[기술자문 컨설팅]
자바애플릿으로 구현한
인증서 기반의 전자서명

한국소프트웨어진흥원

공개SW기술지원센터

<Revision 정보>

일자	VERSION	변경내역	작성자
2007. 5.11	0.1	초기 작성	양선주
2007. 5.14	0.2	테스트 결과 추가	양선주

목 차

1. 문서 개요

본 문서는 여론 조사, 민원신청, 온라인뱅킹 및 인터넷 쇼핑몰 등 인터넷 상에서 본인 서명이 필요한 경우 인증을 사용하는 전자서명을 자바 애플릿으로 구현한 것을 클라이언트의 기능적 측면에서 테스트하여, 향후 이에 대한 기술 자문 컨설팅의 참고 자료로 활용하기 위해 제작되었다.

가. 문서의 목적

다음과 같은 세부적인 목적을 달성하기 위하여 작성되었다.

○ 자바애플릿 기반 전자서명 테스트 개요

○ 오픈웹이 개발한 자바애플릿 기반 전자서명 사용자 테스트 결과

나. 본 문서의 사용방법

다음과 같은 방법으로 사용할 수 있다.

○ 오픈웹이 개발한 자바애플릿 기반 전자서명 사용자 테스트 결과 자료로 활용할 수 있다.

2. 대상 기관

기관명*	한국소프트웨어진흥원	웹사이트	http://www.software.or.kr
주 소*	서울시 송파구 가락본동 79-2 KIPA 빌딩 12층		
연락처*	02-2141-5062	E-MAIL*	yjcho@software.or.kr
내용	한국정보사회진흥원의 문의로, 오픈웹에서 개발한 전자서명 자바 애플릿에 대한 클라이언트 측면의 기능테스트		
비고			

<표 1> 자문 대상기관

3. 자바 애플릿 기반 전자서명 테스트 개요

전자서명은 여론조사, 민원신청, 온라인 뱅킹 및 인터넷 쇼핑몰 결재 등과 같이 인터넷 상에서 서명을 하는 경우 서명 데이터를 암호화하여 위조 및 변조를 방지하고 공개키(PKI) 기반의 보안 암호 알고리즘을 통한 보안성을 확보하기 위해 사용된다.
이러한 전자서명을 할 때 사용하는 것이 인증서로, 인증서의 역할은 크게 두 가지로 볼 수 있다. 데이터를 암호화하는 기능과 데이터를 주고 받는 대상들 간의 신원확인 기능이 그것이다.
이번 자바 애플릿 기반의 전자서명을 개발한 오픈웹(http://openweb.or.kr/)에 따르면, 인증서를 사용한 전자 거래가 현재 솔루션에서 처리되는 구조는 다음과 같다.

① 웹서버가 사용자 컴퓨터로 전송한 양식에, 사용자가 계좌번호, 금액, 보안카드 등 전자서명이 필요한 페이지에서 요구되는 정보를 입력 후 전송
② 입력된 값이 사용자 컴퓨터 내에 가동되는 Active-X Control에 공급됨
③ Active-X Control은 이 데이터에 전자서명을 붙일 필요성이 있는지 확인 후 인증서 암호를 사용자에게 요구하여 확보하고 전자서명 부착(사용자 개인인증서에 포함된 Public Key도 함께 부착됨)
④ 웹서버가 전송한 기관 인증서의 공개키로 암호화하고 공개된 http 프로토콜을 통해 암호화된 정보 전송
⑤ 암호화된 정보를 수신한 웹서버는 보관 중인 Private Key를 이용하여 암호를 해독하고 인증서버에 접속하여 사용자가 송신한 인증서가 유효한지 확인한 후 요청한 작업 처리
⑥ 전송 처리 내역을 사용자의 공개키로 암호화한 후, 암호화된 정보를 사용자에게 전송
⑦ 사용자 컴퓨터는 수신받은 정보를 Active-X Control에 공급하고, Active-X Control은 사용자의 Private Key로 이 정보를 열어 사용자 화면에 출력

이러한 일련의 과정에서 Active-X Control은 Applet 역할을 하는 것으로, 주어진 어떤 응용프로그램 내부에서 특정 기능을 수행하여 해당 응용프로그램의 기능성을 높여주는 부속적인 역할을 담당한다. 이와 같은 역할을 담당할 수 있는 다른 applet으로 Java Applet, Flash Movie, Windows Media Player Applet 등이 있다.
이들 중, Java Applet이 해당 역할을 담당하게 되면 사용자가 계좌번호, 금액, 보안카드 등의 정보 입력이 필요한 페이지에 접근하게 될 때, 사용자의 웹브라우저는 웹서버로부터 Java byte code를 다운로드하고, 클라이언트에서 수행하는 각종 역할을 웹서버가 실시간으로 전송하면서 사용자가 수행해야 하는 부분들은 사용자의 컴퓨터상에 임시적으로 생성되는 Java Virtual Machine에서 실행하게 된다.

4. 전자서명 클라이언트 테스트 방법론

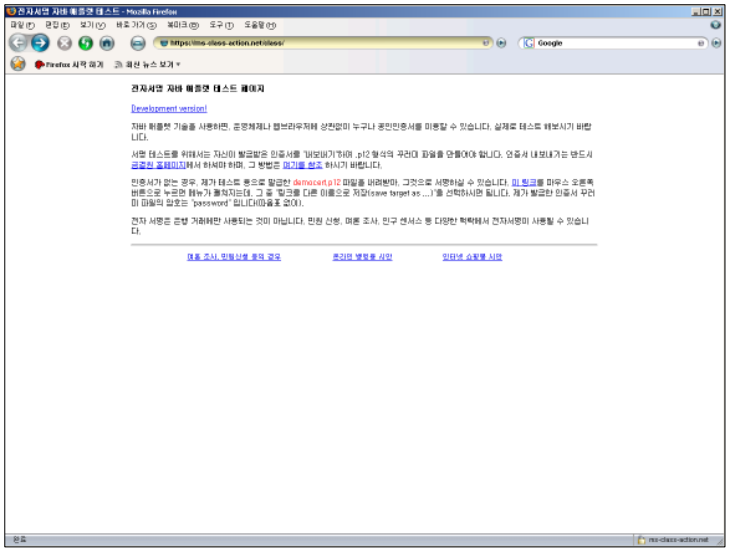
가. 시스템 개요

항목	SAMSUNG ZCP30	SAMSUNG ZCP30	TRIGEM G6432M
CPU	Intel Pentium(R) 4 3.0GHz	Intel Pentium(R) 4 3.0GHz	Intel Pentium(R) 4 3.0GHz
Memory	512MB	512MB	512MB
HDD	Maxter 120GB	Maxter 120GB	WD 160GB
OS	Hancom Desktop 2.0	Fedora Core 6	Booyo Desktop 2.0
Kernel	2.6.19-10hs	2.6.18-1.2798.fc6	2.6.16-333.BS2
Browser	Mozilla Firefox 2.0.0.3	Firefox 1.5.0.9	Firefox 1.5.0.1

<표 2> 전자서명 클라이언트 테스트 시스템 개요

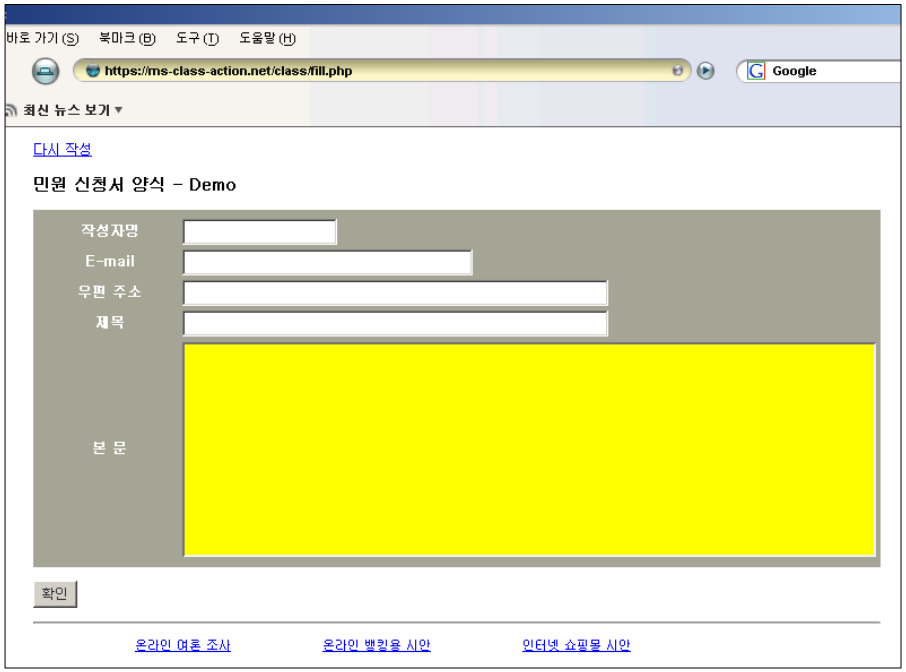
나. 테스트 방법

https://ms-class-action.net/class/ 에서 임시 인증서 이용



<그림 1> 자바애플릿 기반 전자서명 테스트 페이지

테스트 1. 여론조사 및 민원신청 전자서명 테스트

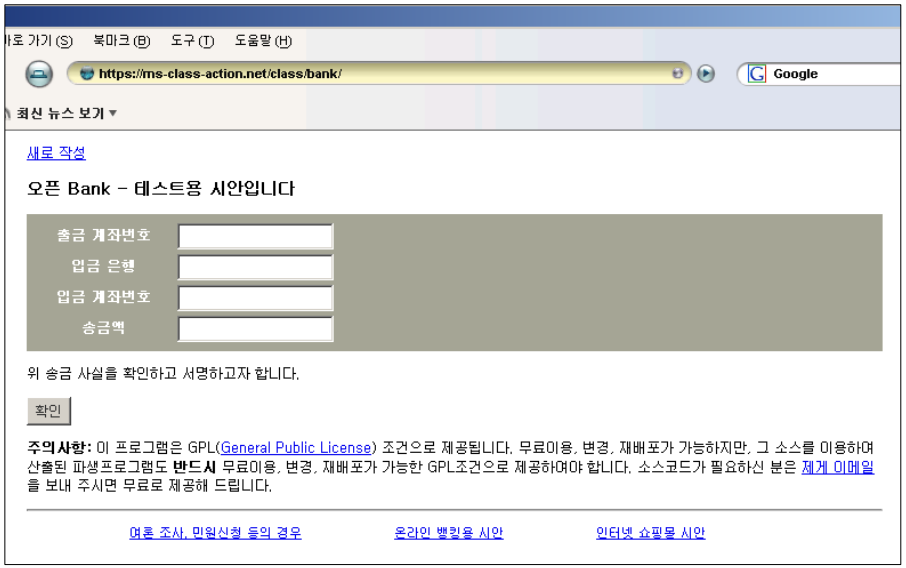


<그림 2> 여론조사, 민원신청 전자서명 테스트

1) 테스트 방법

상기 페이지의 내용에 대해 전자서명을 수행한 후, 서명확인결과가 True/False 로 나타나는지 확인

테스트 2. 온라인뱅킹 전자서명 테스트

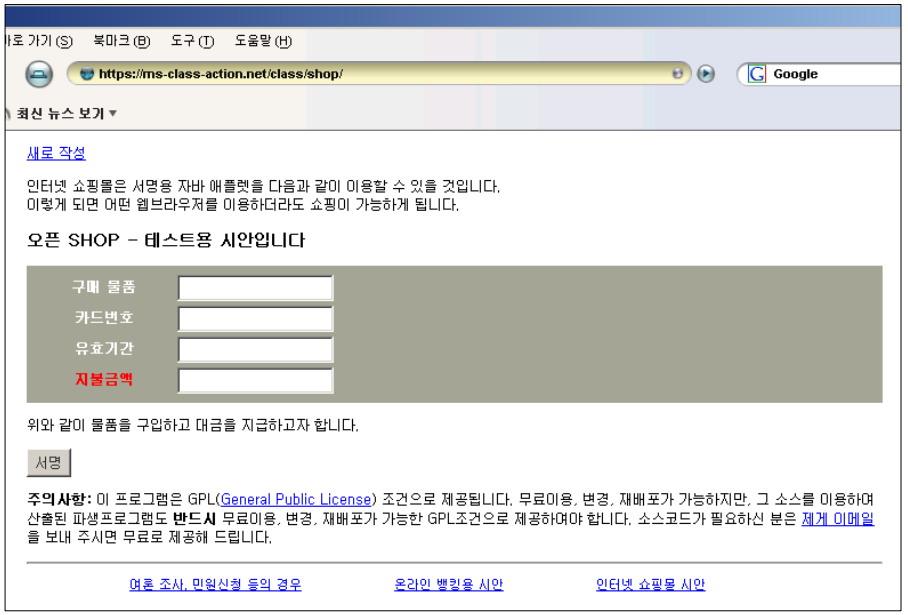


<그림 3> 온라인뱅킹 전자서명 테스트

1) 테스트 방법

상기 페이지의 내용에 대해 시간차를 두고 전자서명을 2회 수행한 후, 서명결과 내용이 변경되는지 확인

테스트 3. 인터넷쇼핑몰 전자서명 테스트



<그림 4> 인터넷쇼핑몰 전자서명 테스트

1) 테스트 방법

상기 페이지의 내용에 대해 시간차를 두고 전자서명을 2회 수행한 후, 서명결과 내용이 변경되는지 확인

5. 전자서명 사용자 테스트 결과

테스트 항목	SAMSUNG ZCP30	SAMSUNG ZCP30	TRIGEM G6432M
여론조사/민원신청	PASS	PASS	PASS
온라인뱅킹	PASS	PASS	PASS
인터넷쇼핑몰	PASS	PASS	PASS
비고			버튼 한글 깨짐

<표 3> 전자서명 사용자 테스트 결과

6. 결론

클라이언트 측면에서 인증서 기반의 전자서명 테스트는, 리눅스 데스크톱의 배포판을 다르게 선택하여(한컴 데스크톱 2.0, 부요 데스크톱 2.0, 페도라 코어 6) 수행하였으며, 이에 따라 브라우저는 Firefox이며 각기 설치된 버전은 다르다.

암호화가 필요한 페이지의 각 입력값에 입력을 하고 전송하면 사용자의 PC에 Java Virtual Machine을 설치하게 되며, 자바 애플릿을 통해 서버와 암호화를 진행하게 된다.

Firefox 1.5.0.1, 1.5.0.9, 2.0.0.3 버전 모두에서 서명결과가 정상적으로 출력되는 것을 확인하였다.