

# SCMS 기반의 스마트카드 후발급 인터페이스의 설계

조재훈\*, 박우전\*\*  
한남대학교 컴퓨터공학과  
cjh553@hotmail.com\* wjpark@ce.hannam.ac.kr\*\*

## Design of Smart Card Post Issuance Interface based on Smart Card Management System

Cho, Jae-Hun\* and Park, Woo-Jun\*\*  
Dept. of Computer Engineering, Hannam University

### 요 약

개방형 카드 플랫폼의 개발로 전통적인 카드 플랫폼 모델의 문제점을 해결할 수 있었으나 기존 카드 관리시스템으로 개방형 카드 플랫폼을 관리 할 수 없었고 그 대안 시스템으로 SCMS가 개발되었다. SCMS가 개방형 카드 플랫폼에 있어 통합 관리를 수행하지만 주요 기능인 카드 후발급에 대한 효과적인 인터페이스를 가지고 있지 못하다. 본 논문에서는 스마트카드 관리시스템을 이용하여 효과적인 카드 후발급을 위한 카드 후발급 인터페이스를 설계하였다.

### 1. 서론

자바 카드와 같은 개방형 카드 플랫폼이 개발되기 이전의 전통적인 카드 플랫폼은 자기 띠(Magnetic Stripe) 형태의 정보 저장 매체를 사용함에 따라 전자화폐, 의료카드 등과 같은 제한된 저장 용량의 카드에 한 가지 애플리케이션만을 탑재하여 사용할 수 밖에 없었다. 이는 자기 띠 형태의 정보 저장 매체의 정보 저장 능력의 한계로 저장되는 정보가 사용자의 기본 정보 및 신용 카드 번호, 비밀번호 등과 같은 사용자 중심의 정보를 저장하는 것에 국한되어 다양한 기능을 제공할 수 있는 새로운 카드 애플리케이션의 개발을 어렵게 하였다. 이러한 결과로 인해 새로운 애플리케이션이 개발될 때마다 새로운 카드 발급시스템이 요구됨으로써 카드제조 환경이 표준화되지 못하였고 이로 인해 사업자들은 많은 혼란을 겪었다. 이러한 문제를 해결하기 위해 개방형 카드 플랫폼이 개발되었다. 개방형 카드 플랫폼은 IC칩을 이용하여 정보 저장 공간을 확장하였기에 한 장의 카드에 다양한 애플리케이션을 탑재하여 사

용할 수 있다. 개방형 카드 플랫폼이 지원하는 기능 중에 하나가 카드 후발급(Post-Issuance)이다. 카드 후발급은 카드 발급기관을 통해 발급받은 카드를 사용하던 카드 사용자가 새로운 카드 애플리케이션을 제공하는 발급기관에 인터넷 등과 같은 통신매체를 통해 접속하여 기존 카드에 애플리케이션을 추가로 탑재하거나 기존 애플리케이션을 카드에서 삭제하여 카드를 재사용하는 것을 말한다. 이와 같은 기능의 개방형 카드 플랫폼을 관리하기 위해서는 기존 카드 관리시스템과는 다른 대안 시스템이 필요하였다. 이를 충족하는 시스템으로 스마트카드 관리시스템(SCMS : Smart Card Management System) 기술이 개발되었다. 본 논문에서는 개방형 카드 플랫폼을 관리할 수 있는 SCMS 기술을 이용하여 카드 후발급 인터페이스 설계에 대해 기술한다. 2장에서 SCMS의 정의와 기능 및 구조에 대해 논하고, 3장에서 SCMS를 이용하여 카드 후발급 인터페이스 설계에 대한 내용을 기술하며, 4장에서 결론과 향후 과제에 대해 기술한다.

## 2. 스마트카드 관리시스템

본 장에서는 스마트카드 관리시스템에 대해 알아보고 스마트카드 관리 시스템이 지니고 있는 기능과 구조에 대해 기술한다.

### 2.1 스마트카드 관리시스템 정의 및 기능

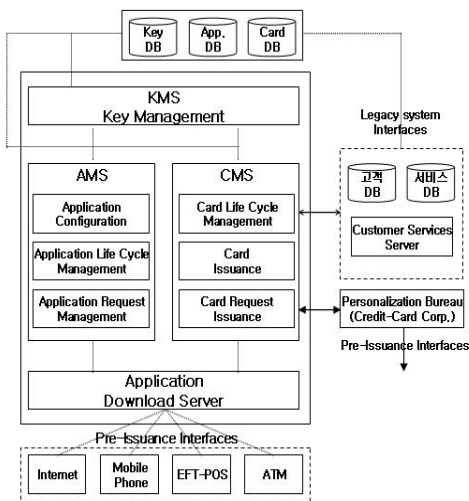
스마트카드 관리시스템(SCMS : Smart Card Management System)은 개방형 카드 플랫폼 기반에서, 특정 카드나 애플리케이션에 종속되지 않고, 스마트카드의 선발급, 후발급 및 모든 관리가 가능하도록 하는 기능을 갖추어야 한다. 스마트카드 관리시스템은 개방형 카드 플랫폼 기반으로 발급된 스마트카드를 안전하고, 효율적으로 관리해주는 시스템으로 다음의 기능들을 지니고 있다.

- 카드 및 애플리케이션 관리
- 프로그램 생성 및 초기화
- 카드의 비즈니스 및 기술적인 규칙 정의
- 자료수집 및 프로그램 정의
- 관련 시스템과의 연계
- 후발급 지원
- 보안(key, secure channel) 설정

위의 기능들을 통해서 스마트카드 관리시스템은 안전한 보안 모듈과의 연계를 통해 카드의 발급에서부터 폐기까지의 모든 과정에 관여하고 있다.

### 2.2 스마트카드 관리시스템의 구조

현재 금융권과 신용카드 업계에서 개발하고 있는 스마트카드 관리시스템은 기본적으로 [그림 1]과 같은 구조를 가지고 있다.



[그림 1] SCMS의 구조

스마트카드 관리시스템 각 모듈의 기능을 살펴보면 [표 1]과 같다.

[표 1] SCMS의 개별 모듈 기능

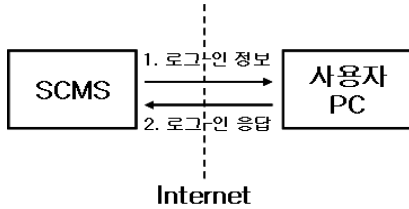
모 들	기 능
<b>CMS</b> (Card Management Server)	스마트카드의 전체적인 라이프-사이클(life-cycle)을 관리하는 서버로써 카드발급 프로세스, 데이터 Import and Export, 카드형식, 종류의 정의 등과 같은 기능을 처리하며, Personalization Bureau에서의 카드발급을 위한 발급 데이터의 배치 프로세스 스케줄링(Scheduling of batch processes)등 기능 처리
<b>AMS</b> (Application Management Server)	스마트카드에 탑재되는 애플리케이션의 전체적인 라이프-사이클을 관리하는 서버로써 애플리케이션의 정의, 애플리케이션 추가/제거/블록/언블록, 애플리케이션 발급 정보 조회, 후발급(Post-Issuance) 요구처리 등의 기능 처리
<b>KMS</b> (Application Management Server)	CMS, AMS를 운영하기 위하여 요구되는 키들에 대한 프로파일 생성, 관리하는 서버로써 HSM(Hardware Security Module)과 연동하여 키 값의 정의, 키 라이프-사이클 관리 등의 기능을 수행
<b>ADS</b> (Application Download Server)	ADS는 다양한 네트워크(Wireless LAN, PSTN, Internet 등)를 통하여 요청되는 후발급 처리에 대해서 CMS, AMS, KMS와 연동하여 사용자의 스마트카드에 다양한 애플리케이션을 동적으로 다운로드 시켜주는 역할을 수행

## 3. SCMS를 이용한 카드 후발급 인터페이스 설계

본 절에서는 개방형 카드 플랫폼이 지원하는 카드 후발급 기능을 SCMS를 이용해 사용자가 인터넷을 통해 애플리케이션 관리를 쉽고 간단하게 할 수 있도록 카드 후발급 인터페이스를 설계하였다. 총 5단계이며, 1단계 로그-인 절차, 2단계 후발급 신청 절차, 3단계 SCMS와 카드 간 인증 절차, 4단계 카드 애플리케이션 추가 및 삭제 절차, 5단계 로그-아웃 절차로 구성하였다. [그림 2]는 인터넷을 통해 후발급을 제공 받기 위한 사용자의 인증을 나타내고 있다. 카드 선발급 과정에서 SCMS에 접근하기 위한 ID와 Password와 같은 사용자의 기본 정보들은 SCMS의 고객 DB에 저장된다.

1단계: 로그-인(Log In) 절차

- ① 인터넷과 연결된 PC로 사용자 인증을 받기 위해 로그-인 정보를 SCMS로 전송
- ② SCMS는 고객 DB를 통해 로그-인 정보를 확인하여 결과 응답

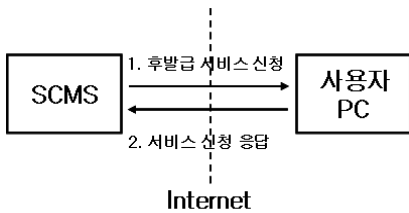


[그림 2] 후발급 제공자의 SCMS 로그인(Log In) 절차

[그림 3]는 상기 1단계 과정을 완료하고 카드 후발급 신청을 통해 SCMS와의 3단계 준비과정을 준비하는 것을 보여준다.

2단계: 후발급 신청 절차

- ① 인터넷과 연결된 PC를 통해 사용자 인증 후 SCMS에 후발급 서비스 신청
- ② SCMS는 신청한 서비스에 대한 응답을 전송

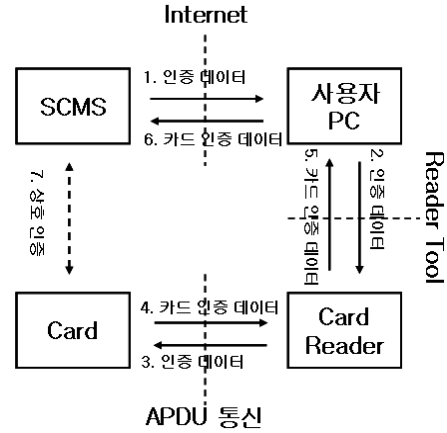


[그림 3] 카드 후발급 신청 절차

3단계: SCMS와 카드와의 인증 절차

- ① SCMS에서 카드 확인을 위해 PIN NUMBER와 같은 인증 데이터를 PC에 전송
- ② PC는 SCMS에서 제공한 Reader Tool을 이용 수신된 인증 데이터 정보를 Card Reader에 전송
- ③ Card Reader는 카드 통신규약인 APDU 통신을 이용해서 Card에 인증 데이터를 전송
- ④ Card는 수신된 인증 데이터 정보를 분석하여 APDU 통신을 이용 Card Reader에 그 결과를 전송
- ⑤ Card Reader는 Reader Tool을 통해 Card에서 전송받은 결과를 PC에 전송
- ⑥ PC는 SCMS에 그 결과를 전송하고 SCMS는 분석한 뒤에 정상인지 판단
- ⑦ 정상인지 판단되면 SCMS와 Card는 상호인증을 확인

3단계 절차에서 SCMS가 전송받은 데이터를 분석하여 정상인지 판단되면 상호인증이 되어 카드에 대해 후발급을 통해 지원 받을 수 있는 애플리케이션을 설치/제거 할 수 있는 접근 권한을 부여 받는다. [그림 4]는 후발급 제공자의 SCMS와 카드와의 인증절차를 보여준다.



[그림 4] 후발급 제공자의 SCMS와 카드와의 인증 절차

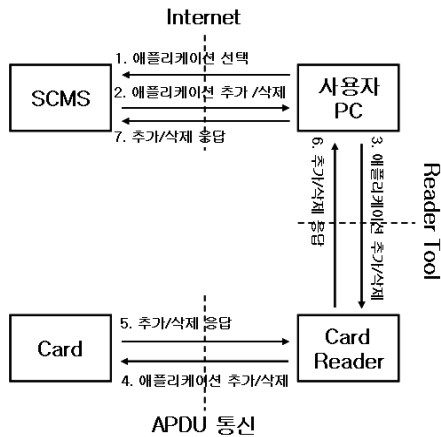
상호인증이 끝나고 카드에 대한 접근 권한을 부여 받은 후 다음 단계는 카드 후발급 과정에서 가장 중요하다고 할 수 있는 부분인 카드에 애플리케이션을 탑재하거나 삭제하는 과정이다.

4단계: 카드 애플리케이션 추가 및 삭제 절차

- ① PC는 SCMS에서 추가/삭제하고자 하는 애플리케이션을 선택
- ② SCMS는 PC가 선택한 애플리케이션을 추가/삭제에 대한 정보를 컴퓨터로 전송 애플리케이션 추가할 경우 애플리케이션 코드가 함께 전송, 애플리케이션 삭제의 경우 삭제를 하는 명령어와 해당 애플리케이션 인식자가 포함된 정보를 전송
- ③ PC는 Reader Tool을 통해 수신된 정보들을 Card Reader에 전송
- ④ Card Reader는 PC로부터 전송받은 정보들을 APDU 통신을 이용 Card에 전송
- ⑤ Card는 Card Reader로부터 전송받은 애플리케이션 추가/제거 명령을 수행한 후 이에 대한 응답 메시지를 Card Reader에 전송
- ⑥ Card Reader는 전송받은 응답 메시지를 PC로 전송
- ⑦ PC는 Card Reader로부터 전송받은 응답 메시지를 SCMS에 전송

4단계 절차를 통해 Card는 애플리케이션 추가/삭제 명령을 이행했다는 것을 SCMS 알려 애플리케이션 추가/삭제 과정을 완료하여 그 결과를 SCMS

에 연동된 DB에 저장한다. [그림 5]은 4단계 카드 애플리케이션 추가 및 삭제 과정을 나타낸 것이다.



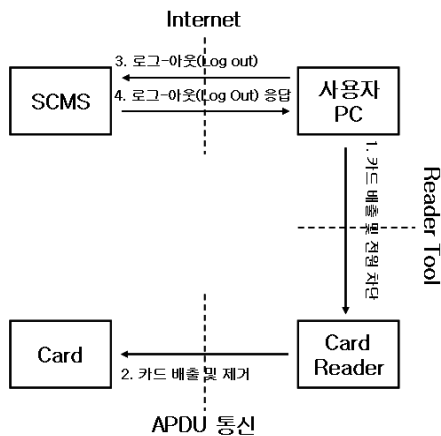
[그림 5] 애플리케이션 추가 및 삭제 절차

4단계 절차가 종료되면 로그-아웃 절차를 수행한다. 5단계는 로그-아웃으로써 이를 통해 모든 과정을 완료하고 Card Reader에 삽입된 Card를 안전하게 제거하고 전원을 차단하여 카드 후발급 과정 절차를 끝낸다.

5단계: 로그-아웃(Log Out) 절차

- ① PC는 카드 애플리케이션의 추가/삭제 과정 완료 후 Card Reader에 Card 배출 명령 및 전원 차단 명령(Power Off) 전송
- ② Card Reader는 명령 수신 후 Card 배출 후 Card Reader 전원을 차단
- ③ PC는 SCMS에 로그-아웃(Log Out) 메시지 전송
- ④ SCMS는 PC에 로그-아웃(Log Out) 응답 메시지 전송

5단계 절차는 [그림 6]과 같다.



[그림 6] SCMS 로그-아웃(Log Out) 절차

#### 4. 결론

현재 스마트카드에 다양한 카드 애플리케이션을 탑재하거나 삭제할 수 있는 개방형 카드 플랫폼 기술의 적용사례가 증가하고 있다. 이에 따라 스마트카드를 통합적으로 관리할 수 있는 스마트카드 관리 시스템 필요하여 금융권과 신용카드 업계를 중심으로 스마트카드 관리시스템이 개발되는 중에 있다. 본 논문에서는 향후 개발되어 사용될 스마트카드 관리시스템 기술을 이용하여 개방형 카드 플랫폼이 지원하는 주요 기능이라 할 수 있는 카드 후발급 과정을 위한 인터페이스를 설계하여 제안하였다. 제안된 카드 후발급 인터페이스가 기존 인터페이스와 비교하여 모든 과정 처리 절차가 간결하고 안정적이므로 향후 개발될 스마트카드 관리시스템에서 제안한 카드 후발급 인터페이스의 사용이 기대된다. 향후 연구 과제로서는 인터넷을 통한 후발급 인터페이스뿐만 아니라 무선 환경, PSTN망을 통한 후발급 인터페이스에 대한 연구가 필요하다.

#### 참고문헌

- [1] Global Platform, "Open Platform Card Specification", Ver.2.0.1, 7 April 2000.
- [2] Global Platform, "A Primer to the Implementation of Smart Card Management and Related Systems", Ver.1.0 October 2000.
- [3] Global Platform, "SCMS Functional Requirement", Ver.4.0, December 2004.
- [4] 김성중, "Java 카드기반 사용자인증 방법에 관한 연구", 한남대학교 대학원 석사학위논문, 2002.
- [5] <http://www.kebt.co.kr>.
- [6] <http://www.smartro.co.kr>.
- [7] <http://hismartech.com>.