

# 전자지불 시스템을 위한 스마트카드 에뮬레이터의 설계와 구현

김애영, 용승림, 이상호  
이화여자대학교 컴퓨터학과  
e-mail:{kay, dragon, shlee}@ewha.ac.kr

## Design and Implementation of a Smart Card Emulator for Electronic Payment System

Ae-Young Kim, Seung-Lim Yong, Sang-Ho Lee  
Dept. of Computer Science and Engineering, Ewha Womans  
University

### 요 약

네트워크의 발달과 전자상거래의 급속한 성장은 전자정보를 이용하는 다양한 형태의 지불수단을 등장시켰고, 그 다양한 지불수단들은 급속도로 개발되고 있다. 특히 스마트카드는 보안성이 상당히 높고 대용량의 데이터 저장에 가능하기 때문에 전자지불수단을 위한 매개체로 주목을 받고 있다. 그러나 현재의 스마트카드 관련 개발 환경은 개발비용이 상대적으로 높고 개발한 프로토콜이나 시스템의 안전성 및 효율성 등을 실험하기가 어려우며 개인 컴퓨터환경에서 응용 서비스를 개발하기가 어렵다는 취약점이 있다. 따라서 이러한 취약점을 해결할 수 있는 응용 프로그램의 개발이 필요하다. 본 논문에서는 추가적인 하드웨어의 확장 없이 보유하고 있는 컴퓨터 환경에서 전자지불 시스템을 위한 응용 서비스를 적용하고 테스트할 수 있는 스마트카드 에뮬레이터를 설계하고 구현하였다.

### 1. 서론

네트워크라는 특수한 공간 속에서 전자화폐와 같이 전자정보를 이용하는 다양한 형태의 지불수단이 등장하였다. 이러한 금융권의 전자화 체제로의 전환은 기존의 마그네틱선 카드를 이용한 지불시스템을 대신하여 다양한 전자지불 방식을 수용할 수 있고 보안성을 더욱 높일 수 있는 새로운 매개체를 필요로 한다. 현재의 마그네틱선 카드를 이용한 결제방식으로는 취약한 보안성, 한계 있는 데이터 저장량, 쉬운 카드 위·변조 등과 같은 문제로 인해 전자상거래 참여자에게 다양한 서비스를 제공하는 것이 불가능하기 때문이다. 이 문제를 해결하기 위한 대안으로 요즘 주목받고 있는 매개체의 하나가 바로 스마트카드이다. 더욱이 스마트카드는 모바일 폰과 같은 무선환경에서도 지불을 위한 매개체로서의 역할 수행이 가능하다.

그러나 스마트카드는 새로 개발한 응용 서비스

의 안전성이나 효율성 등을 테스트하기가 어렵고 기존 카드에 새로운 응용 서비스를 추가하기가 어려우며 개발비용이 상대적으로 높다. 또한 개인 컴퓨터 환경에서 응용 서비스를 개발하기가 어렵다는 문제점도 있다. 따라서 이러한 문제를 해결할 수 있는 응용 프로그램이 필요하다.

본 논문에서는 가상 카드 터미널과 가상 스마트카드와 같은 개념의 도입으로 하드웨어의 추가 없이 보유하고 있는 컴퓨터 환경의 프로세서, 메인 메모리, 또는 디스크 매체 등을 이용하여 스마트카드 에뮬레이터를 설계하고 구현하였다. 구현된 에뮬레이터는 새로 개발한 응용 서비스 모듈의 안전성 또는 효율성을 쉽게 테스트할 수 있으며 개발에 필요한 비용, 시간, 인적노력 등을 줄이는 효과를 가져온다.

### 2. 스마트카드 기반의 전자지불 시스템

스마트카드는 플라스틱 카드에 IC(Integrated

Circuit) 칩이 내장되어있는 전자식 카드이다. 스마트카드의 데이터 저장은 파일 시스템을 통해 이루어진다. 스마트카드의 파일 시스템은 트리 형태의 계층 구조로 구성되어 EEPROM에 안전하게 저장된다. 저장된 데이터 중에서 직불, 신용, 전자화폐, 인증서와 같은 특정 응용이나 서비스와 관련된 전용 파일은 요소파일들의 기능적인 그룹으로 이루어지며 각 파일은 접근 가능 조건을 다르게 유지하여 보안성을 높인다[5,7].

스마트카드는 화폐와 관련된 가치 및 정보를 담는 매개체로서 지불시스템에 적용시킬 수 있으며 스마트카드를 기반으로 한 전자지불 시스템은 대면 상거래나 전자상거래와 같은 비대면 상거래에서 모두 활용 가능하고 다양한 부가 서비스가 가능하며 스마트카드의 물리적 안정성에 근거하여 화폐의 안전성을 보증한다.

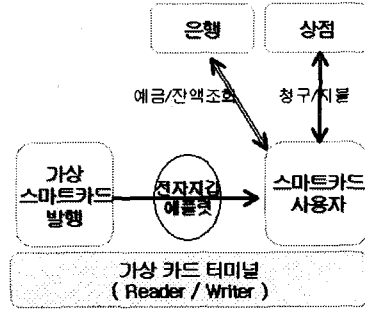
스마트카드 기반의 전자지불 시스템의 흐름은 스마트카드 및 카드 터미널, 응용 서비스 등에 따라서 다소 차이가 있으나 본 설계에서는 기본적인 흐름을 따른다. 전자지불 시스템에 참여하는 객체는 발행기관, 스마트카드, 카드 터미널, 사용자, 상점, 그리고 은행이다. 사용자는 발행기관을 통해서 발급 받은 스마트카드에 연계되어있는 은행의 계좌로부터 원하는 금액을 전자화폐로 인출 받아 충전한다. 그리고 상점에서 구입한 물품에 대하여 요구된 금액을 스마트카드의 전자화폐로 지불하기 위해서는 비밀번호의 입력 및 검증, 공개키 검사, 서명 검사 등의 보안 절차를 거쳐야하며, 그 이후에 요구액에 해당하는 전자화폐 인출을 처리하고 전자화폐의 잔액 정보를 갱신한다. 이러한 모든 흐름 및 정보교환은 카드 터미널을 통하여 이루어진다.

### 3. 전자지불 시스템을 위한 스마트카드 에뮬레이터의 설계

본 장에서는 새롭게 설계된 전자지불 시스템을 위한 스마트카드 에뮬레이터의 전체 구성과 시스템의 설계를 위한 기반 환경을 살펴본 후 전자지불 시스템의 구성요소를 살펴본다.

#### 3.1 전체 시스템 구성 및 환경

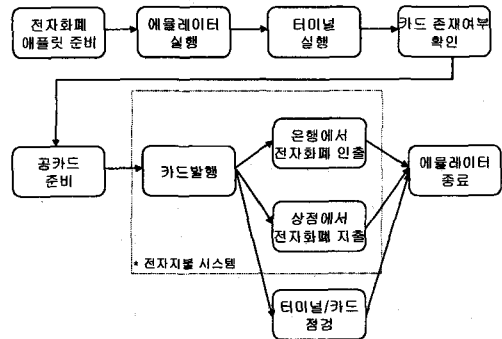
본 논문에서 설계된 스마트카드 에뮬레이터에 적용된 전자지불 시스템의 참여자는 [그림 3.1]과 같이 가상 카드 터미널, 가상 스마트카드, 스마트카드 소유자, 은행 그리고 상점이다.



[그림 3.1] 에뮬레이터의 전체 구성

가상 카드 터미널은 가상 스마트카드와의 통신을 처리하며 가상 스마트카드에는 전자지불 시스템의 응용 서비스인 전자지갑 애플릿을 탑재하여 전자화폐와 같은 화폐가치를 저장한다. 은행은 사용자가 자신의 계좌 잔액을 조회하여 전자화폐로 인출할 수 있는 범위를 확인하고 잔액 내에서 전자화폐를 인출하도록 하는 기관이다. 상점은 사용자가 잔액이 충분한 스마트카드를 사용하여 물품을 구매 및 지불할 수 있는 곳이다.

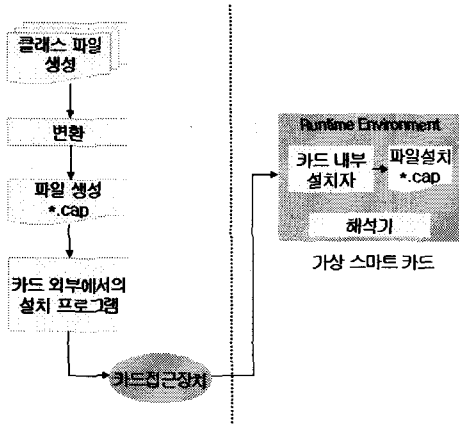
각 참여자들이 상호 작용하는 전자지불 시스템을 위한 스마트카드 에뮬레이터는 [그림 3.2]와 같은 흐름을 따라 운용된다.



[그림 3.2] 에뮬레이터의 전체 흐름도

전자지불 시스템에 적용시킬 스마트카드의 개발을 위해서는 카드 터미널과 개발된 응용 서비스를 탑재할 스마트카드와 같은 하드웨어적인 확장이 필요하다. 그러나 본 절에서는 하드웨어의 확장 없이 개인 컴퓨터 환경에서 해결할 수 있는 가상 카드 터미널과 이 가상 카드 터미널과 직접적으로 관련이

있는 가상 스마트카드가 전체 시스템의 기본 환경이 된다. 가상 카드 터미널은 플로피디스크 드라이브를 사용하며 설계된 가상 스마트카드는 물리적인 스마트카드의 카드부분, 입출력장치, ROM과 RAM, 프로세서 등은 제외하고 EEPROM부분의 기능을 플로피디스크에서 수행하도록 한다. 이중에서 카드의 발행은 가상 스마트카드의 생성이며, 자세한 흐름은 [그림 3.3]과 같다.



[그림 3.3] 가상 스마트카드의 생성 과정

이 흐름은 자바 API를 기반으로 하는 실제 스마트카드의 생성 시 애플릿이 탑재되는 흐름과 동일하다. 다만 본 설계에서는 개인 컴퓨터 환경을 이용하기 위하여 애플릿이 탑재되는 카드부분을 실제 카드가 아닌 플로피디스크로 대체하였다. 본 설계에 따르면 플로피디스크에 전자지갑과 같은 자바코드 모듈을 변환시킨 \*.cap 파일이 탑재된 가상 스마트카드로 전자지불 시스템의 흐름에 대하여 시뮬레이션 및 파일 구조를 확인하도록 한다.

### 3.2 전자지불 시스템

[그림 3.2]에서 보는바와 같이 은행 및 상점은 가상 스마트카드와 잔액조회, 인출, 지불 등의 프로토콜을 수행한다. 스마트카드기반의 전자지불 시스템에서 은행의 주요 기능은 전자화폐의 인출이다. 가상 스마트카드 측면에서 은행으로부터의 인출은 가상 카드 터미널을 통하여 전자화폐의 가치를 저장하는 것이다. 상점의 주요 기능은 구매이며 스마트카드 소유자가 상점에서 구입한 물품의 청구액만큼 가상 스마트카드 내에 있는 전자화폐를 지불한다. 구매거래는 전자지불 시스템 내에서 가장 빈번하게 발

생하고 상점의 터미널이 안전한 장비라는 보장이 없기 때문에 상점의 보안모듈과 스마트카드간의 상호인증 및 거래에 대한 서명을 필요로 한다. 스마트카드용 응용 프로그램을 자바 카드에서는 애플릿이라고 하는데, 본 논문에서도 동일하게 적용하여 전자지불 시스템에 사용되는 방법의 하나인 전자지갑을 애플릿으로 구성한다.

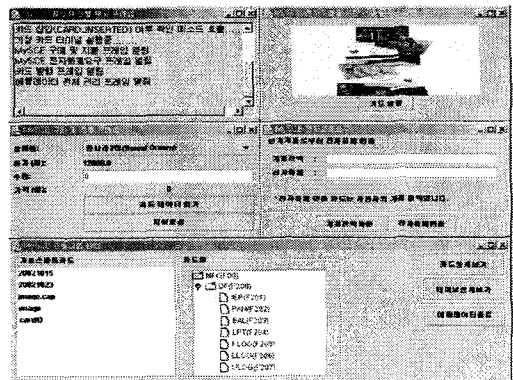
가상 스마트카드 내에 탑재될 전자지갑 애플릿의 파일 구조는 국내 금융결제원에서 제정한 표준을 따른다. 다른 애플릿과 마찬가지로 루트인 마스터파일의 하부계층으로 전자지갑 전용파일이 형성되고 세부적인 기능인 전자화폐 정보파일, 주계좌 정보파일, 전자화폐 잔액파일, 그리고 마지막 구매 거래내역 파일 등과 같은 요소파일이 전용파일 밑으로 생성된다.

가상 카드 터미널과 가상 스마트카드가 적용된 전자지불 시스템의 흐름은 실제적인 전자지불 시스템의 흐름과 유사하다. 다만 가상터미널을 구성할 수 있는 OCF(Open Card Framework)의 API가 기반이 되고 있기 때문에, 스마트카드와 관련된 물리적인 장비의 필요 없이 각 참여자간의 프로토콜이 이루어진다.

### 4. 전자지불 시스템을 위한 스마트카드 에뮬레이터의 구현 및 결과

에뮬레이터의 구현은 윈도우2000에서 JDK1.4를 기반으로 자바 프로그래밍을 돕는 가와(Kawa), GUI를 제공하는 스윙(SWING) 등을 이용하였다.

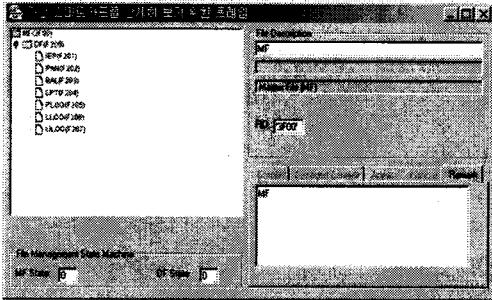
구현된 에뮬레이터의 초기 프레임 상태는 [그림 4.1]과 같다.



[그림 4.1] 에뮬레이터의 초기 프레임

본 에뮬레이터에서는 가상 카드터미널 환경이 구동된 후 생성되는 모든 진행 상황을 진행보고 프레임틀을 통하여 메시지로 확인하며, 카드발행 프레임에서 미리 구성해놓은 전자지갑과 같은 애플릿을 탑재한 가상 스마트카드를 발행 받는다. 발행 받은 카드에 연계된 계좌로부터 전자화폐를 인출 받아 저장시키고, 그 전자화폐는 구매 및 지불 프레임에서 구매한 아이টে 대해 지불하는데 사용한다.

[그림 4.1]의 하단에 있는 전체 관리 프레임에서는 카드상세보기 버튼을 통하여 [그림 4.2]와 같은 가상 스마트카드 프레임을 연다. 실험대상의 애플릿에 대한 실험 및 확인은 해당 애플릿을 탑재한 가상 스마트카드를 발행한 후 본 프레임에서 파일 구조를 파악하고 각 파일의 정보를 확인함으로써 가능하다.



[그림 4.2] 에뮬레이터의 가상 스마트카드 상태

### 5. 결론 및 향후 연구과제

전자 미디어의 하나인 스마트카드는 급성장하는 전자지불 시스템 개발 분야에서 아주 적합한 매개체로 주목받고 있다. 스마트카드 기반의 전자지불 시스템의 개발은 전자적 거래에 의존하고 있는 모든 경제 활동의 안전성과 효율성을 높인다. 그러나 전자지불 시스템을 위한 응용 서비스는 관련 장비가 고가이고, 개발 기간이 길고, 테스트하기가 쉽지 않고, 개발비용이 높다는 점에서 개발이 쉽지 않다. 따라서 이러한 문제를 해결할 수 있는 응용 서비스 개발을 위한 응용 프로그램 또는 응용 시스템이 필요하다.

본 논문에서 설계 및 구현한 전자지불 시스템을 위한 스마트카드 에뮬레이터는 추가적인 하드웨어의 확장 없이 개인 컴퓨터에서 전자지갑과 같은 응용 서비스를 포함하는 전자지불 시스템을 구성하거나 실험하는 것이 용이하며 응용 서비스 개발의 효율성

을 높이고 개발비용을 감소시킨다. 따라서 본 에뮬레이터는 전자화폐 및 전자지갑과 같은 전자지불 시스템을 위한 응용 서비스 개발 및 연구에 유용하게 사용될 수 있다.

향후 연구과제로는 구현된 에뮬레이터의 구현시 설계 및 보안상의 문제점은 없는지 살펴보는 것과 전자지갑과 같은 애플릿을 수정할 때에는 별도의 자바 에디터를 사용해야하나 에뮬레이터 안에서 간편하게 수정하고 구성할 수 있도록 하는 환경을 제공하는 스마트카드 에디터를 설계하고 개발하는 것이다.

### 참고문헌

- [1] J. Borst, B. Preneel and V. Rijmen, "Cryptography on Smart Cards," Computer Networks, Vol. 36, pp.423-435, 2001.
- [2] S. Brands, "Off-Line Cash Transfer by Smart Cards," CS-R9455, MIT Press, 1994.
- [3] Z. Chen, *Java Card Technology for Smart Cards : Architecture and Programmer's guide*, Addison-Wesley, 2000.
- [4] H. Dreifus and J. T. Monk, *Smart Cards: A Guide to Building and Managing Smart Card Applications*, John Wiley & Sons, pp.121-214, 1998.
- [5] W. Rankl and W. Effing, *Smart Card Handbook*, John Wiley & Sons Inc., 2000.
- [6] Open Card Consortium, "OpenCard Framework 1.2 Programmer's Guide, IBM," 1999.
- [7] 금융결제원, "금융IC카드 표준", 금융결제원, 2000.
- [8] 김영진, 전용성, 전성익, 정교일, "Java Card Platform을 내장한 Smart Card의 구현", 정보과학회지, pp.33-43, 2001.
- [9] 이윤철, "전세계 카드 기술 및 시장 동향", ETRI, 2002.
- [10] 한국정보보호진흥원, "스마트카드 기술개발 동향", KISA, 1999.