제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

M-Commerce를 위한 전자 서명 시스템*

황기태*, 김남윤**, 강성민*, 이재우*
*한성대학교 컴퓨터시스템공학부
**한성대학교 정보공학부
e-mail : calafk@hansung.ac.kr

Implementation of Digital Signature System for M-Commerce

Kitae Hwang*, Namyun Kim**, Sungmin Kang*, Jaewoo Lee*
*Division of Computer System Engineering, Hansung University
**Division of Information Engineering, Hansung University

요 약

M-Commerce 에서 전자 서명은 필수적인 요소이다. 본 논문에서는 PKI 를 기반으로 모바일 단말기에서 약정이나 계약을 체결할 수 있는 전자 서명 시스템을 설계 구현한 예를 보인다. 이를 위해 XML 구조의 계약서를 저작할 수 있는 도구를 개발하고, 계약서를 관리하는 서버와 PDA 단말기 상에서 전자 서명하는 모듈 그리고 고객이 계약을 확인할 수 있는 시스템을 구현하였다.

1. 서론

최근 하드웨어 및 네트워크 기술의 발전으로 인해 Cellular Phone, PDA(Personal Digital Assistant), Smart Phone 등 고성능 모바일 단말기들이 개발되고 있으며, 사용이 급격히 늘어가고 있다. 또한 인터넷을 기반으로 하는 전자 상거래 응용들이 무선 통신을 이용한 전자 상거래인 M-Commerce[1] 로 구현되고 있다. 이러한 추세는 "Any Where, Any Time" 이라는 전자 상거래의 패러다임을 수용할 수 있는 모바일 단말기의 급속한 개발 및 무선 통신의 발전에 기인한다.

한편 M-Commerce 가 안정적으로 확장되기 위해서는 몇 가지 고려해야 할 사항이 존재한다. 첫째, 무선 통신의 대역폭이 유선 인터넷에 비해 작다. 둘째, 무선 단말기는 제한된 자원을 갖고 있다. 낮은 CPU 처리 속도, 작은 메모리 및 디스플레이 크기 등으로 인해 응용 시스템 개발 시 이러한 점을 충분히 고려하여야 한다. 셋째, 전자 상거래에서 필수적인 보안 문제를 해결해야 한다. 즉, 데이터의 암호화/복호화 뿐만 아니라 전자 서명(Digital Signature) 기술이 제공되어야 한다. 전자 서명은 부인 봉쇄 기능을 통해 전자 상거래의 신뢰도를 높이는 중요한 기술이라고 할 수 있다. 현재 전자 서명을 위한 보안 시스템은 PKI(Public Key Infrastructure) [2]에 기반을 두고 있다.

본 논문은 PKI 를 기반으로 M-Commerce 상에서 전자 서명 시스템의 설계/구현한 내용을 다룬다. 무선 통신 및 단말기의 제약 조건을 고려하여 경량의 XML 계약서 및 ActiveX 컨트롤을 제작하였다. 본 연구의 목적은 PKI 기반의 전자 서명 시스템의 테스트 베드를 개발하고 이들의 효율성을 평가하여 M-Commerce 시스템을 설계하는 근간을 제공하는데 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 전자 서명 기술을, 3 장에서는 구현한 전자 서명 시스템을, 4 장에서 결론을 서술한다.

2. 전자 서명

PKI 에 기반한 전자 서명을 생성하기 위해서 사용자는 개인키(private key)와 공개키(public key)를 생성한다. 그리고 공개키는 인증 기관(Certificate Authority)이 서명하여 디렉토리에 저장된다. 메시지를 전자 서명하기 위해서는 먼저 해쉬 함수를 통해 해쉬 값을 생성한다. 해쉬 함수는 임의 길이의 메시지를 고정된 작은 크기의 값으로 변환하는 함수이다. 해쉬 값은 RSA[3]

* 본 논문은 2002 년도 중소기업청 산학연 컨소시엄 사업비를 지원받았음.

와 같은 공개키 암호 알고리즘과 사용자의 개인키를 이용하여 암호화되어 서명 값이 생성된다. 일반적으로 네트워크를 통해 서명을 전송할 때에는 원본 메시지, 송신자의 인증서, 서명 값 등을 함께 전송한다.

전자 서명을 확인하는 과정은 수신된 데이터에 있는 인증서를 이용하여 송신자의 공개키를 추출한다. 그리고 공개키를 통해 서명 값을 복호화하여 생성된 해쉬 값과 원본 메시지로부터 계산된 해쉬 값을 비교하여 전자 서명을 검증한다. 이 과정에서 송신자의 인증서가 유효 기간전에 폐기 되었는지의 유무를 파악하기 위해 CRL(Certificate Revocation List)[3]이나 OCSP(Online Certificate Status Protocol)[4]를 사용한다.

공개키 암호 알고리즘으로는 RSA, ECC 등이 존재하나 본 논문에서는 유선 환경에서 사용되는 전자서명 기법이 무선 환경에서 적합한지 유무를 검증하기 위해 RSA 알고리즘을 이용한다. 그리고 인증서는 X.509 인증서를 사용한다.

3. 전자 서명 시스템

3.1 응용 대상

본 논문에서는 전자 계약 혹은 약정서를 다루는 무선 인터넷 응용을 대상으로 하였다. 즉, 외판원이 PDA 를 가지고 고객을 방문하여 자동차 보험 계약이나 카드 발급, 혹은 기타 물품 구입 등을 시도하거나, 개인이 자신의 단말기를 이용하여 물건 구입, 영화 예매, 자동차 보험 가입 등의 행위를 하는 응용 시스템을 구체적인 대상으로 설정하였다.

3.2 시스템 구성

시스템은 그림 1 과 같이 콘텐츠 서버, 무선 단말기, 고객 컴퓨터, 관리자 컴퓨터로 구성된다.

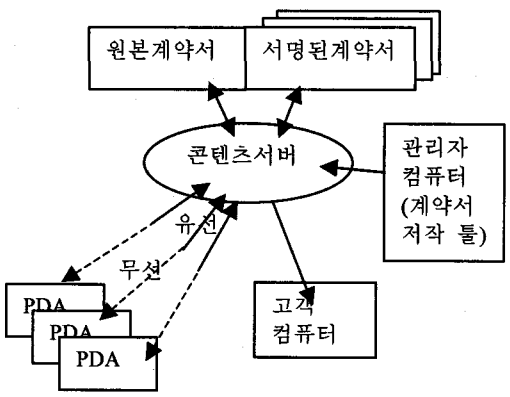

그림 1. 시스템 구성

무선 단말기로는 PDA 를 대상으로 하였으며, Compaq 3850, 3950 시리즈를 사용하였다. Compaq PDA 는 PocketPC 2002(WinCE 3.0)을 탑재하며, ME(Mobile Explorer)를 이용하여 무선으로 인터넷에 접속하도록 구성되었다. 그리고 전자 서명을 위해 WinCE 용 무선 보안 툴킷을 이용하였다. 계약서를 서명한 후에는 콘텐츠 서버에 업로드한다.

관리자 컴퓨터는 계약서 및 약정서를 작성하여 콘텐츠 서버에 업로드한다. 무선 단말기의 디스플레이 한계 및 호환성의 이유로 기존의 워드 파일들을 사용하기에는 어려움이 존재한다. 그러므로 본 논문에서는 XML 로 계약서나 약정서를 정의한다. 별도의 계약서 저작도구를 개발하여 무선 단말기 디스플레이의 픽셀 수를 고려하여 계약서를 저작할 수 있게 하였다.

콘텐츠 서버는 Window 2000 운영체제를 기반으로 IIS(Internet Information Server)를 설치하고 MS-SQL 서버를 이용하여 콘텐츠를 저장한다. 콘텐츠 서버가 관리하는 계약서는 원본 계약서와 서명된 계약서로 구분된다. 원본 계약서는 XML 계약서 저작도구를 이용하여 관리자에 의해 작성되며, PDA 에서 서명된 계약서는 콘텐츠 서버의 데이터베이스에 저장된다. 웹 페이지들은 JSP 로 인터페이스되며 JSP 컨테이너는 Tomcat 을 이용하였다.

고객 컴퓨터는 개인이 서명한 계약서를 확인하기 위해 사용된다. 고객은 자신의 계정으로 로그인한 후 서명한 계약서의 리스트 및 내용을 볼 수 있다.

3.3 시스템 동작

시스템의 각 요소들의 동작 과정은 다음과 같다.

(1) 시스템 관리자는 계약서 저작 툴을 이용하여 XML 형식으로 원본 계약서를 작성하여 콘텐츠 서버에 올려 놓는다.

(2) 계약서를 작성하고자 하는 개인 혹은 외판원은 PDA 에서 ME(Mobile Explorer)를 이용하여 무선 인터넷으로 콘텐츠 서버에 로그인하고 HTML 페이지를 다운 받는다. 브라우저는 HTML 에 명시된 ActiveX 를 로드한다.

(3) PDA 에 설치된 ActiveX 콘트롤이 XML 형식의 계약서를 다운로드 받은 후 해석하여 화면에 출력하고 사용자의 입력을 받는다.

(4) 사용자는 계약서나 약정서가 필요로 하는 내용을 채운 다음, 전자 서명 버튼을 클릭하여 전자 서명을 실행한다.

(5) 전자 서명된 계약서를 콘텐츠 서버로 전송한다.

(6) 콘텐츠 서버는 전자 서명된 계약서를 데이터베이스에 저장한다.

(7) 고객은 자신의 계약이 제대로 체결되었는지를 확인하기 위해 콘텐츠 서버에 접속하고 로그인한다.

(8) 고객은 콘텐츠 서버로부터 자신이 계약한 계약서나 약정서 리스트를 보고 확인하고자 하는 계약서를 선택한다.

(9) 콘텐츠 서버는 서명된 계약서를 출력하는 ActiveX 콘트롤을 고객 컴퓨터로 전송한다.

(10) 고객 컴퓨터 상에서 ActiveX 콘트롤은 서명된 계약서를 다운받고 이를 복호화하여 서명을 확인한 후 계약서를 출력한다.

3.4 E-Sign : PDA 모듈

PDA 에서 실행되는 모듈은 E-Sign 이라고 불리며, ATL 라이브러리를 이용하여 ActiveX 콘트롤로 구현되었다. PocketPC 2002 에서 ActiveX 는 웹 서버로부터 다운될 수 없기 때문에 E-Sign 은 미리 PDA 에 설치되어 있어야 한다.

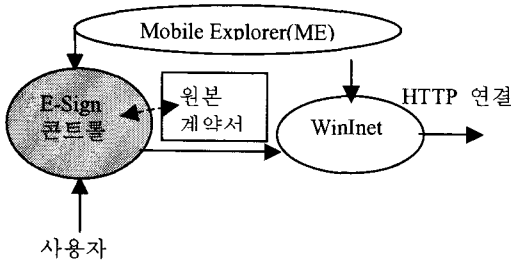

그림 2. E-Sign 콘트롤 및 PDA 실행 환경

그림 2 는 PDA 에서 실행되는 모듈 및 PDA 의 실행 환경을 보여 준다. 무선으로 서버에 연결하기 위해서는 기본적으로 ME 를 통한다. ME 는 컨텐츠 서버로 다음과 같은 HTML 코드를 로드한다.

```
<object width="xxx" height="yyy" classid="clsid:sssss">
<param name="FileName" value="con.xml">
</object>
```

ME 는 object 태그의 classid 에서 지정된 ActiveX 콘트롤(E-Sign)을 로드한다. E-Sign 이 로드된 후, ME 는 다시 <param> 태그에 지정된 FileName 프로퍼티 값 con.xml 을 E-Sign 에 전달한다. E-Sign 은 con.xml 을 콘텐츠 서버로부터 다운 받기 위해 HTTP 패킷을 생성하고 WinInet 라이브러리를 이용하여 콘텐츠 서버로부처 다운 받는다.

E-Sign 콘트롤은 XML DOM API 를 이용하여 con.xml 을 파싱한 후 PDA 에 출력하고 사용자로부터 필요한 정보를 입력하게 한다. 그리고 사용자가 서명 버튼을 클릭하면 전자 서명을 생성한다. 이 때 사용자가 입력한 데이터를 가진 계약서 정보를 다시 XML 데이터로 생성한 후 XML 데이터를 해쉬 및 암호화하여 전자 서명을 생성한다. 이 암호화 정보가 바로 서명 데이터이다. 마지막으로 XML 데이터, 서명 데이터, 사용자의 인증서 등을 묶어 서버로 업로드한다. 이때 WinInet 라이브러리를 이용한다.

3.5 E-SignDecoder: PC 모듈

E-SignDecoder 콘트롤은 ActiveX 콘트롤로서 서명된 계약서를 확인할 수 있는 콘트롤이다. 고객은 자신의 컴퓨터에서 콘텐츠 서버로 접속하여 로그인하며 언제든지 자신의 계약 사항을 확인할 수 있다. 또는 관리자가 컴퓨터에서 콘텐츠 서버에 접속하여 계약서에 서명된 전자 서명이 옳은 것인지 검증할 수 있다.

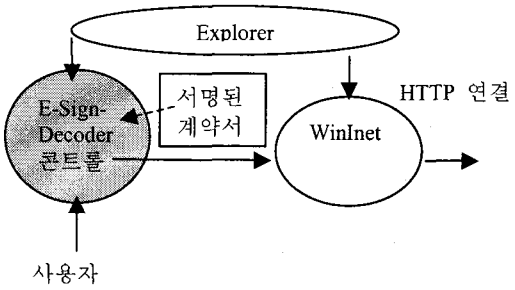

그림 3. E-SignDecoder 콘트롤 및 실행 환경

그림 3 은 개인용 PC 에서 고객 혹은 관리자가 서명된 계약서를 다운 받고 이를 복화화하여 계약 내용을 확인하는 환경을 보여준다. 콘텐츠 서버에 접속하여 확인하고자 하는 서명된 계약서를 클릭하면 웹 브라우저는 다음과 같은 형식의 HTML 문서를 서버로부터 받게 된다.

```
<object width="xxx" height="yyy" classid="clsid:ttttt"
        codebase="E-SignDecoder.cab">
<param name="FileName" value="con.sign">
</object>
```

E-SignDecoder 이 서명된 계약서를 받기까지는 E-Sign 콘트롤의 동작 과정과 동일하다. E-SignDecoder 콘트롤이 서명된 계약서(con.sign)를 받으면 이를 풀어서 전자 서명과 계약서 XML, 고객의 인증서로 분리한다. 그리고 전자 서명을 인증서 내의 공개키를 이용하여 복호화하여 얻은 해쉬 값을 추출한다. 그리고 계약서 XML 을 해쉬하여 해쉬 데이터를 생성한 다음 복호화된 해쉬 값과 비교한다. 서명이 확인되면 계약서 XML 을 해석하여 화면상에 계약서의 내용을 출력한다.

3.6 XML 계약서

MS 워드나 기타 편집기를 통해 생성된 문서는 크기와 호환성 문제로 PDA 등의 무선 단말기에 사용하기에는 무리가 있다. 그러므로 본 연구에서는 XML 문서를 생성하는 저작 도구를 개발하여 사용하였다. 표 1 은 계약서나 약정서에 제작시 사용된 XML Tag 를 보여주고 있다.

표 1. 모바일용 전자 계약서를 위한 XML 태그셋

XML 태그 이름	기능
contract	계약서 전체를 표현하는 태그

head	헤더 부분: title 태그를 포함
title	계약서 제목
form	계약서 내용, 여러개의 area 포함
area	한 페이지 정의: textlabel, input, datelabel, esignlabel 포함
textlabel	텍스트 스트링
input	사용자 입력 지정: 텍스트, 콤보 박스, 라디오 버튼 등
datelabel	날짜
esignlabel	전자서명 버튼

3.7 실행 결과

본 절에서는 전자서명 시스템을 실행한 결과를 보인다. 그림 4 는 계약서 저작 도구를 이용하여 자동차 매매 계약서를 작성하는 화면이다.

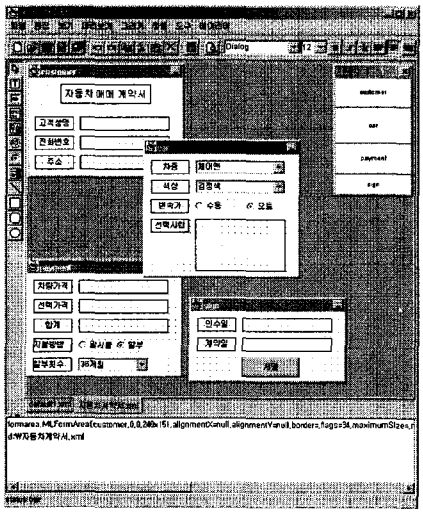

그림 4. 계약서 저작 도구를 사용하는 화면

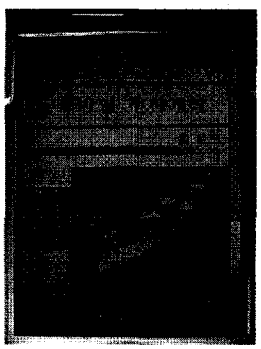

그림 5. PDA 에서 콘텐츠 서버에 접속한 화면

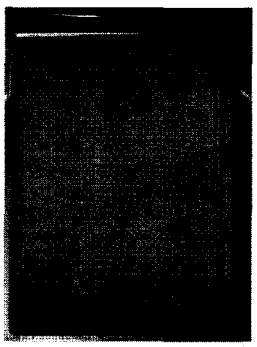

그림 6. E-Sign 콘트롤이 계약서를 출력한 화면

그림 5 는 PDA 에서 콘텐츠 서버에 접속하여 계약서 리스트를 출력한 화면이며, 그림 6 은 PDA 에서 자동차 매매 계약서를 선택한 경우 계약서를 다운로드 받아 화면에 출력하고 사용자로부터 입력을 받는 과정을 보이고 있다. 그림 7 은 고객이 자동차 매매 계약서를 출력한 화면이다.

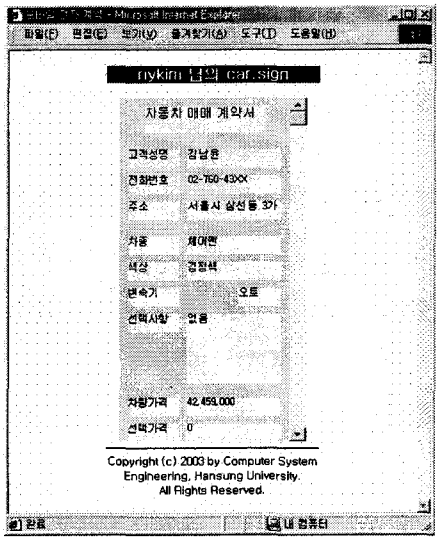

그림 7. E-SignDecoder 가 계약서를 출력한 화면

4. 결론

본 논문에서는 M-Commerce 를 위한 전자 서명 시스템의 구성 요소를 서술한 후 구축한 사례를 설명하였다. 전자 서명 시스템은 XML 계약서와 서명된 계약서를 관리하는 콘텐츠 서버, PDA 에서 전자 서명을 위한 모듈, 그리고 고객 혹은 관리자 PC 에서 전자 서명을 확인하고 계약 사항을 출력하는 모듈로 구성된다. 향후에는 무선 전자 서명 시스템의 성능을 분석하여 유무선 통합 환경에 적용할 수 있는 시스템을 설계할 계획이다.

참고문헌

[1] U. Varshney and R. Vetter, "A Framework for the Emerging Mobile Commerce Applications", Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[2] M. Branchaud, "A Survey of Public-Key Infrastructures", Master's thesis, McGill University, 1997.

[3] S. Burnett and S. Paine, *RSA Security's Official Guide to CryptoGraphy*, RSA Press, 2001

[4] R. Housley, W. Polk, W. Ford, and D. Solo, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile. RFC 2459, IETF, 1999.

[5] M. Myers, R. Ankney, etc., Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol-OCSP. RFC 2560, IETF, 1999.