암호 알고리즘을 이용한 XML 기반 비즈니스 문서의 전자 결재 시스템

김창수* · 정회경**

Electronic Approval System of XML-based Business Document using Crypto Algorithm

Chang-su Kim* · Hoe-kyung Jung**

요 약

산업의 주축이 정보 중심적으로 변화되고 있는 시점에서, 정보 공유에 대한 처리 역시 전자화, 자동화되고, 인터넷을 효율적으로 사용하기 위한 전자상거래 시스템과 비즈니스 정보 시스템이 구축되고 있다. 전자상거래 및 비즈니스 정보시스템에서의 비즈니스 문서의 활용은 비약적으로 증가된 상태이며, 기업내 정보공유에 이르기까지 그 영역이 확대되고 있어 비즈니스 문서의 전자결재 시스템 개발은 필수적이다. 현재 그룹웨어 기반으로 개발된 전자결재 시스템들은 결재처리에서 서명이미지를 삽입하는 방식을 사용하고 있다. 이것은 서명 도용, 전자문서의 가로채기 공격 등 많은 보안 취약성을 지닌다.

본 논문에서는 비즈니스 문서 구조를 가지는 DTD를 기반으로 유효한 비즈니스 XML 문서 작성을 위한 XML 폼 생성기를 구현하였다. 작성된 XML 비즈니스 문서의 기밀성을 보장하고 신속한 전송 처리를 행하기 위하여 서버와 클라이언트의 키 교환에 공개키 교환 방식의 암호 알고리즘의 비밀키를 사용하여 문서를 암호화한 후 전송 가능한 안전한 XML 기반 비즈니스 문서의 전자결재 시스템을 설계 하였다.

ABSTRACT

There are gradually built on electronic commerce and business information system for the effective and automated use of internet while the mainstream of industry moves on information.

It is necessary that a company should develop a electronic approval system because the business documents have application to an electronic commerce, business information system as well

Currently, electronic approval system on groupware is using the way of inserting the image of an approval signature, which is vulnerable on a security by attacks of fraudulent use of electrical signature and eavesdropping on electronic documents.

In this paper, we implementation XML form generator based on DTD having business documents structure for creating a valid business XML documents. we designed electronic approval system based on secured XML which transfers encrypted documents. For the security issues of written XML business documents, it makes use of the crypto algorithm having high performance transaction by the interchange of public key between a server and a client.

키워드

XML, E-business, Crypto, Electronic Approval

* 청운대학교 인터넷학과

** 배재대학교 컴퓨터공학과(교신저자)

접수일자 : 2006. 10. 27

Ⅰ. 서 론

인터넷 환경으로 전환되어 가고 있는 현재의 비즈니스 시스템 상황에서 종이 형태의 비즈니스문서 교환은 제작 시간과 처리절차의 고비용 문제점을 가지고 있으며, 기존 시스템과 거래 주체들과의 상호운용성 및 안정성에 문제를 지니고 있다[1,2]. 이에 전자상거래, 홈뱅킹, 전자결재 등과 같은 안전성을 전제로한 여러 부문의 XML(eXtensible Markup Language)[3]기반의 정보 시스템이 활발히 연구 및 개발되고 있다. 이러한 시스템들은 안전성 측면에서 취약한 인터넷에 보안기술을 적용하여 안전한 인터넷을 구현하는 것이 필수적이다.

인터넷 기반으로 사무자동화가 이루어지고 이러한 변화에 따라 결재처리도 컴퓨터를 이용하여 신속하게 문서를 작성하고, 결재하여 유통시킬 수 있는 전자결재 시스템이 출현하게 되었다[4].

하지만 기존의 전자 결재 시스템은 별도의 패스워드를 입력한 후 전자펜을 이용하여 서명하는 직접 이미지 서명 방식을 사용하고 있어 결재처리에 대한 검증 기능 및 결재 문서의 전송 도중에 결재문서의 내용이 변경되어도 이를 탐지하기가 어렵다. 결재문서의 기안자와 결재자 사이에서 전송되는 결재문서의 가로채기 공격에 대한 대비책 또한 미흡한 형편이다[4,5,6].

이에 본 논문에서는 XML을 이용하여 비즈니스에 사용될 문서 양식을 생성하고 XML문서의 포맷팅(Formatting)을 위해 제안된 인터넷 문서 표준인 XSL(eXtensible Stylesheet Language)[7]을 이용하여 이용 되어질 비즈니스 XML 메시지를 생성한다. 생성된 XML 비즈니스 문서의 기밀성을 보장하고 신속한 전송처리를 행하기 위하여 서버와 클라이언트의 키 교환에 공개키 교환 방식의 암호 알고리즘의 비밀키를 사용하여 문서를 암호화한 후 전송 가능한 안전한 XML 기반의 비즈니스 문서의 전자결재 시스템을 설계 하였다.

Ⅱ. 관련연구

2.1. 전자 결재 시스템

전자결재 처리과정은 기안자는 전자문서편집기(웹폼, 양식 생성기, 워드프로세서 등)를 이용하여 기안 문서를 작성한 후 기안 문서를 HTTP 나 TCP/IP(Transmission Control Protocol/Internet Protocol)를 통해 서버에 전송한다.

기존 전자결재 시스템을 통한 이점은 문서의 전자문서화에 따른 비용, 문서/지식관리를 통해 신속한 정보 검색과 공유에 의한 시간과 간소화된 업무처리절차에 의한 생산성 향상을 가져올 수 있는 장점이 있지만 보안공격에 대한 단점을 가지고 있다.

2.2. 보안 서비스

XML을 활용한 전자상거래상의 문서 교환뿐만 아니라 XML을 적용한 응용분야의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 이에 비즈니스 문서의 교환 과정에서 필요한 보안에 대한 표준화 작업이 빠르게 진행되고 있다.

XML 문서교환을 하는데 있어 불법 보안 위협에 대한 제공할 수 있는 보안 서비스의 고려사항은 다음과 같다.[6,8,9].

◉기밀성(Confidentiality)
◉인증(Authentication)
◉무결성(Integrity)
◉부인 봉쇄(Non-Repudiation)

2.3. 암호 알고리즘

XML 기반의 비즈니스 문서 전자 결재 시스템에서 기반이 되는 암호 알고리즘은 데이터의 암호화를 위해 사용할 KEY값을 분배할 수 있도록 해 주는 Diffie-Hellman 키 분배 알고리즘과 비대칭키 방식의 하나로 DES(Data Encryption Standard) 알고리즘이 갖는 짧은 키 길이의 문제를 해결하고 빠른 속도를 제공할 수 있는 알고리즘으로 개발된 IDEA(International Data Encryption Algorithm) 알고리즘을 사용한다[8,10].

Ⅲ. 시스템 설계

3.1. XML 비즈니스 문서 생성기

그림 1은 XML 비즈니스 문서 생성기의 구성을 나타내고 있다.

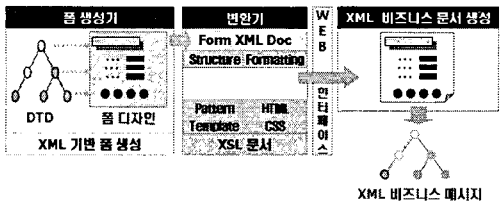

그림 1. XML 비즈니스 문서 생성기
Fig. 1. XML Business Document Generator

DTD(Document Type Definition)기반의 비즈니스 문서 폼을 생성시키기 위한 폼 생성기와 작성된 XML 폼 문서와 웹 형식의 문서 변환을 위한 스타일 시트 문서를 통한 비즈니스 문서를 만들게 되는 웹 문서 변환기, 마지막으로 비즈니스 DTD의 문서 구조를 갖는 XML 메시지를 생성하는 비즈니스 XML 문서 생성기 등의 세 부분으로 구성되어 있다.

3.1.1 폼 생성기

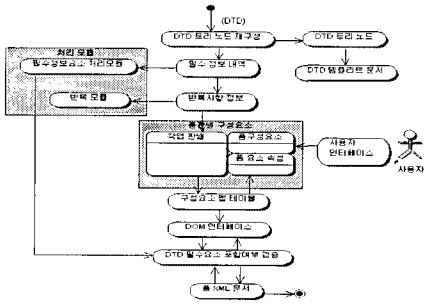

그림 2. 폼 생성기 구성 모듈
Fig. 2. Form Generator Component Module

그림 2는 폼 생성기의 구성 모듈을 나타내고 있다. 비즈니스 문서를 위한 DTD를 입력으로 받아 폼 구성에 반영 할 트리 노드 형태로 재구성하게 된다. 트리구조를 생성하는 과정에서, 폼 상에 생성되어질 아이템의 유효성 검사를 하기 위해서 필수 정보 내역과 그 패턴을 보관하게 된다.

아이템의 표현적인 속성과 논리적 구조 속성, 이벤트 속성 각각을 사용자 인터페이스를 통해 WYSIWYG한 방식으로 작성되며, 폼 정보를 갖는 XML 문서가 생성되기 전에 폼 문서를 검증하게 된다.

3.1.2 XML 비즈니스 메시지 생성

XML 비즈니스 메시지 생성은 변환을 통해 생성된 폼 기반의 HTML 문서에서 부여된 사용자의 데이터와 비즈니스 문서의 구조를 갖는 DTD 템플릿 문서를 통해 DTD에서 요구하는 필수 비즈니스 항목을 포함하고 있으며, 각 항목에 대한 이벤트 스크립트를 포함하고 있고, 사용자 입력 결과를 XML 비즈니스 메시지로 재구성 할 수 있도록 하였다. 그림 3은 폼 생기를 통해 생성된 웹 폼 문서와 웹 폼 문서에 사용자 입력에 의해 생성된 XML 메시지를 보여주고 있다.

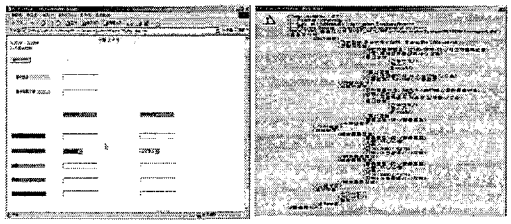

그림 3. 웹 폼 문서 및 XML 비즈니스 메시지
Fig. 3. Web Form Document and XML Business Message

3.2 XML 비즈니스 문서 전자 결재 시스템

3.2.1 시스템 정의

안전한 XML 비즈니스 문서 전자 결재 시스템은 암호 알고리즘을 이용하여 앞에서 설명한 보안서비스 기술을 만족하도록 설계하였다. 결재방식에 있어서 기존의 전자결재 시스템이 사용하는 이미지 서명 대신 암호 알고리즘인 SHA(Sucure Hash Algorithm)로 해쉬값을 생성한 후 RSA(Rivest, Shamir and Adleman) 공개키 알고리즘을 이용한 전자서명 방식을 이용하여 무결성 문제와 부인봉쇄 문제가 해결 가능하도록 하였다.

본 시스템은 그림 4와 같이 클라이언트와 서버로 구성되어 있다. 클라이언트는 웹 브라우저, 암호모듈, 결재모듈, 통신모듈로 구성되고, 서버는 웹 서버, 암호모듈, 통신모듈, 문서관리 모듈, 키 관리 모듈, 데이터베이스로 구성된다.

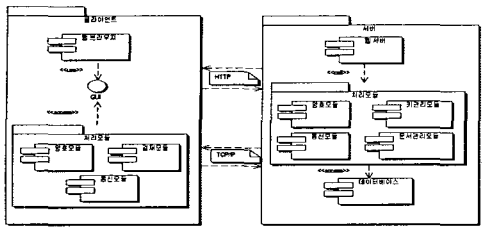

그림 4. 시스템 구성도
FIG. 4. System Diagram

3.2.2 결재모듈

결재모듈에서는 XML 비즈니스 문서 생성기로 작성된 XML 비즈니스 문서를 암호모듈을 이용하여 RSA 공개키 알고리즘으로 XML 비즈니스 기안문서와 결재문서의 전자서명과 검증 기능을 수행하고, IDEA 로 전송할 기안 문서를 암호화한다. 전자서명으로 문서의 무결성 문제와 서명의 부인봉쇄 문제가 해결되고, 기밀성 문제는 문서의 암호화로 해결된다.

1) 기안자의 결재요구

기안자의 결재요구는 서버에 접속한 후 결재모듈이 실행되고 비밀키 교환이 이루어진 후 가능하다. 결재요구는 그림 5와 같은 순서로 진행된다.

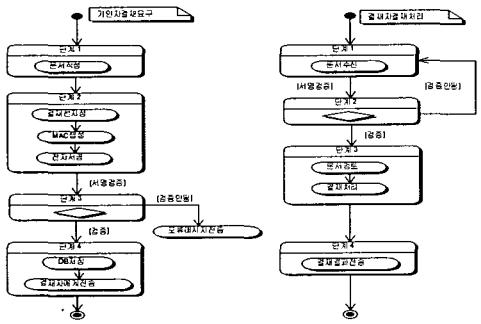

그림 5. 결재 요구 및 처리 흐름도
Fig. 5. Diagram of Approval request and transaction

[단계 1] 기안자는 전자문서(M)를 작성한다.

[단계 2] 전자문서의 해쉬값 H(M)을 구하고 자신의 개인키로 서명한다. 그리고 전자문서를 비밀키 알고리즘으로 암호화한다.

$Sign_{Private\_Drafter}[H(M)]||En_{Session\_key}(M)$

[단계 3] 서버는 암호화된 전자문서를 복호화한 후 H'[M]을 생성한다. H'[M]과 기안자의 공개키를 가지고 서명 검증을 한다.

$Verify_{Public\_Drafter}[Sign_{Private\_Drafter}[H(M)]] \equiv H[M] \equiv H'[M]$

[단계 4] 서버는 서명 검증이 완료되면 문서를 데이터베이스에 저장한 후 처리결과 메시지를 전송한다.

2) 결재자의 결재처리

결재자는 서버로부터 전자문서를 전송받아 결재처리를 한다. 문서 기안 단계와 마찬가지로 결재모듈의 실행시 비밀키 교환이 이루어진다.

[단계 1] 서버로부터 암호화된 전자문서(M)와 서버가 서명한 기안자의 공개키를 전송받는다.

$Sign_{Private\_Drafter}[H(M)]||En_{Session\_key}(M)||Sign_{Private\_server}(Public\_Drafter)$

[단계 2] 결재자는 세션키를 사용하여 전자문서(M)를 얻는다. 전자문서(M)의 해쉬값 H'(M)을 생성하고, 기안자가 서명한 해쉬값을 기안자의 공개키로 복호화하여 H(M)을 얻는다. 두 해쉬값 H(M)과 H'(M)을 비교하여 무결성을 검증한다. 만약, 두 값이 동일하지 않으면 결재처리를 취소한다.

$De_{session\_key}[En_{Session\_key}(M)] \equiv M$

$Verify_{Public\_Drafter}[Sign_{Private\_Drafter}[H(M)]] \equiv H(M) \equiv H'(M)$

[단계 3] 전자문서(M)를 검토한 후 해쉬값 H(M)에 자신의 개인키로 서명한다.

$Sign_{Private\_signer}[H(M)]$

[단계 4] 서버에 결재정보(결재, 보류, 거부 등)와 서명값을 서버에 전송한다.

$Doc\_Num||Sign\_Info||Sign_{Private\_signer}[H(M)]$

3.2.3 암호모듈

암호모듈은 안전한 XML 비즈니스 문서의 전송을 위한 문서의 암호화/복호화, XML 비즈니스문서에 대한 전자서명과 검증을 위한 암호 기술을 지원한다.

문서의 안전한 전송을 위해 Diffie-Hellman의 공개키 교환 알고리즘과 IDEA를 지원하고, 문서의 결재처리를 위해서는 공개키 알고리즘으로 RSA, 해쉬 알고리즘으로 SHA를 지원한다.

3.2.4 통신모듈

통신모듈은 결재모듈과 문서관리 모듈로부터 전송받은 암호화된 XML 비즈니스문서를 TCP/IP소켓(Socket)을 통해 클라이언트나 서버에 전송하는 기능을 한다.

3.2.5 문서관리모듈

문서관리 모듈은 클라이언트로부터 전송되는 XML 비

즈니스 기안문서와 결재문서를 암호모듈을 이용하여 무결성을 검증하고, 데이터베이스에 저장 및 관리하는 기능을 한다.

서버는 문서를 데이터베이스에 저장할 때 기안자와 교환한 세션키를 사용하여 암호화된 문서를 복호화한 후 저장한다. 결재자에게 문서를 전송할 때는 결재자와 교환한 세션키로 암호화하여 전송한다.

3.2.6 키관리모듈

키관리모듈은 클라이언트의 공개키를 데이터베이스에 저장 및 관리하는 기능을 한다. 서버에서 결재자에게 XML 비즈니스 기안문서를 전송할 때 기안자의 공개키를 함께 전송하며, 클라이언트의 공개키 변경요구가 있을 때 이를 처리한다.

공개키는 클라이언트의 공개키 변경요구로 변경될 수 있다. 이때 서버와 주고받는 메시지의 형태는 다음과 같다.

[단계 1] 클라이언트는 먼저 새로운 공개키/개인키의 쌍을 생성한다. 그리고 이전의 개인키를 사용하여 이전의 공개키와 새로운 공개키를 암호화한다.

$En_{Old\_PrivateKey}[New\_PublicKey||Old\_PublicKey1]$

[단계 2] 서버는 데이터베이스에 있는 클라이언트의 공개키로 전송받은 메시지를 복호화한 다음 두 공개키를 비교 검증한다.

$De_{Old\_PublicKey2}[En_{Old\_PrivateKey}[New\_PublicKey||Old\_PublicKey_1]]$

$Old\_PublicKey_1 \equiv Old\_PublicKey_2$

3.2.7 전자결재 프로토콜

안전한 XML 비즈니스 문서 전자 결재 시스템은 그림 6과 같은 전자결재 프로토콜에 따라 동작한다. 이 프로토콜은 결재요구와 결재처리 부분으로 나눠진다.

XML 비즈니스 문서에 대한 결재요구 절차는 기안자가 XML 문서 생성기를 사용하여 XML 비즈니스 문서를 작성하여 서버에 전송하면서 이루어진다. 결재처리 절차는 결재자가 서버로부터 결재요구 메시지 확인 후 기안문서를 전송받아 이루어진다.

기안자와 결재자는 서버에 연결하기 위해서 웹 브라우저를 이용한다. 즉, 문서에 대한 결재요구나 사용자 검색은 HTTP를 이용한다. 그러나, 결재요구와 결재처리를 위한 서버와의 통신은 소켓을 이용한다. 소켓을 통한 결재요구와 결재처리는 안전한 데이터 전송을 위해 암호통신으로 이루어진다.

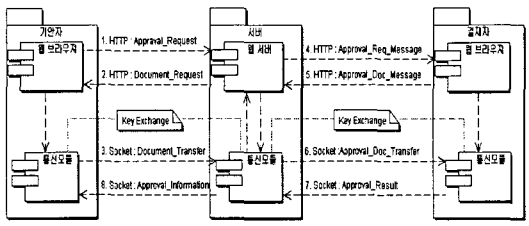

그림 6. 전자결재 프로토콜
Fig. 6. Electronic Approval Protocol

Ⅳ. 결 론

정보 통신 환경의 급변화는 기존의 비즈니스 문서 전자 결재 체계를 빠른 속도로 변화시키고 있으며 보다 효율적인 체계로의 개선이 요구되고 있어 전자 결재에 사용될 문서의 전자화, 효율화 및 안전한 문서 전송에 대한 관심이 많아지고 있다.

대부분의 기존 전자 결재 시스템들은 별도의 양식작성기를 사용하여 문서를 작성하고 , 문서결재에 전자펜을 이용한 이미지 서명방식을 사용하고 있다. 이 시스템들은 서명에 대한 검증 기능이 없을 뿐만 아니라 서명 이미지의 위조 등 많은 보안 문제를 지니고 있다.

이에 본 논문에서는 XML을 이용하여 비즈니스에서 사용될 폼을 디자인 하고 폼 문서로부터 XML 비즈니스 메시지를 생성할 수 있는 XML 비즈니스 문서 생성기를 구현하였다. 또한 XML 비즈니스 문서 생성기를 통해 생성된 XML 비즈니스 문서를 암호 라이브러리를 이용하여 인터넷 환경에서 전자결재가 안전하게 이루어지도록 하는 XML 비즈니스 문서 전자결재 시스템을 설계 하였다.

본 논문에서 구현한 XML 비즈니스 문서 생성기는 폼 문서의 수정 요구에 능동적인 대응이 가능하도록 구현하였고, 비즈니스 프레임워크나 전자 결재 상에서 문서 교환의 편리성과 상호운용성을 제공하고 있다. 또한, 설계한 XML 비즈니스 문서 결재시스템은 기존의 특정 포맷의 문서 형식에 따른 문서 교환이 아닌 XML 기반의 문서 교환으로 상호 운용성을 가지며, 전자결재 시스템들이 지니고 있는 보안 취약성을 암호 기술을 이용하여 해결하였다.

공개키 알고리즘을 사용하여 파일의 해쉬값을 생성한 후 이 해쉬값에 전자서명을 하도록 하였고, 공개키 알고리즘으로는 RSA, 해쉬 알고리즘으로는 SHA 를 적용하였

다. 문서 전송 시에는 Diffie-Hellman 의 공개키 교환 알고리즘을 이용하여 키를 교환하고 비밀키 알고리즘으로 IDEA 를 이용하여 문서를 암호화하는 방식을 채택하였다. 이렇게 함으로써, 기존의 시스템들이 지니고 있던 문서의 무결성, 부인봉쇄, 기밀성 문제 등 여러 보안문제를 해결하였다.

본 논문에서 구현한 XML 비즈니스 문서 생성기는 무선 인터넷 서비스 분야에 XML 기반의 전자 문서 생성을 위한 폼 개발에 유용하게 이용되리라 사료되며, XML 비즈니스 문서 결재 시스템을 일반 사무 처리에 이용할 경우, 비용측면이나 시간측면, 생산성 측면 등에서 많은 이점을 얻을 수 있을 뿐만 아니라,인터넷 기반으로 전환되고 있는 사무자동화에 많은 기여를 할 것으로 기대된다.

참고문헌

[1] "eCommerce 글로벌 리포트"한국 커머스넷, 이정열, 2000, 다우

[2] "Creating Interactive Web Forms from XML Document" Aoki, Yoshinori, XML2000

[3] eXtensible Markup Language, http://www.w3.org/TR/XML

[4] 장용철, 오태석, 오무송, "암호화를 이용한 전자결재 시스템의 설계 및 구현" 한국정보처리학회 논문지 제 4 권 제 8 호, 1997. 8

[5] 이진용, 권혁인, 김영찬, "인터넷 EDI 설계 및구현" 한국정보과학회 가을 학술발표논문집 Vol. 25, No. 2, 1998

[6] 이종현, 구영회. 현대암호, SoftForum. 1997

[7] "The XSL companion", Neil Bradley, ADDISONWESLEY

[8] "Inside Secrets JavaScript & JScript", James Jaworski, SYBEX

[9] Bruce Schneier, Applied Cryptography 2nd, John Wiley & Sons, Inc. 1996

[10] Warwick Ford, Computer Communications Security : principles, Standard Protocols and Techniques, Prentice-Hall Inc. 1996

저자소개

김 창 수(Chang-Su Kim)

1996년 배재대학교 전자계산학과(이학사)
1998년 배재대학교 전자계산학과(이학석사)
2002년 배재대학교 컴퓨터공학과(공학박사)
2001년~2004년 배재대학교 IT 교육센터 책임강사
2005년~현재 청운대학교 인터넷학과 전임강사
※관심분야 : XML, ebXML, Semantic web, 멀티미디어문서정보처리, u-Logistics

정 회 경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG-21 유비쿼터스 센서 네트워크