XML 전자서명 메커니즘 구현과 응용

전형득*, 송유진*

*동국대학교

Implementation and It's Application of XML Signature Mechanism

Hyung-Deuk Jeon*, You-Jin Song*

*Dongguk University

요 약

최근 기업에서 인터넷을 활용한 전자문서 교환이 급증함에 따라 교환되는 문서의 안전한 전달을 위한 보안 서비스 문제가 대두되고 있다. B2B 전자문서 교환은 기업간 문서의 신속한 교환과 처리과정의 자동화를 통해 기업 업무 자동화에 큰 기여를 하고 있는 전자문서 교환방식(EDI)을 통해 이루어진다. 그러나 현재의 전자문서 교환방식은 해당 소프트웨어 개발과 통신망에 대한 부대 비용으로 인해 광범위하게 채택되지 못하고 있다. 이러한 문제를 해결하기 위한 방안으로 현재 광범위하게 사용되고 있는 웹기반 표준문서인 XML을 이용한 전자문서 교환이 새롭게 떠오르고 있다.[1] 본 논문은 XML 전자서명 메커니즘을 구현하고 XML 기반 전자조달 시스템에의 응용이 목표이다. XML전자서명 기술을 이용해 전송되는 XML문서의 무결성, 인증 그리고 송수신 부인봉쇄의 보안 서비스를 제공하고, 전자조달 시스템에의 적용에 관한 것이다.

1. 서론

최근 기업에서 인터넷을 활용한 전자문서 교환이 급증함에 따라 교환되는 문서의 안전한 전달을 위한 보안 서비스 문제가 대두되고 있다. B2B 전자문서 교환은 기업간 문서의 신속한 교환과 처리과정의 자동화를 통해 기업 업무 자동화에 큰 기여를 하고 있는 전자문서 교환방식(EDI)을 통해 이루어진다. 그러나 현재의 전자문서 교환방식은 해당 소프트웨어 개발과 통신망에 대한 부대 비용으로 인해 광범위하게 채택되지 못하고 있다. 이러한 문제를 해결하기 위한 방안으로 현재 광범위하게 사용되고 있는 웹기반 표준문서인 XML을 이용한 전자문서 교환이 새롭게 떠오르고 있다.[1]

XML을 활용한 기업간 전자조달 시스템은 기존 시스템과의 통합이 용이하고, 기존 인프라를 활용하여 시스템 도입으로 인한 비용과 시간을 절약할 수 있다. XML 기반 전자조달 시스템의 안전한 메시지 전송은 시스템의 신뢰성과 효율성을 높이고, 가치를 보유한 트랜잭션을 처리할 수 있어 시스템의 부가가치를 높이게 된다.

본 논문은 XML 전자서명 메커니즘을 구현하고 XML 기반 전자조달 시스템에의 응용이 목표이다. XML전자서명 기술을 이용해 전송되는 XML문서의 무결성, 인증 그리고 송수신 부인봉쇄의 보안 서비스를 제공하고, 전자조달 시스템에의 적용에 관한 것이다. 분석 및 설계 와 구현 그리고 전자조달 시스템에의 응용에 대해 기술하고 결론을 맺는다.

2. 관련연구

XML 전자서명은 W3C에서 정의하고 있는 XML-Signature Syntax and Processing 표준안을 따르고 있다.[12] XML 전자서명 기능을 제공하는 NEC, IBM, ETRI의 XML전자서명에 대해 살펴본다.

NEC XML 전자서명 라이브러리는 XML 문서를 정규 XML문서로 변환하는 기능과 전자서명 생성 및 검증의 기능을 제공한다.[10]

IBM의 XML Security suite는 XML문서에 대한 전자서명을 생성 및 검증하는 기능, 정규 XML문서로 변환하는 기능, XML을 이용한 접근제어 기능을 제공한다. 또한 엘리먼트단위의 데이터를 선택적으로 암호화하는 기능을 제공하고 있다.[11]

ESES는 XML 전자서명 표준안에 기반하여 개발되었으며, XML 문서의 전자서명을 위한 정규화기능. 메시지 다이제스트 기능와 필요한 여러 API를 제공한다. 또한 검증되어진 국내 표준 알고리즘과 AES 표준 알고리즘을 지원한다. [6]

XML 전자서명 기능을 제공하는 NEC, IBM, ETRI의 기능을 비교해 보면 다음과 같다.

	속도(생성/검증)	사용알고리즘	지원플랫폼	안전성
NEC	5Sec	DSAwithSHA1	java기반	평가
IBM	5Sec	RSAwithSHA1	java기반	평가
ETRI	2Sec	KCDSA/Rijnael	java기반	상용화

표 1 전자서명 기능의 비교

3. XML 전자서명 설계

XML전자서명은 XML문서에서 디지털 콘텐트를 포함하고있는 부분이나 문서 전체를 대상으로 전자서명을 수행한다.

3.1 XML 전자서명 기능설계

3.1.1 XML 전자서명 기능설계 흐름도

XML문서를 전자서명 처리하기 위해 사용자나 전자조달 시스템으로부터 XML 문서를 읽어온 후 인증기관으로부터 수신자의 공개키를 받아 다이제스트 계산을 수행한다. 다이제스트 값을 송신자의 비밀키로 암호화하고, 서명 값을 생성한 후 원본 문서와 서명 문서를 합쳐서 클라이언트로 전송 되고, 클라이언트는 인증기관으로부터 송신자의 공개키를 받아 서명 문서를 검증하는 절차를 거쳐 문서의 무결성을 확인한다.

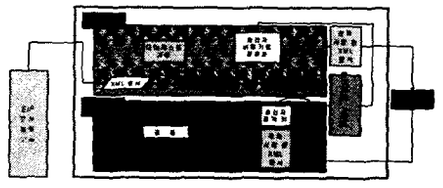

그림 1 XML Security Manager의 기능 흐름도

3.1.2 XML 전자서명 기능 명세도

XML 전자서명은 정규화를 위해 Canonical XML 알고리즘, 서명을 위한 RSAwithSHA1 알고리즘을 사용한고, 다이제스트 생성을 위해 SHA1 해쉬 알고리즘을 사용한다.

서명 생성에 필요한 키 정보를 위해 KeyInfo요소를 생성하고, 이를 기반으로 RSAKeyValue요소와 RSA 공개키 값을 설정한다. 생성된 XML 전자서명 문서의 무결성 검증을 위해 KeyInfo 요소의 X509Data 공개키에 관한 정보를 통해 검증하게 된다. 그림 2는 전자서명의 생성과 검증 과정에서 사용되는 자바 패키지들의 관계를 나타낸다.

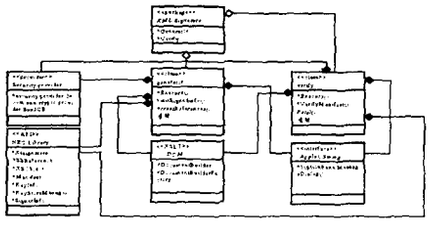

그림 2 XML 전자서명 기능명세도

3.1.3 서명 생성 및 검증

서명을 처리하는 과정은 서명 대상문서를 입력받아 XML 문서로 타당한지 체크하고, 서명을 위한 비밀키를 요청한다. KeyInfo요소를 생성하여 DefaultRSA알고리즘을 설정한다. 이를 기반으로 RSAKeyValue요소와 RSA 공개키 값을 설정한다. 생성된 KeyInfo 요소는 Signature 요소에 포함되어 서명계산을 수행한 후 생성한다.

서명구조는 루트 요소인 <Signature>로 시작하여 SignedInfo와 KeyInfo에 서명 생성과 검증에 필요한 정규화 알고리즘, 서명 알고리즘, 변환 알고리즘, 다이제스트 알고리즘, 서명값 그리고 키 정보가 포함된다.

서명을 검증하는 단계는 생성된 XML 전자서명 문서가 제 3자에 의해 변조되지 않았는지의 무결성을 검증하는 단계이다. XML 전자 서명된 문서를 스트림으로 입력받아 KeyInfo 요소의 RSA공개키를 이용해 검증한다.

X.509 인증서 공개키 검증 단계는 XML 전자서명된 문서에 존재하는 KeyInfo의 X509Data 요소에 공개키에 관한 정보가 포함되어있어 그 유효성을 검증할 수 있다.

XML문서를 스트림으로 입력받아 XML문서의 유효성을 확인하고, keystore로부터 읽어들인 키를 이용해 KeyInfo에 포함되는 공개키를 검증한다.

3.2 XML 전자서명 Sequence Diagram

3.2.1 XML 전자서명 전 과정 Sequence Diagram

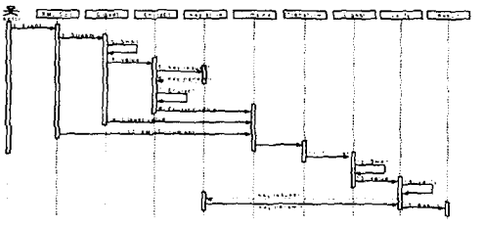

그림 3 XML 전자서명/검증 Sequence Diagram

사용자는 XML 형식의 발주서 또는 납품서를 전자서명 하기 위해 서명 이벤트를 발생시킨다. XML 전자서명을 위해 키 저장소로부터 송신자의 비밀키를 요청하고 서명을 수행한다. 완료된 서명 문서는 전송모듈을 통해 클라이언트로 전송된다. 클라이언트는 수신한 XML 전자서명 문서의 무결성을 검증하고, 문서를 관리하게 된다.

3.2.2 XML 전자서명 생성 Sequence Diagram

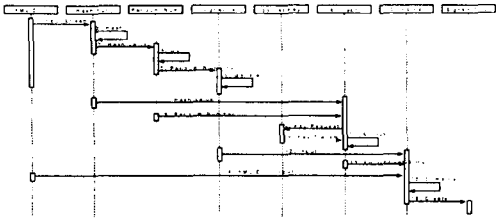

그림 4 XML 전자서명 생성 Sequence Diagram

XML 문서는 전자서명 수행 이벤트와 함께 해쉬 함수를 통과해 메시지 다이제스트를 생성하게 되고 송신자의 비밀키를 키 저장소로부터 요청하여 암호화한 다음 서명 문서를 생성한다. 생성된 XML 저자서명 문서는 XML HTTP를 이용해 클라이언트의 특정 폴더로 전송된다. 클라이언트에서는 수신한 문서를 검증하기 위해 검증 이벤트를 발생시킨다.

3.2.3 XML 전자서명 검증 Sequence Diagram

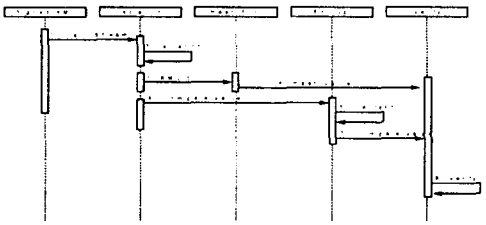

그림 5 XML 전자서명 검증 Sequence Diagram

서버로부터 수신한 XML 전자서명 문서를 검증하기 위해 클라이언트는 메시지 다이제스트와 XML 문서 그리고 암호화된 비교 값을 분리한다. 수신한 다이제스트와 클라이언트 측에서 생성한 다이제스트를 비교하여 XML 전자서명 문서를 검증한다. 문서의 무결성이 확인되면 이 문서를 관리한다.

4. EIP 시스템에의 응용

XML 기반 전자상거래 환경에서 중요한 가치를 보유한 트랜잭션들을 신뢰성 있게 지원해야 하는 전자조달시스템 환경 구축에 있어서 온라인 인증을 위한 디지털 키 관리와 전자서명 및 데이터 암호화 등의 통합 처리가 용이해야 하며, 광범위한 애플리케이션들과의 상호 호환성 또한 확보되어야 한다.

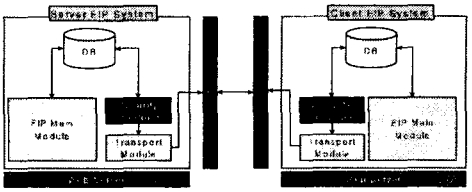

그림 6 EIP 시스템의 전체 구조

기업 간 자재구매 활동은 자재 수요업체가 주문제품에 대한 발주서를 제공하면 법적 효력을 발생하고, 이에 대해 납기일을 고려한 자재 공급업체의 자재 납품서를 전달하게 되며, 자재 수요업체의 자재 검수실적에 따라 검수 조서를 보내게 된다.

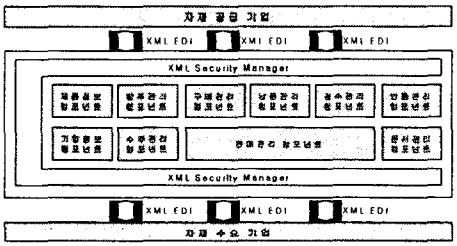

그림 7 XML전자서명의 전자조달 시스템에 응용

5. 분석

기업간 전자조달 시스템에 응용될 XML 전자서명을 수행하기 위해 사용되는 알고리즘은 W3C에서 제안된 알고리즘을 사용하게 되며, 표 2와 같다.

알고리즘	관 련 요 소	알 고 리 즘	규약요건
다이제스트 계산	Digest Method	SHA1	REQUIRED
부호화	Transform	Base64	REQUIRED
MAC	Signature Method	Hmac SHA1	REQUIRED
공개키 방식 서명	Signature Method	DSAwithSHA1(DSS)	REQUIRED
		RSAwithSHA1	RECOMMAND
정규화	Canonicalization Method	정규 XML	RECOMMAND
		정규 XML	REQUIRED
변환	Transform	XSLT	OPTIONAL
		Xpath	RECOMMAND
		Enveloped Signature	REQUIRED

표 2 XML 전자서명 지원 알고리즘 [3]

이러한 표준 알고리즘은 이미 그 신뢰성이 입증되었기 때문에 XML전자서명으로 구현되었을 경우에도 그 신뢰성을 보장한다고 가정한다. 구현된 XML 전자서명기능은 RFC문서 2807의 전자서명 요구사항을 다음과 같이 만족하고 있다.

	요 구 사 항	○	△	×
구조	1. RDF 데이터모델	V		
	2. XML 주소에대한 식별 가능성	V		
	3. XML 문서 전체 또는 일부 적용성		V	
	4. 다중 XML 서명기능			V
	5. XML서명문서 참조 가능성	V		
	6. 디지털 서명이나 MAC 사용의 다양성	V		
	7. 포함 또는 인코드된 문서의 원본에 적용가능성		V	
양식	1. 서명은 XML의 원소로 존재	V		
	2. 원본 문서 루트요소의 불변	V		
	3. 서명의 특정유지하면서 복합문서 제작 가능		V	
	4. 서명은 인코드된 컨텐츠를 캡슐화 가능해야 함		V	

○:만족함 / △:일부 만족함 / ×:만족하지 않음

표 3 XML 전자서명 보안요구사항 만족 정도

Windows 기반의 IIS를 웹서버로 사용하게 되며, 기본 인증은 사용자 이름과 암호를 Base64 인코딩에 의해 웹을 통해 전달하는 보안 방식이다. 이러한 방식은 구현하기 쉬운 반면 중간에 IP 패킷을 가로채서 디코드하면 사용자 이름과 암호가 다른 사람에게 노출될 가능성이 있다. 이것은 사용자가 자신의 자적인 정보를 서버에 보낼 때 목적지 서버가 올바른 서버인지에 대한 어떠한 확인 절차도 이루어지지 않는다는 의미를 내포한다. 따라서 좀 더 안전한 보안 전송 방식인 SSL(Secure Socket Layer)이라는 표준 보안방식을 함께 사용한다.

6. 결론

본 논문에서는 W3C의 국제표준과 요구사항을 만족하는 XML 전자서명 메커니즘을 설계 및 구현하였고, XML 전자서명 기능을 활용하여 기업간 전자조달 시스템에의 응용방안을 제시하였다. XML Security Manager의 향후 과제로는 현재 키를 Keystore에서 읽어오고 있지만, 향후 CA와의 연동을 위한 연구가 진행되어야 할 것이다. 또한 기업간 비즈니스에서 보다 강력한 보안서비스를 제공하기 위해 암호화 기능 또한 제공되어야 한다.

참고문헌

[1] 장우영, 유승범, 장인걸, 차일석, 신동일, 신동규, "XML/EDI 와 XML 전자서명 통합시스템의 설계", 한국 정보처리학회 논문지 제 8권 제 1호, 2001

[2] 송유진, 이희권, 전형득, 한승현, 권헌숙, "전자상거래를 위한 차세대 정보보호서비스에 관한 연구", 한국전자통신연구원, 연구보고서, 2001. 12

[3] W3C, "Extensible Markup Language", http://www.w3c.org/xml

[4] Network Working Group Request for Comments 28087, "XML Signature Requirement", http://www.ietf.org/rfc/rfc2807.txt

[5] 한국후지쯔, "XML과 활용분야" http://kr.fujitsu.com/webzine/tech/issue/xml_use/feature/

[6] 이주영, 김주한, 이재승, 문기영, "안전한 전사상거래 플랫폼 개발을 위한 ESES의 구현", 한국전자통신연구원, 정보처리학회 논문지, 제 8-C권 제 5호, 2001, 10

[7] 원덕재, 이형식, 송준홍, 신동규, 신동인, "XML Signature에 기반한 XML/EDI System의 설계 및 구현", 한국정보처리학회 논문지 제 9권 1호, 2002년

[8] 문기영, 이주영, 박치항, "XML 기반 정보보호 서비스", 한국전자통신 연구원

[9] 송세봉, 장의진, 고훈, 신용태, "Secure XML 메시지 전송시스템 설계", 한국정보처리 학회 논문지 제 8권 1호

[10] NEC, "NEC XML Signature Software Library", http://www.sw.nec.co.jp/soft/xml_s/

[11] IBM, "IBM XML Security Suite", http://alphaworks.ibm.com

[12] W3C, "XML signature syntax and processing", http://www.w3.org/TR/xmldsig-core/

[13] 김지홍, 류재철, 송유진, 염홍열, 이임영, 이만영, "전자상거래 보안기술", 생능출판사, 1999, 9