XML 기반의 모바일 전자결재시스템 구현

구본현, 이민수, 조재익, 문종섭
고려대학교 정보보호대학원
{koo191, leesle, chojaeik, jsmoon}@korea.ac.kr

Implementation of a Mobile Electronic Approval System using XML

Bonhyun Koo Minsoo Lee Jaeik Cho Jongsub Moon
Graduate School of Information Security, Korea University

요 약

본 논문에서는 이동성이 많은 결재자의 업무를 효율적이고 신속하게 처리하기 위해 PDA, 핸드폰과 같은 모바일 장비상에서의 공인인증서를 이용한 결제처리 및 무선 인터넷상의 보안기능을 갖춘 시스템을 개발하였다. 모바일 인터넷의 보안 메커니즘은 정당한 사용자인지를 확인하는 인증, 데이터의 비밀 전송과 변조 여부 확인, 전자서명을 통한 거래 부인 방지 등이 이뤄진다. 이를 위해 RSA 공개키 알고리즘을 사용하여 문서 내용들에 대한 암호화/복호화를 수행하며 SHA-1 해시 알고리즘과 공인인증서를 사용하여 결제처리를 한다. 일반 데스크 탑뿐만 아니라 모바일 장비간의 데이터 패킷 전송을 위해 XML 인코딩과 SOAP 프로토콜을 이용한다.

1. 서 론

지금까지 보안(Security)에 관한 많은 연구가 진행되어 왔고 그 관심이 고조되고 있으며, 국가와 기업은 물론 개인도 질 높은 정보를 수집, 분석 그리고 가공하기 위해 전력을 기울이고 있다. 이러한 정보의 보안을 위하여 다양한 보안 시스템 개발이 크게 활기를 띠고 있다. 유비쿼터스 네트워크의 발전에 따라 언제 어디서나 네트워크에 접속할 수 있는 시스템의 개발이 필요 하게 되었다[1]. 기존의 SK-E Mart, LG CNS 그리고 하나로 통신(주)등의 결재 시스템은 데스크 탑 환경상의 결제 처리만 가능하였으며 모바일상의 처리는 불가능하였다. 또한 보안기능 부분의 구현 부분이 다소 부족하였다.

본 논문에서는 PDA, 핸드폰과 같은 모바일 장비를 이용하여 때와 장소를 가리지 않고 결재시스템에 접근하여 결재 요청된 문서에 대해 결재 처리를 할 수 있는 시스템을 개발하고자 한다.

2. 제안하는 방안

이 절에서는 제안 기법의 개념과 구현한 시스템의 구조에 대해 설명하고, 공인인증서의 데이터코드들에 대한 적용 기법에 데이터베이스에 암호화되어 저장되어지는 기법을 제시한다.

2.1 전체 시스템 설계

본 논문에서는 안전한 데이터의 전송을 위해 RSA 공개키 알고리즘을 사용하여 문서의 내용을 암호화/복호화 시키며, 결재자의 결재처리는 무결성을 입증하기 위해 공인인증서의 원시코드 값에 SHA-1 해쉬 알고리즘을 적용하여 결제코드로 사용한다.

그림 1은 본 논문에서 개발하고자 하는 결재 시스템의 구조도이다. 여기에서 서버/클라이언트간의 상호 신뢰를 위해서 자체 인증기관을 설치하여 인증서를 이용한 신원확인을 수행하고, 네트워크 사이의 전달되는 패킷은 XML SOAP 프로토콜을 이용하여 전송되어진다.

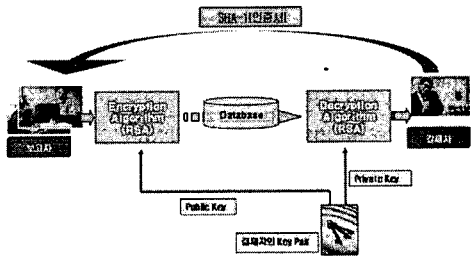

그림 1. 시스템 구조도

2.2 결재처리 및 문서 암호화 기법

문서내용에 대한 암호화 처리는 앞에서 테스트한 RSA 방식으로 암호화되어지며 이 암호화 되어진 내용은

데이터베이스에 저장되어진다. SQL 데이터베이스로의 데이터 전송은 XML 웹서비스를 사용하여 인코딩을 수행한 후 SOAP 프로토콜을 사용하여 전송되어 진다. SOAP 프로토콜을 사용하여 방화벽이나 IPSec등의 보안관련 장비들로 인해 데이터 패킷을 손실하는 것을 막을 수 있다[2]. 또한 PDA, 핸드폰과 같은 모바일 디바이스로의 데이터 전송도 가능해 진다. 보고자는 보고자용 어플리케이션을 통해 결재문서를 전송하면 결재자는 PDA, 핸드폰과 같은 본인의 모바일 디바이스를 이용하여 언제든지 본인에게 결재 요청된 문서를 확인하고 결재 처리를 할 수 있다. 그림 2는 보고자가 문서 전송 시 문서의 내용들은 데이터베이스에 결재자의 공개키와 RSA 암호화 알고리즘을 통해 암호화 되어져 저장이 되어져 있는 데이터베이스의 내용이다.

	idx	db_n...	db_title	db_pwd	db_contents
1	1	관리...	유비쿼...	.	JECptKjeV91hzKpzlnVPeXbzPjVPpcknjT...
2	2	인사...	신규 ...	비고	amSlRsRK+lDDBVN1/TmWv79Ls+WAh...
3	3	관리...	프로젝...	비고	JYSv1hSknrRerFMuwRg+cyl5TnywP3...
4	4	관리...	정비 ...	비고	eokKoxo1gjWZEnmcGePL6S7la+qN6A...
5	5	시설...	IT 사업...	비고	dRbrTera4+SHp8tDCJC5LLptTv6be5jn...
6	6	인사...	동서대...	비고	RsljI0VORwOvKZ1TlAlwMZEHwwrdbO...
7	7	관리...	보안 ...	비고	c/dJ+jSRNNdnpZpNxYTxn+93xpCIM3j...
8	8	관리...	무선 ...	비고	j0dfECmfkI0ONd7Yx57Y7RWmhJAwbOg...
9	9	홍보...	신입회...	비고	ZiVv+mTMO+KnRdblgwY4784meIC2A7t...
10	10	인사...	사내 ...	비고	L2srNAhYO22KPmWg3mPtXLoZUgvgIA...

그림 2. Database 암호화

결재자는 본인의 개인키를 통해 암호화되어진 내용을 복호화 수행 후 결재 처리 시 공인인증서의 원시 데이터 코드에 SHA-1 해시 알고리즘을 적용하여 결재코드를 전송하면 문서는 결재 처리가 이루어지기 되어 있다[3][4]. 그림 3은 인증서의 원시 데이터 코드 내용을 사용하기 위해 개발한 어플리케이션으로 공개키, 인증 기관 등의 데이터들을 추출할 수 있다.

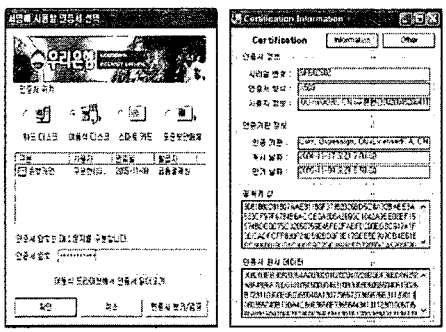

그림 3. 인증서와 테스트 어플리케이션

3. 구현 및 검증

이 절에서는 PDA, 핸드폰과 같은 모바일 장비상에서의 공인인증서를 이용한 결제처리 어플리케이션에 대한 구현내용과 검증 도구를 소개한다.

3.1 PDA, 핸드폰 인터페이스

실제 구현 부분으로 시스템 결제 서버를 구축하고 PDA, 핸드폰과 같은 모바일 장비의 인터페이스를 개발하였다. 서로 다른 장비간의 데이터 전송을 위해 패킷들은 모두 XML 형태로 데이터 인코딩을 거쳐 전송이 이루어지게 된다. 문서의 보고자는 보고용 어플리케이션으로 문서를 전송하면 결재자는 아래 그림과 같이 PDA, 핸드폰과 같은 모바일 장비를 이용하여 본인의 사원번호와 공인인증서 그리고 개인키를 이용하여 보고 문서를 결재 처리 할 수 있다. 그림 4와 5는 실제 개발한 PDA 및 핸드폰의 사용자 인터페이스 화면이다.

그림 4. PDA,핸드폰 인터페이스 화면1

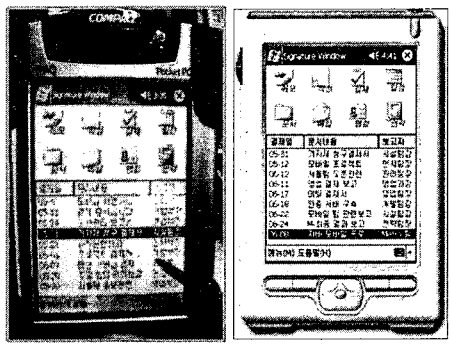

그림 5. PDA, 핸드폰 인터페이스 화면2

3.2 RSA 수행속도 분석 및 검증

PDA, 핸드폰과 같은 제약적인 리소스를 가지고 있는 모바일 디바이스에서 RSA 알고리즘의 암호화 및 복호화를 적용하기 위해서 수행속도를 분석할 필요가 있었다. 이에 PDA및 핸드폰 개발 환경을 적용하여 윈도우 환경에서 테스트를 수행하였다. 또한 이러한 암호화된 내용을 데이터베이스에 저장하기 위해 적절한 문자로 인코딩할 필요가 있었다. 그림 6은 이러한 인코딩과정을 테스트하기 위해 개발한 RSA 암호화/복호화 어플리케이션이다. 테스트과정을 거친 RSA 암호화/복호화와 결재처리는 XML 웹서비스를 이용하여 서버 측에서 처리하도록 구현하였다.

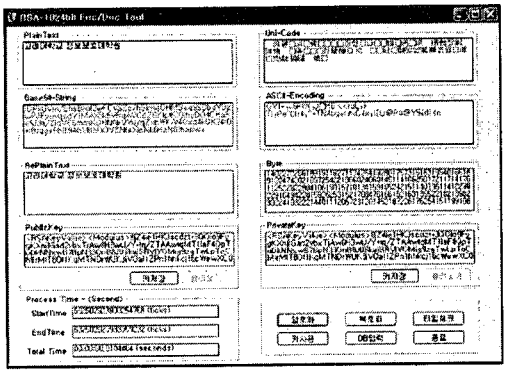

그림 6. RSA 인코딩변환 분석어플리케이션

그림 7은 테스트용 어플리케이션으로 7회 암호화와 복호화 처리 속도 및 필요한 문자열로 인코딩한 방식의 화면이다. 테스트용 어플리케이션으로 테스트를 수행한 결과 최대 878 밀리세컨드(millisecond) 최소 318 밀리세컨드(millisecond)까지 수행되었고 평균 암호화 수행속도는 100회를 수행 했을 때 426 밀리세컨드(millisecond)로 모바일 장비에서도 지연시간을 최소화 시켰다. 그림 3은 20byte를 기준으로 암호화/복호화 평균 수행속도를 분석하기 위한 어플리케이션이다. 적절한 인코딩 방식으로 전환을 하지 않고 쿼리문을 전송 시에 올바른 데이터 값을 전송할 수 없는 문제점이 있었다. 분석 어플리케이션을 통해서 Uni-Code와 ASCII 인코딩 방식을 사용하여 데이터베이스에 저장 시에는 문서의 내용이 일부 손실되는 현상이 발생하였다. 본 논문에서는 Base64-String 방식을 적용하여 인코딩을 적용하였다.

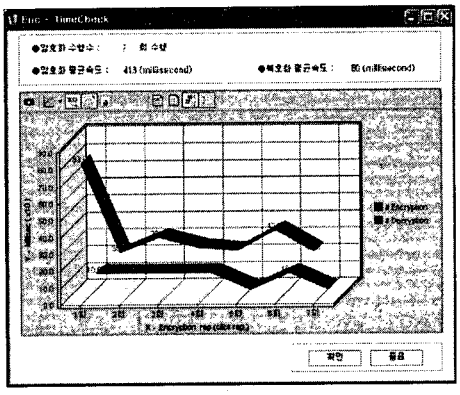

그림 7. RSA 암호화 수행속도 분석(7회)

4. 결론

본 논문에서는 기존의 결재 시스템을 XML과 SOAP 프로토콜을 이용하여 모바일 환경 상에서 처리할 수 있는 시스템을 개발 하였다. 보다 안전한 데이터 전송을 위해 RSA 암호화, 복호화 알고리즘 및 ID기반의 공인 인증서를 통한 결재 처리를 할 수 있도록 시스템을 설계하였다. 온라인상의 주민등록번호를 대체하는 식별자의 사용문제에 대해 크게 이슈가 되고 있다. 이러한 대체 수단으로 인증서와 ID를 연계한 서비스 모델을 이용하는 것을 본 논문에서 제시하였다. 본 논문의 시스템 구조를 ID 기반의 무선공인인증서비스와 연계하여 무선 상에서도 보다 안전한 서비스를 제공할 수 있을 것이다.

향후 연구 과제는 기존의 공인인증서비스들과 하나로 연결하여 유무선 통합 공인인증서비스를 개발하는 것이다.

참 고 문 헌

[1] 김진환, "사용자 인증 보안을 위한 온라인 서명 시스템", 한국 정보보호학회 논문집, 2002

[2] 김지현, 이광수, "XML 전자서명제품의 표준 적합성 시험 방법 및 구현", 한국정보보호학회 논문집, 2004

[3] 이국희, 이상곤, 정원영, 김태근, 문상재, "해쉬 알고리즘 개발 및 디지털 이동통신을 위한 인증시스템에의 응용", 한국 정보보호학회 논문집, 1998

[4] 황석근, 조한혁, "디지털 서명과 해쉬함수", 한국정보보호학회 논문집, 1992