한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

전자서명 장기검증 기능 적용을 위한 PDF 표준 개선방안

박선우°, 정재욱*, 원동호*†
°*성균관대학교 정보보호연구소
e-mail:{swpark°, jwjung*, dhwon*}@security.re.kr

Improvement of the PDF Standard to Apply Long Term Electronic Signatures

Sunwoo Park°, Jaewook Jung*, Dongho Won*
°*Information Security Group, Sungkyunkwan University

● 요 약 ●

2008년 국제표준 ISO 32000-1로 지정된 PDF 표준은 전자서명에 대한 표준을 함께 제공함으로써 PDF 문서의 신뢰성을 확보하고자 하였다. 하지만 ISO 32000-1에 포함된 전자서명 관련 표준은 서명에 사용된 인증서의 유효기간이 만료되면 전자서명의 유효성을 검증할 수 없기 때문에 장기적으로 보존되는 문서의 신뢰성을 보장하는데 적절하지 않다. 따라서 본 논문에서는 PDF 국제 표준인 ISO 32000-1의 전자서명 관련 표준을 분석하고 전자서명 장기검증 기능을 적용할 수 있는 방안을 제시한다. 본 논문에서 제안한 내용을 활용한다면 다양한 PDF 소프트웨어에서 호환 가능한 전자서명 장기검증 기능을 제공할 수 있을 것이며, 이를 통해 PDF 문서의 신뢰성을 향상시킬 수 있을 것이다.

키워드: 전자서명(Electronic Signature), 장기전자서명(Long Term Electronic Signature), PDF(Portable Document Format)

I. 서론

전자문서의 유통이 활성화됨에 따라 전자문서의 신뢰성 확보에 대한 중요도가 높아지고 있으며, 최근에는 장기적으로 보존되는 문서의 신뢰성 확보에 대한 관심도 함께 증가하고 있다. 2008년 국제표준 ISO 32000-1로 지정된 PDF(Portable Document Format) 표준은 전자서명에 대한 표준을 함께 제공함으로써 PDF 문서의 신뢰성을 확보하고자 하였다. 하지만 ISO 32000-1에 포함된 전자서명 관련 표준은 서명에 사용된 인증서의 유효기간이 만료되면 전자서명의 유효성을 검증할 수 없기 때문에 장기적으로 보존되는 문서의 신뢰성을 보장하는데 적절하지 않다. 따라서 본 논문에서는 ISO 32000-1의 전자서명 관련 표준을 분석하고, 전자서명 장기검증 기능을 적용할 수 있는 개선된 표준안을 제시한다.

II. 배경 지식

2.1 장기전자서명

일반적인 전자서명은 전자서명에 사용된 암호 알고리즘이 취약해지거나 검증에 사용될 인증서가 만료될 수 있기 때문에 오랜 시간이 지난 후 전자서명을 검증하는데 제한을 받는다. 따라서 전자서명을 장기적으로 보관하고 관리할 수 있는 기술이 요구되고 있다. 현재 이러한 전자서명의 장기 검증 문제를 해결하기 위해 다양한 연구가 진행되고 있으며, IETF에서 표준화된 대표적인 장기검증 기술로는 타임스탬프 토큰에 기반을 둔 IETF RFC 3126 “Electronic Signature Formats for long term electronic signatures(ESF)”와 IETF RFC 4998 “Evidence Record Syntax(ERS)”가 있다[1][2]. ESF는 전자서명 장기검증을 위한 전자서명문 생성 및 보관 형식을 정의한 표준으로, IETF RFC 2630에서 정의한 전자서명문 형식에 타임스탬프 토큰과 인증서 검증정보를 포함하는 방법을 명시한다. ESF는 전자서명의 장기 검증을 위한 가장 기본적인 형식을 제공하고는 있지만, 장기검증 대상 문서의 수가 많을 경우에는 장기검증 형식의 생성이 어렵기 때문에 현실적인 모델은 아니다. ERS는 ESF를 확장시킨 표준으로 Hash -Tree를 이용하여 다수의 전자서명 문서의 유효성 보증을 가능하게 하였다.

2.2 ISO 32000-1

ISO 32000-1은 전자문서가 생성되거나 출력되는 환경에 독립적일 수 있도록 전자문서의 표현을 정의한 표준으로 Adobe사에서 개발한 개방형 표준이다[3]. 현재는 ISO(Inter national Organization for Standardization)에서 유지 관리하고 있으며, PDF와 관련된 여러 파생된 표준의 토대가 되고 있다. ISO 32000-1에 정의된 PDF 문서는 기본 타입의 Data Object들로 구성되어 있으며, File Structure에서

† 교신저자, dhwon@security.re.kr

각 Object에 대한 저장 방법, 접근 방법, 업데이트 방법을 결정한다. File Structure는 기본적으로 Header, Body, Cross reference table, Trailer로 구성된다. Document Structure는 Object가 사용되는 방법을 결정하며, Content Stream은 페이지의 외형 또는 그래픽적인 엔티티를 표현하는 명령의 순서를 포함하고 있다.

ISO32000-1에서는 8개의 기본타입 Object를 제공하며, 이 중 Dictionary Object를 사용하여 전자서명과 관련된 정보를 저장한다. Dictionary Object란 key와 value로 이루어진 여러 엔트리들을 테이블 형태로 표현한 Object이다.

III. ISO 32000-1 전자서명 관련 표준 분석

ISO 32000-1에서는 전자서명과 관련된 정보들의 저장을 위해 Dictionary Object를 사용하도록 명시하고 있다. Signature dictionary의 주요 엔트리에 대한 정보는 아래 [표 1]과 같다.

표 1. Signature dictionary의 주요 엔트리 정보
Table 1. Information of entries in a signature dictionary

Key	Type	Value
Type	name	dictionary의 종류를 정의하며, 값은 Sig로 고정하여 사용한다.
Filter	name	서명 값을 검증할 때 사용할 Handler의 이름을 기술한다.
SubFilter	name	signature 값과 key를 인코딩하는 방식에 대해 기술한다. Adobe 필터를 사용하는 경우 adbe.x509.rsa_sha1, adbe.pkcs7.detached, adbe.pkcs7.sha1을 사용할 수 있다.
Contents	byte string	실제 서명 값이 들어간다. 공개키 기반 서명인 경우에 Contents는 DER 인코딩된 PKCS#1 binary data object이거나 DER 인코딩된 PKCS#7 binary data object일 수 있다.
Cert	array or byte string	서명 값을 생성하거나 검증할 때 사용되는 X.509 인증서 체인을 표현하기 위한 byte string의 배열로, 인증서 체인이 하나인 경우에는 byte string으로 표현한다.
Byte Range	array	Digest 연산을 수행한 byte 범위, 즉 원문의 범위를 기술한다. Integer 쌍(시작 offset, 바이트 길이)의 배열로 표현된다.

PDF 소프트웨어는 Signature dictionary에 저장된 값들을 사용하여 전자서명 검증을 수행할 수 있다. ISO 32000-1 표준에 따른 전자서명 검증 프로세스는 다음 그림 1과 같다.

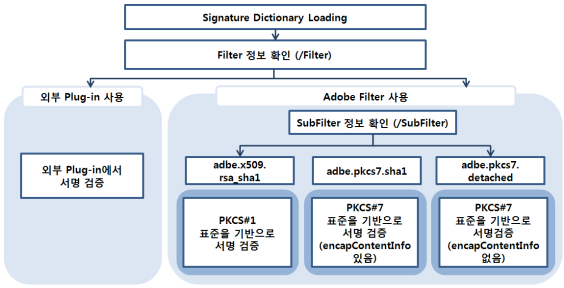

그림 1. PDF 전자서명 검증 프로세스
Fig 1. Process of digital signature verification on PDF

① PDF 파일에 첨부된 Signature Dictionary 정보를 읽어온다.
② 전자서명 검증을 위한 핸들 값이 명시된 Filter 엔트리를 확인하고, Filter 값에 따라 전자서명을 검증한다. 전자서명 검증은 크게 외부 Plug-in을 사용하는 경우와 Adobe Filter를 사용하는 경우로 나누어 볼 수 있다.
③ Filter에 외부 Plug-in 값이 저장되어 있는 경우에는 해당 핸들러를 사용하여 전자서명을 검증한다. 외부 Plug-in을 사용하는 경우의 전자서명 검증을 위한 구체적인 방법은 명시되어 있지 않다.
④ Adobe Filter를 사용하는 경우에는 SubFilter의 정보를 확인하여 서명 값의 인코딩 정보를 확인한다.
Adobe에서 지원하는 SubFilter로는 adbe.x509.rsa_ sha1, adbe.pkcs7.sha1, adbe.pkcs7.detached 세 가지가 있다. 각 SubFilter에 따른 검증 방식은 다음과 같다.

- adbe.x509.rsa_sha1

서명 검증에 필요한 원문, 서명 값, 인증서를 모두 Signature dictionary에서 확인할 수 있다. 우선 Signature dictionary의 ByteRange 엔트리에서 서명의 대상이 되는 원문의 범위를 확인하고 해당 범위만큼의 원문 데이터를 추출한다. 그리고 Cert 엔트리에서 인증서 값을, Contents 엔트리에서 서명 값을 추출한 뒤 서명 검증을 수행한다.

- adbe.pkcs7.sha1

서명 검증은 크게 Contents 엔트리 값인 PKCS#7 Signed Data의 검증과 원문 검증의 두 부분으로 나누어 진행될 수 있다. PKCS#7 Signed Data의 검증은 PKCS#7의 표준을 따른다. 이 때 Signed Data의 원문정보가 될 수 있는 encapContent Info에는 실제 원문에 대한 SHA-1 해쉬 값이 들어가며 서명 값은 원문의 SHA-1 해쉬 값에 대한 서명 값이 된다.

- adbe.pkcs7.detached

서명 검증은 크게 원문의 추출과 Contents 엔트리 값인 PKCS#7 Signed Data의 검증의 두 부분으로 나누어 진행될 수 있다. PKCS#7 Signed Data의 검증은 PKCS#7의 표준을 따른다. 이 때 Signed Data의 원문정보가 될 수 있는 encap ContentInfo가 생략되어있기 때문에 Signature Dictionary의 ByteRange에서

명시한 범위만큼의 원문을 추출하는 작업이 먼저 수행되어야 한다. PKCS#7 Signed Data는 서명 값과 인증서를 포함하고 있기 때문에 추출된 원문과 함께 서명 검증이 가능하다.

ISO 32000-1에서는 Signature dictionary를 통해 일반적인 전자서명 검증은 가능하지만, 전자서명 장기검증 기능을 제공하기는 어렵다. 이에 본 논문에서는 전자서명 장기검증 기능을 제공할 수 있도록 표준의 개선방안을 제안할 것이다.

IV. 전자서명 장기검증 기능 적용을 위한 표준 개선방안

ISO 32000-1 표준에서 전자서명 장기검증 기능을 지원하기 위해서는 우선 Signature dictionary에 해당 전자서명의 장기검증 정보에 대한 식별정보와, 전자서명 장기검증의 지원 가능 여부를 확인할 수 있는 엔트리의 추가가 필요하다. Signature dictionary에 추가되어야 하는 엔트리의 정보는 아래 [표 2]와 같다.

표 2. Signature dictionary의 추가 엔트리 정보
Table 2. Information of additional entries in a signature dictionary

Key	Type	Value
LongTerm Sig	boolean	전자서명 장기검증을 위한 정보가 존재하는 경우 True, 아닌 경우 False 값을 사용한다.
S	text string	장기전자서명의 식별자가 저장된다.

본 논문에서는 Signature dictionary의 엔트리 추가 외에도, 전자서명 장기검증을 위한 정보 저장을 위해 dictionary 형태의 object를 정의한다. Long Term Signature dictionary의 각 엔트리에 대한 주요 정보는 아래 [표 3]과 같다.

표 3. Long Term Signature dictionary의 주요 엔트리 정보
Table 3. Information of entries in a signature dictionary

Key	Type	Value
Type	name	dictionary의 종류를 정의하며, 값은 LTSig로 고정하여 사용한다.
Filter	name	장기전자서명 값을 검증할 때 사용할 Handler의 이름을 기술한다.
SubFilter	name	장기전자서명의 검증 방식과 인코딩 방식에 대해 기술한다. 본 논문에서 정의한 SubFilter로는 adbe.file.es-a, adbe.file.ers, adbe.svr.es가 있다.
S	text string	장기전자서명의 식별자가 저장된다.
Contents	byte string	전자서명 장기검증을 위한 데이터가 저장된다. SubFilter가 adbe.file.es-a 또는 adbe.file.ers인 경우에는 장기전자서명 값이 저장되며, adbe.svr.es인 경우에는 서비스서버에게 검증요청을 하기위한 메시지토큰이 저장된다.
Time	array	장기전자서명 값을 생성하거나 검증할 때
stamp Cert	or byte string	사용되는 TSA 인증서 체인을 표현하기 위한 byte string의 배열로 인증서 체인이 하나인 경우에는 byte string으로 표현한다.
Service Server	text string	SubFilter가 adbe.svr.es인 경우 검증을 요청할 서비스서버의 정보가 저장된다.

PDF 소프트웨어는 Long Term Signature dictio nary에 저장된 값들을 사용하여 전자서명 검증을 수행할 수 있으며, 검증 프로세스는 그림 2와 같다.

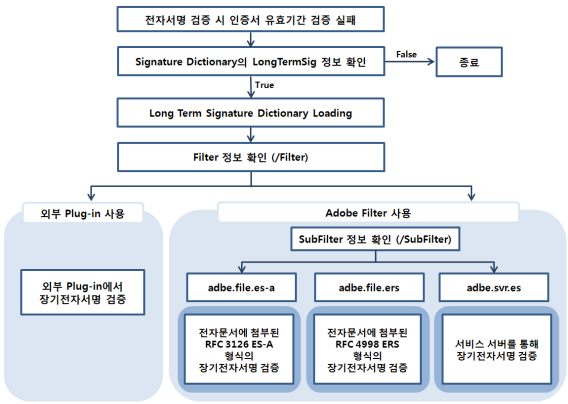

그림 2. PDF 전자서명 장기검증 프로세스
Fig 2. Process of long term digital signature verification on PDF

① 전자서명 검증 시 인증서 유효기간 검증에 실패한 경우, LongTermSig 엔트리를 통해 전자서명 장기검증이 가능한지를 확인한다. LongTermSig 엔트리의 값이 False인 경우, 전자서명 장기검증을 위한 정보가 존재하지 않으므로 프로세스를 종료시킨다.

② LongTermSig 엔트리의 값이 True인 경우 S엔트리 값을 통해 해당 전자서명의 장기검증을 위한 Long Term Signature dictionary 정보를 읽어온다.

③ 전자서명 장기검증을 위한 핸들 값이 명시된 Filter 엔트리를 확인하고, Filter 값에 따라 장기전자서명을 검증한다. 전자서명 장기검증은 크게 외부 Plug-in을 사용하는 경우와 본 논문에서 정의한 Adobe Filter를 사용하는 경우로 나누어 볼 수 있다.

④ Filter에 외부 Plug-in 값이 저장되어 있는 경우에는 해당 핸들러를 사용하여 장기전자서명을 검증한다. 외부 Plug-in을 사용하는 경우의 전자서명 장기검증을 위한 구체적인 방법은 명시하지 않는다.

⑤ 본 논문에서 정의한 Adobe Filter를 사용하는 경우에는 SubFilter의 정보를 확인하여 장기전자서명의 검증 방식과 서명 값의 인코딩 정보를 확인한다.
본 논문에서 정의한 SubFilter로는 adbe.file.es-a, adbe.file.ers, adbe.svr.es. 세 가지가 있다. 각 Sub Filter에 따른 검증 방식은 다음과 같다.

- adbe.file.es-a

Contents 엔트리에서 RFC 3126 표준의 ES-A 형식의 장기전자서명 값을 추출한 뒤, RFC 3126표준에 따라 검증을 수행한다.

- adbe.file.ers

Contents 엔트리에서 RFC 4998 표준의 ERS 형식의 장기전자서명 값을 추출한 뒤, RFC4998 표준에 따라 검증을 수행한다.

- adbe.svr.es

ServiceServer 엔트리에서 검증을 수행할 서비스 서버의 정보를 읽어온 뒤, Contents 엔트리에 저장된 검증 요청 메시지 토큰을 서비스 서버로 전송한다. 서비스 서버를 이용한 장기전자서명의 검증 프로토콜은 향후 연구에서 제안하도록 한다.

V. 결론

본 논문에서는 전자서명 장기검증 기능을 제공하기 위한 PDF 표준의 개선방안을 제안하였다. 본 논문에서 제안한 내용을 활용한다면 다양한 PDF 소프트웨어에서 호환 가능한 전자서명 장기검증 기능을 제공할 수 있을 것이며, 이를 통해 PDF 문서의 신뢰성을 향상시킬 수 있을 것이다. 향후에는 서비스 서버를 이용한 장기전자서명의 구체적인 검증 프로토콜에 대한 연구가 필요하다.

참고문헌

[1] D. Pinkas, J. Ross, N. Pope, “Electronic Signature Formats for Long Term Electronic Signatures”, RFC 3126, IETF, 2001.

[2] T. Gondrom, R. Brandner, U. Pordesch, “Evidence Record Syntax (ERS)”, RFC 4998, IETF 2007.

[3] Document management — Portable document format — Part 1: PDF 1.7, ISO 32000-1, 2008.

Acknowledge

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소지원사업으로 수행된 연구임
(2012-0005861).