情報保護學會論文誌
第14券 第4號, 2004. 8

XML 전자서명 제품의 표준적합성 시험 방법 및 구현

김 지 현†, 이 광 수‡
숙명여자대학교

A Conformance Testing Method and its Implementation for XML Signature Products

Jihyun Kim†, Gwangsoo Rhee‡
Sookmyung University

요 약

웹상에서의 전자상거래의 활성화와 더불어 XML이 관련된 응용과 업계 표준의 기반이 되고 있으며, XML 데이터 뿐만 아니라 임의의 콘텐츠에 대한 서명을 XML로 표현하여 무결성, 인증, 부인방지의 보안 기능을 제공하는 XML 전자서명에 대한 표준화가 W3C와 IETF의 공동 작업으로 수행되고 있다. 이러한 추세에 따라 XML 전자서명을 구현한 제품 개발이 증가하고 있으며, XML 전자서명을 구현한 제품은 다른 제품들 간의 상호운용성을 지원하기 위해 관련 기술 표준을 정확하게 준수하여 구현되어야 한다. 본 논문에서는 시험 절차와 시험 케이스 등을 포함하는 XML 전자서명 표준적합성 시험 방법을 제시한다. 시험 케이스들은 XML 서명 표준을 분석하여 도출되었으며, 본 논문에서 제시된 시험 방법을 구현한 XML 표준적합성 시험 도구의 설계와 용법을 설명한다.

ABSTRACT

The XML has been becoming a basis of the related application and industry standards with proliferation of electronic transactions on the web, and the standardization on XML Signature, which can be applied to the digital contents including XML objects from one or more sources, is in the progress through a joint effort of W3C(World Wide Web Consortium) and IETF(Internet Engineering Task Force). Along with this trend, the development of products implementing XML Signature has been growing, and the XML Signature products are required to implement the relevant standards correctly to guarantee the interoperability among different XML Signature products. In this paper, we propose a conformance testing method for testing the XML Signature products, which includes a testing procedure and test cases. The test cases were obtained through analysis of XML Signature standards. Finally we describe the design and uses of our XML Signature conformance testing tools which implements our testing method.

Keywords : *XML Signature, Conformance Test, Interoperability*

Ⅰ. 서 론

국내외 정보통신망의 급속한 확산과 정보통신 기술의 발전 및 시장의 국제적인 개방화, 경쟁화가 진행되면서 정보통신 제품 간의 상호운용성은 필수적인 요소로 자리하고 있다. 이러한 추세에 따라 동일한 표준을 구현한 제품들 간의 상호 운용 여부를 시험하는 상호운용성 시험에 대한 연구가 국내외에서 진행

접수일 : 2003년 12월 23일 ; 채택일 : 2004년 7월 7일
* 본 연구는 숙명여자대학교 2003년도 교내 연구비 지원에 의해 수행되었음.
† 주저자 : yeronica@sookmyung.ac.kr
‡ 교신저자 : rhee@sookmyung.ac.kr

되고 있으며[1-4], 상호운용성을 지원하기 위한 기본 요건으로 개별 제품이 관련 표준에 따라 적합하게 구현되어 있는지를 시험하는 표준적합성 시험의 중요성이 강조되고 있다[5]. 정보보호 제품의 경우 표준적합성 시험은 상호운용성의 전제 조건으로서 뿐만 아니라 제품의 보안성을 적절히 제공하고 있는지를 평가하는 기준으로서의 의미도 갖는다. 정보보호 제품의 표준적합성 시험의 필요성 증가에 따라 국내외에서 S/MIME, IPsec, PKI 등의 정보보호 제품의 표준적합성 시험에 관한 연구가 진행되고 있다.[6-8] 표준에 따라 적합하게 구현된 제품은 상호운용성에 보다 유리한 입지를 확보할 수 있을 뿐만 아니라 이를 검증받음으로써 제품에 대한 신뢰도를 높이게 되고 시장에서의 경쟁력을 확보할 수 있게 된다.

본 연구에서는 XML 전자서명을 구현하는 정보보호 제품의 표준적합성 여부를 평가하기 위해 관련 표준을 분석하여 시험 항목을 도출하고, 시험 방법을 제시한다. 이를 기반으로 표준적합성 시험을 지원하는 XML 전자서명 표준적합성 시험 도구를 설계하고 구현한다.

본 논문의 나머지 부분의 구성은 다음과 같다. 2장에서는 연구의 배경 지식이 되는 XML 전자서명의 표준 현황에 대해 설명하고, 표준적합성 시험을 기존의 정보통신 제품에 적용되고 있는 일반적인 절차를 중심으로 설명한다. 또한, 연구 사례로 XML 전자서명의 상호운용성 시험을 조사하여 기술한다. 3장에서는 XML 전자서명의 표준적합성 시험에 대한 시험 방법과 시험 항목을 기술하고, 시험 도구가 표준적합성 시험에 사용되는 경우 서명의 송신 측면에서 이루어지는 시험 과정과 수신 측면에서 이루어지는 시험 과정을 설명한다. 4장에서는 연구를 통해 개발한 XML 전자서명의 표준적합성 시험을 지원하는 시험 도구를 살펴보고, 5장에서는 결론과 향후 연구 과제를 제시한다.

II. 배경지식

2.1. XML 전자서명 표준현황

IETF와 W3C의 공동 작업으로 표준화가 진행되고 있는 XML 전자서명[9]은 XML 트랜잭션 내에서 사용될 수 있도록 설계된 전자서명으로 XML 데이터뿐만 아니라 하나 이상의 임의 형식의 데이터에 대한 전자서명을 지원하고, 서명된 데이터에 대해서는 데이터 무결성, 송신자 인증, 송신자 부인방지 등의 보안기능을 제공한다. [표 1]은 IETF XML 전자서명 문서의 현황을 나타내고 있다. XML 전자서명 표준은 RFC3275[10]와 RFC2807[11], RFC3076[12]이며, RFC3275는 제안 표준(Proposed Standard)인 RFC3075[13]를 대체하는 서명의 구문과 처리에 대한 드래프트 표준(Draft Standard)이다. RFC 3275는 XML전자서명의 구조와 유형을 비롯하여 서명의 생성과 검증에 관한 처리 규칙, 사용되는 알고리즘을 명세하고 있다. RFC2807은 XML 전자서명 작업반의 작업 범위, 서명 명세서, XML 서명 명세서를 구현한 응용 소프트웨어의 설계 원리, 범위, 요구사항 등을 나열하고 있다. RFC3076은 논리적으로 동등하지만 물리적 특성의 외형적 표현이 서로 달라 서명 값이 상이한 문제를 해결하기 위해 두 문서가 동일한지 또는 애플리케이션이 XML 1.0과 XML 이름 공간이 허용하는 변환을 제외하고는 문서를 변경하지 않았음을 결정하기 위한 방법을 제시한다. 인터넷 드래프트 제외형 XML 정규화 버전 1.0[14]에서는 XML 객체의 이식성 향상을 위한 정규화 변환을 규정하고 있으며, 인터넷 드래프트 XML 서명 XPath 필터 2.0[15]에서는 집합 연산을 이용하여 XPath 변환을 보다 효율적으로 구현할 수 있는 방안을 제시하고 있다.

표 1. XML 전자서명 표준문서 현황

분류		문서
IETF/W3C	표준 제정	드래프트 표준	RFC3275 XML 서명의 구문과 처리
		제안표준	RFC3075 XML 서명의 구문과 처리
	제정중	정보문서	RFC2807 XML 서명 요구사항
			RFC3076 정규 XML 버전 1.0
인터넷 드래프트			제외형 XML 정규화 버전 1.0
			XML 서명 XPath 필터 2.0

2.2. 표준적합성 시험

일반적인 정보통신 제품의 프로토콜 표준적합성 시험의 절차는 [그림 1]과 같다. 표준적합성 시험을 시행하기 위해 선행되어야 하는 작업은 시험 대상의 표준 프로토콜을 분석한 다음 이를 바탕으로 시험 규격 구조(TSS : Test Suite Structure)와 TSS에 따라 프로토콜로부터 세부적인 시험 목적(TP :

Test Purpose)을 도출하는 것이다. TP의 추출 후 시험 대상 제품과 시험기의 관계를 설정하는 추상 시험 방법(ATM : Abstract Test Method)이 선택된다. TP 단계에서는 하나의 TP마다 순서가 있는 시험 이벤트(Test Event)의 조합인 하나씩의 시험 케이스(TC : Test Case)를 작성하고, TC의 집합과 함께 ATM을 반영하는 추상 시험 규격(ATS : Abstract Test Suite)을 구성한다. 시험 규격은 표준적합성 시험을 수행하고, 시험 목적을 갖는 시험 그룹의 전체 집합으로 시험 규격 구성 시 필요에 따라 시험 대상의 입력으로 사용되는 데이터인 테스트 벡터를 포함한다. 이러한 ATS로부터 실행 가능한 시험 규격(ETS : Executable Test Suite)을 생성하여 실제 시험을 수행하고 결과를 도출하는 과정으로 표준적합성 시험이 진행된다.[16]

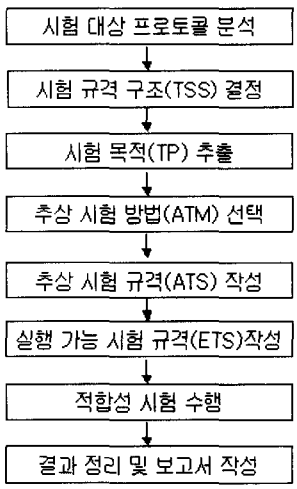


그림 1. 적합성시험절차

2.3. XML 전자서명의 상호운용성 시험

상호운용성 시험이란 동일한 표준을 구현하고 있는 시스템 간의 접속성, 연동성, 상호 동작 여부를 확인하는 시험이며, XML 전자서명에 대한 상호운용성 시험은 W3C와 IETF의 XML 서명 작업반에서 XML 전자서명 표준의 승격을 위한 작업으로 진행되어 왔다. 시험 결과는 XML 전자서명을 구현한 제품사들(Baltimore, Ubisecure, Wedgetail, Fujitsu, GapXse, HP, IAIK, Infomosaic, IBM, Microsoft, NEC, Phaos, RSA, Apache, XMLSec, DataPower)간의 상호운용성 여부를 시험한 후 결과를 웹상에 공표하고 있다. 이를 위해 수행된 상호운용성 시험에서는 RFC3275의 표준 문서에 명시된 요구사항을 비롯하여 구현된 기능, 연산 등을 시험 케이스로 항목화하고, 상호운용성 매트릭스[15]에 애플리케이션 기능의 12개 항목과 알고리즘의 9개 항목을 시험 항목으로 제시하고 있다. 시험 방법은 상호운용성을 지원하는 제품에 완전히 적합하게 구현한 공개된 테스트벡터를 입력한 후 일련의 테스트벡터를 유효하게 처리하는지의 여부를 시험하여 상호운용성 여부를 판단한다. XML 전자서명 상호운용성의 웹 사이트를 통해 공개되어 상호운용성 시험에 사용되는 테스트벡터[17]는 Merlin Hughes가 개발한 merlin-xmldsig-fifteen, merlin-xmldsig-sixteen, merlin-xmldsig-twenty-three 패키지가 있으며, 이외에 Phaos사의 'Phaos XML Toolkit[18]'으로 생성된 01-phaos-xmldsig-two 패키지가 있다.

위의 상호운용성 시험들에서 사용되는 테스트벡터는 표준적합성 시험에 필요한 다양한 기능과 알고리즘의 조합을 가진 테스트벡터를 필요로 하는 표준적합성 시험에는 충분하지 않은 개수의 테스트벡터를 포함하고 있으며, 시험 항목의 기능과 알고리즘을 조합하여 사전에 생성된 서명을 사용하고 있기 때문에 시험에 사용하는 데이터로는 제한적이다. 충분한 표준적합성 시험을 위해서는 여러 가지 기능과 알고리즘의 조합을 포함하는 다양한 테스트벡터들을 확보하는 것이 중요하다. 본 연구에서는 요구되는 기능 및 알고리즘 조합을 반영하는 테스트벡터를 개별적으로 생성하거나 혹은 다양한 테스트벡터들을 주어진 조건에 따라 일괄적으로 생성할 수 있는 기능을 가진 시험 도구를 제안한다.

Ⅲ. XML 전자서명 표준적합성 시험

XML 전자서명을 위한 표준적합성 시험을 위한 별도의 연구나 도구는 발표되어 있지 않으며, XML 전자서명 상호운용성 시험에 사용되는 테스트벡터[17,18]들이 표준적합성을 시험하기 위한 간이 도구로 이용되고 있으나, 테스트벡터의 수나 종류가 극히 제한되어 있으며 그 이용 방법도 아주 불편한 수준이다.

표준적합성 시험은 시험 대상이 되는 XML 전자서명 제품이 서명을 수신하는 기능과 서명을 송신하는 기능이 분리되어 구현되었거나 통합하여 구현된 제품이 시험 대상이 될 수 있으므로, 본 논문에서는

제품이 서명을 수신하여 검증하는 기능의 수신자 측면에서의 시험과 서명을 생성하여 전송하는 송신자 측면에서의 시험을 분리하여 수행하는 표준적합성 시험 방법을 제안한다. 본 장에서는 시험에 필요한 표준 문서를 분석하여 표준적합성 여부를 검사하기 위해 시험 항목을 제시하고, 시험 도구를 이용한 시험 과정을 설명한다.

3.1. 시험 방법

XML 전자서명을 구현한 시험 대상 제품의 표준적합성 검사를 수행하기 위한 방법으로 소프트웨어 공학 측면에서 제시되고 있는 소프트웨어 시험 방법인 화이트박스 시험과 블랙박스 시험이 표준적합성 시험을 위해 고려되었다. 화이트박스 시험은 프로그램의 소스 코드를 분석하여 내부의 논리 구조를 시험할 수 있도록 시험 케이스를 설계하는 기법으로 시험 제품의 소스 코드를 비롯하여 내부의 변수, 처리 논리 등에 접근할 수 있는 개발 단계에서 개발자의 자체 시험에 적합한 반면, 블랙박스 시험은 외부와의 입출력을 통해 소프트웨어의 기능이나 성능을 시험하는 것이며 완제품에 대한 시험에 적합하다. 본 연구에서는 XML 전자서명의 표준을 구현한 완제품에 대한 표준적합성을 시험하므로 블랙박스 시험 방법을 적용하여 시험 도구를 구현하였다.

[그림 2]는 시험 도구를 이용한 표준적합성 시험 과정이다. [그림 2]의 왼쪽에 도식한 순서에 따라 시험 대상 제품의 서명 검증 기능의 표준적합성 검사를 수행하기 위해 시험 규격 구조에 의해 시험 도구의 테스트벡터 생성 기능을 이용하여 필요한 테스트벡터를 생성한다. 테스트벡터는 시험 대상 제품의 서명 수신 기능으로 입력한 후 동작 시험으로 서명을 검사하고, 테스트벡터 처리에 따라 표준적합성 결과를 도출하고 보고서를 작성하게 된다. 이 과정에서 시험자는 서명 검증 기능의 표준적합성 검사 과정을 전반적으로 지휘하고 제품의 동작 시험을 수행하는 과정에서는 필요에 따라 제품의 명세와 개발자를 비롯한 제공자의 도움을 받아 시험을 수행하게 된다.

[그림 2]의 오른쪽 도식한 순서에 따라 시험 대상 제품의 서명 생성 기능의 표준적합성 검사를 수행하기 위해 시험 규격 구조에 따라 시험 대상 제품이 시나리오와 지정된 시험 항목을 포함하는 서명을 명세에 의해 생성한다. 제품이 생성한 서명은 시험 도구의 서명 검증 기능을 통해 시험 도구에 입력되고, 표준적합성 검사를 수행하여 결과 및 보고서를 생성하여 출력한다. 이 과정에서 시험자는 서명 생성 기능의 표준적합성 검사 과정을 전반적으로 지휘하고, 서명을 생성하는 단계에서는 제품의 제공자나 개발자의 지원 하에 제품의 기능을 정확히 파악한 후 명세에 따른 서명이 생성되도록 할 수 있다.

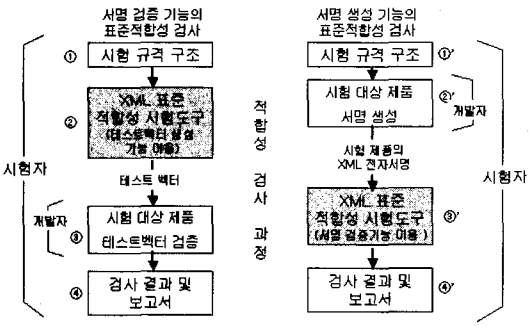


그림 2. 시험 도구를 이용한 표준적합성 검사 과정

3.2. 시험 항목

XML 전자서명의 표준적합성 시험을 위해 본 연구에서는 표준 문서[10]에 기초하여 시험 도구를 통해 시험 가능한 항목을 도출하였으며, 이는 IETF와 W3C에서 시행하고 있는 상호운용성 시험을 위해 구축된 매트릭스[17]와 사실상 동일하다.

XML 전자서명 제품의 표준적합성 시험은 XML 전자서명 제품이 준수해야 할 표준으로 IETF와 W3C에 의해 개발된 드래프트 표준인 'RFC3275 XML 서명의 구문과 처리'와 정보 RFC인 'RFC 3076 정규 XML', 'RFC2807 서명 요구사항'에서 명시된 표준 명세에 따라 구현되었는지를 시험한다. 이 중 개별 시험 항목의 도출에 사용된 표준 문서는 RFC3275이며, RFC2807은 전반적인 참고자료로 이용되었으며 RFC3076은 개별 항목이 아니라 XML 서명 처리에 필요한 정규화 과정 전반에 걸친 요구사항으로 적용되었다. [표 1]에 명시된 XML 전자서명 문서 현황에서 인터넷 드래프트는 RFC 출간을 위한 임시 문서로 공식적인 지위를 가질 수 없으며, 언제든지 변경되고 삭제될 수 있으므로 표준 문서로 참조되거나 관련 제품이 인터넷 드래프트 문서의 명세에 대한 적합성을 요구할 수 없음을 RFC2026[19]에서 권고하고 있기 때문에 인터넷 드래프트 상의 요구사항들은 시험 항목에 포함되지 않는다.

표 2. 시험 도구를 이용한 XML 표준적합성 시험 항목

서명 처리 규칙	서명 생성	3.1	필수	서명 생성 규칙
	서명 검증	3.2	필수	서명 검증 규칙
서명 형식	포함형(Enveloping)	4.5	필수	서명 원소 안에 서명 대상 객체 포함
	피포함형(Enveloped)	4.3.3.3, 6.6.4	필수	서명 대상 객체가 서명 원소 포함
	분리형(Detached)	4.4.3	필수	서명 대상 객체와 서명 원소가 분리됨
서명 알고리즘	DSA	6.4.1	필수	서명 알고리즘에 DSA, RSA, 또는 HMAC 사용
	RSA	6.4.2	권고	
	HMAC	6.3.1	필수	
다이제스트 알고리즘	SHA1	6.2.1	필수	다이제스트 알고리즘에 SHA1 사용
정규화 알고리즘	주석 제거 정규화	4.3.1, 6.5	필수	SignedInfo 원소에 정규화를 적용하되 주석은 제거 또는 유지
	주석 포함 정규화		권고	
XPointer	XPointer(/)	4.3.3.2	권고	XPointer 표현 /를 사용
	XPointer(id("ID"))		권고	XPointer 표현 id("ID")를 사용
변환 알고리즘	주석 제거 정규화	6.6.1	필수	Reference 원소의 처리에 주석 제거 정규화나 주석 포함 정규화, Base64, XPath 표현, XSLT 표현 등을 사용
	주석 포함 정규화		권고	
	Base64	6.6.2	필수	
	XPath	6.6.3	권고	
	XSLT	6.6.5	선택	
검증키 표현	DSA 공개키	4,4, 4.4.2	필수	DSA 또는 RSA 공개키 데이터를 직접 표시
	RSA 공개키		권고	
	Retrieval Method	4.4.3	권고	검색 방법 또는 키 이름으로 검증키 표시
	Key Name	4.4.1	선택	
	X.509 인증서	4.4.4	선택	검증키 선택을 위해 X.509 인증서 관련 정보의 표시 방법 선택
	X.509 CRL			
	X.509 IssuerSerial			
	X.509 SKI			
	X.509 Subject Name			
기타 기능	Manifest	5.1	선택	Manifest 기능의 사용
	SignatureProperties	5.2	선택	서명 속성을 표현하는 SignatureProperties 사용

〔표 2〕는 시험 가능한 시험 대상 항목을 나타내며, 이는 본 연구를 통해 개발된 시험 도구를 이용하여 수행할 수 있는 표준적합성 검사 항목들이다. 시험 항목은 표준 명세의 요구 수준에 의하여 규정된 서명형식, 서명 알고리즘, 다이제스트 알고리즘, 정규화 알고리즘, 변환 알고리즘 등을 시험 항목으로 하고, 그 외에 XPointer, 검증키 표현, 기타 기능을 시험 항목으로 포함하고 있다.

3.3.. 시험 도구를 이용한 표준적합성 시험

표준적합성 시험을 위해서는 일련의 시험 항목을 대상으로 표준적합성 시험을 수행하기 위해 반복되는 테스트벡터 생성과 서명의 표준적합성 검사를 개별적으로 수행하여야 한다. 본 연구를 통해 개발한 GUI를 기반으로 하는 XML 전자서명의 표준적합성 시험 도구는 수작업의 번거로움을 덜기위해 GUI 인터

페이스를 이용하여 개별적으로 혹은 일괄적으로 서명을 생성하고 검증하는 기능을 지원할 뿐만 아니라 결과를 보고하는 기능을 제공받을 수 있으므로 표준적합성 검사에 소요되는 시간을 단축하고 시험 효율을 증대시킬 수 있을 것으로 기대한다.

3.3.1 서명 검증 기능의 표준적합성 시험

서명 검증 기능의 표준적합성 시험은 시험 대상 제품이 수신한 전자서명을 표준에 따라 적합하게 처리하는지와 표준 명세의 요구수준에 따라 구현된 전자서명이 포함하고 있는 알고리즘과 기능이 적합하게 처리되도록 구현하였는가를 시험 도구를 이용하여 시험한다.

서명 검증 기능의 표준적합성 시험을 위해 시험 도구는 시험 대상 제품의 입력으로 사용될 완전하게 적법한 전자서명과 오류를 포함한 전자서명을 생성하는 기능을 가진다. 시험 도구를 통해 생성한 테스트벡터는 시험 대상 제품에 입력하여 전자서명 처리 기능의 표준적합성 시험을 동작시험으로 진행한다.

시험 대상 제품의 서명 검증 과정은 프로그램 내부에 감추어져 있을 뿐만 아니라 시험 대상 제품의 서명 검증 결과도 제한된 범위에서 파악이 가능하다. [그림 3]은 시험 도구를 통해 진행되는 서명 검증 기능의 표준적합성 시험 과정을 도식한다.

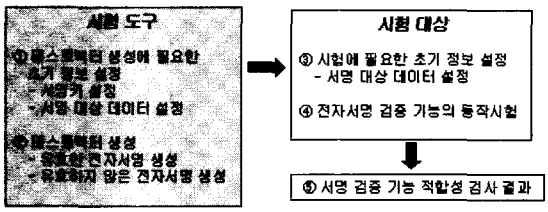


그림 3. 서명 검증 기능 표준적합성 시험과정

시험 대상 제품에 입력되는 테스트벡터는 유효한 서명과 유효하지 않은 서명을 포함하고 있다. 따라서 서명 검증 기능의 표준적합성 시험 결과는 유효한 서명을 유효하게 처리하고, 유효한 서명을 변형하여 오류를 포함하는 서명에 대해서는 유효하지 않은 서명으로 판단하고 오류에 대한 적절한 정보를 얻을 수 있는지 혹은 오류에 적합한 처리 과정을 포함하는지를 시험한다. 시험 대상 제품은 서명 값, 다이제스트 값, 서명 후 서명 대상 객체의 변경 등의 유효하지 않은 서명은 반드시 유효하지 않은 서명으로 처리되어야 한다. 유효한 서명의 테스트벡터가 시험 대상 제품에 입력되어 처리되면 테스트벡터에 포함되어 있는 서명의 알고리즘과 기능을 시험 대상 제품의 서명 수신 기능으로 적합하게 구현되었다고 할 수 있다.

3.3.2 서명 생성 기능의 표준적합성 시험

서명 생성 기능의 표준적합성 시험은 시험 대상 제품이 시험 규격에 따라 생성한 전자서명이 적합하게 구현되었는지를 비롯하여 표준 문서의 요구수준에 따라 특정 알고리즘과 기능을 포함하는 서명이 생성되었는지를 시험한다. 시험 도구는 시험 제품이 생성한 서명을 입력받아 서명의 유효성과 서명이 포함하고 있는 기능과 알고리즘을 분석하여 서명 생성 기능의 표준적합성 검사를 수행하고, 결과를 웹 기반의 보고서 형식으로 출력한다. [그림 4]는 시험 도구를 이용하여 진행되는 서명 생성기능의 표준적합성 시험 과정을 도식한다.

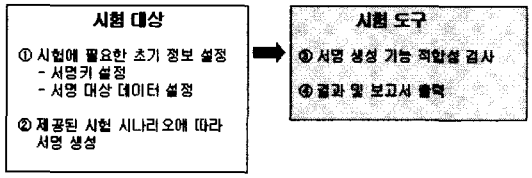


그림 4. 서명 생성 기능 표준적합성 시험 과정

시험 대상 제품은 시험 시나리오의 명세에 따라 서명에 포함되어야 하는 알고리즘과 기능의 시험 항목을 포함한 일련의 서명 생성 명세에 따라 유효하다고 간주되는 서명을 생성한다. 생성될 서명은 시험 대상 제품의 특성상 시험 규격이 포함하는 알고리즘이나 기능을 포함하지 않는 경우가 있을 수 있으며, 이는 특정 기능과 알고리즘이 표준 명세에 따라 구현되지 않았음을 의미한다.

XML 전자서명의 표준적합성 평가자는 시험 대상 제품이 생성한 서명을 받아 시험 도구의 표준적합성 검사 기능을 통해 서명을 일괄 검사하고, 검사된 결과에 따라 개별 서명이 시험 규격에 따라 구현되었는지를 검사한다. 시험 규격에 따라 구현된 개별 서명이 유효한 서명이라면 서명에 포함된 알고리즘과 기능이 서명 생성 기능으로 적합하게 시험 대상 제품에 구현되었다고 평가한다.

Ⅳ. XML 전자서명 시험 도구 구현

본 장에서는 XML 전자서명 제품의 표준적합성

시험을 지원하는 시험 도구를 설계하고, 구현된 시험 도구를 기능 중심으로 설명한다.

4.1. 시험 도구의 구조

시험 도구는 서명 검증 기능의 표준적합성 시험을 위해 테스트벡터를 시험 규격에 따라 생성하고, 서명 생성 기능의 표준적합성 시험을 위해 시험 대상 제품이 생성한 전자서명이 시험 규격에 맞는 유효한 서명을 생성하였는지를 검사하는 두 가지 기능을 중심으로 구성되어 있다. [그림 5]는 구현된 시험 도구의 기본 구조를 나타낸다.

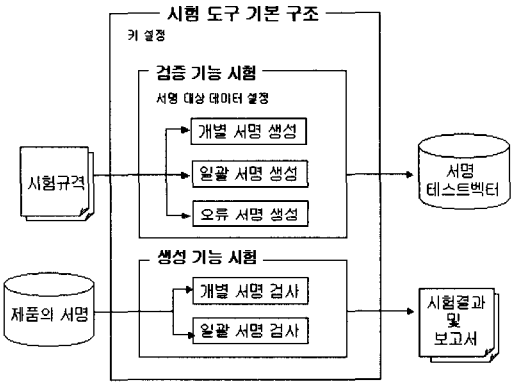


그림 5. 시험 도구 기본 구조

시험 대상 제품의 서명 검증 기능을 시험하기 위해 시험 도구는 시험 대상 제품에 입력될 XML 전자서명 테스트벡터들을 생성하게 되는데, 테스트벡터 생성 방법에는 개별 서명 생성, 일괄 서명 생성, 오류 서명 생성의 세 종류가 있다. 개별 서명 생성 기능은 이용자가 명시적으로 선택한 기능 및 알고리즘의 조합을 포함하는 한 개의 서명으로 이루어지는 개별 테스트벡터를 생성하며, 일괄 서명 생성 기능에서는 이용자가 선택한 시험 항목의 범위 내에서 다양한 기능 및 알고리즘 등에 대한 임의의 조합을 포함하는 서명을 지정한 개수만큼 일괄적으로 생성하고, 오류 서명 생성 기능에서는 유효한 서명으로부터 객체 참조, 해쉬, 서명 값 등의 계산에 오류를 포함하는 서명을 생성하게 된다. 또한, 서명 생성을 위해 서명키를 설정하거나 서명 대상 데이터를 설정하는 기능이 시험 도구에 포함된다.

시험 대상 제품의 서명 생성 기능을 시험하기 위해 시험 대상 제품이 시험 규격에 따라 생성한 서명을 시험 도구에 입력하여 표준적합성 검사를 수행하고 검사 결과를 보고한다. 이 경우 한 개의 서명 파일을 개별적으로 검사하는 개별 서명 검사 기능, 디렉토리 내에 포함된 모든 서명 파일을 일괄 검사하는 일괄 서명 검사 기능을 이용한다.

4.2. 서명 검증 시험 지원 기능

시험 도구가 지원하는 테스트벡터 생성 기능은 세 가지 측면으로 나누어 볼 수 있으며, 이는 개별 전자서명 생성 기능, 일괄 전자서명 생성 기능, 오류 전자서명 생성 기능이다.

개별 전자서명 생성 기능은 세부 시험 항목을 화면에서 선택한 후 선택된 시험 항목을 조합하여 완전하게 유효한 XML 전자서명인 하나의 테스트벡터를 생성하는 기능이며, [그림 6]은 시험 도구에서 개별 서명 생성을 위해 시험 항목을 선택하는 화면이다. 서명 형식, 서명 알고리즘, 다이제스트 알고리즘, 정규화 알고리즘, XPointer, 변환 알고리즘, 검증키 선택, 추가 정보의 각 그룹 항목들이 가지는 세부 항목을 선택하면 선택한 항목을 조합하여 시험 항목으로 포함하는 서명을 생성한다. 일괄 전자서명 생성 기능은 개별 전자서명 생성 기능의 선택 가능한 항목들과 동일한 시험 항목들 중에서 선택한 시험 항목의 범위 내에서 시험 항목을 임의로 조합하여 지정한 개수만큼 테스트벡터를 일괄 생성하는 기능이다. 이는 수작업에 의해 기능과 알고리즘 별로 다양한 조합을

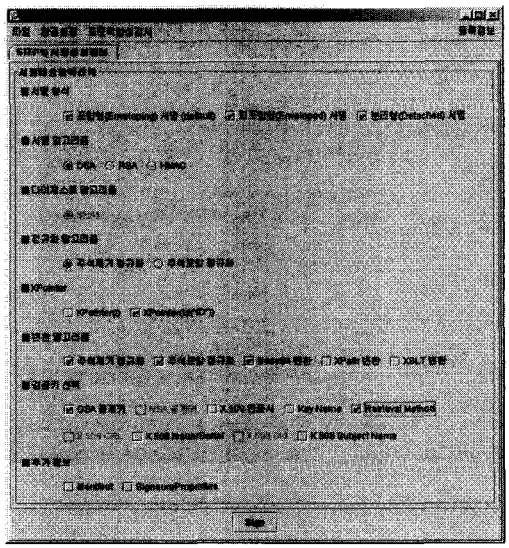
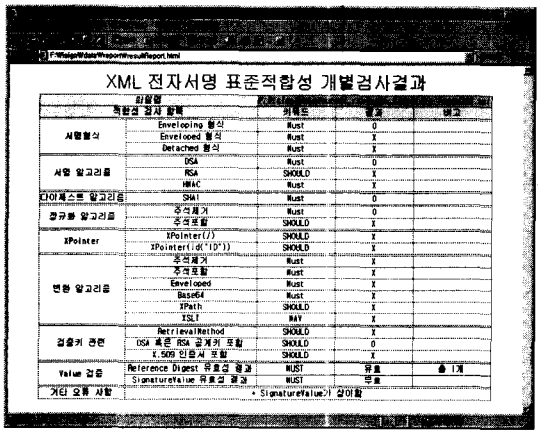


그림 6. 개별 전자서명 생성 화면

가진 일련의 개별 서명을 생성하는 불편함을 개선하여, 다양한 기능과 알고리즘을 조합하여 충분한 테스트벡터를 자동적으로 생성하기 위한 것이다. 오류 전자서명 생성 기능은 시험 제품의 서명 검증 기능의 표준적합성 시험 과정에서 오류를 포함하고 있는 서명에 대한 부정적인 결과를 시험하기 위해 오류를 포함하는 테스트벡터를 생성한다. 시험 도구를 통해 지정할 수 있는 오류 선택 항목은 서명 값 변경, 서명 알고리즘 변경, 정규화 알고리즘 변경, 변환 알고리즘 변경, 다이제스트값 변경, 포함/피포함/분리형 서명 형식의 서명 대상 객체의 내용 변경의 기능을 가지며, 이는 완전하게 적합한 서명을 읽어 각각의 오류 항목을 포함하는 전자서명을 생성한다.

4.3. 서명 생성 시험 지원 기능

시험 대상 제품의 서명 생성 기능의 표준적합성 검사를 위해 시험 도구는 시험 제품이 생성한 서명을 검사하기 위해 하나의 개별 서명 파일의 표준적합성 검사와 일괄적으로 지정된 서명 파일을 검사하는 두 가지 기능을 제공한다. 시험 도구는 시험 제품의 서명 생성 기능의 표준적합성 시험을 수행한 후 검사 결과에 대해 보고서 형식으로 제공하는 기능을 가지고 있다. 보고서는 개별 서명 검사 결과와 일괄 서명 검사 결과의 양식에 따라 해당하는 보고서를 웹 기반으로 볼 수 있도록 생성하는데 [그림 7]은 개별 서명 표준적합성 검사 수행 후 출력되는 보고서를 나타낸다. 보고서 내용은 [표 2]의 시험 항목의 구현 여부를 명시하고 서명이 유효한지 아닌지에 따른 결과를 보여준다. 이를 통해 제품이 생성한 서명이 시험 규격과 일치하는지를 검사하여 표준적합성 여부를 판단한다.


XML 전자서명 표준적합성 개별검사결과

시험항목		시험결과		
	적합성 검사 항목	카테고리	결과	비고
서명형식	Enveloping 형식	Must	0	
	Enveloped 형식	Must	X	
	Detached 형식	Must	X	
서명 알고리즘	DSA	Must	0	
	RSA	SHOULD	X	
	HMAC	Must	X	
다이제스트 알고리즘	SHA1	Must	0	
정규화 알고리즘	주석제거	Must	0	
	주석포함	SHOULD	X	
XPointer	XPointer(/)	SHOULD	X	
	XPointer(id("ID"))	SHOULD	X	
변환 알고리즘	공백제거	Must	X	
	주석포함	Must	X	
	Enveloped	Must	X	
	Base64	Must	X	
	XPath	SHOULD	X	
	XSLT	MAY	X	
검증키 관련	RetrievalMethod	SHOULD	X	
	DSA 혹은 RSA 공개키 포함	SHOULD	0	
	X.509 인증서 포함	SHOULD	X	
Value 검증	Reference Digest 유효성 검증	MUST	유효	총 1개
	SignatureValue 유효성 결과	MUST	유효	
기타 오류 사항		* SignatureValue가 같아함		

그림 7. 개별 서명 검증 결과 보고 화면

V. 결 론

본 논문에서는 XML 서명 표준의 분석을 통한 시험 항목의 도출과 효과적인 시험 방법을 제시하고 있으며, 제시된 XML 서명 표준적합성 시험방법의 특징은 다음과 같다.

- 송신자 측의 XML 서명 생성 부분과 수신자 측의 XML 서명 검증 기능 부분을 분리하여 시험
- 다양한 기능을 시험할 수 있는 테스트벡터들을 간편하게 생성할 수 있음 (일괄 서명 생성 기능 참고)
- 오류를 포함하는 테스트벡터들을 이용하여 관련 기능들의 정확한 구현 여부 시험
- 서명의 유효성 여부뿐만 아니라 시험 대상 XML 서명의 특징 분석에 대한 보고 기능을 통해 서명 생성 기능에 대한 적확한 시험 가능
- GUI 기반의 통합적 시험 도구를 이용하여 시험의 편의성과 효율성 도모

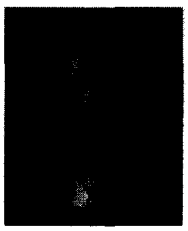
향후 연구 과제는 표준화 작업 진행 중인 제외형 정규 XML 및 XPath 등의 표준적합성 시험을 위한 기능 확장이 필요하고, 표준 명세를 통해 시험 규격을 개발한 후 시험 항목들을 선택하면 이에 따라 시험 케이스들을 자동적으로 추출하여 시험을 진행하여 최종 결과를 보고하는 통합형 시험 도구의 개발이 연구되어야 하며, XML 전자서명 제품의 표준적합성 시험 과정에 대한 표준 연구가 진행되어야 할 것이다. 알고리즘 구현에 있어서는 한국형 전자서명 알고리즘 KCDSA 등을 서명 알고리즘의 시험 항목으로 선택할 수 있는 기능 확장이 추가되어야 할 것이다.

참 고 문 헌

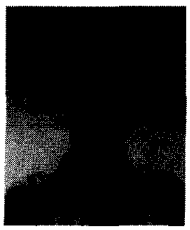
[1] RSA S/MIME Interoperability Center, http://www.rsasecurity.com/standards/smime/interop_center.html
[2] VPNC Testing for Interoperability and Conformance, http://www.vpnc.org/testing.html
[3] IP Security Web Based Interoperability Tester, http://ipsec-wit.antd.nist.gov

[4] 한국정보통신기술협회(TTA), http://www.tta.or.kr
[5] "What is this called Conformance?", http://www.itl.nist.gov/div897/ctg/conformance/bulletin-conformance.htm
[6] 김상춘, 권혁찬, 나재훈, 손승원, 정교일, "정보보호제품의 적합성 시험 평가 현황", 정보보호학회지, 제11권, 제2호, 2001.4.
[7] 장청룡, 김학범, 이홍섭, "국내 정보보호제품의 표준적합성 시험과 인증 체계", 정보보호학회지, 제11권, 제2호, 2001.4.
[8] TAHI Project, http://www.tahi.org
[9] IETF/W3C XML-DSig Working Group, http://www.w3.org/Signature/
[10] D. Eastlake, J. Reagle, D. Sole, "XML-Signature Syntax and Processing", IETF RFC3275.
[11] J. Reagle, "XML Signature Requirements", IETF RFC2807.
[12] J. Boyer, "Canonical XML Version 1.0", IETF RFC3076.
[13] D. Eastlake, J. Reagle, D. Sole, "XML-Signature Syntax and Processing", IETF RFC3075.
[14] John Boyer et al., "Exclusive XML Canonical Version 1.0", IETFI-D, work in progress, 2003 http://phaos.com/products/category/xml.html
[15] John Boyer et al., "XML-Signature XPath Filter 2.0", W3C Recommendation, 2002 http://www.w3.org/TR/xmldsig-filter2/
[16] 한국정보보호센터, "정보보호제품 표준적합성 연구", 기술표준연구00-2, 2000.12.
[17] XML-Signature Interoperability, http://www.w3.org/Signature/2001/04/05-xmldsig-interop.html
[18] Phaos Technology Corporation-Cryptography and XML Products, http://phaos.com/products/category/xml.html
[19] S. Bradner, "The Internet Standards Process - revision 3", IETF RFC2026.

〈著者紹介〉



김 지 현 (Jihyun Kim) 정회원
2002년 2월 : 숙명여자대학교 컴퓨터과학/멀티미디어학 학사
2004년 2월 : 숙명여자대학교 컴퓨터과학과 석사
2003년 12월~현재 : (주)안랩유비웨어 연구원
〈관심분야〉 XML 보안, 홈네트워크 보안, 정보보호



이 광 수 (Gwangsoo Rhee) 종신회원
1981년 2월 : 서울대학교 계산통계학과 졸업
1986년 12월 : 워싱톤대학교 컴퓨터과학과 석사
1990년 5월 : 워싱톤대학교 컴퓨터과학과 박사
1990년 9월~현재 : 숙명여자대학교 정보과학부 교수
2000년 1월~현재: OSIA TG-SEC 의장
〈관심분야〉 네트워크 보안, 알고리즘, 암호학