이동거래를 위한 J2ME기반 전자서명 및 전자지불 시스템 설계 및 구현

이대하° , 김순자*
경 북 대 학 교 전 자 공 학 과
bigsum@palgong.knu.ac.kr , snjkim@ee.knu.ac.kr

Design and implementation of Digital signature and Payment system based J2ME for Mobile Commerce

Dae-Ha Lee° and Soon-Ja Kim*
School of Electronics and Electrical Eng., Kyungpook National University

요 약

J2ME(Java 2 Micro Edition)는 소비자/임베디드 디바이스 시장을 목표로 한 자바2 플랫폼으로서 이는 컨피규레이션(Configuration)과 프로파일(Profile)로 구성된다. CLDC/MIDP(Connected Limited Device Configuration / Mobile Information Device Profile)는 그 중에서도 휴대폰과 양방향 페이저 같은 제한된 메모리를 가진 장치 위에서 사용되는 플랫폼이다. 본 논문에서는 J2ME 기반 하에서 CLDC/MIDP를 이용하여 보안모듈을 작성하고 휴대폰에서도 안전한 전자서명 및 전자지불을 가능케 하여 Mobile Commerce의 기초를 이루었다. 여기서 서명은 XML가반으로 구성되었고, 시스템은 MIDlet으로 구현하였다.

1. 서 론

우리는 지금 메인 프레임의 시대에서 PC의 시대를 지나, 즉 포스트 PC의 시대로 가고 있다. 그리고 그 중심에는 모바일이라는 패러다임이 존재한다. 선(wire)으로부터 자유로운 통신의 시대가 도래한 것이다. 양방향 페이저, 셀룰러폰, 무선기능이 탑재된 PDA 등으로 대표되는 다양한 무선단말장치들은 기존의 데스크탑과 노트북으로 대표되는 컴퓨팅 환경에 커다란 혁명을 불러올 것이다.

이런 무선단말장치에서 제공되는 서비스는 크게 on-line서비스와 off-line서비스 두 가지로 나뉜다. on-line서비스는 기지국이나 다른 중간 매체에 연결하여 서비스를 받을 수 있는데, 항시 연결을 염두에 두어야 하므로 통화요금 문제나 연결이 되지 않을 경우 서비스를 받지 못한다는 점을 고려해야 한다. 그리고 보안문제에 있어서 on-line서비스는 기지국이나 중간매체에서 개인정보가 조작되거나 누출될 염려가 있다. off-line서비스는 개인단말장치 내에 서비스를 할 수 있는 모듈을 내장하여 서비스를 제공하는데, 필요할 때 언제나 이용할 수는 있지만, 단말장치의 자원, 즉 메모리의 제한으로 많은 서비스 모듈을 내장할 수 없고, 또 기능의 개선이나 추가를 위해서는 장치 내부의 변경이 불가피하게 된다. 이런 모듈을 하드웨어적인 방법이 아닌 소프트웨어적인 방법으로 제공한다면 다양한 서비스 제공 및 기능 개선이나 추가가 간편해질 것이다.

CLDC/MIDP(Connected Limited Device Configuration / Mobile Information Device Profile)는 자바가상머신을 휴대폰 상에서 사용할 수 있게 하는 자바플랫폼으로 이를 통하여 기존 off-line서비스의 문제점을 개선하고 ,비록 제한적이기는 하지만 자바의 여러 특성들을 휴대폰에서도 이용할 수 있게 된다. 예를 들어, 어떤 서비스를 필요로 할 때, 장치의 변경 없이 서비스 모듈들을 제공하는 서버로부터 필요한 모듈을 다운로드 받아, 자바가상머신으로 구동하여 서비스를 이용하면 된다. on-line서비스에서 염려되었던 개인정보 조작이나 누출은 off-line에서 보안서비스 모듈을 통해 해결할 수 있다.

본 논문에서는 CLDC/MIDP를 이용하여 보안모듈 및 이를 이용한 전자서명 및 전자지불 시스템을 설계 및 구현하였는데, 2장에서는 CLDC/MIDP와 KVM, 그리고 기본연산 모듈 및 XML서명 등에 대해 살펴보고, 3장에서는 전자서명 및 전자지불 시스템에 대해 논하고, 4장에서는 구현, 5장에서는 결론 및 고찰, 향후과제를 제시한다.

2. 기본개념

2.1 CLDC / MIDP

자바플랫폼은 크게 두 가지 요소, 즉, 자바가상머신과 클래스 라이브러리, 다른 말로 표준API 집합으로 구성된다. 그리고 이러한 자바플랫폼은 자바2 플랫폼으로 진화했고, 이는 또 J2EE(Java 2 Enterprise Edition), J2SE(Java 2 Standard Editon), J2ME(Java 2 Micro Edition) 라는 세 가지 영역으로 분할되었다. 이것은 각각 엔터프라이즈 서버시장, 데스크탑 시장, 소비자/임베디드 디바이스 시장을 목표로 한 역할 분담이었다. 이 중에서 J2ME는 컨피규레이션(Configuration)과 프로파일(Profile)로 분할된다. 여기서 컨피규레이션이란 자바 가상머신과 코어API 들에 대한 명세를 의미하고, 프로파일은 그 상위의 클래스 라이브러리, 즉, 표준 API들에 대한 명세를 의미한다. 이러한 개념적인 분할이 필요한 이유는 메모리 크기와 CPU 성능 등이 동일한 디바이스들의 집합을 하나로 묶어서 컨피규레이션을 정의하고, 이러한 컨피규레이션을 바탕으로 각 디바이스들의 기능, 혹은 버티컬(vertical) 시장의 요구사항에 맞추어 프로파일을 정의함으로써, 플랫폼의 통일성과 다양성을 동시에 만족시킬 수 있기 때문이다. 컨피규레이션에는 CDC(Connected Device Configuration)와 CLDC(Connected Limited Device Configuration)가 있는데 차이점은 메모리 용량에 관한 것이다. CLDC는 메모리가 제한된 환경, 즉 휴대폰이나 양방향 페이저 같은 기기에서 사용되고, CDC는 셋톱박스나 화상전화기 등과 같은 메모리 용량이 비교적 큰 기기에서 사용된다. CDC는 현재 JCP(Java Community Process)에서 표준화 진행 중에 있다. MIDP(Mobile Information Device Profile)는 무선단말기에서 사용되는 프로파일을 말한다[1].

2.2 KVM(Kilobyte Virtual Machine)

KVM은 작은 크기의 가상머신을 목표로 설계되었다. KVM의 K는 Kilobyte를 의미하는 것으로서, KVM의 디자인 목표가 킬로바이트 단위의 가상머신이었음을 나타낸다. KVM은 클래스 라이브러리를 모두 포함해서 최대 128K를 목표로 하고 있다. CLDC는 KVM을 기본 가상머신으로 채택하고, 거기에 코어 API에 대한 정의를 포함한 J2ME 컨피규레이션인 것이다. 따라서 KVM은 CLDC의 일부분이라고 생각해도 무방할 것이다[1,2].

2.3 기본연산 모듈

J2SE에서 제공되는 많은 클래스들이 J2ME에서는 제공되지 않으므로 필요한 모듈은 직접 만들어야 한다. J2SE에서 제공되던 BigInteger 클래스가 J2ME에서는 제공되지 않기 때문에 BigInteger 클래스가 제공하는 큰 정수연산 모듈을 별도로 구현해야만 한다. 기본적인 사칙연산 외에 제곱, 모듈, 멱승모듈 연산 등을 효율적인 알고리듬을 통해 구현하였다. 암호화 알고리듬에 많이 쓰이는 멱승모듈 연산은 계산량이 많으므로 속도개선을 위해 여러 가지 알고리듬이 사용된다. 본 논문에서는 속도향상을 위해 제곱연산과 모듈연산의 기본특성을 이용하였다. 제곱연산 알고리듬은 곱하기 연산 알고리듬의 절반 정도 연산횟수를 갖고 속도는 곱하기 연산보다 최대 2배 정도 빠르다. 멱승모듈 연산 알고리듬을 나타내면 표 1과 같다[3].

표 1에서의 연산횟수는 제곱연산이 (t+1)회, 곱하기 연산이 최대 (t+1)회, 모듈연산이 최대 2(t+1)회이다. 모듈연산은 나누기 연산을 이용하므로 그 속도는 나누기 연산과 같다. 나누기 연산은 다른 연산에 비해 몇 배 느리므로 모듈연산을 최소화하는 것이 속도향상을 위해선 필수적이다. 모듈연산의 기본특성 중에서

$$x \cdot y \bmod(n) = (x \bmod(n)) \cdot (y \bmod(n))$$

를 이용하여 적절한 횟수만큼 제곱연산과 곱하기 연산을 한 뒤 그 다음에 모듈연산을 하게되면 속도향상을 이룰 수 있게 된다. 본 논문에서는 제곱연산과 곱하기 연산을 6회 정도 한 뒤 모듈연산을 하도록 하고 있다.

표 1. 멱승모듈 연산 알고리듬

INPUT : $a \in Z_n$, and *integer* $0 \le k < n$, $k = \sum_{i=0} k2^i$

OUTPUT : $a^k \bmod n$

1. $A \leftarrow 1$
2. *For* i *from* t *down to* 0 *do the following* :
   2.1 $A \leftarrow A^2 \bmod(n)$
   2.2 *If* $k_i = 1$, *then* $A \leftarrow A \cdot a \bmod(n)$
3. *Return* (A)

2.4 전자 서명을 위한 XML 서명 요소

서명에 사용되는 XML 서명요소는 두 부분으로 나뉘는데, 첫 번째는 서명정보(SignedInfo)부분이고, 나머지 한 부분은 그 서명정보에 대한 서명값(Value)을 나타내는 부분이다. XML 서명요소에 대한 태그들을 나타내면 표 2와 같다[4,5].

표 2. 디지털 서명을 위한 XML 서명요소

```
<Signature>
 <SignedInfo>
  (CanonicalizationMethod)? 서명정보를 표준화하는 알고리듬
  (SignatureMethod)         표준화된 서명정보를 서명하는 알고리듬
  <Reference URI = ?>       서명될 데이터를 나타냄
    (Transforms)?           데이터를 해쉬하기 전에 표준화함
    (DigestMethod)          데이터를 해쉬하는 알고리듬
    (DigestValue)           해쉬된 데이터값
  </Reference>+
 </SignedInfo>
   (SignatureValue)         서명된 값
   (KeyInfo)?               공개키 값
</Signature>
```

3. 전자서명 및 전자지불 시스템

3.1 보안 모듈

본 논문에서는 CLDC/MIDP 기반 위에 MIDlet이라는 휴대폰 환경에 맞는 Application형태로 보안모듈을 개발하였다. 보안모듈에는 큰 정수연산을 담당하는 기본연산 모듈(Basic Module), 해쉬모듈(SHA), 대칭키 암호화 모듈(DES), 공개키 암호화 모듈(RSA) 등이 있다. 향후에는 타원곡선 알고리듬을 이용한 암호화 모듈을 올릴 예정이다. 타원곡선을 이용하게 되면 적은 키 길이로도 충분한 안전성을 얻을 수 있기 때문에 휴대폰과 같은 제한된 메

모리를 가진 기기에서는 꼭 필요하다. 보안모듈 구성은 그림 1과 같이 할 수 있다.

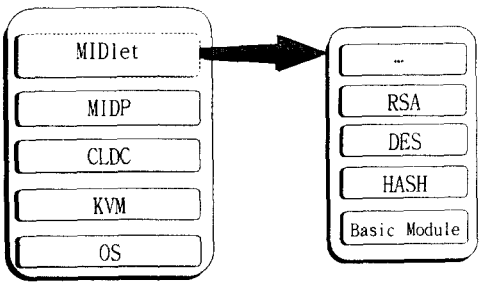

그림 1. 보안모듈

3.2 전자서명 시스템

휴대폰 상에서 자체적으로 공개키와 비밀키를 생성한 후 전자서명을 하고 그것을 다시 XML 서명 형태로 바꾼 다음 서명이 필요한 곳에 보내게 된다. 여기서 XML 서명은 XML의 특징인 구조성을 가지게 되어 좀더 명확하고 빠른 서명절차를 이룰 수 있게 된다. 그림 2는 전자서명 시스템을 나타낸다[6].

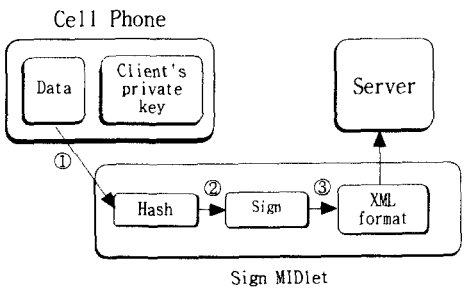

그림 2. J2ME기반 전자서명 시스템

3.3 전자지불 시스템

SET 지불 프로토콜을 이용하여 전자지불 시스템을 구축하였고 전체적인 트랜잭션은 8개로 축소하였다.
그림 3은 전자지불 시스템의 구성을 보이고 있고, 각각의 트랜잭션은 다음과 같다[7].
① 지불초기화 요구 ② 지불 초기화 응답 ③ 지불 요구 ④ 인증요구 ⑤ 인증응답 ⑥ 지불응답 ⑦ 대금지불 요구 ⑧ 대금지불 응답 .

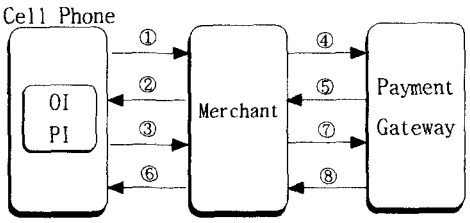

그림 3. J2ME 기반 전자지불 시스템

4. 구 현

두 시스템은 모토롤라의 MIDP 시뮬레이터를 이용해 구현하였으며, 웹서버로는 아파치 1.3.9를 사용하였다.
그림 4는 전자서명 구현이고, 그림 5는 전자지불 구현이다[8].

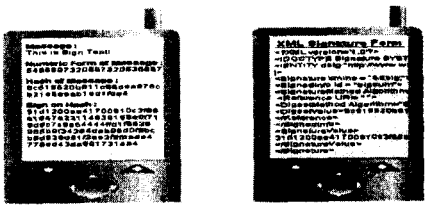

그림 4. 전자서명 구현

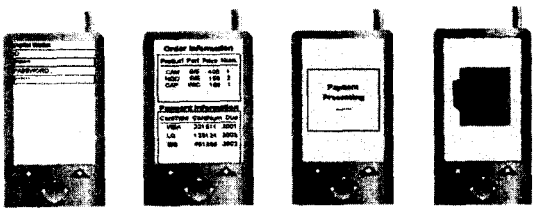

그림 5. 전자지불 구현

5. 결론 및 고찰

J2ME기반 하에서 보안모듈을 작성하고, 이를 이용한 전자서명 및 전자지불 시스템을 구축해본 결과 휴대폰으로 전자거래가 가능함을 알 수 있었으며, 나아가 Mobile Commerce의 가능성을 확인하였다. 향후에는 타원곡선을 이용한 보안모듈개발과 CDC기반의 전자 지불 프로토콜에 대한 연구가 이루어져야 할 것이다.

6. 참고문헌

[1] 배준현, "무선단말을 위한 자바플랫폼 : CLDC/MIDP" August, 2000, 마이크로소프트웨어
[2] Sun Microsystems "J2ME Technology for Creating Mobile Devices", May, 2000
[3] Alfred J.Menezes, "Handbook of Applied Cryptography" p596-597, p71,615
[4] Richard D. Brown, "Digital Signatures for XML", July 1998, http://www.ietf.org/internet-drafts/draft-ietf-xmldsig-signature-00.txt
[5] IETF W3C, "XML-Signature Core Syntax and Processing",2000, http://www.w3.org/TR/xmldsig-core/
[6] 이대하, "XML 표준전자문서의 Java 기반 서명 시스템 설계", 한국 정보과학회 2000 춘계학술발표 논문집(A) 제 27권 1호, pp. 475-477
[7] Visa/MasterCard, "Secure Electronic Transaction Specification", Version 1.0, 1997
[8] Motorola, "Motorola SDK Components for J2ME" Developer Edition, Drop #4, 2000