디지탈 서명을 사용한 선지불 IC 카드 데이타 보호 메카니즘

김종룡*,신현삼**○,염기환**,탁재영**
* 현대공고, ** 한국통신

A Mechanism of Secure Data in Prepaid IC Card using a Digital Signature

Kim-Jong ryong*, Shin-hyunsam**,Yum-Kihwan**, Tak-Jaeyoung**
* Hundai Technical high school, **Korea Telecom

요 약

본 논문에서는 IC 카드를 선지불카드로 사용하기 위하여, 카드 내의 데이타를 안전하게 보호할 수 있는 새로운 메카니즘이 제안되었다. 이 메카니즘에서는, 데이타 메모리가 OTPROM 영역과 EEPROM 영역으로 구분되고, 각 영역의 데이타는 논리적으로 서로 연동되게 설계되었다. 그리고 OTPROM 영역으로 되어 있는 특정영역에 대해서는 접근제어와 물리적 안전성이 제공되어 재사용 하는 것과 오류를 자동정정하는 것이 가능하다. 이 카드는 디지탈 서명 알고리듬을 사용하여 인증을 받은 사람에 의해서만 발급될 수 있다. 그리고 일반 사용자는 인증과정을 수행하지 않으므로 사용이 간편하다.

1.서론

IC 카드는 플라스틱제의 카드에 마이크로프로세서 및 반도체 메모리를 내장한 매체이다. 자기 줄무늬(magnetic stripe)가 부착된 종래의 카드의 기억용량이 72 바이트인 것에 비해 IC 카드는 2 ~ 8 킬로바이트로 10 ~ 100 배 정도의 용량[1][2]이 있고, 또 그 내용도 마이크로프로세서를 이용하여 다른 사람이 쉽게 접근할 수 없게 한 것이 특징이다.[3][5] 따라서 IC 카드는 공중전화카드와 같은 선지불카드와 다양한 정보를 수록한 전자신분증, 신용카드 등 여러 분야로 그 이용과 보급이 확산될 전망이다.

IC 카드가 선지불카드나 신용카드로 이용되면 현금의 역할을 대신하게 되므로 카드의 위조나 카드 내부의 데이타 변조, 손실 등에 대한 철저한 대비책이 마련되어야 한다. 현재 국내에서는 공중전화카드를 IC 카드로 대체하기 위하여 일부 지역에서 시험 운용 중에 있다. 그리고 현재 사용되고 있는 IC 카드는 단순 메모리카드로서 카드 내부의 데이타 변조에 대한 대비책으로 금액의 감소만 가능한 물리적인 구조를 채택함으로써 재사용이 불가능하도록 되어있다. 재사용이 되지못할 경우 카드의 제조단가와 버려진 카드로 인한 환경오염 등의 문제점이 있기 때문에 재사용이 가능한 새로운 형태의 IC 카드에 대한 연구가 이루어져야 한다.

안전성의 제고를 위하여 카드 사용 단말기에서 개인식별번호나 비밀번호를 입력하여 인증작업을 수행할 수 있다. 그러나 일반 사용자가 카드를 사용할 때마다 인증작업을 수행하는 것은 처리 시간이 길어지거나 데이타의 양이 많아지는 단점이 있다. 따라서 공중전화카드와 같이 대중성이 있는 선지불카드는 간편한 절차로 사용될 수 있도록 개발되어야 한다.

본 논문에서는 IC 카드가 재사용될 수 있고 또한 간편하게 사용될 수 있도록 하기 위한 방안으로 새로운 메카니즘을 제안한다. 제2장에서는 데이터의 변조를 효과적으로 방지할 수 있고 재사용이 가능한 새로운 IC 카드의 데이터 보호 메카니즘을 제안 하였으며 제3장에서는 인증과정의 안전성과 카드 내부의 데이타에 대한 안전성을 분석하였으며 제4장에서는 불법자의 공격 유형을 분석하고 대비책에 관하여 고찰하였다.

2. 선지불 IC 카드 데이타 보호 메카니즘 제안

2.1. 기존의 데이타 보호 방법 및 문제점

현재의 데이타 보호 방법중 한 가지는 PROM형태의 메모리를 권종금액에 해당하는 도수만큼 비트단위로 부가하고 한 도수 사용할 때마다 한 비트씩을 지워나가는 방식이다. 또 다른 방식은 금액영역의 데이타는 EEPROM 영역으로 만들어 금액 및 금액백업 정보를 기록하거나 지울 수 있도록 하되 원래의 금액과 비교하여 감소될 수는 있어도 증가되지는 못하게 하는 논리회로를 첨가하는 방식이다. 이러한 방식들은 위조나 변조를 하더라도 원래금액 이상이 되지 않게 하는 것으로서, 안전성은 있으나 재사용할 수 없는 단점이 있으며, 사용 후 버려졌을 때 환경오염을 일으킬 수 있는 문제점도 있다. 또한 이러한 방식은 금액 및 금액백업정보가 동시에 지워지는 경우가 발생할 수 있다

2.2. 새로운 데이터 보호 메카니즘의 제안

본 논문에서는 IC 카드가 선지불 카드로서, 간편하게 사용될 수 있고 또한 위조 및 변조 없이 안전하게 재사용될 수 있도록 하기 위한 방안으로 새로운 메카니즘을 제안한다.

카드내의 데이타를 안전하게 보호하기 위하여 물리적으로 재생할 수 없는 영역과, I/O 단자를 통하여 데이타의 기록/삭제가 가능한 영역으로 데이타메모리를 구성하였다. 그리고 논리적인 방법으로 카드내의 데이타가 특정영역에 연동되게 설계하였다. 또한, 사용상의 편의를 위하여 사용자가 이용하는 영역은 인증과정을 수행하지 않고 자유롭게 데이타의 입출력이 가능하도록 하고, 특정영역을 따로 두어 이 영역에는 일반사용자의 접근을 금지시키고 발행자만 RSA 디지탈 서명 방식[4]을 사용하여 인증절차를 거친 후 접근이 가능하도록 설계하였다. 즉, 발행자가 카드를 발급할 때만 *Master* 카드를 사용하여 인증절차를 거치도록 하고 일반 사용자는 인증절차 없이 간편하게 사용할 수 있도록 IC카드를 설계하였다. 발행자의

인증절차는, 먼저 정당한 발행자임을 확인하고 다음으로 Master 카드의 적법성을 확인한다. 접근후 물리적인 방법으로 기준잔액을 산정하고 이를 토대로 잔액에 대한 오류 발생시 자동정정되도록 하였다.

2.2.1. 제안된 IC 카드의 메모리 설계(memory map design)

본 논문에서 제안하는 카드의 메모리는 1K비트의 메모리를 가정하여 설계하였으며 실제 제작시는 재사용 횟수를 감안하여 확장할 수 있다. 그 구조는 그림 1에서와 같으며 제조자영역(manufacture section, MFS)에는 칩제조자 정보, 제조년도, 로트번호, 주문자코드 등이 기록되며 ROM type으로 만들어진다. 발행자영역(issuer section, IRS), 마스트비트영역(master bit section, MBS), 카운트비트영역(counter bit section, CBS)과 시큐리티비트영역(security bit section, SBS)은 OTPROM(one time programmable ROM) type으로 만들어진다. 발행자영역에는 국가코드, 카드종류코드, 카드권종코드 등 발행자의 필요한 정보를 기록할 수 있다.

번지	초기상태	명칭
0 3		MFS
4 8		IRS
9	11111111	MBS
10	11111111	CBS
11 15	11111111 11111111	SBS1
16 20	11111111 11111111	SBS2
21 25	11111111 11111111	SBS3
26 27	11111111 11111111	CDS
28 127	11111111 11111111	UDS

그림 1. 제안된 IC 카드의 메모리 설계

마스트비트영역은 재사용 횟수가 계산되며 제조당시 이 영역은 모든 비트가 "1"로 세트되어 있고 그 상태로는 사용할 수 없으며, 최소 1회의 데이타 입력작업을 거친 후 사용이 가능하다. 즉, 발행자의 인증작업을 거친 후 사용되도록 하였다. 그리고 두 번의 재사용을 위하여 한번 발급할

때마다 상위의 2비트씩을 지우도록 설계하였다. 이 영역은 시큐리티비트영역을 비롯하여 모든 카드 동작의 기준이 되고 이 영역에 접근하기 위해서는 인증작업을 거쳐야 한다. 카운트비트영역은 불법으로 마스트비트영역에 접근을 시도하는 경우 그 횟수를 계산한다. 시큐리티비트영역은 1회의 최초사용과 2회의 재사용을 위하여 3개의 소영역으로 구분하였다.

금액영역(cash data section, CDS)과 사용자영역(user data section, UDS)은 EEPROM type으로 제조되어 전기적으로 기록 및 삭제가 가능하며 금액영역에는 현재 남은 금액이 기록된다. 사용자영역은 사용자의 개인적인 정보를 저장하거나 발행자가 특수한 서비스를 제공할 목적으로도 사용될 수 있다.

논리적인 방법으로 카드 내의 모든 데이타가 마스트비트영역에 연동되게 하였으며 이 영역에는 일반 사용자의 접근을 금지시켰다. 금액영역의 데이타는 마스트비트영역의 제어를 받으므로 카드 내부 데이타의 변조를 방지하고, 일반 사용자가 카드를 사용할 때는 인증과정을 수행하지 않아도 되기 때문에 간편하게 사용할 수 있도록 하였다. 그리고 물리적으로 재생이 되지 않는 영역인 시큐리티비트영역의 데이타로 기준잔액을 산정하고, 이를 토대로 잔액에 대한 오류 발생시 내부 프로그램에 의해 자동정정되도록 하였다. 발행자가 카드를 발급할 때는 Master 카드를 사용하여 디지탈 서명 방식을 사용한 인증절차를 거치도록 하였다.

2.2.2. IC 카드내의 CPU의 기능

IC 카드 내의 CPU는 인증작업시 연산 수행과 각 메모리의 영역이 연동되게 하는 기능의 수행, 외부로부터 들어오는 명령어의 해독작업을 수행하기 위하여 사용되어지며 그 프로그램은 ROM 영역에 보관된다.

(1) 각 영역별 메모리의 연동 기능

① MBS는 제조당시에는 모두 "1"로 세트되어 있고 한번 발급할 때마다 상위의 두 비트씩을 지우도록 하며 그 내용이 3F(hex)이면, CDS와 SBS1을 연동시키고 카드권종금액의 1/40 감액시 마다 SBS1의 상위 한 비트를 지운다.

② MBS의 내용이 0F(hex)이면 SBS1을 Clear시키고 CDS를 Set시킨다. 그리고 CDS와 SBS2를 연동시키고 카드권종금액의 1/40 감액시 마다 SBS2의 상위 한 비트를 지운다.

③ MBS의 내용이 03(hex)이면 SBS1, SBS2를 Clear시키고 CDS를 Set시킨다. 그리고 CDS와 SBS3을 연동시키고 카드권종금액의 1/40 감액시 마다 SBS3의 상위 한 비트를 지운다.

④ MBS의 내용이 00(hex)이면 CDS, SBS1, SBS2, SBS3을 Clear시킨다. (재생 불가능 상태)

⑤ MBS의 내용이 FF(hex)이면 카드의 모든 동작이 Locking된다.

⑥ MBS에 기록 작업시는 디지탈 서명 방식의 인증과정을 거치게하며 적법자로 확인되면 기록을 허용하고 틀린 경우 CBS의 두 비트를 지우며 CBS의 내용이 00(hex)이면, MBS를 Clear 시킨다.

(적법자든, 비적법자든 틀린 횟수가 4회가 되는 순간 재생 불가능 상태로

전환)

(2) 오류 발생시 정정기능 및 금액에 대한 Security 기능

① MBS 의 내용이 3F(hex)이면 SBS1을 기준으로 하며, 금액영역의 기록 작업시에는 다음의 과정을 수행한다.

● 현재 남은 SBS의 비트수를 카운트하여 기준잔액 범위를 산정한다.

비트당 금액 = 카드권종금액 ÷ 40

기준잔액 = 현재 남은 비트수 비트당 금액

기준잔액 범위 = 기준잔액 ~ (기준잔액-비트당금액)

● CDS의 데이타가 기준잔액 범위를 벗어난 경우 기준잔액을 기록한다.

(불법 변조자가 금액을 변조하려 했을 경우나, 단말기의 오동작으로 인하여 오기(誤記)시 기준잔액으로 자동정정한다)

② MBS의 내용이 0F(hex)이면 SBS2를 기준으로 ①과 같이 동작한다.

③ MBS의 내용이 03(hex)이면 SBS3을 기준으로 ①과 같이 동작한다.

3. 인증과정

3.1. 인증과정에 관한 분석

본 논문에서 제안한 방식대로 설계된 대상 카드의 메모리에 데이터입력기를 이용하여 데이타를 입력할 때 거쳐야하는 2단계의 인증과정을 [그림 2]에 나타내었으며 인증 알고리듬은 RSA 디지탈 서명 방식을 사용하였다.

RSA디지탈 서명방식은 Rivest, Shamir 및 Adleman에 의해 제안된 RSA 공개키 암호법에 기반한 것이다. RSA시스템은 매우 큰 정수의 소인수 분해가 어렵다는 가정에서 설계된 것으로 암호시스템 구성은 다음과 같다.

(1) 암호시스템 구성

① 두개의 큰 소수 p와 q를 생성하여 n=pq를 계산한다.

② Eular 함수값 $\phi(n)=(p-1)(q-1)$과 서로 소가 되는 e를 계산한다.

$(\gcd(e, \phi(n)) \equiv 1)$

$\phi(n)$ 과 e로부터 유클리드 알고리듬을 사용하여 $ed=1(\mathrm{mod}\,\phi(n))$ 이 되는 d를 계산한다.

이로부터 다음과 같은 공개키 암호시스템을 구성한다

공개키 : n, e

비밀키 : d, p, q

암호화 : $C=E(M)\equiv M^d(\mathrm{mod}\ n)$

복호화 : $M=D(C)=D(E(M))\equiv C^e d \bmod n \equiv M^{ed} \bmod n$

공개키 암호 시스템에서 통상적인 서명의 특징을 만족시키면서 전자적으로 실현하는 방법은 다음과 같다. 여기에서 시스템 구성은 암호시스템과 동일하다.

(2)서명 생성과정

① A는 B로부터 메시지 M을 전송 받는다.

② 메시지 M을 0과 nA사이의 정수로 변환한 블럭을 구한다.

③ 블럭에 자신의 비밀키 dA를 멱승 하여 서명 S를 생성한다.

④ 서명 S를 B에게 전송한다.

(3)확인과정

① S에 A의 공개키 eA를 사용하여 M을 복호하여 전송한 M과 동일한지 확인하여 A임을 증명한다.

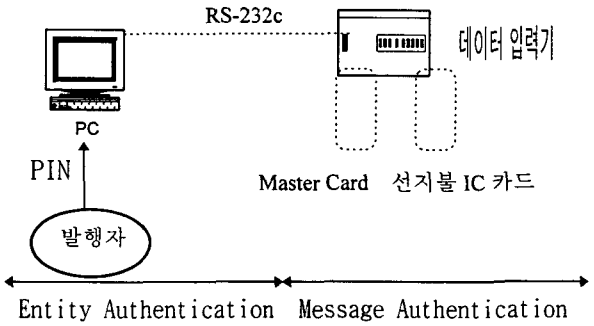

그림 2. 2단계의 인증과정

인증과정은 그림 2에서와 같이 사용자 인증(entity authentication)과 메시지 인증(message authentication) 으로 나누어 시행하도록 하여다.[6][7][8] 사용자 인증은 데이타 입력(최초 발급시 데이타 입력 및 재발급시 데이타 입력)작업을 허락 받은 적법자임을 인증하는 과정으로 데이타입력기를 운용하는 PC에서 PIN(personal identification number)을 입력하여 Master 카드로부터 인증을 받는 과정이다. 메시지 인증은 선지불 IC 카드로부터 Master 카드가 적법한 것인지를 인증받는 과정이다. 그 절차는 Master 카드는 선지불 IC 카드가 전송한 메시지를 자신의 비밀키로 디지탈 서명을 하여 선지불 IC 카드로 되돌려 보낸다. 그리고 선지불 IC 카드는 자신의 메시지와 서명을 복호한 값과 비교하여 동일하면 사용자의 접근을 허락한다.

Master 카드와 선지불 IC 카드 사이의 인증작업이 한 대의 데이타입력기 내에서 이루어지기 때문에 어떠한 데이타도 외부로 유출되지 않는다. 그러므로 인증과정은 안전하다고 볼 수 있다.

4. 불법사용자의 공격에 대한 고찰

4.1 선지불 IC 카드 내부 데이타의 변조를 시도하는 경우

선지불 IC 카드를 물리적으로 내부의 데이타를 분석한 후 데이타를 변조하여 불법으로 사용하는 경우를 예상할 수 있다. 기존의 방식으로 사용되는 단순 메모리카드의 경우는 분석이 비교적 쉬우므로 메모리에 접근할 수 있다. 그러나 메모리를 제어하는 논리회로 부분을 제거해야 되는데, 일단 물리적 분석(칩의 개봉)된 것은 다시 사용하기 어려우므로 변조하기 어렵다. 본 논문에서 제안하는 방식의 경우도 분석은 가능하나 CPU의 제어 하에 메모리가 칩 내부에서 MBS의 상태에 연동된다. 그리고

MBS는 OTP type 이고 초기값을 최대값으로 세팅하기 때문에 변조해도 의미가 없다. 외부에서 I/O단자를 통하여 MBS에 접근하는 것은, 인증과정을 거쳐야되기 때문에 불가능하다.

4.2. Master 카드를 모방하는 경우

(1)접근 제어키로 사용되는 Master 카드를 모방하여 외부에서 접근을 시도하는 경우

많은 선지불 IC 카드의 물리적인 분석을 통해 선지불 IC 카드의 식별자에 따른 종류별 공개키를 분석하여 Master 카드의 비밀키를 풀려고 시도하는 경우를 예상해 볼 수 있다. 그러나 비밀키는 Master 카드의 비밀영역에 보관되므로 카드 소지자 자신도 풀기 어렵다. 2차적인 안전장치로 공격자가 물리적 분석을 해도 경제적으로 의미가 없을 정도의 충분히 많은 종류의 식별자를 만들어 제조년도별로 랜덤하게 사용하고 단말기에서 인식하도록 할 수 있다.

(2)시행 착오법으로 접근을 시도하는 경우

불법 시도 횟수를 카운트하여 4회 이상의 불법 시도시 영원히 사용 할 수 없게 한다

4.3. Master 카드와 선지불 IC 카드를 둘 다 모방하는 경우

(1) PIN을 아는 사람(예: 발행자의 직원이었던 사람)에 의해 Master 카드가 도난 당한 경우를 예상할 수 있다. 이 경우는 법적/제도적 방지 대책과 관리적 방지 대책으로 예방되어야 할 것이며 범죄 징후가 탐지되는 즉시 조치를 취할 수 있기 위해서는 Master 카드마다 고유의 ID가 있어야 한다. 또한 사고 ID를 가진 Master 카드의 사용을 막기 위해서는 각 Master 카드의 ID가 비밀키의 일부로 첨가되고 단말기에서 인식하여 사용을 방지할 수 있다. 그러나 단말기의 원격관리가 전제되어야 하므로 Master 카드를 철저하게 관리하여 사전에 예방해야 한다.

(2) 카드사용단말기(공중전화기 등...)를 속이는 경우

단말기를 원격관리하고 단말기와 선지불 IC 카드가 상호를 인증하는 작업을 수행하여 막을 수 있으나 사용상 편리성이 문제된다.

4.4. 위조하는 경우(복제하여 생산하는 경우)

(1) 칩의 복제에 의한 위조의 가능성

국내의 반도체 생산회사는 물론이고 외국에서 복제되어 들어오는 경우도 고려해야 한다. 복제를 막을 수는 없으나 단말기가 원격 관리된다는 전제하에서 단말기와 선지불 IC 카드가 상호를 인증하는 작업을 통하여 위조카드를 가려낼 수 있는데, 이 경우 사용상 편리성이 문제된다.

(2) 제조된 제품이 발행자의 손에 들어가기 전에 유출되는 경우

기존의 방식에서는 일단 1회는 사용되어질 수 있다. 그러나 제안하는 방식에서는 최초 사용 시에도 데이타 입력작업이 한 번은 이루어져야 하고 데이타 입력작업을 수행하기 위해서는 반드시 인증작업을 거쳐야 되기 때문에 1회의 사용도 불가능하다.

5. 결 론

본 논문에서는 IC 카드 내의 데이터를 안전하게 보호하기 위하여 물리적인 방법과 논리적인 방법을 병행하는 방식으로 메모리를 관리하였다. 그리고 물리적인 방법으로 기준잔액을 산정하고, 이를 토대로 잔액에 대한 오류 발생시 자동정정되도록 하여 데이터에 대한 신빙성을 높였다. 본 논문에서 제안된 IC 카드는, 인증작업시 데이타입력기의 외부로 데이타의 유출이 없으므로 인증과정이 안전하다는 것과 이 카드는 카드 내부의 데이타에 대하여 안전성이 있음이 분석되었다.

처리해야할 데이터의 양, 빠른 수행시간, 안전성 등을 충분히 고려한 인증 알고리즘의 개발에 관하여 연구가 이루어져야 할 것이며 IC카드에 적합한 CPU의 개발과 발행시의 편리성에 대하여도 지속적인 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] ISO, "*Identification cards - Recording technique - part2 : Magnetic stripe*," ISO/IEC 7811-2, 1992.

[2] 김장현 역, "프리페이드 카드의 실제와 도입의 안내," pp. 282-283, 세화출판사, 1993.

[3] Philips Communication systems, *Key management service, secret and public key systems*, PSSM, 1992.

[4] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Comm. of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[5] 한국전자통신연구소 : "현대암호학," pp. 197-201, 1991.

[6] Hans-Peter Konigs, "Cryptographic identification methods for smart cards in the process of standardization," *IEEE Comm. Magazine*, pp. 42-48, June 1991.

[7] A. Fiat and A. Shamir, "How to prove yourself : practical solutions to identification and signature problems," Proc. Crypto'86, pp. 186-194, May 1986.

[8] M.Hellman, "An overview of public key cryptography," *IEEE Comm. Society Mag.*, vol. 16, pp. 24-32, Nov. 1978.