 대한 권고사항

앞서 수행한 전자문서 소프트웨어의 전자서명 기능에 대한 안전성을 분석해본 결과, 몇몇 전자문서 소프트웨어는 인증서의 기본 검증조차 수행하지 않음을 확인할 수 있었다. 또한 기본 검증을 수행하는 경우라도 인증서의 유효기간 검증에 신뢰할 수 없는 시간 정보를 사용하거나, 표준을 준수하여 구현되지 않는 등 여러 보안상 문제점을 발견할 수 있었다. 이에 본 논문에서는 전자문서 소프트웨어에서 개발자가 전자서명 기능 구현 시 고려할 사항을 정리해 봄으로써 신뢰할 수 있는 전자서명 기능을 구현하기 위한 가이드라인을 제공하고자 한다. 본 논문에서 제안한 권고사항을 만족하여 전자서명 기능을 구현한 전자문서 소프트웨어는 전자서명 기능에 대한 최소한의 안전성을 확보할 수 있다.

7.1 전자서명 생성에 대한 권고사항

7.1.1 전자서명 표시 기능 제공

전자문서 소프트웨어는 사용자가 전자서명의 존재 여부를 확인하고 검증할 수 있도록 문서에 전자서명이 표시되는 기능을 제공해야 한다. 전자서명 표시 기능은 기본적으로 전자서명의 검증 결과, 서명자 정보, 서명 시간을 표시해야 하며 사용자가 전자서명과 관련된 세부 내용을 확인하고자 하는 경우 전자서명에 사용된 알고리즘, 전자서명 검증에 사용된 인증서의 정보 등 세부 내용도 함께 제공해야 한다. 또한 전자서명 검증이 실패한 경우 이를 사용자가 쉽게 확인할 수 있도록 하여 문서의 무결성을 보장할 수 없음을 알려야 한다.

7.1.2 전체 문서에 대한 전자서명

전자 서명 기능을 제공하는 전자문서 소프트웨어의 경우 전체 문서에 대한 신뢰성 확보를 위해 서명의 대상이 되는 원문의 범위를 전체 문서로 설정해야 한다. 다시 말해 전체 문서에 대한 전자서명이 이뤄져야 한다. 하지만 국세청 연말정산 간소화 서비스와 같이 타임스탬프 서비스와 같은 특정 서비스를 제공하기 위해, 구현상의 이유로 불가피하게 전체 문서에 대한 전자서명을 수행할 수 없는 경우가 존재할 수 있다. 이러한 경우 전자서명으로 무결성이 보장되지 않는 부분에 대해서도 무결성이 보장될 수 있도록 별도의 메커니즘을 제공해야 한다.

7.1.3 서명데이터 영역의 불필요한 데이터 삭제

전자문서에 첨부되는 전자서명의 서명값이 저장되는 영역은 원문의 범위로 지정되지 못한다. 따라서 전자서명 값이 저장되는 영역에 전자서명 값 이외의 불필요한 데이터가 들어간다면 그 데이터의 무결성은 보장할 수 없게 되며, 이는 국세청 연말정산 간소화 서비스의 Contents 엔트리 내부 데이터 변조 테스트를 통해 확인할 수 있다. 또한 해당 데이터의 변조가 가능하다는 점을 이용해 악의적인 사용자가 악성코드와 같은 실행코드를 삽입하는 경우 그 피해가 더 커질 수 있다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어는 전자서명 값이 저장되는 영역에 불필요한 데이터가 들어가지 않도록 구현해야 한다.

7.1.4 인증서 상태 검증

Adobe Acrobat, Foxit Phantom, Nuance PDF Converter와 같이 폐지 또는 효력 정지된 인증서를 사용한 서명 생성이 가능한 경우에는 추후 서명 부인 문제가 발생할 수 있다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어는 서명자의 서명

부인방지를 위해 폐지 또는 효력정지 상태인 인증서의 사용 방지 기능을 제공해야 한다. 인증서의 유효성을 확인하기 위해서는 CRL 또는 OCSP를 이용할 수 있으며, 인증서의 실시간 상태 정보를 필요로 하는 경우에는 OCSP를 사용할 것을 권고한다[18].

7.1.5 인증서 유효기간 검증

전자서명 기능을 제공하는 전자문서 소프트웨어는 서명자의 서명 부인방지를 위해 유효기간이 만료된 인증서로 전자서명을 수행하지 못하도록 유효기간 만료 인증서의 사용 방지 기능을 제공해야 한다. 유효기간 검증 수행을 위한 시간정보로는 쉽게 조작할 수 있는 사용자 컴퓨터의 시간정보가 아닌 신뢰할 수 있는 서버로부터 가져온 시간정보를 사용하기를 권고하며, 타임 스탬프 토큰을 사용할 수도 있다.

7.2 전자서명 검증에 대한 권고사항

전자서명 기능을 제공하는 전자문서 소프트웨어는 전자서명에 대한 검증뿐만 아니라 전자서명에 사용된 인증서에 대한 정확한 검증도 함께 수행되어야 한다. 전자서명에 사용된 인증서 검증에는 각 단계별로 다음과 같은 사항이 고려되어야 한다.

7.2.1 인증서 경로 구축

인증서 경로 구축에 대한 결과와 신뢰 가능 여부를 사용자가 쉽게 확인할 수 있도록 해야 한다. 특히 인증서 경로 구축을 실패하였거나 인증서를 신뢰할 수 없는 경우 반드시 사용자에게 이를 알려 전자서명을 완전하게 신뢰할 수 없음을 경고해야 한다. 또한 신뢰할 수 있는 최상위인증기관의 인증서를 사용자가 등록할 수 있는 기능이 제공되어야 한다. 하지만 혼글, 전자공증 서비스와 같이 최상위인증기관이 고정되어 있는 경우에는 해당 기능이 생략될 수도 있다.

7.2.2 인증서 서명 검증

Foxit Phantom, Nuance PDF Converter와 같이 전자서명 검증 단계에서 인증서의 서명 검증을 수행하지 않는 경우, 악의적인 사용자가 타인으로 가장하여 서명을 생성하여도 수신자는 이를 확인할 수 없게 된다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어는 전자서명 검증에 사용된 인증서의 무결성을 확인하기 위해 반드시 인증서의 서명 검증을 수행하여야 하며, 인증서의 서명 검증이 실패한 경우 반드시 사용자에게 이를 알려 전자서명을 완전하게 신뢰할 수 없음을 경고해야 한다.

7.2.3 인증서 상태 검증

Foxit Phantom, Nuance PDF Converter와 같이 전자서명 검증 단계에서 인증서 상태 검증을 수행하지 않는 경우, 악의적인 사용자가 타인의 유출된 키를 사용하여 서명을 생성하여도 수신자는 이를 확인할 수 없게 된다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어는 전자서명의 검증 시 전자서명 검증에 사용된 인증서의 유효성을 확인하기 위해 반드시 CRL 또는 OCSP를 이용하여 인증서의 상태 검증을 수행하여야 한다. 특히 인증서의 실시간 상태 정보를 필요로 하는 경우에는 OCSP를 사용할 것을 권고한다. 만약 인증서가 폐지 또는 효력정지의 상태라면 반드시 사용자에게 이를 알려 전자서명을 완전하게 신뢰할 수 없음을 경고해야 한다.

7.2.4 인증서 유효기간 검증

혼글과 같이 전자서명 검증 단계에서 인증서의 유효기간 검증을 수행하지 않는 경우, 악의적인 사용자가 시간이 지나 안전성이 떨어진 타인의 키를 위조하여 서명을 생성하여도 수신자는 이를 확인할 수 없게 된다. 따라서 전자서명 기능을 제공하는 전자문서 소프트웨어는 전자서명 검증 시 검증에 사용된 인증서의 위조 및 변조에 대한 안전성 확보를 위해 인증서의 유효기간 검증을 수행하여야 하며, 인증서의 유효기간이 만료된 경우 반드시 사용자에게 이를 알려 전자서명을 완전하게 신뢰할 수 없음을 경고해야 한다. 유효기간 검증 수행을 위한 시간정보로는 쉽게 조작할 수 있는 사용자 컴퓨터의 시간정보가 아닌 신뢰할 수 있는 서버로부터 가져온 시간정보를 사용하기를 권고하며, 타임 스탬프 토큰을 사용할 수도 있다.

VIII. 결 론

전자문서는 문서가 변경 및 수정되어도 이를 확인하기 어렵다는 특성을 가지고 있기 때문에 문서의 진본성을 확인하는 것이 전자문서 이용에 중요한 역할을

한다. 따라서 전자문서에 대한 법적인 유효성과 무결성을 확보하기 위해 전자서명 기술이 활용되며, 다양한 전자문서 소프트웨어들은 전자문서의 신뢰성을 보장하기 위해 전자서명 생성 및 검증 기능을 제공하고 있다. 하지만 이러한 소프트웨어들이 전자서명 생성 및 검증을 정상적으로 수행하는지에 대한 연구가 미비하여 이를 완전하게 신뢰하기 어렵다. 이에 본 논문에서는 전자서명 기능을 제공하는 전자문서 소프트웨어들의 안전성을 분석하고, 분석 내용을 기반으로 전자서명 기능 구현에 대한 권고사항을 제시하였다. 본 논문에서 제시한 안전성 분석 결과와 전자서명 기능 구현에 대한 권고사항은 소프트웨어 개발자에게는 보다 안전한 제품을 설계하고 개발하는데 도움을 줄 것이며, 평가자에게는 전자서명 기능을 제공하는 문서 작성 소프트웨어를 이해하고 이에 대한 평가를 적절하게 수행하는데 도움이 될 것이다. 또한 이는 전자문서에 첨부된 전자서명에 대한 신뢰성을 높여 전자문서 이용의 활성화에 기여할 수 있을 것이다.

참고문헌

〔1〕 오관석, 전자정부와 u-패러다임, 진한엠엔비, 2010.

〔2〕 R.C. Merkle, "A certified digital signature," Advances in Cryptology, CRYPTO'89, LNCS 435, pp. 241 - 250, 1989.

〔3〕 M. Bellare and S.K. Miner, "A Forward-Secure Digital Signature Scheme," Advances in Cryptology, CRYPTO'99, LNCS 1666, pp. 431-448, 1999.

〔4〕 R. Housley, W. Polk, W. Ford, and D. Solo, "Internet x.509 public key infra- structure certificate and CRL profile," RFC 3280, Apr. 2002.

〔5〕 Y. Lee, J. Ahn, S. Kim, and D. Won, "A PKI System for Detecting the Ex- posure of a User's Secret Key," Proceedings of EuroPKI, LNCS 4043, pp. 248 - 250, 2006.

〔6〕 Adobe Community, http://forums. adobe.com/community/acrobat

〔7〕 "Document management - Portable document format - Part 1: PDF 1.7," ISO 32000-1, Jan. 2008

〔8〕 B. Kaliski, "PKCS#7: Cryptographic Message Syntax Version 1.5," RFC 2315, Mar. 1998

〔9〕 CEOworld Magazine, http://ceoworld. biz /ceo/2010/04/13

〔10〕 S. Park, C. Lee, K. Lee, J. Kim, Y. Lee, and D. Won, "Security Analysis on Digital Signature Function Imple- mented in PDF Software," Procee- dings of FGIT, LNCS 7105, pp. 327-334, 2011.

〔11〕 MS 오피스, http://office.microsoft.com/ko-kr/products

〔12〕 이창빈, 박선우, 이광우, 김지연, 남정현, 이영숙, 원동호, "워드프로세서의 전자서명 기능에 대한 취약성 분석," 한국컴퓨터정보학회논문지, 16(8), pp. 109-118, 2011년 8월

〔13〕 한글과컴퓨터, http://www.hancom.co.kr

〔14〕 법무부 전자공증시스템, http://enotary. moj. go.kr

〔15〕 국세청 연말정산간소화서비스, http://www. yesone.go.kr/home/ragaw008.jsp

〔16〕 타임스탬프솔루션, http://www.timestamping.co.kr

〔17〕 C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol," RFC 3161, Aug. 2001.

〔18〕 Y. Lee, I. Kim, S. Kim, and D. Won, "A Method for Detecting the Exposure of OCSP Responder's Session Private Key in D-OCSP-KIS," Proceedings of EuroPKI, LNCS 3545, pp. 215-226, 2005.

부 록

〔표 A-1〕 전자문서 소프트웨어의 전자서명 기능에 대한 안전성 분석 결과 및 수정 권고사항

	전자서명 표시 기능 제공	전체 문서에 대한 전자서명	서명 데이터 영역의 불필요한 데이터 확인	전자서명 검증	인증서 경로 구축	서명 검증	상태 검증	유효기간 검증	수정권고사항
Adobe Acrobat X Pro	O	O	O	O	O	O	◐	△	· 전자서명 생성 시 인증서 상태검증을 수행해야 함 · 유효기간 검증에 신뢰할 수 있는 시간정보를 사용해야 함
Foxit Phantom	O	O	O	O	?	X	X	△	· 신뢰할 수 있는 최상위인증기관 인증서 등록기능을 제공해야 하며, 경로 구축 결과를 확인할 수 있게 해야 함 · 서명검증, 상태검증을 수행해야 함 · 유효기간 검증에 신뢰할 수 있는 시간정보를 사용해야 함
Nuance PDF Converter	O	O	O	O	?	X	X	△	· 신뢰할 수 있는 최상위인증기관 인증서 등록기능을 제공해야 하며, 경로 구축 결과를 확인할 수 있게 해야 함 · 서명검증, 상태검증을 수행해야 함 · 유효기간 검증에 신뢰할 수 있는 시간정보를 사용해야 함
MS Word	O	-	-	O	O	O	O	△	· 유효기간 검증에 신뢰할 수 있는 시간정보를 사용해야 함
훈글	O	X	O	O	O	O	O	◑	· 전체 문서에 대해 전자서명을 수행해야 함 · 전자서명 검증 시 인증서 유효기간검증을 수행해야 함
법무부 전자공증 서비스	O	O	O	O	O	O	O	O	-
국세청 연말정산 시스템	O	△	X	-	-	-	-	-	· 서명데이터 영역에 불필요한 데이터가 들어가지 않도록 해야 함

O: 정상적으로 검증을 수행함/안전하게 기능을 수행함
X: 검증을 수행하지 않음/안전하게 기능을 수행하지 않음
△: 검증을 수행하지만 취약점이 존재함
◐: 전자서명 검증 시에만 인증서의 상태 검증을 수행함
◑: 전자서명 생성 시에만 인증서의 유효기간 검증을 수행함
?: 최상위인증기관의 인증서 등록 기능이 없으며, 인증서 구축 경로를 보여주지 않음

〈著者紹介〉

박 선 우 (Sun-woo Park) 학생회원
2006년 8월: 서울여자대학교 정보보호공학과 졸업
2007년 1월~2010년 7월: 한국정보인증 연구원
2011년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 암호이론, PKI 등

이 창 빈 (Chang-bin Lee) 학생회원
2010년 2월: 학점은행제 전자계산학과 졸업
2012년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2012년 1월~현재: 한국무역정보통신 연구원
〈관심분야〉 정보보호, 암호이론, 정보보호 제품 보안성 평가, PKI 등

이 광 우 (Kwang-woo Lee) 종신회원
2005년 2월: 성균관대학교 정보통신공학부 졸업
2007년 2월: 성균관대학교 컴퓨터공학과 석사
2011년 8월: 성균관대학교 전자전기컴퓨터공학과 박사
2011년 9월~2012년 2월: 성균관대학교 전자전기컴퓨터공학과 박사후연구원
2012년 3월~현재: 삼성전자 책임연구원
〈관심분야〉 정보보호, 암호이론, 프로토콜 안전성 분석, 디지털 복합기 보안 등

김 지 연 (Jee-yeon Kim) 정회원
1995년 2월: 성균관대학교 정보공학과 졸업
1997년 2월: 성균관대학교 컴퓨터공학과 석사
2008년 2월: 성균관대학교 컴퓨터공학과 박사
1996년~2007년: 한국정보보호진흥원(現 한국인터넷진흥원) 선임연구원
〈관심분야〉 암호프로토콜, 암호이론, 정보보호관리체계 인증 등

이 영 숙 (Young-sook Lee) 종신회원
1987년 2월: 성균관대학교 정보공학과 졸업
2005년 2월: 성균관대학교 정보보호학과 석사
2008년 2월: 성균관대학교 컴퓨터공학과 박사
2009년 3월~현재: 호원대학교 사이버수사경찰학부 교수
〈관심분야〉 암호프로토콜, 암호이론, 네트워크 보안 등

원 동 호 (Dong-ho Won) 종신회원
1976년~1988년: 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
〈관심분야〉 정보보호, 암호이론, 정보이론 등