The Journal of Korean
Institute of CALS/EC
Vol. 4, No. 3, Dec. 1999

스마트카드 모델의 기준에 관한 연구*

황선태**, 이 형**

Study on a Basis of a Smart Card Model

Suntae Hwang, Hyoung Lee

Abstract

In general, the electronic commerce systems comprise the background system, terminal, network and smart cards. Among them, the smart card systems are expected to take a great portion of applications for the convenience of rapidly improving technology. The technology includes adopting RISC processors or co-processors for cryptography and developing new memory systems based on the standardization.

In this paper, we investigate the overall trends of the technology and the standardization process of smart cards. We also propose the guidelines to enhance the capabilities of designing H/W and S/W related to COS(Chip Operating System).

Key Word : 보안, 전자지갑, COS, 스마트카드, ISO

* 본 논문은 1998년도 한국정보보호센터의 위탁과제로 수행된 연구의 일부임.

** 대전대학교 정보통신공학과 교수

1. 서 론

사회 환경 및 거래 관계가 복잡해짐에 따라 신분 확인 및 보안 유지에 대한 요구가 증가하게 되었다. 스마트카드는 기존 카드가 행할 수 없었던 양방향 통신, 정보의 보호 기능 등을 수행할 수 있으며, 개인을 확인할 수 있고 이동성이 뛰어나며 마그네틱 카드와 비교하여 복제가 매우 어렵고, 암호 알고리듬을 카드 내부에서 수행하여 보안상 매우 좋은 이점을 지니고 있다. 즉, 암호 시스템에서 Key의 중요성을 감안할 때, Key가 카드 외부로 노출이 안되므로, 고도의 안전성을 확보할 수 있다. 또한 마이크로 프로세서 및 대용량의 메모리를 보유함으로써, 개인의 서명, 필체, 지문 등 생물학적 특징을 인식할 수 있으며 다양한 서비스의 제공이 가능하다[김철, 1996; Rankl, 1997].

인터넷이 점점 대중화되고 보이지 않는 상점과 소비자 사이의 신뢰관계가 무척 중요하게 부각되면서 안전하게 물건을 구매하고 정보를 얻을 수 있는 방법이 필요하게 되고, 따라서 스마트카드의 중요성과 그 실용성이 더욱 증대되고 있다. 또한 지불행위 기능의 스마트카드뿐만 아니라 개인 신분증명 및 암호화 통신, 전자서명을 위한 용도로서의 스마트카드의 중요성도 많은 흥미를 끌고 있으며, 특히 원격 액세스에서 스마트카드의 사용 영역은 점차 더 늘어날 것이다.

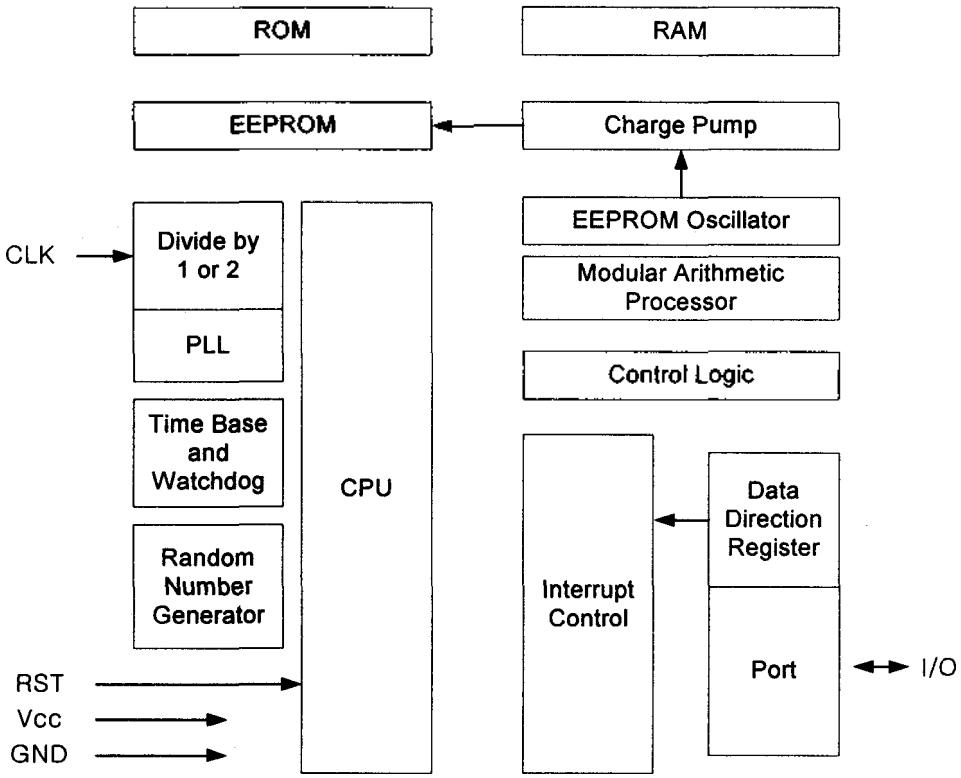
본고에서는 2장에서 스마트카드의 H/W 규격과 ISO 7816 규정에 관해 설명하고, 3장에서는 국내외에서의 스마트카드 관련 표준화 및 기술 개발에 따른 동향을 분석하고 있다. 4장에서는 국내 스마트카드의 COS 제작에 대한 기준을 제안하고 있으며, 마지막으로 5장에 결론이 기술되어 있다.

2. 스마트카드 규격

2.1 하드웨어 규격

일반적인 접촉식 카드의 IC Chip 내부 구조는 <그림 1>과 같고 ISO 7816의 제안을 따르고 있다[ISO, 1997].

<그림 1>에 나타난 H/W, 즉 Die의 크기는 휘어질 때의 손상을 방지하기 위해서 가능한 한 얇고, 또한 면적도 25mm^2 이내로 할 것을 제안하고 있다. 스마트카드 Chip에는 그림에서 나타나듯 5개의 활성화된 접점이 존재한다. CPU는 8-bit부터 32-bit RISC Processor까지 개발되고 있다. ROM은 주로 16/32K-bytes 용량으로 데이터, COS 그리고 Lookup Table 등을 저장하는 반면, RAM은 1K-bytes 미만으로 전압이 공급되는 동안만 CPU의 연산을 위해 이용된다. 또 EEPROM (Electrically Erasable Programmable ROM)은 8/16K-bytes로 전압이 공급되는 동안에는 데이터의 저장이나 변경 등이 가능하나 단전된 상태에서는 저장된 데이터는 그대로 유지된다. 이 EEPROM에 기억되는 내용으로는 Card ID Number, PIN, 잔액 그리고 Credit 한계 등이다. Charge Pump는 EEPROM에 기록하기 위해 필요한 전압 치를 만들어 주고, Phase-locked Loop(PLL)은 단말기에서



<그림 1> 스마트카드 Chip 구조

공급되는 Clock Frequency가 Modular Arithmetic Processor(MAP)에서 사용될 수 있도록 분주해주는 역할을 담당한다. 마지막으로 MAP은 Random Number Generator에 의해 생성된 수를 이용하여 암호화 알고리듬을 효율적으로 수행시키는 역할을 담당한다.

2.2 ISO 7816 규격

ISO 7816은 전체 10개 Parts로 구성되어 있으며 스마트카드의 H/W 및 S/W의 특성을 정의하고[ISO, 1997: ISO, 1985], 단말기와 카드간의 메시지 전달, 카드 내부의 화일과 보안 구조 등의 개략은 다음과 같다. 논리적 채널은 논리적으로 한 개의 DF와 연관되는데 결국 한 개의 DF가 한 개의 응용 프로그램과 대응된다. 카드의 용도가 다양할 경우 여러 개의 DF를 사용하고 각 DF는 각각의 용도에 맞는 EF들을 가지게 된다.

-. Master File(MF) : MF는 화일 시스템의 Root에 해당된다. 시스템이 MF에 Application을 저장하는 것을 허락하지만, 그것은 다중 응용 카드(Multi-functional Cards)에서만 의미가 있다.

-. Dedicated File(DF) : 화일 통제 정보를 포함하며 Elementary File(EF)이나 DF

의 상위 레벨로, Root 레벨의 유일한 DF를 MF라 한다.

-. Elementary File(EF) : 실지 데이터를 저장하는 화일로 카드 운영 체계에 의해 사용되는 Internal EF와 단말기 등에 의해 사용되는 Working EF로 구분된다.

-. ATR File : 카드의 동작 조건 등을 나타내는 EF.

화일 참조 방법으로는, 첫 번째로 2-byte의 화일 식별자를 사용하는 방법으로 MF는 '3F00'으로 지정되어 있고, 두 번째로 MF나 현재 DF로부터 참조 하고자하는 화일까지 Path를 지정하는 방법, 세 번째로 5-bit짜리 단축 EF 식별자를 이용하여 참조할 수 있고, 마지막으로 1~16 Byte의 DF 이름으로 DF를 참조할 수 있다.

메시지 보안의 목적은 카드에서 입출력되는 메시지의 인증과 비밀유지에 있다. 데이터 부분의 코딩은 CLA의 지시가 없는 한 반드시 ASN.1(ISO 8825)의 규칙을 따라야 한다. 따라서 ISO 7816의 메시지 보안 형태는 BER(Basic Encoding Rule of ASN.1)-TLV 코딩을 따른다. 카드의 보안 상태는 특정한 화일에 대한 접근을 금하는 것으로 Global 보안 상태, File-specific 보안 상태 그리고 Command-specific 보안 상태로 나눈다. 이 보안 상태는 ATR, PTS 혹은 인증 관련 명령어의 수행 후의 상태를 나타낸다. 카드의 보안 메커니즘으로 다음의 4가지가 있다.

-. 카드 소유자의 권리를 보호하기 위해 패스워드를 이용한 인증.

-. 단말기 인증을 위해 사용되는 Key를 이용한 인증.

-. 카드 공급자의 권리를 보호하기 위한 데이터 인증.

-. 단말기와 카드간의 전송 정보를 보호하기 위한 데이터 암호화.

또 Application Protocol Data Unit (APDU)은 명령어나 그에 따른 응답을 나타내며 각각 단말기로부터 카드로 혹은 그 반대 방향으로 전송되는 메시지이다. 이 메시지는 CLA, INS, P1, P2를 포함하는 4-byte 헤더와 또, Lc, 데이터 부분, Le를 포함하는 임의의 가변 길이의 바디로 되어 있다. CLA는 명령어나 응답이 ISO 7816 규정을 어느 정도 준용하는가 등을 나타내며, INS는 1-byte의 명령어 코드를 나타낸다. 매개변수 Byte인 P1, P2는 특정 변수가 필요한 명령어에서 사용된다. 또 Lc는 명령어 데이터 부분의 Byte 수를 나타내고 Le는 응답 메시지 데이터부분의 예상되는 최대 Byte 수를 나타낸다..

3. 스마트카드 관련 표준화 및 기술 동향

칩 카드와 관련된 주요 표준화 기구들은 ISO, ANSI, CEN, ETSI 등을 들 수 있다. ISO(International Organization for Standard)는 백여 국 이상의 국가별 표준화 기구들을 대표하며 전문분야에 따라 산하에 기술위원회(Technical Committee, TC), 소위원회(Subcommittee, SC)를 두고 있고 ANSI (American National Standards Institute)는 ISO에 투표권을 행사할 수 있으며 미국 내 기업들로 구성된 단체이다. CEN(European

<표 1> 스마트카드의 국제표준

표 준	세 부 내 용
ISO 7816 IC cards with contacts	IS 7816-1 Physical Features IS 7816-2 Location and dimension of contacts IS 7816-3 Transmission Protocols IS 7816-4 Inter-Industry commands for interchange IS 7816-5 Numbering system CD 7816-6 Data components for inter-industry interchange TF 7816-7 Other commands TF 7816-8 Security
ISO 9992 Financial transaction cards - ICC and CAD message	IS 9992-1 Structure and concepts DIS9992-2 Commands and response, data elements and structures, functions and messages
ISO 10202 Financial transaction cards - Security	IS 10202-1 Life cycle DIS 10202-2 Transaction process CD 10202-3 Relationships of cryptographic keys DIS 10202-4 Secure Application Modules(SAM) CD 10202-5 Algorithm use DIS 10202-6 Verification of cardholder CD 10202-7 Management of keys WD 10202-8 Overview and general principles
ISO 10536 Contactless chip cards	IS 10536-1 Physical features DIS 10536-2 Coupling area position and dimensions CD 10536-3 Contactless interface electrical features
ANSI	X3 Data processing systems X9 Financial institutions - security standards X12 Interchange of electronic data
CEN TC224	WG1 Physical features WG2 ICC systems - general considerations WG3 Features of interface devices WG4 ICC communications WG5 Device/host communication WG6 User interface WG7 PIN presentation WG8 Flexible thin cards WG9 Telecommunications applications WG10 Financial transaction IC applications - payment spec. WG11 Transport applications WG12 Health applications WG14 Airline applications

※ WD(Working Draft), CD(Committee Draft), DIS(Draft International Standard), IS(International Standard), TF(Task Force division of ISO), TC(Technical Committee division of ISO), WG(Working Group division of ISO)

Committee for Standardization)은 ISO와 협력관계에 있으나 투표권은 없다. 또한 ETSI (European Telecommunications Standards Institute)는 주로 GSM 셀룰라폰 업체가 참여하고 있다[IC, 1998].

3.1 ISO와 관련 표준

ISO는 이미 접촉식 스마트카드에 대한 표준을 완료하였다. ISO 7816은 접촉식 칩 카드에 대한 국제표준으로 플라스틱의 물리적 특성, 사이즈, 전기적 접점의 위치 및 기능 등을 정의하고 있다. ISO는 또한 근거리 및 원거리에 사용될 ISO 10536, ISO 14443 등 비접촉식카드에 대한 표준을 제정하고 있다. <표 1>은 관련 표준의 대강을 나타내고 있다.

세계의 3대 신용카드회사인 Europay, MasterCard, Visa가 금융카드와 단말기에 관한 EMV 국제 표준에 동의하여 1996년 말에 최종 스펙이 완료되었고, 지급 시스템을 위한 EMV96 Integrated Circuit Card (ICC) 사양이 스마트카드를 기초로 한 전세계 지급시스템의 기반을 이룬다. EMV '96은 ICC Specification, ICC Terminal Specification, ICC Application Specification 등의 세 Parts로 구성되어 있다. 첫 번째 Part는 스마트카드와 POS 단말기를 제조하기 위한 전기적, 기계적 사양들을 정의하고 있다. 두 번째 Part는 스마트카드와 POS 단말기의 상호작용을 정의하고 있으며, 세 번째 Part는 단말기의 카드 어플리케이션 처리 방식 및 금융거래의 지급과정 그리고 예외 사항들의 처리 방법 등에 대해 설명하고 있다[EMV, 1996: IC, 1998].

3.2 칩 제조 기술의 동향

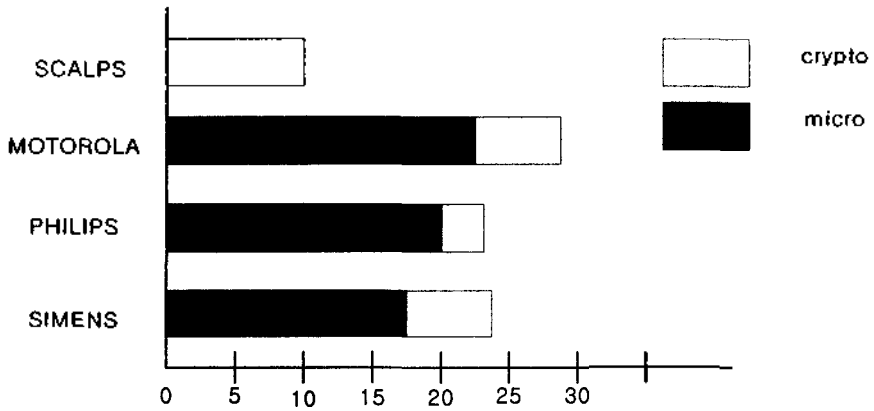
1974년 Innovation S. A.의 Roland Moreno에 의해서 처음으로 스마트카드에 대한 특허가 출원된 이후 최초의 스마트카드는 1977년 BULL사와 Motorola사의 합작으로 등장하였다. 그 때의 스마트카드는 Memory와 Controller 부분이 분리된 2칩으로 이루어진 형태였고, 그 후 3년 뒤인 1980년 Motorola사에 의해서 SPOM01이라고 명명된 단일 칩 스마트카드가 최초로 개발되었다. 현재의 일반적인 스마트카드는 신용카드 크기 정도의 플라스틱에 IC Chip을 장착한 것으로 8개의 접점을 통하여 외부 단말기와 상호 인터페이스 하도록 설계 되어있다. 일반적으로 스마트카드는 8비트 마이크로 프로세서를 주로 사용하는데 가장 널리 사용되는 마이크로 프로세서는 모토롤라의 68HC05 및 인텔의 80C51이다[IEEE, 1997].

일반적으로 스마트 카드용 Arithmetic Co-processor는 모듈러 연산을 위한 회로를 내장하고 있다. 이 모듈러 연산을 기반으로 한 상용 Co-processor의 성능 및 응용 분야는 <표 2>와 같고 제조 회사별 마이크로프로세서에서 Crypto-processor가 차지하는 면적은 <표 3>에 나타나 있다. 우수한 스마트카드를 구현하기 위하여 실리콘의 면적 및 공정기술, 비트 수, 동작 속도, 알고리즘, 신뢰성 있는 회로, 메모리 용량, 전력소비율, 범용성 등 다양한 면을 검토하여야 한다. 또 스마트카드를 이용하여 응용분야에

<표 2> 상용 Co-processor의 특징

칩 명	제조회사	core uP	제조기술	연산알고리즘	주파수(MHz)	최대 N (비트)	응용분야
ST16CF54	SGS	68HC05	1.2uCMOS	Montgomery	5	768	비공개
ST16KL74	SGS	68HC05	1.2uCMOS	Montgomery	5	1024	비공개
SLE44C200	Siemens	80C51	1uCMOS	Simens	5	540	CAFE, DSM-fax CP8
P83C852	Philips	80C51	1.2uCMOS	Quisquater	10	648	DX, Mimosa, Starcos
P83C856	Philips	80C51	1.2uCMOS	Qusquater	10	1328	비공개
MC68C06S29	Motorola	68HC05	1.2uHCMOS	Montgomery	5	1024	French health card
RSA512	AMTEC	co-uP	0.5uCMOS	Bucci/Barrett	100	513	banking, X.25 security
SCALPS	UCL	custom	1.5uCMOS2ML	Montgomery	6	512	university prototype
CY512i	Cylink	80C31	1.5uCMOS	Massey-Omura	15	512	비공개
CRIPT	CNET	custom	1.2uCMOS	bit-by-bit	25	1024	PCMCIA cards
PCC200	Pijnenb	co-uP	1uCMOS2ML	비공개	20	1023	GSM and banking

<표 3> Microprocessor 면적 (mm^2)



효율적으로 적용하기 위해서는 COS에서의 자료구조 관리 기능, 데이터가 저장되는 형태, 디렉토리의 제공여부, 화일 형태의 종류(순차, 랜덤, 환형 화일), 록인 및 감사추적 기능, 엑세스 컨트롤, 암호 함수 라이브러리 등의 기능을 고려하여야 한다[F&G, 1997: F&G, 1998].

최근에는 Co-processor가 내장되어 있지 않아도 공개키 암호 시스템을 스마트카드에 구현할 수 있는 ECC(Eliptic Curve Crypto-system)가 등장하여 점차 관심을 끌고 있다[Thom, 1996].

3.3 COS 제작 및 응용 기술의 동향

스마트카드를 운용하기 위해서는 내장된 IC Chip을 운영해주는 COS가 필요하고, 그 외에 정보의 보안을 위한 인증 및 Digital 서명과 사용하고자 하는 업무의 성격에 맞는 데이터 구조의 정의 및 프로그램 작성이 필요하다. 스마트카드의 COS는 현재 G&D의 STARCOS, Gemplus의 MPCOS, Schlumberger의 Multiflex등 다양한 종류가 존재하며 이 COS들은 스마트카드를 구동시키는 기본적인 사양에 있어서 ISO 7816을 만족시키지만 각 COS 간에는 전반적으로 호환이 안 된다. 현재 32-bit Chip 제조기술의 발달과 더불어서 여러 Application을 하나의 카드에 저장할 수 있고, COS가 각각 달라도 임의의 Application을 탑재할 수 있도록 Multi-Application Operating System인 Mastercard의 MAOS와 SUN으로부터 기술 도입하여 사용하는 VISA의 JAVA카드가 등장하고 있다.

이와 같은 스마트카드를 적용할 수 있는 분야들은 Telecommunications, Financial Services, Travel and Transportation Ticketing, Health Care and Insurance, Network Access, Electronic Purse 등 다양하다. 이 중 초기에 가장 많이 응용된 것이 'Reloadable Pay Phone Card'인 공중 전화 스마트카드와 교통카드이다. 또한 근래 들어서 독일, 스페인, 싱가포르 등 세계 10여 개 국에서는 전자지갑용 스마트카드가 상당히 사용되고 있다. 이미 유럽 등지에서 사용되고 있는 GSM Phone에서는 자신의 스마트카드를 이용해서 유럽 내 타 국가간에 아무런 구애를 받지 않고 지불행위와 함께 통화를 할 수 있다[IC, 1998].

이와 같이 전자상거래가 보편화되고 암호기술의 발달로 계약, 쌍방 서명 등의 작업들이 좀 더 안전하게 원격으로 행해질 수 있게 된다. 특히 여기서 주로 구현되는 공개키 방식에서 개인의 비밀키를 자신의 PC에 저장하는 경우 스마트카드에 저장하는 것보다 이동성과 보안성이 훨씬 떨어진다. 따라서 안전한 전자상거래 프로토콜인 SET이나 C-SET 및 PC/SC 등의 기술 개발은 PC와 전자상거래, 스마트카드를 안전하고 편리하게 연결시켜 주는 역할을 한다[PC/SC, 1997; ECDG, 1997].

4. 스마트카드 설계 기준

스마트카드의 요체인 COS의 구조적 특성과, 디자인 시 고려 사항 그리고 안전성 확보를 위한 테스트 방법론은 다음과 같다.

4.1 COS의 구조

현재 사회전반에 걸쳐서 스마트카드 이용이 확대되고 있다. 특정한 Application을 수행하기 위해서는 기본적으로 COS(Chip Operating System)가 있어야 하고 그 위에 Application Program이 존재하게 되는데, JAVA Card나 MULTOS가 아닌 일반적인 COS에 대해서는 각 COS에 적당한 화일 구조와 명령어 등이 갖춰져야 한다[IC, 1998; 김철, 1996; Rankl, 1997]. COS는 마이크로 프로세서에 내장되어 있는 시스템

프로그램으로서 응용 프로그램의 H/W 접근을 가능하게 할뿐만 아니라 스마트카드의 기본적인 기능을 결정한다. COS의 주된 기능은 카드와 단말기 사이의 데이터 송수신, 명령어 수행 제어, 데이터 관리 그리고 암호 알고리듬의 수행 등이다. 이와 같은 COS는 처음에는 개개의 응용 분야 별로 개발이 되었으나 점차 통합 환경에서 여러 종류의 응용 프로그램에 대해 수행이 가능하도록 설계되어야 하고, 이를 위해 Multi-application OS 개발뿐만 아니라 응용 프로그램의 크기를 소형화하고 실행 속도를 높여주는 방법이 강구되어야 한다.

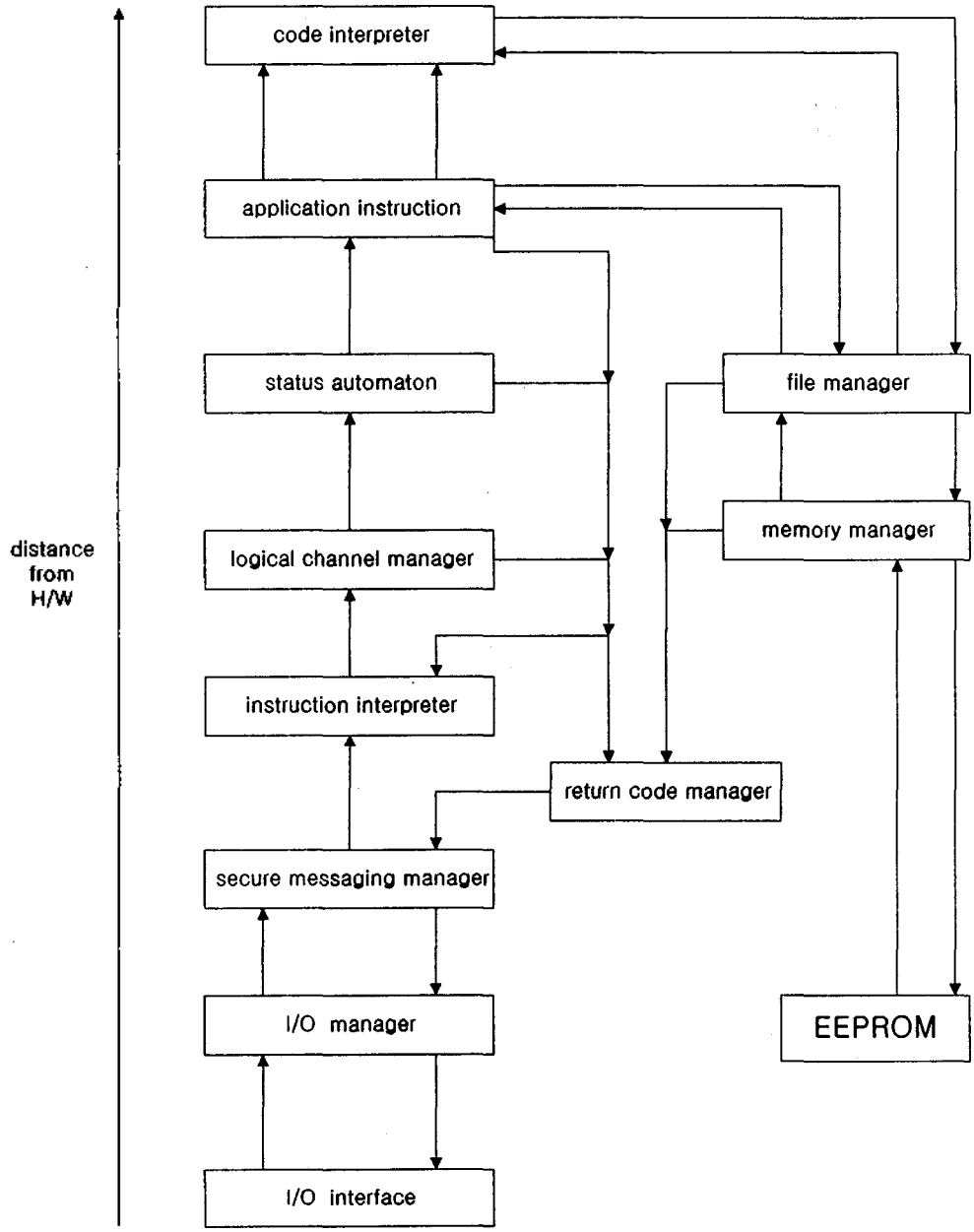
4.1.1 명령어 처리 과정

COS에서의 일반적인 명령어 처리 과정은 <그림 2>에 제시된 것과 같다. 우선 카드에서 수행될 명령들은 Serial I/O Interface를 통해 보내지고, I/O Manager는 에러를 체크한다. 검증된 명령어들은 필요시 Secure Messaging Manager에 의해 해독되고 Instruction Interpreter에 의해 해석된다. 만약 해석이 불가능하면 Return Code Manager가 Return Code를 생성한 후 I/O Manager를 통해 단말기로 보낸다. 반면 제대로 해석이 되어진 명령어는 Logical Channel Manager에 의해 Channel이 선택되어지고 다시 Status Automaton에 의해서 명령어의 상태가 체크된다. 그 후 Application Instruction 내의 코드는 Code Interpreter에 의해 수행되어진다. 만약 화일 참조가 필요하면 화일 Manager가 데이터의 Logical 주소들을 카드의 Physical 주소들로 바꾸어 주고 화일들의 Access 조건들도 체크 해준다. 또한 화일 Manager는 EEPROM을 관장하는 Memory Manager를 활용한다. 여기서 일반적인 처리 Module 들의 설계 시 고려 사항은 다음 Section에서 살펴본다.

4.1.2 설계 및 구현 원칙

S/W의 디자인 에러는 대부분 구현 시에 나타나며, 이를 수정하기 위해서는 많은 대가를 치루게 된다. COS와 같이 소형이며 안정성이 최우선인 S/W의 설계 시에는 더욱 이를 고려하여야 한다. 이와 같은 관점에서 볼 때 적은 비용으로 안정성을 높이기 위하여 Module들을 이용하는 Modular Design 방식이 요구된다.

현재의 COS 설계는 H/W-dependent Assembly어를 사용하는데 반해 앞으로는 C나 Java와 같은 고급 언어를 점차 사용하여야 할 것이다. 그러나 COS의 Core 부분은 여전히 Assembly어를 사용해야 하고 화일 Manager, State Automaton, Instruction Interpreter 등과 같은 Module들은 고급 언어로 프로그램이 가능할 것이다. 그리하면 개발 시간이 단축되고, 테스트가 한층 용이해 짐으로 인해 보다 높은 안정성이 확보될 수 있다. 그런 반면 C와 같은 고급 언어로 작성된 프로그램은 같은 기능을 하는 Assembly어로 작성된 프로그램 보다 20% 내지 40%의 ROM이 추가로 더 필요할 뿐만 아니라 RAM도 더 요구된다. 이런 현상은 칩의 제한적인 면적의 한계 때문에 당장 극복하기 어려우나 장차 고집적 반도체 기술의 개발로 실현이 가능하다.



<그림 2> COS의 일반적인 명령어 처리 순서

4.1.3 프로그램 코드 구역 정의

스마트카드의 칩은 최초에 ROM에 프로그램 코드가 들어 있고 EEPROM은 비어 있다. 이러한 가장 큰 이유 중의 하나는 1-bit 당 EEPROM에서 차지하는 면적이 ROM에서 차지하는 면적 보다 4배나 더 크기 때문이다. 따라서 Cost의 상승과 면적의 한계성 때문에 단지 필요한 데이터만 EEPROM에 저장되며, 경우에 따라 특별한 암호화 알고리듬이나 명령어 등이 Load 되기도 한다. 이와 같은 EEPROM은 대체로 5개의 영역으로 구분된다. 첫 번째 영역은 H/W-protected 부분으로 한번 기록된 데이터가 다수 회 참조되는 부분이고, 두 번째는 COS 관련 테이블이나 포인터가 저장되는 영역이고, 세 번째는 응용 프로그램 영역으로 특수 응용 명령어나 알고리듬이 자리하는 부분이며, 네 번째 영역은 화일 구조에 대한 정보를 저장하고, 마지막으로 화일 처리를 위해 필요한 여분의 메모리 영역이 존재한다. COS는 항상 메모리 사용에 대한 관리를 한다. 한가지 EEPROM의 단점은 읽고 쓰는 횟수에 제한이 있고 시간이 1ms/1byte 정도 걸리며. RAM은 ROM이나 EEPROM과는 달리 전압이 공급되지 않으면 모든 데이터가 소실된다[Hendry, 1997]. 따라서 일반적인 256-byte RAM은 10-byte Register, 26-byte Stack, 50-byte 변수 영역, 70-byte 암호화 알고리듬을 위한 Working Space 그리고 100-byte I/O Buffer 등으로 구성되어져야 한다. 100-byte보다 훨씬 큰 I/O Buffer가 필요한 경우에는 RAM의 자료를 모두 EEPROM에 저장하고 RAM 전체를 사용할 수도 있다. 그러나 EEPROM의 Access 속도가 상대적으로 무척 느리기 때문에 결국 RAM의 크기를 증가 시켜서 이를 보완해 주는 방법이 제한된 면적 내에서 고려되어야 한다.

4.1.4 스마트카드의 데이터 구조

최초의 스마트카드는 직접 주소 방식을 주로 사용하였으나, 최근에는 복잡한 계층 구조 화일 형식에다 논리 주소 방식을 사용하고 있다. 모든 화일들은 Hexadecimal Code의 주소로 지정되며 화일 관리자는 메모리 사용을 최소화하도록 설계되어 있다. 또한 Object-oriented COS의 개념을 이용하여 화일을 처리하며, 이 화일들은 화일 구조와 액세스 조건을 포함하는 헤더와 데이터를 포함하는 바디의 두 부분으로 형성된다. 이 바디 부분의 데이터는 헤더를 통해서 액세스가 가능하며 헤더와 바디는 EEPROM 상의 서로 다른 장소에 위치한다. 헤더의 내용은 사용자에 의해 변동이 불가능하고 따라서 우발적인 삭제나 참조로부터 보호되어진다. 따라서 한 개의 응용 프로그램이 존재하는 스마트카드에는 한 개 이하의 DF가 필요하고, 복수개의 응용 프로그램에 대해서는 그에 상응하는 수의 DF가 필요하다. 한 예로 만약 한 개의 스마트카드를 전자지갑과 의료정보용으로 사용한다면 하나의 MF 밑에 두 개의 DF가 존재하고 각 DF 밑에 관련 EF들이 존재하게 된다. 또한 화일을 액세스하기 위한 한 방법으로 2 byte의 FID(File ID)를 사용할 수 있는데, MF는 지정된 '3F00'를 갖는다. 따라서 GSM에서는 DF의 첫 번째 Byte가 '7F'를 갖고, MF 밑의 EF는 '2F'를 가지며 DF 밑의 EF는 '6F'를 고유하게 갖게 한다.

이와 같이 함으로서 화일의 구분과 액세스 처리를 화일 매니저가 효율적으로 한다.

스마트카드의 화일 구조 종류로는 Transparent, Linear Fixed, Linear Variable, Cyclic 등을 들 수 있다. Transparent 화일 구조는 Binary 형태를 갖춘 이상적인 구조로 Read/Write시 오프셋을 이용하여 Byte나 블록 단위로 액세스가 가능하기 때문이다. 사용되는 명령어로는 Read/Write/Update Binary가 있으며 오프셋이나 한번에 액세스 가능한 블록 크기는 실질 메모리의 크기에 따른다. 이와 같은 화일은 Digitized Passport 사진 같은 작은 양의 데이터를 저장하는데 쓰인다. Linear Fixed 데이터 구조는 Byte들의 집합인 동일한 길이의 레코드들의 모임으로서 각 레코드 단위로 액세스가 가능하고 Read/Write /Update Record 명령어가 사용된다. 레코드 번호는 1부터 254까지이며, 각 레코드의 크기는 1부터 254 Byte의 정해진 길이를 갖는 것으로 전화번호부 화일 등이 있다. Linear Variable 구조는 Linear Fixed 화일에서의 메모리 낭비를 줄이기 위한 방법으로 각 레코드는 필요한 만큼의 공간만을 사용하고, 길이를 지정해 주는 데이터 필드를 필요로 하며 그 외 특성은 Linear Fixed 구조와 같다. 이 방법은 스마트카드와 같이 제한된 메모리 용량의 사용을 극대화시키는데 큰 이점이 있다. 마지막으로 Cyclic 데이터 구조는 254 Byte 이내의 일정한 길이의 레코드들이 254개 이하 존재하며, 현재 레코드를 기준으로 이전 레코드와 다음 레코드로 불러어져 액세스된다. 이 기법은 스마트카드의 프로토콜 화일에 이용되며, 가장 오래된 레코드가 제일 먼저 새 레코드에 의해 치환됨으로 인해 작은 메모리 영역을 효율적으로 사용할 수 있는 이점이 있음으로 적절하다.

4.1.5 Atomic Routines 기능

Atomic Routine이라는 것은 작은 단위의 S/W로서 일단 실행을 시작하면 반드시 끝내야 되는 부분으로 Critical Section과 같은 의미이다. 스마트카드가 단말기 내에서 작동 중에 실수로 카드를 제거하거나 전기 공급이 순간적으로 중단되는 경우 EEPROM 화일의 내용을 부분적으로만 갱신하는 등의 문제점을 처리하기 위하여 사용된다. 특히 전자지갑과 같은 경우 잔고를 갱신하는 중에 이와 같은 일이 일어나면 무척 심각한 사태를 초래할 수 있다. 스마트카드 H/W는 Atomic Routine 문제를 처리해 주지 않기 때문에 S/W적으로 처리하는 수밖에 없으며, 이 처리 과정은 다음과 같이 가능하다. 우선 필요한 모든 데이터를 저장할 수 있는 버퍼와 State Flag을 EEPROM에 설치한다. State Flag은 버퍼 데이터의 Valid와 Invalid를 가리킨다. 첫째로 화일의 데이터가 물리적인 주소 및 길이와 함께 버퍼에 복사되고 Flag은 Valid로 세팅된다. 다음으로 COS가 새 데이터를 화일의 그 주소에 기록하고 Flag을 Invalid로 세팅한다. 만약 ATR 이전에 COS가 부팅 되거나 새 데이터가 화일에 기록되는 중에 문제가 발생하면, 시스템이 리셋 된 후 Flag은 여전히 Valid 상태이므로 COS가 버퍼의 데이터를 해당 화일의 원래 주소에 Restore 한다. 단말기 조작자는 단말기의 경고음이나 메시지로부터 재 작업을 지시 받는다. 이와 같은 Atomic Routine 방

식은 두 가지의 해결 해야할 문제점을 갖고 있다. 첫째는 버퍼 영역에 대한 수많은 기록 및 삭제로 인한 EEPROM의 수명 단축이고, 둘째는 버퍼 처리 때문에 스마트카드 처리 시간이 2, 3배 더 걸리는 것이다. 여기서 첫 번째 EEPROM의 수명 단축 문제는 버퍼의 위치를 주기적으로 바꿔줌으로 인해 EEPROM 상의 한 부분만을 집중적으로 사용하는 것을 피함으로서 어느 정도 해결할 수 있다. 두 번째로 처리 시간 지연 문제는 중요한 화일의 처리 때만 버퍼를 사용하는 방식으로 향상시킬 수 있다.

4.1.6 저장 Data 보호와 보안 기능

스마트카드의 ROM에는 COS 및 암호 알고리듬 등이 저장되어 있고, EEPROM에는 PIN과 Key를 비롯한 데이터 화일들이 저장되어 있다. 일반적으로 IC 칩의 설계는 VHDL (Very-High-Speed-IC Hardware Description Language) Core Library를 이용하여 CPU와 메모리가 단일 칩 상에 설계되므로, 내부의 기억 내용을 알기 위해서는 칩 분해를 해야 한다. 따라서 스마트카드와 단말기의 H/W를 포함한 암호화 칩을 에폭시 수지 등으로 처리하면 이를 물리적으로 벗겨낼 때 칩이 손상되거나, 빛 혹은 공기와 접촉 시 회로가 파괴되는 기법을 응용할 수 있다. 또 전기적으로 무리하게 EEPROM 등의 내용을 읽으려고 시도할 때 내장되어 있는 특수한 논리회로에 의하여 자동 삭제되는 자폭기능(Kill Bit Logic)을 설치한다면 스마트카드의 내용을 역추적 하는 Reverse Engineering은 사실상 거의 불가능하며 저장된 화일들은 안전하게 보호될 수 있다.

또한 1999년 5월에 Visa Smart Card의 Protection Profile이 공지되어 있는 상태이다. 이 드래프트는 ISO 15408을 근거로 Smart Card의 보안 요구사항을 취합/분석하여 산업계에 제공하려는데 있다. Target of Evaluation(TOE)은 집적회로, OS, 그리고 응용 프로그램 등으로 IC Card의 제조, Common /Application Data File의 실행, 암/복호화 기능에 대한 기준 등이 포함된다 [VISA, 1999].

4.2 S/W 테스트

S/W 에러 문제는 프로그램 역사이래 항상 존재하고 있다. 특히 스마트카드와 같이 대부분의 중요 프로그램이 ROM에 저장되는 경우에는 에러 발견 시 Debugging이 불가능하며, ROM 자체를 교환해야 한다. 따라서 다음과 같은 스마트카드 관련 S/W 테스트 방안이 요구된다.

스마트카드의 Security는 정보 저장의 보안뿐만 아니라 암호화 알고리듬의 완벽한 수행에 있으며, 관련 PIN이나 비밀키 들은 특별한 비밀 명령어로 액세스가 가능하다. Security는 카드 제조 시뿐만 아니라 PIN이나 비밀키가 로드 되는 초기화 및 발급 단계에서도 신중히 고려되어야 한다. 특히 기존 명령어들의 합성에 의한 오 동작으로 데이터를 읽거나 쓸 수 있는 경우도 배제 시켜야 한다. 스마트카드의 Security는 응용 프로그램 제공자가 직접 테스트를 할 수 있으나 이는 한계가 있고, 제 삼의 공인된 기관이 수행할 경우가 가장 합리적이다. 이와 같은 S/W의 객관적인 신뢰성을 측정하기 위해 미 국방성에 의해 TCSEC(Trusted

Computer System Evaluation Criteria)가 출판되어 범 세계적인 모델이 되었으며 유럽도 이에 근거하여 ITSEC(Information Technique System Evaluation Criteria)를 1990년에 발표하였다. ITSEC는 3가지 위험을 상정하고 있다. 즉 데이터에 대한 무자격자의 접근(Confidentiality), 데이터에 대한 권한 밖의 변경(Integrity), 기능에 대한 권한 밖의 변경(Availability) 등에 대한 설계 및 테스트를 함으로서 Security의 신뢰성을 제고한다[Rankl, 1997].

스마트카드 COS는 각 Module별 설계 및 테스트 그리고 통합 테스트를 거쳐서 설치하게 된다. COS는 모든 응용 케이스에 대해 일일이 테스트를 해야 하는 반면, 응용 프로그램에 있어서는 DF나 EF들의 데이터들에 연관된 테스트만을 실행해야 한다. COS에 대한 테스트는 다음에 나열한 순서대로 진행해야 하는데, 우선 전송 테스트를 완료함으로서 나머지 테스트들을 위한 바탕을 마련한다.

(a) 데이터 전송 테스트
- ATR 및 PTS(패리티 에러, ATR/PTS 구조 및 내용)
- 데이터 전송(Start/Data/Stop-bits, 전송 규칙 등)
- 전송 프로토콜 T=0/1
- Messaging 보안 문제

(b) 명령어 테스트
- 가능한 모든 Class 및 명령어 Bytes
- 모든 명령어의 기능
- Micro/Macro 명령어 순서

(c) 화일 테스트
- MF, DF의 정의 및 위치
- 화일의 크기, 구조, 속성, 내용 및 액세스 조건

5. 결론

1974년 스마트카드의 개념이 처음 소개된 이래 지금까지 그 탁월한 보안성과 편리성의 잠재력 때문에 스마트카드는 금융 뿐 아니라, 교통, 통신, 사용자 접근 제어, 인터넷 전자상거래에 이르기까지 사회 전반에 걸쳐 급속히 그 응용력을 확대해 나가고 있다. 근래에 들어 인터넷이 발전하고 PC를 이용한 상거래 및 각종 보안 제품이 출시되면서 개인의 신분 증명과, 지불수단, 공개키 기반구조에서의 Key 저장용 등으로 스마트카드가 각광을 받고 있다.

이에 본 연구에서는 기존의 스마트카드 관련 기술과 국제적인 표준화 동향을 검토하고, 국내에서 스마트카드를 설계할 때 안전성과 편리성 그리고 호환성에 따른 COS의 설계를 위한 지침을 분석하였다. 그에 따라 고 집적화 된 Chip에 필요한 프로그램과 데이터를 저장하기 위해 FeROM 등 새로운 메모리 이용이 요구되고 있다. 또한 S/W의 안전성 확보를 위해 제시된 테스트 방법론이 디자인 시 반드시 고려될 때 스마트카드의 보안성 및 신뢰성을 확보할 수 있다. 특히 비정상적인 Transaction의 종료시에는 Atomic Routine 개념을 도입함으로써 데이터의 안정성을 보장받을 수 있다.

따라서 제시된 스마트카드 모델 설계의 기준에 의하여 S/W 및 데이터의 안정성이 확보되고 이의 활용이 확산될 것이다.

참고 문헌

[ISO, 1997] ISO, 'ISO 7816', International Org. For Standardization, 1997

[ISO, 1985] ISO, 'ISO 1177', International Org. For Standardization, 1985

[EMV, 1996] EMV, 'EMV 3.0 Integrated Circuit Card Specification for Payment Systems', 1996

[Tenen, 1997] J. Tenenbaum, T. Chowdhry, S. Hughes, 'An Internet Commerce Architecture', IEEE Computer, May 1997

[Rivest, 1978] R. Rivest, A. Shamir, L. Adleman, 'A Method for Obtaining Digital Signatures and Public-key Cryptosystems', Communications of ACM, Vol. 21, No. 2, 1978, pp. 120-126

[Hendry, 1997] M. Hendry, 'Smart Card Security and Applications', Artech House, 1997

[Thom, 1996] J. Thomasson, 'Advances in Smartcard IC Technology' ,SGS-Thomson, Technical Article TA164, 1996

[Glass, 1991] A. Glass, 'Why should secure cards be smart?', Proceedings of Smart Card 2000 Conference, 1991, pp. 39-50

[IEEE, 1997] 'IEEE Spectrum', IEEE, Feb. 1997, pp. 16-80

[F&G, 1997] 'Smart Card Technology International', Faulkner & Gray Inc., 1997

[F&G, 1998] 'Smart Card Technology International', Faulkner & Gray Inc., 1998

[정준원, 1998] 정준원, 정성원, 김영균, 이민우, '전자지불 시스템 기술 및 표준 동향 분석', 정보처리학회지, 제5권 제2호 1998, pp. 91-106

[IC, 1998] 한국 IC 카드 연구조합, 'IC카드 산업 동향 보고서', 1998

[PC/SC, 1997] PC/SC WG, 'PC/SC Specification Release 1.0', 1997

[ECDG, 1997] European Commission DG III, 'C-SET Specification', 1997

[김철, 1996] 김철, '암호학의 이해', 영풍문고, 1996

[Rankl, 1997] W. Rankl, W. Effing, 'Smart Card Handbook', John Wiley & Sons, 1997

[VISA, 1999] www.visa.com, Visa Smart Card Protection Profile, 1999

저자소개

황선태 (e-mail:hwang@dragon.taejon.ac.kr)

서강대학교 수학과 이학사
Case Western Reserve University 전자계산학과 석사
Case Western Reserve University 전자계산학과 박사
현재 대전대학교 정보통신공학과 교수
관심분야 : Smart Card, Security, VLSI Testing

이 형 (e-mail: hlee@dragon.taejon.ac.kr)
서울대학교 수학과 이학사
성균관대학교 전자계산학과 석사
조선대학교 컴퓨터공학과 박사
현재 대전대학교 정보통신공학과 교수
관심분야 : Graphics, Security