2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

IMT 2000에서의 USIM을 위한 구조 설계 및 응용 프로그램 구축에 관한 연구

하남수*, 홍인식*
*순천향대학교 정보기술공학부
e-mail:ha@cse.sch.ac.kr

A Study on Design of Structure and Construction of Application for USIM in IMT 2000

Nam-Su Ha*, In-Sik Hong*
*Division of Information Technology Engineering,
SoonChunHyang University

요약

제 3세대 이동통신인 IMT2000에서 단말기는 기존의 통신수단으로서의 역할과 함께 인증, 지불, 로열티 등 다양한 어플리케이션을 이용한 서비스를 가능하게 하는 수단이 될 것이다. 이것을 가능하게 하는 핵심요인은 USIM이라는 IC 카드가 단말기에 내장되기 때문이다. 본 논문에서는 USIM의 구조에 대한 관련 기술과 단말기와 USIM 사이의 프로토콜 형식 및 안전한 지불을 위한 Off-Line 결제 모델을 제안하였다. 제안한 모델은 하드웨어 자체의 제약으로 인해 적절한 크기의 어플리케이션 설계와 효율적인 프로토콜의 설계가 필요하다. 유효성을 입증하기 위해 관련표준을 고찰하였고 썬마이크로 시스템의 Java card 2.1.1 툴킷을 이용하여 시뮬레이션하였다.

1. 서론

IMT 2000 시스템에서는 지금의 GSM 방식에서 사용중인 SIM 카드가 더욱 발전되고 표준화된 형태인 USIM(Universal Subscriber Identity Module)으로 인하여 M-Commerce가 활성화될 것이다. 즉, M-Commerce의 핵심은 IMT 2000 단말기에 내장되는 USIM이다. USIM은 IC 카드의 일종으로 COS(Chip Operating System)라고 불리는 다양한 32비트 OS가 탑재되고, 64KByte의 저장공간을 갖는다. USIM과 단말기간의 통신은 APDU(Application Protocol Data Unit) 포맷을 이용한다. 현재 COS는 마스터 카드의 MULTOS, 비자카드의 OPEN FLATFORM, 썬 마이크로시스템의 Java Card, 마이크로소프트의 Windows for Smart Card 등이 존재한다. 본 논문은 차세대 COS라 불리는 Java Card에 기반을 두었다. 유효성을 입증하기 위해 제안한 Off-Line 결제 모델은 기존의 GSM 규격인 ISO 7816 스펙과 3GPP의 문서들을 기준으로 하였고, 썬 마이크로시스템의 Java Card 2.1.1 Tool Kit을 이용하여 소프트웨어적으로 시뮬레이션 하였다.

2. 관련기술

2.1 Java Card

Java 카드는 UIM 카드나 스마트 카드, 또는 메모리에 제한이 있는 장치들이 자바로 작성된 어플리케이션을 수행할 수 있도록 해준다. Java Card에 다운로드된 어플리케이션은 애플릿이라고 한다. Java 카드 기술은 자바 언어의 장점을 가지고 있는 안전하고 이식 가능한 그리고 멀티-어플리케이션이 가능한 플랫폼을 제공한다.

2.1.1 Java Card의 장점

Java Card 기술의 장점은 다음과 같다.

1) 어플리케이션 개발이 쉽다.
2) 보안성이 뛰어나다.
3) 하드웨어에 독립적이다.
4) 애플릿 방화벽으로 인해 여러 개의 응용 프로그램을 저장하고 관리할 수 있다.
5) 호환성이 뛰어나다.

2.1.2 Java Card 구조

1) Java Card 구성요소

- JVM(Java Virtual Machine): Java Card는 매우 제한된 메모리 상에서 자바 가상 머신을 구동하기 위해 가상 머신을 두 개로 분리한다. 즉, 하나는 카드의 외부에서 수행되고, 또 하나는 카드 내부에서 수행된다.
- JCRE(Java Card Runtime Environment)

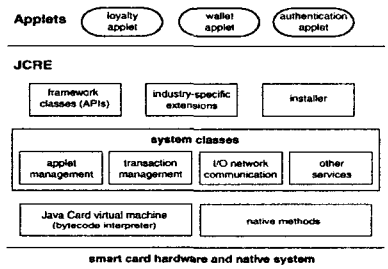


그림 1 Java Card Runtime Environment

- Java 카드 Installer & Off-카드 Installation 프로그램: Java 카드에서는 Installer라고 불리우는 모듈이 CAP 파일을 다운로드하고 설치하는 메카니즘을 가지고 있다. 또 카드안에서는 Java 카드 Installer가 수행되고 있어서 외부의 Off-카드 Installation 프로그램과 협력하여 CAP 파일의 다운로드와 설치를 한다.
- Java Card API: Java Card API에는 카드 어플리케이션을 작성하기 위한 자바 클래스와 패키지가 정의되어있다.

· java.lang: 자바 언어의 일부분만을 지원
· javacard.framework: JCRE와의 상호작용, APDU 전송 프로토콜 지원
· java.security: 암호화 키 생성, 난수 발생, 디지털 서명 생성, 메시지 축약
· javacardx.crypto: 암호화 기능을 위한 프레임워크 제공

2) 어플리케이션 식별자(AID)

Java Card에서는 각각의 애플릿 인스턴스들이 AID로 식별되고, 선택된다.

RID(5바이트)	PIX(0-11바이트)

ISO가 각 회사에 RID를 부여하고, 각 회사들은 PIX를 각각의 어플리케이션에 부여한다.

4) 애플릿의 개발과정

애플릿의 개발과정은 다음과 같다.

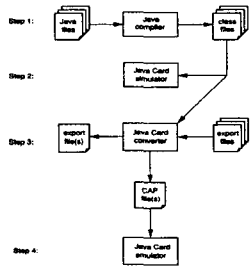


그림 2 애플릿 개발과정

2.2 USIM의 구조 및 설계

2.2.1 USIM

1) 전송 프로토콜

프로토콜이란 각각의 상이한 장비간에 오류없이 데이터를 전송하기 위한 규약을 의미한다. USIM과 터미널 사이에는 비동기식 반이중 통신 프로토콜을 사용한다. Transport Layer에서 Terminal과 USIM 사이에는 APDU 전송타입을 사용한다.(T=0, 1)

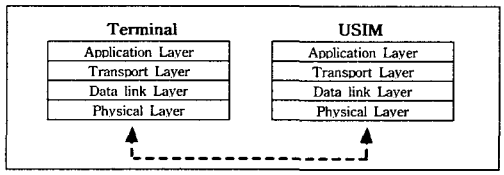


그림 3 전송 프로토콜

2) USIM의 Application의 구조

USIM에서의 파일 시스템은 다음과 같다.

MF(Master File) : 파일 시스템의 루트
DF(Dedicated File) : 디렉토리 파일
EF(Elementary File) : 데이터 파일

3) Command와 Response의 구조

- Command APDU의 구조

Code	Length	Description	Grouping
CLA	1	Class of instruction	Header
INS	1	Instruction code	
P1	1	Instruction parameter 1	
P2	1	Instruction parameter 2	
Lc	0 or 1	Number of byte in the command data field	Body
Data	Lc	Command data string	
Le	0 or 1	Maximum number of data bytes expected in response of the command	

Case	Structure
1	CLA INS P1 P2
2	CLA INS P1 P2 Le
3	CLA INS P1 P2 Lc Data
4	CLA INS P1 P2 Lc Data Le

- Response APDU Structure

APDU는 data field와 2byte의 명령어 상태를 나타내는 field로 구성된다. 다음은 주요 Response 명령어 형식의 예이다.

Code	Length	Description
Data	Lr	Response data string
SW1	1	Status byte 1
SW2	1	Status byte 2

· Normal processing

SW1	SW2	Description
'90'	'00'	정상 종료
'91'	'XX'	Proactive command 요청

4) USIM Application Toolkit(USAT)

USAT는 USIM Application Toolkit의 약자로서 네트워크를 통한 어플리케이션 서버와의 트랜잭션을 수행하고, USIM 카드의 Proactive Command에 의하여 단말기에 메뉴를 표시할 수 있다.

- Proactive command: USAT를 사용함으로써 USIM에 어플리케이션을 실행할 수 있는 기능을 추가하게 되었다. 즉, 과거의 종속적인 개념에서 벗어나 USIM은 어플리케이션의 드라이버로서 사용자, Mobile, Network의 명령어가 시작되는 것이다.

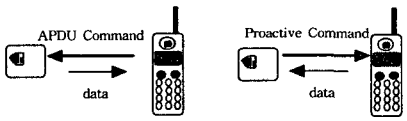


그림 4 USAT 명령어 체계

3. Off-Line 결제 모델 설계

본 장에서는 Off-Line 결제가 가능한 모델에 따라 전자지갑 어플리케이션이 포함된 USIM을 설계하였다.

3.1 USIM 카드에 내장되는 데이터

USIM에 내장되어야 하는 필수 데이터들은 USIM 내의 EEPROM 에 저장된다. USIM에서 EEPROM의 용량은 64K로 가정한다. 64K 중에서 16K는 Java Virtual Machine에 할당되고 나머지 부분이 실질적인 데이터 저장 역할을 하게된다. 용량 문제로 인한 데이터 크기가 시스템 구현의 제약요소가 된다.

3.2 USIM에서의 상호 인증

USIM의 애플리케이션과 상점과는 인증서를 교환하여 서로 검증함으로써 상대방을 인증한다. 데이터 인증은 USIM 내부의 데이터의 인증을 위하여 단말기를 통하여 상점의 터미널에서 이루어진다. 공개키 기법에 기반을 둔 디지털 서명을 이용하여 USIM의 개인화(personalization) 후의 부정한 데이터의 변조를 감지한다.

3.3 USIM에서의 암호화

상점의 컴퓨터와 연결되면 먼저 암호화 방법에 대하여 협상을 시작한다. 즉 암호화 방법, 트랜잭션 카운터, 난수 등의 정보를 교환한 다음, 서로 인증서를 교환하고, USIM 어플리케이션이 자신의 Master Key를 공개키 알고리즘으로 암호화하여 상점의 터미널로 보낸다. 상점의 터미널은 USIM의 공개키로 이를 해독하여 Master Key를 알 수 있고 이 Master Key를 이용하여 미리 정해진 알고리즘에 따라 USIM Write Key, Terminal Write Key, USIM MAC Write Key, Terminal MAC Write Key를 생성한다. 데이터의 무결성과 송신자의 인증은 MAC(Message Authentication Code)로 구현할 수 있다.

3.4 전자지갑 프로그램에서 필요한 APDU 집합

전자지갑에서 기본적으로 지원해야하는 APDU 명령어들은 다음과 같다.

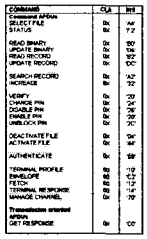


그림 5 전자지갑 프로그램에서 지원되어야 할 APDU 집합

3.5 시뮬레이션에 사용될 전자지갑 프로그램의 구성요소

본 장에서는 시뮬레이션에 사용되는 전자지갑 프로그램의 구성요소와 루틴은 다음과 같다.

1) 전자 지불이나 충전 과정에서 일시적으로 저장되는 정보들
2) 전자 지갑에서 필요한 파일들
3) Complete Parameter Update C-APDU를 위한 TLV 레코드 태그들
4) 초기화 루틴
5) SELECT 루틴
6) DESELECT 루틴
7) 각종 APDU 명령어 처리 루틴
8) INITIALIZE_TRANSACTION 루틴

9) COMPLETE_TRANSACTION 루틴
10) INITIALIZE_UPDATE 루틴
11) COMPLETE_UPDATE 루틴
12) VERIFY_PIN 루틴

4. 시뮬레이션

본 장에서는 앞장에서 설계한 Off-line 결제 모델의 유효성을 검증하기 위하여 지불 시스템의 각 부분들을 소프트웨어로 시뮬레이션 하였다. 시뮬레이션 도구로서는 JC 2.1.1 Tool kit을 사용하였고, IDE로서는 JBuilder3을 사용하였다.

4.1 시뮬레이션 시스템 구성도

시뮬레이션은 순수하게 소프트웨어로만 이루어진다. 즉, USIM 이나 단말기, 상점의 컴퓨터(CAD) 등이 소프트웨어로 구현되고, TCP/IP 통신을 이용하여 데이터를 주고받고, 단말기 위주로 시뮬레이션 하였다.

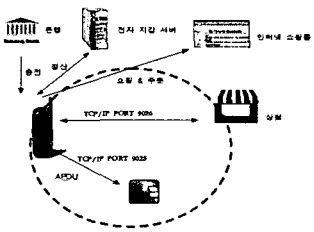


그림 6 시뮬레이션 구성도

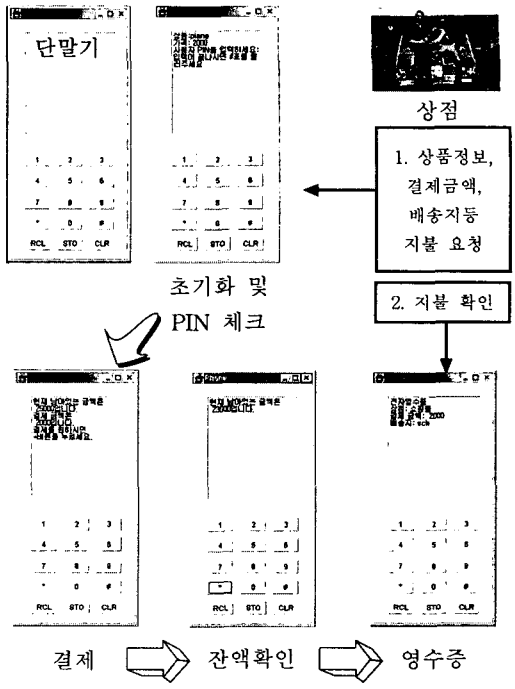
4.2 Off-line 지불 시뮬레이션 시나리오

상점의 컴퓨터는 전화번호나 BLUETOOTH를 이용하여 단말기에 결제를 요청한다. 단말기는 결제에 필요한 초기화를 시작한다. 상점의 컴퓨터와 서로 인증서를 교환한다. 인증서의 공개키를 이용하여 암호화된 Session Key를 발생시킬 수 있는 Master Key 데이터를 서로 교환한다. Session Key에 대하여 일치가 되면 이 Session 키를 이용하여 모든 데이터를 암호화한다.

4.3 Off-line 지불 시뮬레이션 흐름도

PowerOn->단말기, 카드간 인증->GlobalPIN 체크->AppPIN체크->상점접속->인증서교환->구매요청->구매정보 전송받음->잔고체크->구매확인->영수증 전송받음

4.4. Off-Line 지불 시뮬레이션



5. 결론

제 3세대 이동통신인 IMT 2000은 이동통신의 역할 뿐만아니라 각종 서비스를 제공할 것이다. 이것을 가능하게 하는 핵심요인은 단말기에 내장되는 USIM이다. USIM으로 인해 개인 인증이 가능하고 이러한 인증 정보를 바탕으로 각종 서비스가 가능하여 다양한 수익모델이 발생할 것이다. 그리고 현재 스마트 카드의 제약조건인 별도의 장치가 필요하지 않아 M-COMMERCE가 활성화 될 것이다. 본 논문에서는 Java Card를 기반으로 하여 USIM이라는 핵심구조에 대하여 고찰해보았고, 소프트웨어적으로 시뮬레이션하여 검증하였다.

참고문헌

[1] Chen "Java Card Technology for Smart Cards" Addison Wesley 2000
[2] S.Brands "Off-Line Cash Transfer by Smart Cards" CWI'1994
[3] J.Bos and D.Chaum "Smart Cash: a practical electronic payment system" Technical Report CS-R9035 CWI'1990
[4] T. Trans and R. Cohen "Hybrid Recommender Systems for Electronic Commerce"
[5] Ivor Horton "Beginning Java2" . WROX