스마트카드 관리시스템 기술

손영설 | TTA, IC카드 기술위원회 위원
KT 서비스개발연구소 선임보연구원

교통카드, 전자화폐, 의료카드 등 다양한 기능과 뛰어난 보안성, 그리고 기존 IT산업과의 유기적인 결합 등의 장점을 갖는 스마트카드 산업은 2004년 세계 시장의 1/4 이상을 아태지역이 차지할 것으로 전망된다. 이번 특집에서는 교통카드 부문에서 세계적으로 독보적인 위치를 차지하고 있는 우리나라가 스마트카드의 다양한 분야에서 시장을 선점할 수 있도록 관련 표준화 기술 및 시장동향에 대해 살펴보고자 한다.

– 스마트카드 특집 순서 –

한 장의 카드를 이용하여 다양한 애플리케이션 서비스를 제공받고자 하는 고객욕구와 전통적인 카드 플랫폼(Native COS : Chip Operating System) 모델이 가졌던 개발의 어려움, 높은 비용지출, 특정 Native COS 기술에 의존적인 프로그램 개발로 인한 비표준화된 카드환경 등은 개방형 카드 플랫폼의 개발을 가져왔으며, 이를 위한 새로운 카드 비즈니스 모델 지원과 카드 관리를 지원할 수 있는 SCMS 기술이 등장하였다. 본 논문에서는 다중 애플리케이션 서비스 환경에서의 SCMS의 역할과 기능을 살펴보고, 이를 위한 SCMS의 요소 기술에 대해서 기술하도록 한다.

1. 서론

전통적인 스마트카드 관리시스템은 자기 띠(magnetic stripe) 형태의 단일 애플리케이션 서비스를 탑재한 카드를 관리하는 시스템으로 신용카드 번호, 사용자 정보 및 리스크(risk) 관리 등의 고객 중심의 관리기능을 가졌다. 그러나, 최근 들어 IC칩 기반의 멀티 애플리케이션을 지원하는 개방형 카드 플랫폼(자바카드, 멀토스 카드)이 보편화됨에 따라 새로운 IC칩 관리, 카드 서비스 및 비즈니스 처리 등의 다양한 변화 요소들을 처리할 수 있는 스마트카드 관리시스템(SCMS : Smart Card Management System)이 새로이 요구되고 있다. 스마트카드 관리시스템은 다양한 서비스 제휴 사업자의 애플리케이션 서비스를 카드에 탑재하고, 탑재된 애플리케이션 및 카드에 대한 전체 라이프 사이클(life cycle)을 안전하고, 효율적으로 관리하는 기능을 수행한다. 국내 시장에서도 통신사업자와 신용카드사 사업자들이 SCMS를 도입 하였거나 도입을 고려하는 움직임이 분주하다. 이들 사업자들은

자사의 고유 서비스만을 탑재한 스마트카드를 발급하는 것이 아니라, 타 사업자와의 제휴를 통합한 복합 서비스를 카드에 탑재하여 발급을 하고 있다. 예를 들어, 유무선 통신사업자, 은행, 신용카드사 그리고 인터넷 사업자 등의 대형 사업자간에 컨버전스(convergence) 모델이 형성되고 있다.

본 논문에서는 개방형 플랫폼 카드를 기반으로 다중 응용서비스를 제공함에 있어서 필수적으로 구축하여야 하는 스마트 카드 관리시스템에 대해 기술한다. 2장에서는 환경변화에 따른 스마트 카드 관리시스템의 역할과 기능에 대해서 기술하며, 3장에서는 개방형 플랫폼 카드의 관리 및 발급기능에 대해서 기술하며, 4장에서는 스마트카드 관리시스템의 보안기술에 대해서 기술하고, 5장에서는 향후 기술방향을 기술함으로써 결론을 맺고자 한다.

2. 스마트카드 관리시스템

한 장의 카드를 이용하여 다양한 애플리케이션 서비스를 제공받고자 하는 고객욕구와 전통적인 카드 플랫폼(Native COS : Chip Operating System) 모델이 가졌던 개발의 어려움과 높은 비용지출, 특정 Native COS 기술에 의존적인 프로그램 개발로 인한 비표준화된 카드환경 등은 개방형 카드 플랫폼의 개발을 가져왔으며, 이를 위한 새로운 카드 비즈니스 모델 지원과 카드 관리를 지원할 수 있는 SCMS 기술이 등장하였다. 스마트카드 사업에서의 SCMS 기술 도입은 스마트카드 사업 참여자로 하여금 독립된 역할 정립과 복잡한 비즈니스 네트워크를 단순화시킴으로써 효율적인 카드 및 애플리케이션 관리를 꾀할 수 있도록 하고 있다. 따라서 SCMS는 사업 참여자의 효율적인 관리와 표준 카드 플랫폼, 데이터 베이스 그리고 기존 시스템과 인터페이스 핸들링이 가능하여야 하며, 카드 플랫폼과 애플리케이션의 형상 관리가 가능하여야 한다.

2.1 SCMS의 기능

- 카드 및 애플리케이션 관리 : SCMS는 스마트카드 및 카드 애플리케이션의 라이프 사이클(life cycle) 관리기능을 가진다. 스마트카드의 라이프 사이클[GP 2.1.1 기준]은 OP_READY → INITIALIZED → SECURED → CARD_LOCKED → TERMINATED로 천이하며, 카드 애플리케이션은 INSTALLED → SELECTABLE → LOCKED로 천이한다. 이에 따라 SCMS는 카드 및 카드 애플리케이션을 관리하게 된다. [1]
- 프로그램 생성 및 초기화 : SCMS는 카드 애플리케이션의 발급 및 관리를 위해서 상품 프로그램을 생성하게 된다. 카드 상품 프로그램이란 스마트카드의 사양과 따른 카드 애플리케이션의 특성을 고려한 카드에 따른 카드 애플리케이션 포트폴리오(portfolio) 구성을 말하며, 이는 카드 프로파일과 애플리케이션 프로파일을 통해서 정의할 수 있다.
- 카드 비즈니스 규칙 정의 : 상기 과정에서 생성된 카드 프로그램은 발급되는 카드의 사양과 카드 프로그램의 상관관계를 통해서 운영되어진다. 이는 스마트카드 발급자의 정책과 카드의 물리적 사양에 따라서 SCMS는 비즈니스 규칙을 정의하여 서비스를 제공한다.
- 자료수집 및 프로그램 정의 : SCMS는 선/후 발급(pre/post-issuance)을 위하여 각 카드 애플리케이션의 로딩 및 발급을 위하여 필요한 카드

[1] Global Platform, "Open Platform Card Specification", Ver.2.0.1, 7 April 2000

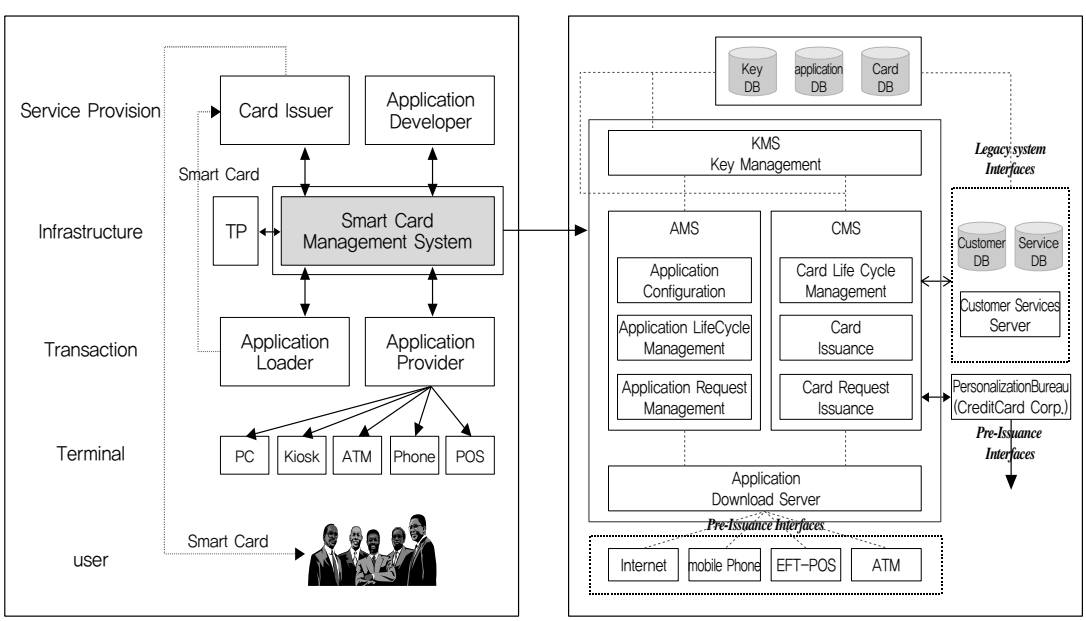
프로파일(card profile), 애플리케이션 프로파일(application profile), 키 프로파일(key profile) 등의 자료를 수집한다.

- 유관 시스템 인터페이스 : SCMS는 다중 카드 애플리케이션 발급을 위해 유관 시스템과의 인터페이스를 통하여 필요한 데이터 수집 및 관리기능을 수행한다. 공인인증기관(CA), 애플리케이션 제공자의 서버, 기존 서비스 시스템(legacy service system) 등과 연결되어 실시간 또는 배치형태의 업무처리 기능을 수행한다.
- 후발급 지원 : SCMS 기능의 대표적인 기능으로써 전용 COS 카드에서 불가능했던 후발급 기능을 개방형 플랫폼 카드를 기반으로 지원이 가능하다. 현재 SCMS의 후발급은 인터넷 및 무선 네트워크를 통하여 PC 또는 휴대폰 단말을 이용하여 카드로 처리되고 있다. 점차 다양한 네트워크를 통해서 다양한 단말(Set-up Box, PDA, ATM 등)을 통해서 후발급이 진행될 것이다.
- 기타

  상기 기능들 외에 SCMS는 카드 및 카드 애플리케이션의 상태 조회, 고객서비스 이용통계, 스마트카드 발급통계 등의 다양한 통계자료를 산출하며, SCMS 관리를 위한 관리자 지정 및 권한부여 등의 기능도 수행하게 된다.

2.2 SCMS의 구조

2.1에서 기술한 SCMS 기능을 수행하기 위하여 SCMS[2]는 〈그림 1〉과 같은 여러 요소 시스템으로 구성되어진다. 현재 시장에 출시되고있는 SCMS 상품들은 MS Windows와 Unix 등과 같은 호스트 플랫폼상



〈그림 1〉 SCMS의 구조

[2] Global Platform, "A Primer to the Implementation of Smart Card Management and Related Systems", Ver.1.0 October 2000

에서 구현되어, Multos 카드와 자바카드 2종류의 카드 플랫폼에 맞추어 운영되고있다. Multos 카드는 Multos CA의 통제하에 인증서 기반으로, 자바카드는 카드 발급자가 정의하는 키(Key) 기반으로 카드 및 애플리케이션을 관리한다.

■ CMS(Card Management Server)

스마트 카드의 전체적인 라이프 사이클을 관리하는 서버로써 카드발급 프로세스, 데이터 Import and Export, 카드형식, 종류의 정의 등의 기능을 처리하며, 또한 Personalization Bureau에서의 카드발급을 위한 발급 데이터의 배치 프로세스 스케줄링(Scheduling of batch processes) 등의 기능도 처리한다.

■ AMS(Application Management Server)

스마트 카드에 탑재되는 애플리케이션의 전체적인 라이프 사이클을 관리하는 서버로써 애플리케이션의 정의, 애플리케이션 추가/제거/블록/언블럭, 애플리케이션 발급정보 조회, 후발급(Post-Issuance) 요구처리 등의 기능을 처리한다.

■ KMS(Key Management Server)

CMS, AMS을 운영하기 위하여 요구되는 키들에 대한 프로파일을 생성, 관리하는 서버로써 HSM(Hardware Security Module)과 연동하여 키 값의 정의, 키 라이프 사이클 관리 등의 기능을 수행한다.

■ ADS(Application Download Server)

애플리케이션 다운로드 서버는 다양한 네트워크(Wireless LAN, PSTN, Internet 등)를 통하여 요청되는 후발급 처리에 대해서 CMS, AMS, KMS와 연동하여 사용자의 스마트 카드에 다양한 애플리케이션을 동적으로 다운로드 시켜주는 역할을 수행한다.

■ Legacy 서버

레가시(Legacy) 서버는 SCMS 시스템과 연동하여 각종 서비스를 처리하는 서버군들로 고객DB 서버, 대외 접속서버, 각종 서비스 서버들을 망라한다.

3. SCMS의 카드 애플리케이션 발급

기존의 카드관리 시스템이 선발급만을 처리하였던 반면에 멀티 애플리케이션 카드 플랫폼을 지원하는 SCMS가 제공할 서비스는 사전에 카드에 탑재하여 사용자에 배포하는 선발급 기능과, 사용자에게 카드가 전달된 후 다양한 네트워크 인프라를 통하여 배포된, 사용자가 원하는 카드 프로그램을 발급하는 후발급 기능을 제공한다. 선발급을 위한 과정은 다음과 같다.

3.1 SCMS의 선발급(pre-issuance)

■ Card & Application Configuration

SCMS은 사용자로부터 카드 신청서를 접수받아 카드발급을 위한 발급전문(card profile, application profile 및 key profile)을 생성하게 된다. 이러한 프로파일은 Personalization Bureau의 발급 시스템 장비 프로그램을 고려하여 특정형태의 프로파일 또는 규격에 정의하는 형태의 프로파일(예 ; Global Platform 규격의 경우 XML 파일로 생성)을 생성하게 된다.

■ Communication with Personalization Bureau

상기 과정에서 생성된 각 프로파일 데이터는 발급장비(예 ; DC-9000)를 보유한 Personalization Bureau로 전달되게 되며, 시설보안이 완비된 발급공간에서 실제 카드를 발급하게 된다. 국내의 경우 Personalization Bureau가 카드의 전사 작업 및 카드의 초기화(Initialization) 작업을 수행하는 1차 기관과 카드 애플리케이션의 Loading/Personalization을 수행하는 2차 기관(예 ; 신용카드

사) 형태로 운영되고 있다. SCMS 시스템은 대부분 이러한 2차 기관과 안전한 네트워크 채널을 형성하고 발급 데이터를 전송하게 된다.

■ Card Issuance

2차 기관에서는 카드 발급을 위한 전문을 SCMS 시스템으로 전송받아 발급장비와 연결된 발급 프로그램(발급장비의 제어 및 발급기능 수행)을 전달하기 위하여 P3(Pre-personalization Preparation Process)에서 발급전문을 가공한다.

3.2 SCMS의 후발급(post-issuance)

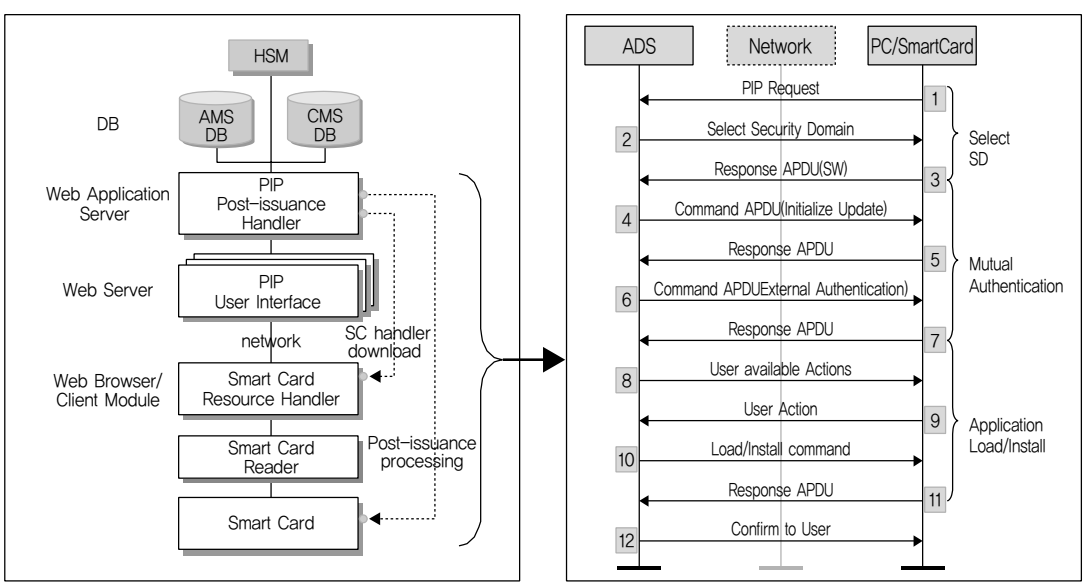
신규 카드 프로그램의 추가, 기존 카드 프로그램의 삭제 또는 업데이트의 수행은 SCMS의 핵심기능 중의 하나이다. 기존의 CMS에서 불가능했던 카드 프로그램의 동적관리가 WAP(Wireless Application Protocol) G/W를 이용한 무선환경, 인터넷, PSTN망을 이용한 유선환경 속에서 가능함에 따라 핸드폰, 공중전화기, 키오스크(Kiosk), PC 등의 다양한 서비스 액세스 접점을 통해서 카드 프로그램의 후발급을 수행한다. 현재 대부분의 개방형 플랫폼 카드는 인터넷을 통한 웹(web)기반의 후발급이 이루어지고 있으며, 해당 처리 모듈은 웹 애플리케이션 서버(예 ; Web Logic, iPlanet, Tomcat 등) 상에서 구현되며, 이를 위해 J2EE, SOAP,UDDI, ebXML, CORBA 등의 Web/Java 기술을 적용한다.

■ Issuance flow

후발급을 위한 발급전문 생성은 SCMS의 각 요소 서버와 연동하여 생성되게 되며, 선발급의 발급전문 생성과 P3 기능을 동시에 수행하게 된다. 사용자 카드에 프로그램의 추가, 삭제작업은 자바카드의 경우 보통 12단계의 절차를 통해서 이루어지게 되며 상세 절차는 아래 〈그림 2〉와 같다.

① 사용자가 PIP(Post Issuance Personalization) 서비스를 신청한다.

② ADS(Application Download Server)는



〈그림 2〉 자바카드 후발급 절차

CM(Card Manager)의 Security Domain을 선택한다.

③ 카드 응답 코드를 ADS로 전송한다.

④ 상호 인증을 위한 Host Challenge 값을 생성하여 카드로 전송한다.

⑤ 카드는 Card Challenge 및 세션 키를 생성하여 카드 Cryptogram을 생성하여 ADS로 전송한다.

⑥ ADS는 세션키를 생성 및 Card를 검증하고, Host Cryptogram을 생성하여 카드로 전송한다.

⑦ 호스트를 검증하고 이에 대한 응답코드를 전송한다.

⑧ ADS는 상호인증을 수행한 후 CMS 및 AMS와 연동하여 카드로부터 읽은 CIN(Card Image Number)를 기반으로 사용자가 선택한 액션형태(애플리케이션 종류, 카드 정보 등)를 전송한다.

⑨ 사용자는 상기 과정의 액션을 선택하여(카드 프로그램의 업데이트, 추가, 삭제) 이를 요청한다.

⑩ ADS 서버는 CMS, AMS, KMS와 연동하여 사용자가 선택한 작업을 수행하기 위한 APDU 명령어 스크립트를 작성하고, 이를 스마트카드로 전송한다. 이때, P3기능인 발급전문을 함께 전송한다.

⑪ 카드 프로그램의 추가인 경우 카드 프로그램의 Loading, installation, registration 과정을 거쳐 카드상에서 실행 가능한 애플리케이션 라이프사이클을 변경한다. 이에 대한 카드 응답코드를 호스트로 전송한다.

⑫ ADS 서버는 SCMS에 정상적인 카드 애플리케이션 상태로 변경하고 이에 대한 응답코드를 클라이언트로 전송한다.

4. SCMS의 보안

개방형 네트워크인 인터넷에서 스마트 카드 애플리케이션의 후발급(Post-issuance)은 높은 보안성을 요구하게 되며, SCMS는 KMS 서버와 HSM(Hardware Secure Module) 장비를 이용하여 카드 및 애플리케이션의 보안을 관리한다.

4.1 Card Holder and Card verification

■ Card Holder authentication

SCMS 서비스를 제공받기 위해서는 카드 소지자는 자신의 카드 비밀번호를 입력한 후 카드 소지에 대한 정당성을 인증받아야 한다.

■ Card Verification

위/변조된 카드에 대한 정당성을 인증하기 위하여 Challenge-Response기반의 상호인증 메커니즘을 사용하여 카드 진위여부를 검증하며, 또한 Risk Management을 위하여 SCMS에서 B/L 등록여부도 체크한다.

4.2 Data integrity and Confidentiality

SCMS에서 인터넷을 통하여 스마트 카드에 전달되는 데이터의 무결성과 기밀성을 보장하기 위하여 대칭키 기반의 암호 알고리즘(3DES)을 사용하게 되며, SCMS에서 스마트카드로 전송되는 APDU의 데이트 필드는 보안채널(secure channel)을 형성하여 안전하게 전송되어진다.

■ 데이터 필드 암호화

Step 1 : 스마트카드에서 생성한 8바이트 난수 값 (r_2)을 좌측 4바이트 값(r_{2_LBS}), 우측 4바이

트 값(r_{2_MSB})으로, 외부단말에서 생성한 난수 8바이트 값(r_1)을 좌측 4바이트 값(r_{1_LBS})과 우측 4바이트 값(r_{1_MSB})으로 나누어, $r_{2_MSB} \| r_{1_LBS} \| r_{2_LBS} \| r_{1_MSB}$로 재정렬하여 파생 데이터($R_d$)를 생성한다.

$R_d = r_{2\_MSB} \| r_{1\_LBS} \| r_{2\_LBS} \| r_{1\_MSB}$

Step 2 : 상기 과정에서 생성한 파생 데이터(R_d)를 스마트카드에 기 설정된 암호화용 마스터키(K_E)를 이용하여 암호화용 세션 키(S_{E_K})를 생성한다.

S_{E_K} = 3DES(R_d, K_E)

Step 3 : 상기 과정에서 생성한 암호화용 세션 키(S_{E_K})를 이용하여 Command APDU의 데이터 필드(D)를 암호화 한다. 이때 데이터 필드의 길이가 8의 배수가 아닌 경우 패딩 규칙에 따라서 '0x00'를 패딩한다.

D_e = 3DES(D, S_{E_K})

■ Command APDU의 MAC 생성

Step 1 : 데이터 필드 암호화의 Step 1과 동일하다.

Step 2 : 상기 과정에서 생성한 파생 데이터(R_d)를 스마트카드에 기 설정된 MAC 생성용 마스터키(K_A)를 이용하여 MAC 생성용 세션 키(S_{A_K})를 생성한다.

S_{A_K} = 3DES(R_d, K_A)

Step 3 : 상기 과정에서 생성한 MAC 생성용 세션 키(S_{A_K})를 이용하여 Le를 제외한 Command APDU(D') 전체를 암호화한 후 이를 MAC으로 사용한다.

$D' = CLA \| INS \| P1 \| P2 \| Lc \| Data$

MAC = 3DES(D', S_{A_K})

■ Command APDU의 전송

SCMS는 데이터 필드의 값을 스마트 카드로 전송시 상기 데이트 필드 암호화 과정을 통해서 암호화되며, Command APDU 전송시 상기 MAC 생성과정을 통해서 생성된 MAC_4값을 붙여서 SSL(Secure Socket Layer)기반의 네트워크를 통하여 스마트카드로 전송하게 된다. 이를 통해서 SCMS와 스마트카드는 상호간의 통신에 있어서 암호성(confidentiality), 무결성(Integrity), 인증(authentication) 등의 암호특성을 만족시킨다. [3]

5. 결론

최근 정부 당국에서 현재 사용 중인 MS형태의 현금카드(2005년까지) 및 신용카드(2008년까지)가 스마트카드로의 전환을 의무화하도록 공시함에 따라 국내 스마트카드 시장이 점차 확대될 것으로 예상되며, 이와 더불어 개방형 플랫폼 카드의 보급도 급격하게 늘어날 것으로 예상된다. 이에 따라 국내 금융 및 통신사업자들의 본격적인 SCMS 도입도 가시화될 것으로 사료된다. SCMS를 도입할 사업자들은 자사의 상품 특성과 대용량 발급 그리고 향후 확장성 등을 충분히 고려하여야 할 것으로 생각되며, 개방형 플랫폼 카드기술과 보안기술에 대한 충분한 이해가 선행되어야 할 것이다.

[3] ISO/IEC 7816-3, Information Technology -identification cards-integrated circuit(s) cards with contacts, Electronic Signals and Transmission Protocol, 1997