



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

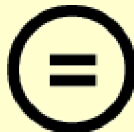
다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

工學碩士 學位論文

비접촉 교통카드를 위한 RFID
통합 플랫폼에 관한 연구



2009年 2月

釜慶大學校大學院

制御計測工學科

劉相榮

工學碩士 學位論文

비접촉 교통카드를 위한 RFID
통합 플랫폼에 관한 연구

指導教授 李 炯 基

이 論文을 工學碩士 학위논문으로 提出함



2009年 2月

釜慶大學校大學院

制御計測工學科

劉 相 榮

劉相榮의 工學碩士 學位論文을 認准함

2008年 12月



목 차

목차	i
Absrtact	iii
I. 서론	1
II. 본론	3
1. RFID의시스템 구성 요소	3
가. RFID 방식의 구분	3
나. RFID의 동작 원리	5
다. TAG	6
라. 안테나	7
마. 리더기	8
2. RFID 표준 ISO 방식의 고찰	9
가. RFID 활용 - 국내 교통카드의 예	9
3. 통합 플랫폼의 구현	11
가. 시스템 구성도	11
나. 시스템 목표 사항	12
다. 키의 구성	14
라. 키의 계층 구조	15
마. F-SCAN 알고리즘	19
바. 구성회로도	22
사. 시스템 구성 모습	24

아. PC와 연계 동작	26
III. 실험 및 고찰	27
IV. 결론	31
참고문헌	33
감사의 글	34



A Study on RFID Integrated Platform for Contactless Traffic Card

Sang-Yeong YU

*Department of Control & Instrument Engineering Graduate
School of Pukyong National University*

Abstract

The RFID card is a essential element for ubiquitous environments. A representative application is contactless traffic card for public transportation system such as bus or subway. Especially, as RFID card is certified using the single in-line memory module (SIMM), it is activated as traffic card for specific public transportation system owned by a self-governing body. The international organization for standardization strives for usage of public key for RFID, it does not come into the market. This paper presents RFID integrated platform for contactless traffic card wherre various SIMM is installed to give convenience to customer and expand flexibility of RFID card.

I. 서론

RFID는 무선 주파수를 이용해 상품과 사물에 내장된 정보를 근거리에서 읽어내는 기술로써 물류, 유통, 조달, 군사, 식품, 등 다양한 사업 영역에서 경제적 파급 효과를 창출할 수 있는 핵심 기술로 각광받고 있다. 또한 최근 주목받는 유비쿼터스의 기초기술로 활용되어 사용이 점차 확대되고 있다.

일반적으로 RFID는 소형 전자 칩과 안테나로 구성된 전자태그를 사물에 부착하여 전자 태그의 고유 주파수를 통해 사물을 인식하거나 사물이 주위 사물을 인식할 수 있게 하여 기존 IT시스템과 실시간으로 정보를 교환/처리할 수 있도록 한다. 이 기술은 이미 2차 대전 당시 영국 공군이 적 전투기의 식별하는데 사용되어 현재는 민간의 RFID 기술이 도입되어 진화발전되었다.

이러한 RFID는 각종물류, 산업 현장 제조 공장과 물품의 흐름이 있는 곳이면 어디에서나 적용이 가능하다. 그래서 ISO(International Organization for Standardization) / IEC(International Electrotechnical Commission)의 JTC1(Joint Technical Committee) / SC(Sub-Committee)31 전문위원회를 중심으로 RFID global 표준화가 진행되고 있으며, 국내에서도 국내 표준이 정립된 상태이다. 그래서 최근 몇 년 사이에 RFID의 실용화를 위한 연구와 시범사업, 기업현장에 적용하는 사례가 활발하게 이루어지고 있다.

RFID의 중요한 부분은 정보의 안전성에 있다. 이 안전성은 SAM(Secure Access Module) 혹은 SIMM(Single In-line Memory Module)으로 인증된

사용자만이 사용 가능 하게 되어 안전성이 보장된다. 하지만 여러 이해 집단에서 각각의 키를 제조 생성하게 되었고, 단말기 등의 사용 또한 이 키에 따라서 승인된 사용자만 사용 가능하게 한다.

국가 표준화 단체에서도 이점을 파악하여 공용키의 사용을 위한 개발에 들어가 진행 중에 있으나, 아직 사용은 되고 있지 않다. 여러 가지 종류의 키를 사용가능 하게 하는 통합 플랫폼의 개발은 사용하고자 하는 키를 부착 시 바로 사용 가능 하게 하는 이점이 있고 또한 차후에 발생하는 새로운 키의 대응에서도 빠른 능력을 가진다.

본 논문에서는 여러 가지 SIMM을 공통으로 사용하는 플랫폼의 단말기를 구현하는데 사용상의 용이함을 구하고 차후에 발생하는 다른 키의 발생으로 인한 개발 손실을 줄이는데 그 목적이 있다.



II. 본론

1. RFID의 시스템 구성 요소

RFID 시스템은 리더, 안테나, 태그 세가지로 구성되어서 비접촉식으로 정보를 인식한다.

일반적으로 많이 사용되는 수동형 시스템은 RFID의 리더인 RF캐리어 신호를 송신하고, 신호를 받은 태그는 RF 신호가 들어오면 이것의 진폭 또는 위상을 변조하여 태그에 저장된 데이터를 리더로 송신한다. 태그로부터 되돌려 받은 변조신호는 리더에서 복호/복조화 되어 태그정보가 해독되는 것이 기본 원리이다. 태그는 고유의 ID를 가지므로 복제 등의 영향이 적다.

가. RFID 방식의 구분

RFID시스템의 주요방식은 크게 태그의 읽고/쓰기(READ/WRITE), 전원 유무, 리더, 태그 간 Air Interface로 구분할 수 있다.

표 1에서 태그에 동작에 따른 RFID시스템의 구분을 표시 하였다.

표 1 . RFID 구분

RFID 방식별 구분		주요특징
태그 Read/Write 능력	읽기전용 (Read Only)	<ul style="list-style-type: none"> • 제조시 프로그래밍 정보내용은 변경 불가 • 가격 저렴하여 바코드와 같이 단순 인식 분야 사용
	한번 쓰고 여러번 읽기(WORM)	<ul style="list-style-type: none"> • 사용자가 데이터 기록 후 변경 불가
	읽기 쓰기 (Read/Write)	<ul style="list-style-type: none"> • 몇 번이고 기록 및 데이터 변경이 가능 • 고가이지만 다양한 분야에서 사용가능
태그 전원유무	능동형 (Active)	<ul style="list-style-type: none"> • 태그에 배터리등의 전원 부착 • 수십m 원거리 통신 가능 • 가격고가, 수명 제한, UHF대역사용
	수동형 (Passive)	<ul style="list-style-type: none"> • 태그에 전원 없음 • 10m이내 근거리 통신용 • 가격이 저렴하고 수명이 반영구적 (약10년이상)
무선 주파수 대역	135kHz 이하	<ul style="list-style-type: none"> • FA용 동물인식등 근거리용도 • 시스템 가격이 저렴
	13.56MHz	<ul style="list-style-type: none"> • IC카드 신분증등 1m 이내에서 활용 • 데이터 전송상의 신뢰성이 높음
	UHF 파	<ul style="list-style-type: none"> • 433MHz(Active),860-950MHz 대역 • 마이크로파 대역에 비해 무선 인식 성능 우수 • ISO/IEC, EPC 태그등 국제적으로 활성화 전망
	마이크로파	<ul style="list-style-type: none"> • 2.45GHz의 ISM 대역 이용 • UHF 대역에 비하여 수분, 금속 적용환경에서 인식을 저하

나. RFID의 동작 원리

RFID 기술은 원거리에서도 물리적인 접촉없이 인식이 가능하고, 여러 개의 정보를 동시에 판독하거나 수정할수 있는 장점 때문에 바코드를 대체하거나 보완할 수 있는 기술로 현재 유통 분야 뿐 아니라 물류, 교통, 보안, 가전 분야에 까지 나날이 확대 적용되고 있다. 이 RFID 시스템은 리더, 안테나, 태그 등 세가지로 구성되어 사람, 차량, 상품 교통카드 등을 비접촉식 태그를 이용하여 인식하게 하는 기술이다.

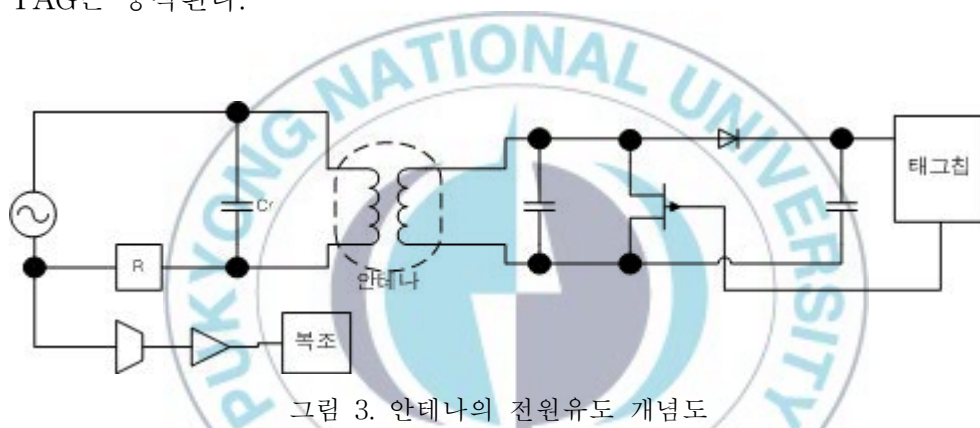


그림 2. RFID의 구동 개략 흐름도

다. TAG

TAG는 표 1과 같이 구분되어 지고 그림1과 같이 통합된 안테나를 갖춘 IC 칩을 일컫는 말이다. 이는 장비나 사물에 부착되어 수동 또는 능동형으로 동작하고, 리더기에 정보를 제공하는 역할을 한다.

그림 2와 같이 안테나에서 유도된 자기장은 정류기를 거쳐 전원을 유도하고 유도된 전원을 정류 하여 TAG에 필요한 전원을 얻고 이를 이용하여 TAG는 동작된다.



전자파 결합을 이용한 RFID 시스템의 경우 태그 칩의 소비 전력에 따라 인식거리가 결정된다. 태그칩의 전력 소모는 수백 μW 에서 수십 μW 로 발전하고 있다.

태그가 동작되는 소비전력을 알고 있으면 거리 r 에서 태그가 수신가능한 전력을 이용하여 인식거리를 식(1.1)을 이용하여 이론적으로 계산할 수 있다.

$$R \leq \frac{\lambda}{4\pi} \sqrt{\frac{EIRP \cdot G_{tag}}{P_{tag}}} \quad (1.1)$$

라. 안테나

안테나는 태그와 리더기에 부착되며, 정보와 전원의 송출과 생성의 역할을 하는 단위이다. RFID 상에서 사용되어지는 안테나는 크게 다이폴 타입, 유도결합 미-앤더 타입 등방에 가까운 방사 패턴 타입이 사용되어지며, 이중 태그 안테나는 제조사의 레퍼런스를 사용하는 경우가 많다.

수동 태그의 경우 리더기에서 송출한 RF신호의 Carrier 신호에서 전원을 공급받으므로 리더기 안테나의 설계 스펙이 시스템의 전체 성능을 반영하기도 한다.

그림 3은 마이크로파 대역 태그 후방 산란을 이용한 데이터 전송을 보여준다. 태그칩은 부하저항 R_L 과 입력 커패시턴스 C_2 의 병렬형태이고, 스위치를 이용하여 Z_{mod} 값을 바꿈으로써 태그 안테나 양단의 임피던스 Z_t 값을 부하변조 시킨다.

$$Z_t = jX_r + R_r = \frac{1}{j\omega C_2 + \frac{1}{R_L} + \frac{1}{Z_{mod}}} \quad (1.2)$$

식 (1.2)에서 Z_{mod} 를 변화시킴으로써 태그 안테나에서 산란되는 전력을 변화시키면 리더에서 이를 감지하여 데이터를 인식한다.

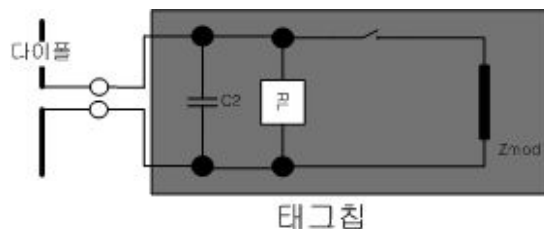


그림 4. 태그의 전원 등가 회로

마. 리더기

리더기는 그림 4와 같이 리더기 안테나를 통하여 전원을 공급 후 TAG 정보를 해독 수집하는 역할을 한다.

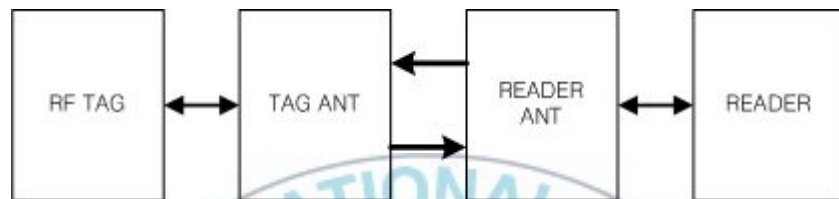


그림 5. 전원 및 DATA 이송 흐름도

태그의 데이터를 읽거나, 태그에 데이터를 쓰는 기능을 한다. 또한 리더는 수동형(Passive) 또는 반수동형(semi-passive) 태그에 원격으로 전력을 공급하는 기능을 한다. 그림 5는 리더와 수동형 태그 간의 신호전달 과정을 설명하고 있다.

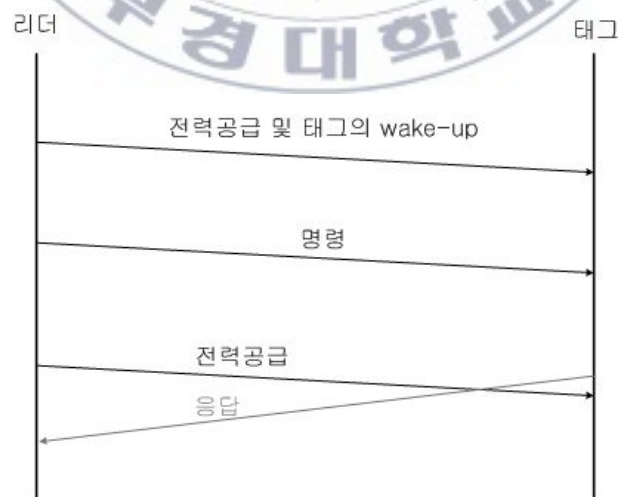


그림 6. 리더와 수동형 태그 간의 신호전달

2. RFID 각 표준 ISO방식의 고찰

RFID는 ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)에서 세계 공통 표준 사양을 제시하고 있다.

여기서 사용할 비접촉 개인 신상정보카드(The general title Identification Cards - Contactless intergrated circuit(s) card)의 규정된 내용은 다음과 같다.

- Part 1 : 물리적 특성
- Part 2 : Radio frequency power and interface
- Part 3 : 초기화(Initialization)와 Anticollision
- Part 4 : 송신 프로토콜(Tranmission Protocols)

위의 내용을 4차 개정을 통하여 현재 ISO 7816의 규정과 IEC 14443의 규정으로 정의되어져 있다.

가. RFID활용 - 현재 국내 교통카드의 예

국내에서는 현재 교통카드를 중심으로 RFID가 사용 중에 있으며 그 사용이 점차 소액 결제와 무인 판매 등의 결제 방식에 사용되고 있고 확대되는 추세에 있다. 현재 사용되는 방식의 구성은 다음과 같다.

(1) ISO/IEC 14443A

- 인코딩 방식 : 맨체스터(Manchester)방식과 모디파이드-밀러(Modified Miller)방식 혼용.
- FAT(File Allocation Table)사용으로 인한 어드레스 벡터(번지 지정)방식을 사용하지 않음.

(2) ISO/IEC 14443B

- NRZ(Non Return to Zero) 방식의 사용.
- FAT(File Allocation Table)사용으로 인한 어드레스 벡터(번지 지정)방식을 사용하지 않음.

(3) MIFARE

- NRZ(Non Return to Zero) 방식의 사용.
- 어드레스 벡터의 지정 명령으로 데이터의 Read/Write 명령을 수행
- 현 국내 절대 다수의 카드에서 사용 중.

여기서는 단일 플랫폼에서 3가지 방식을 공유하는 기기를 고려하여 설계하였다.

3. 통합 플랫폼 구현

가. 시스템 구성도

그림 6에서 알 수 있듯이 안테나에서 발생되는 무선 신호가 태그를 깨우고(Awake) 전원을 발생한다. 태그에서 무선 신호를 발생시키면 안테나에 신호가 감지되고 이것을 리더기에 전달되어 정보를 전달한다.

여기서 태그(TAG)는 7종의 교통 카드를 중심으로 테스트 하는 것으로 한다.

안테나와 리더기는 ISO/IEC14443A/B와 MiFARE의 SIMM을 장착하여 구성하여 확장성을 가지게 한다.

리더기에서 수집된 정보는 이더넷(Ether-Net) 또는 모뎀등에 연결되어 외부 디바이스와 정보를 교환 할 수 있게 구성하고 각각의 사양은 외부에서 모니터링 또는 사용이 용이하게 한다.

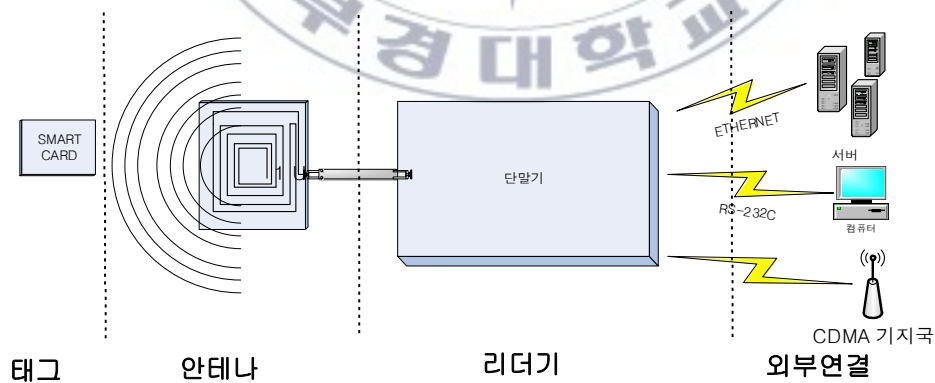


그림 6. 시스템 구성 개요

나. 시스템 구성 목표

본 논문에서의 시스템의 구성 블록선도는 그림 7과 같다.

(1) SIMM의 확장성

현재 교통카드 등의 END-User 들이 사용하는 카드의 종류 교통 카드가 주종을 이루고 있음. 선불 및 후불 카드의 SIMM 개수를 최대8개로 가정하고 설계 기준은 최대 8개의 SIMM이 삽입되는 것을 기준으로 한다. 이는 현재 국내에서 사용되는 카드의 대다수를 커버 하는 것이고, 또 사용의 목적에 따라서 확장 보드를 이용하여 확대가 가능한 것으로 한다.

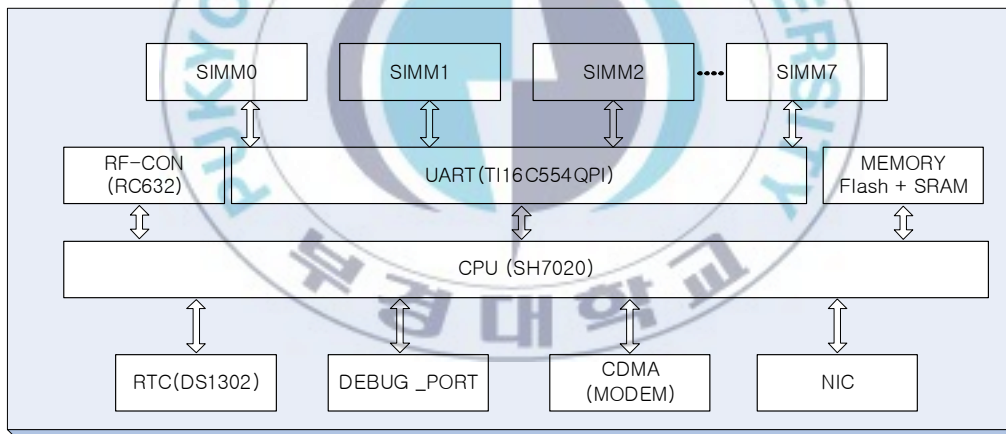


그림 7. 시스템 구성 블록선도

(2) 다양한 인터페이스(INTERFACE)의 적용 가능 구조 설계

사용자의 다양한 요구에 부합할 수 있도록 하는 방법으로 디버그를 별도로 UART를 확장할 수 있도록 설계하였다. 이번 논문상에서는 UART를 4개로 설계하였고 이를 위하여 TI16C554의 칩셋을 사용하여 확장가능 하게 설계하였으며 또한 향후 확장 사용을 위한 여분을 남겨 두었다.

또한 이더넷(Ether-Net)과 기타 통신 방법에 대한 대응을 위한 필요 여분을 설계시 반영하여 두어서 사용의 폭을 넓히는데 주안점을 두었다.

(3) 다양한 SIMM(PSAM)의 장착으로 인한 호출 처리 속도

다수의 SIMM(PSAM)의 삽입으로 인하여 빠른 시간내 응답을 줄 수 있는 알고리즘을 구현하였다. 기존의 기기들은 한가지의 SIMM(PSAM)을 사용하였으나 본 논문은 다양한 SIMM의 사용으로 인하여 SIMM Scan Time의 문제가 대두 하게 되었다. 그리하여 다양한 SIMM을 장착하고 이를 호출하는 F-SCAN 알고리즘이 필요하게 되었고 이를 구현하는데 주안점을 둔다. 본 논문에서는 600[msec]이내에 전송 및 결제 완료를 목표로 알고리즘을 구현하였다.

다. 키의 구성

(1) 전자화폐 시스템의 거래를 위해 사용되는 키-A사의 예
A사 전자 화폐에서 사용되어지는 키는 다음과 같다.

KMP_{CSAM} : 구매키 변형·분배를 위한 마스터키

KMUC_{CSAM} : 전자화폐공동망센터에서 관리하는 파라미터 갱신키
변형·분배를 위한 마스터키

KMINDC_{CSAM} : 전자화폐공동망센터의 개별거래 검증키
변형·분배를 위한 마스터키

KMTM_{CSAM} : 전자화폐공동망센터의 총액거래 검증키
변형·분배를 위한 마스터키

KML_{PPSAM} : 가치 저장키 변형·분배를 위한 마스터키

KMUB_{PPSAM} : 발행기관에서 관리하는 파라미터 갱신키
변형·분배를 위한 마스터키

KMINDS_{SSAM} : 시스템서비스제공자의 개별거래 검증키
변형·분배를 위한 마스터키

KMUS_{SSAM} : 시스템서비스제공자에서 관리하는 파라미터 갱신키
변형·분배를 위한 마스터키

KMP_{PSAM} : 구매키 검증을 위한 마스터키

KMUC_{PSAM} : 전자화폐공동망센터에서 관리하는 파라미터 갱신키
검증을 위한 마스터키

KME_{CSAM} : 비밀번호 등 암호화키 변형·분배를 위한
마스터키 (2004.6월 수정)

KDINDC_{PSAM} : 전자화폐공동망센터의 개별거래 검증을 위한
서명 생성시 사용하는 키

KDTM_{PSAM} : 전자화폐공동망센터의 총액거래 검증을 위한 서명
 생성시 사용하는 키
KDUS_{PSAM} : 시스템서비스제공자에서 변형·분배되어진 파라미터
 갱신키
KDINDS_{PSAM} : 시스템서비스제공자의 개별거래 검증을 위한 서명
 생성시 사용하는 키
KDL_{IEP} : 변형·분배되어진 가치저장키
KDP_{IEP} : 변형·분배되어진 구매키
KDUC_{IEP} : 전자화폐공동망센터에서 변형·분배되어진 파라미터 갱
 신키
KDUB_{IEP} : 발행기관에서 변형·분배되어진 파라미터 갱신키
KDE_{IEP} : 변형·분배되어진 암호화키 (2004.6월 수정)
DP_{KEY} : 지불SAM과의 거래를 위하여 구매키(KMP)로부터
 변형·분배되어진 구매키로 나뉜다.

라. 키의 계층 구조

(1) 전자화폐(IEP)의 키 계층 구조

그림 8은 전자 화폐(IEP)의 키 계층 구조를 나타내고 있다. 전자화폐 시
 스템에서 사용되는 암호 키는 계층적 구조를 가지며 각 IC카드는 상위 마
 스터키와 자신의 파라미터를 이용하여 생성된 고유한 키를 갖는다. 또한,
 발행기관에서 관리하는 가치 저장키(KDL), 가치 저장키의 갱신키(KDUB)
 와 전자화폐공동망센터에서 관리하는 구매키(KDP, DP), 구매키의 갱신키
 (KDUC)와 같이 키들을 용도별로 분리하여 사용함으로 키의 사용분야와
 빈도에 따른 계층 구조를 갖는다.

가치 저장키(KDL), 구매키(KDP, DP)와 같이 사용빈도 수가 많은 키들은 외부의 노출 가능성이 높으므로, 사용빈도 수가 적어 외부노출 가능성이 작은 각각의 갱신키를 이용해서 갱신한다.

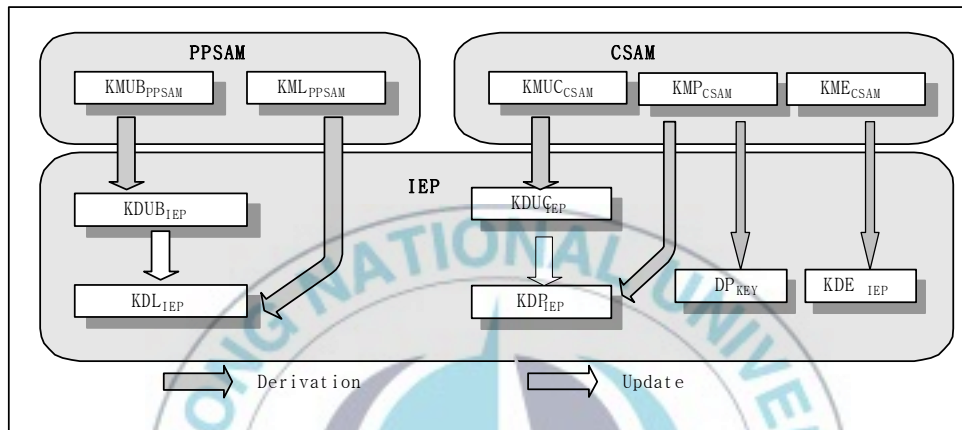


그림 8. IEP의 키 계층 구조도

(2) PSAM의 키 계층구조

그림 9는 PSAM의 키 계층 구조를 나타내고 있다. 전자화폐의 계층 구조 암호 키 시스템과 동일한 방식으로 각각의 PSAM은 상위 마스터키와 자신의 파라미터를 이용하여 생성된 고유한 키를 갖는다. PSAM에서는 전자화폐공동망센터에서 관리하는 KMP, KMUC, KDINDC, KDTM과 시스템서비스제공자가 관리하는 KDUS, KDINDS, KDCOMP를 갖는다.

그림 10과 같이 전자화폐공동망센터가 생성/관리하는 키의 갱신은, 먼저 CSAM에서 KCOMS를 이용하여 SSAM과 상호인증한 후, KMUS를 이용하여 새로운 키를 암호화한 상태로 시스템서비스제공자에게 전송한다. 시스템서비스제공자는 KMUC에 관한 정보를 가지고 있지 않으므로 암호화

된 새로운 키의 내용을 확인할 수 없다.

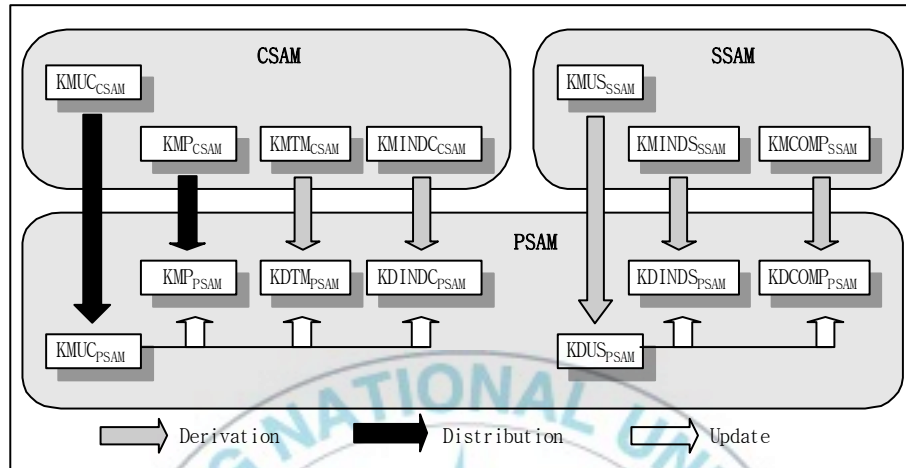


그림 9 PSAM의 키 계층 구조도

SSAM은 PSAM과 온라인으로 연결된 상태에서 KMCOMP를 이용하여 상호인증한 후, 전자화폐공동망센터로부터 수신한 암호화된 키를 PSAM에 전송하고, PSAM은 KMUC를 이용하여 암호화된 키를 복호화하여 자신의 키를 갱신한다. 만약, 수신된 키가 KMTM 또는 KMINDC일 경우에는 이를 KDTM 또는 KDINDC로 변형하여 갱신하고 KMTM 또는 KMINDC는 삭제한다. 시스템서비스제공자가 생성/관리하는 키의 갱신은 SSAM과 PSAM이 온라인으로 연결된 상태에서 KMCOMP를 이용하여 상호인증한 후, KMUS로 새로운 키를 암호화하여 PSAM에 전송한다. PSAM은 KDUS를 이용하여 암호화된 키를 복호화 하여 자신의 키를 갱신한다.

(3) 전자화폐의 키 갱신

전자화폐의 키 갱신은 그림 11과 같이 발행기관이 생성/관리하는 가치 저장키의 갱신과 전자화폐공동망센터가 생성/관리하는 구매키의 갱신으로

구분된다.

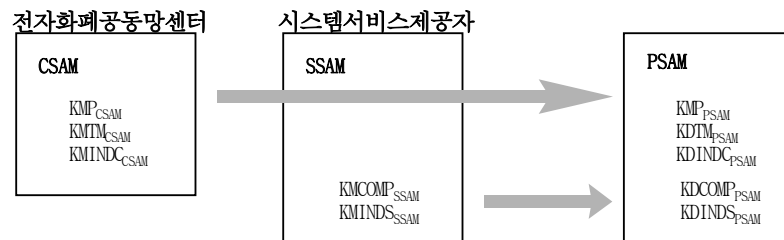


그림 10. PSAM의 키 갱신

가치 저장키의 갱신은 전자화폐가 PPSAM과 온라인으로 연결되었을 때 PPSAM에 의해 이루어진다. 이때 키의 안전한 전달을 위해서 발행기관의 KMUBPPSAM과 IEP의 KDUBIEP를 사용하여 상호 신분인증과 새로운 가치 저장키를 암호화/복호화해서 키의 노출을 방지한다.

구매키의 갱신은 PSAM의 키 갱신 절차에 따라 구매키가 갱신된 PSAM에 의해 KMUC를 이용하여 이루어진다.

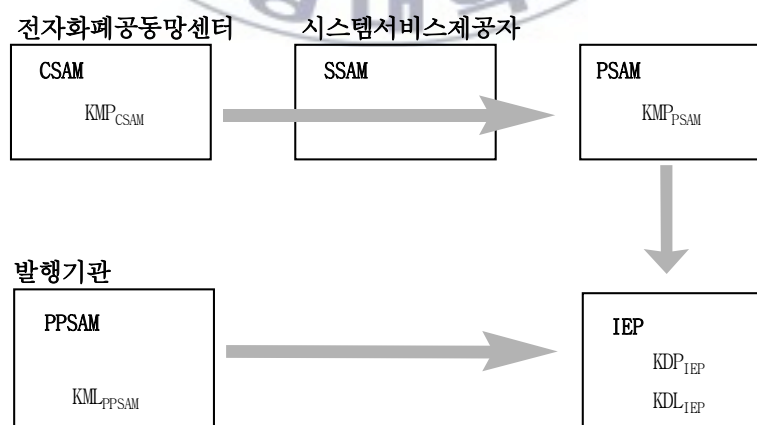


그림 11. IEP의 키 갱신

마. F-Scan 알고리즘

본 논문에서 사용한 MIFARE를 위한 일반 보안 기능을 적용한 알고리즘은 다음과 같다. 암호화 알고리즘은 DES를 사용한다. DES 사용 시

- Key Size : 8 bytes
- Input Block Size : 8 bytes
- Output Block Size : 8 bytes를 사용한다.

키와 data 응답 사이 해독과 전달은 그림 12와 같은 방식으로 이루어진다.

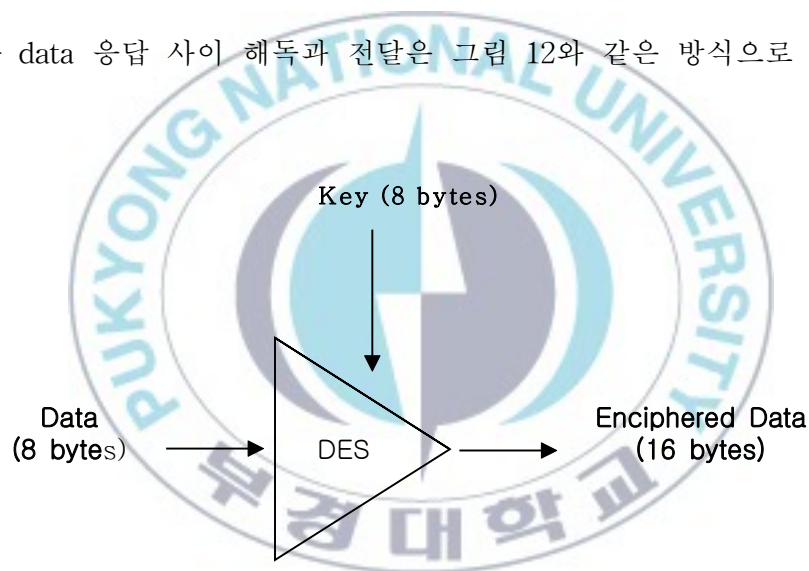


그림 12. 암호 알고리즘을 적용하는 방식의 예

이와 같이 DATA를 암호 알고리즘에 키 값과 같이 수행하여 암호화된 16BIT의 값을 만들어 낸다. 위 수행의 역방향은 그림 13과 같이 수행하고 이루어진다.

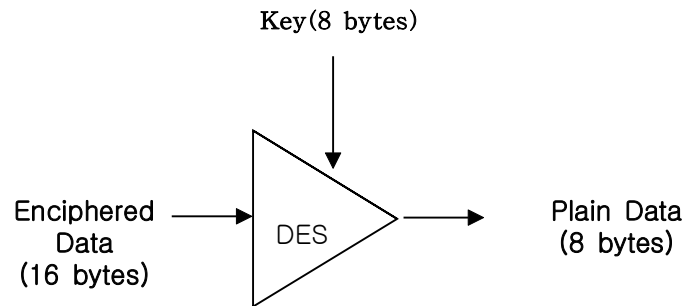


그림 13. 암호를 해독하는 방식의 예

그림과 같은 방식으로 암호 해독과 디코딩이 이루어진다. 위의 수행은 암호화의 수행이며 키 값이 암호의 디코딩과 엔코딩의 중요한 키가 됨을 알 수 있다. 위의 과정은 전체 수행에 항상 수행되어 지므로 암호화가 되지 않은 데이터의 외부 누출로 인하여 발생할 수 있는 해킹 등의 위험에서 안전장치가 될 수 있도록 해준다. 동일한 암호키의 값은 존재하지 않는다. 그러므로 사용시 암호키의 스캔을 미리 수행하고 버퍼 등의 보조 장치에 키 값을 미리 가지고 있는 것이 빠른 수행에 필수적인 사항이 된다.

그림 14의 수행 Flow-Chart는 암호화의 관계를 제외한 나머지 기능별로 언급한 것이다.

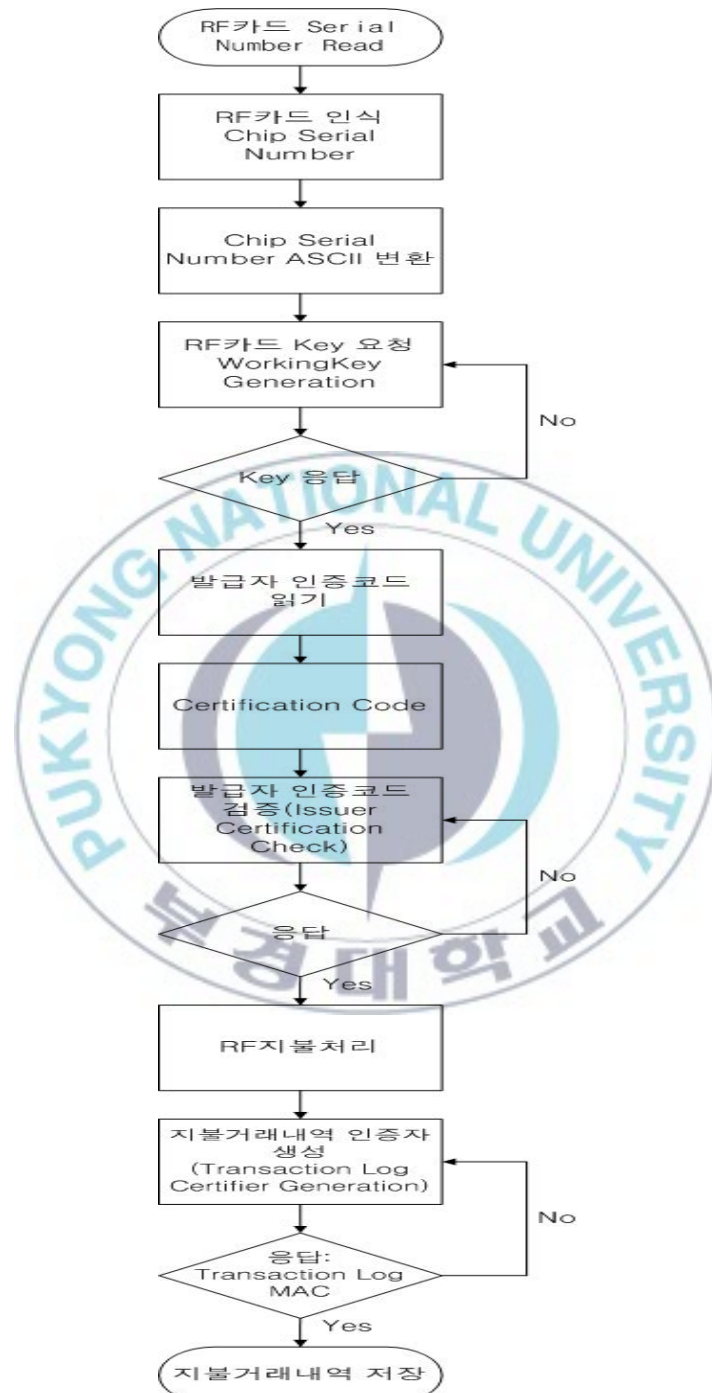


그림 14. 지불거래에 따른 흐름도

바. 구성 회로도

그림 15는 RFID 리더기 메인 보드의 회로도를 나타내며, 그림 16은 RFID SIMM 파트 회로도를 나타내고 있다.

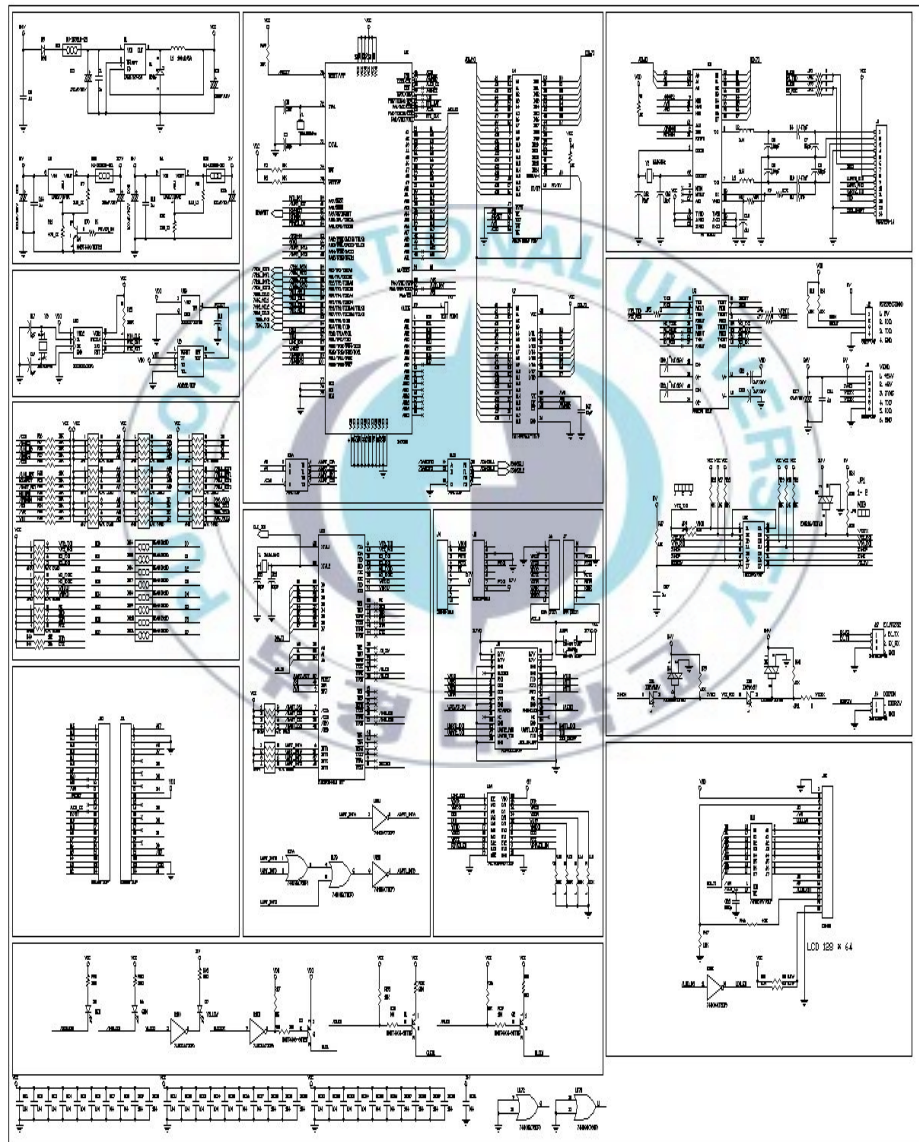


그림 15. RFID 리더기 메인 보드 회로도

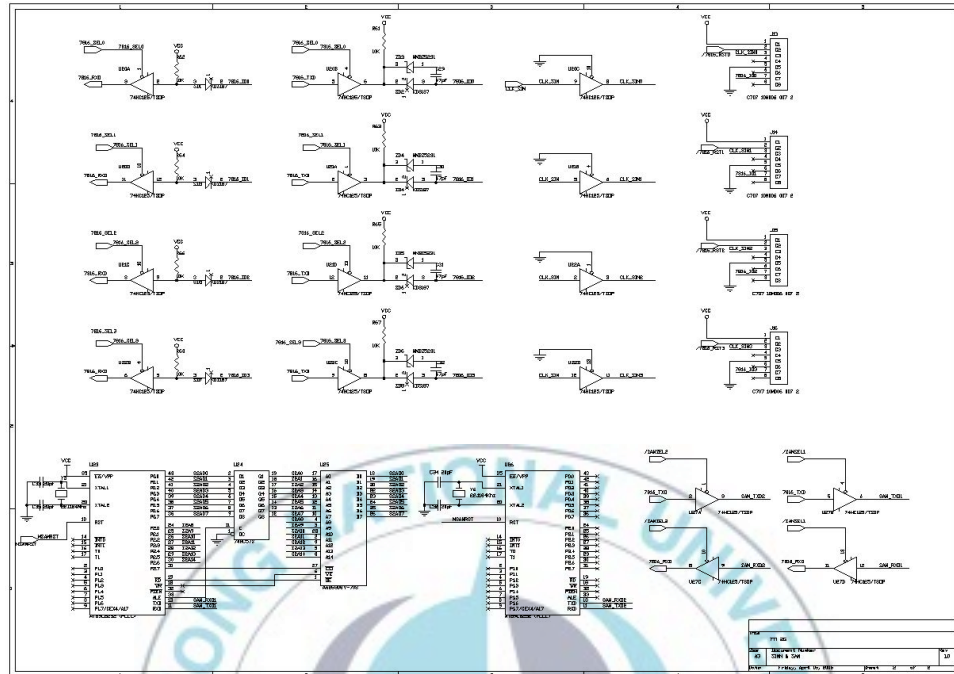


그림 16. RFID SIMM PART 회로도

사. 시스템 구성 모습

(1) 안테나

그림 17과 같은 안테나에는 MIFARE와 ISO/IEC14443 A/B 타입의 태그를 읽을 수 있는 방식으로 설계 되어 있다.

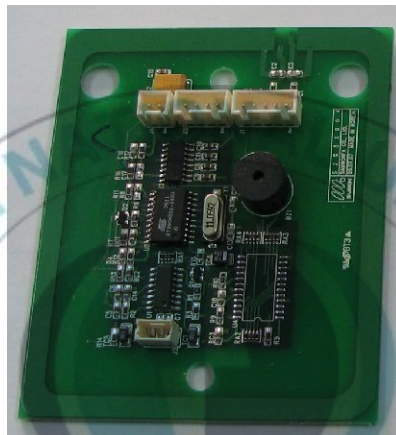


그림 17. 안테나

(2) 리더기

그림 18의 A 부분은 CDMA 모뎀의 접속 부위이다. 이 부분은 CDMA모뎀이 접속 가능한 소켓이고, 접속하면 모뎀 통신으로 외부와 연결이 가능하도록 되어 있다.

그림 18의 B 부분은 확장 슬롯이며, 그림 19에서 리더기 메인 보드 후면에 SIMM 소켓을 8개 장착가능 하게 설계되어 있고, 이는 여러 가지 SIMM을 장착 가능하게 한다.

단말기 사이즈와의 관계로 SIMM의 확장을 8개로 설계되었으나 추후 확장시 확장될 수 있는 여분은 남겨두었으므로 확장이 가능 하다.

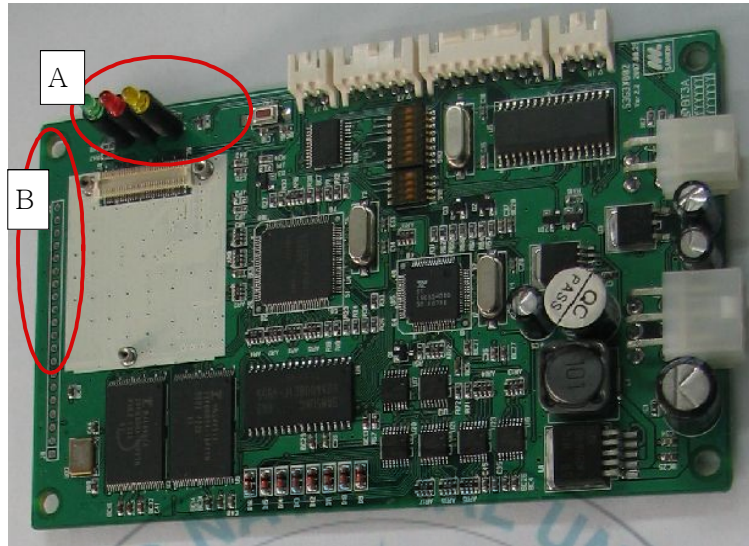


그림 18. 리더기 메인 보드 전면

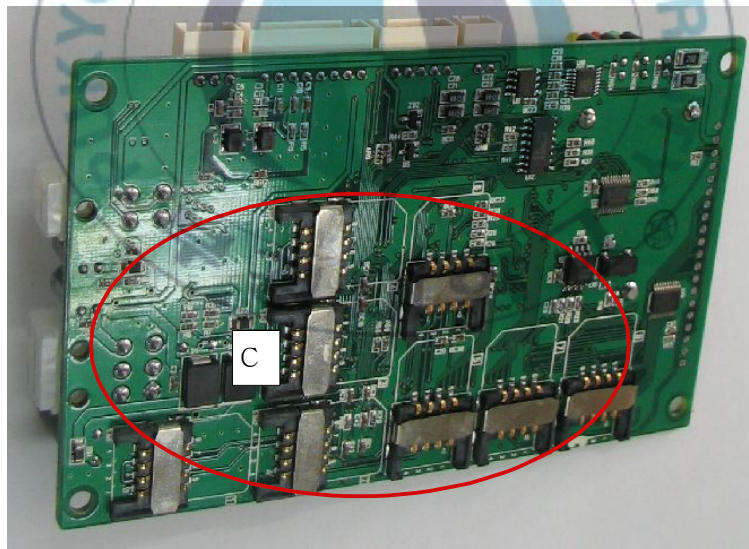
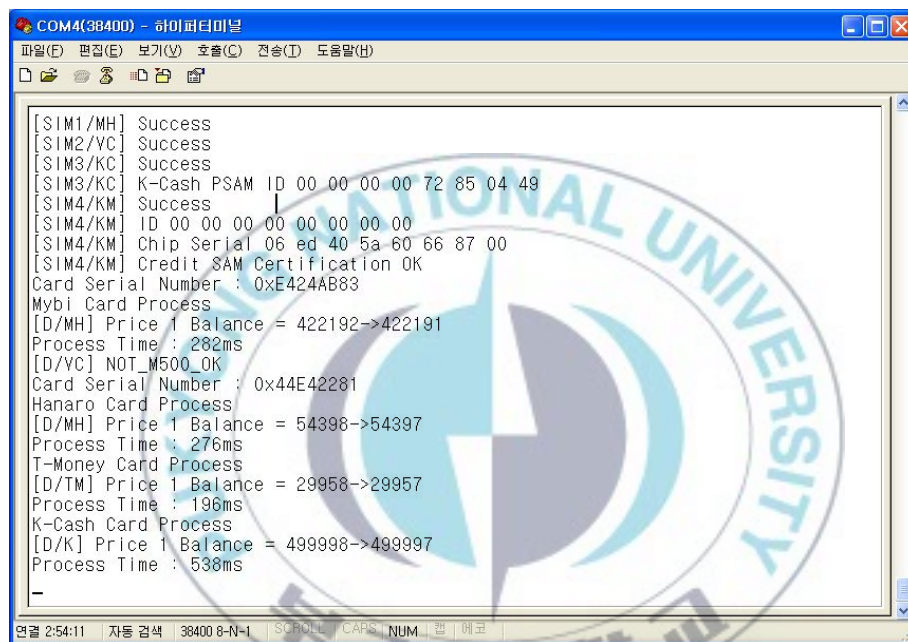


그림 19. 리더기 메인 보드 후면

아. PC와 연동 동작

결과를 산출하기 위한 모니터링을 위하여 PC를 사용하여 결과치를 상출하였으며, 그림 20과 같은 결과를 나타내었다.



```
[SIM1/MH] Success
[SIM2/YC] Success
[SIM3/KC] Success
[SIM3/KC] K-Cash PSAM ID 00 00 00 00 72 85 04 49
[SIM4/KM] Success
[SIM4/KM] ID 00 00 00 00 00 00 00 00
[SIM4/KM] Chip Serial 06 ed 40 5a 60 66 87 00
[SIM4/KM] Credit SAM Certification OK
Card Serial Number : 0xE424AB83
Mybi Card Process
[D/MH] Price 1 Balance = 422192->422191
Process Time : 282ms
[D/YC] NOT_M500_OK
Card Serial Number : 0x44E42281
Hanaro Card Process
[D/MH] Price 1 Balance = 54398->54397
Process Time : 276ms
T-Money Card Process
[D/TM] Price 1 Balance = 29958->29957
Process Time : 196ms
K-Cash Card Process
[D/K] Price 1 Balance = 499998->499997
Process Time : 538ms
-
```

그림 20. 카드 처리 모니터링 화면

Ⅲ. 실험 및 고찰

통합 플랫폼의 동작 결과를 얻기 위하여 사용된 시험 조건은 다음과 같다.

1. 1개 카드당 100회의 거래 승인 요청 및 거래 플로우 준수
2. 거래 시작 - 종료 간 Time (TICK)을 측정 하여 PC로 전송
3. 사용되어지는 카드는 선불과 후불을 사용하며, 현재 국내에서 사용되는 카드를 이용한다. 총 7개사의 카드 샘플을 사용하였다.

위 사항을 준수 하여 시험을 실행하였고 그에 따른 결과는 표 2와 같다.

표 2. 태그 샘플 카드의 실행 결과

NO	카드사별처리속도(ms)						
	선불					후불	
	하나로	마이비	T-Money	VisaCash	K-Cash(금융결제원)	KB후불(KB신용카드)	T-Money후불(롯데카드)
1	277	282	196	278	538	153	92
2	277	282	196	278	534	153	92
3	276	283	196	278	543	153	92
4	277	283	196	278	539	153	92
5	277	282	197	278	539	153	92
6	278	282	197	278	539	153	92
7	277	282	197	278	534	153	92
8	277	282	196	278	536	153	92
9	276	282	194	278	539	153	92
10	279	283	197	278	539	153	92
11	278	282	196	278	539	153	92
12	276	284	196	278	539	153	92
13	277	282	196	278	539	153	92
14	277	282	194	278	539	153	92
15	277	282	197	278	539	153	92
16	277	282	197	277	539	153	92
17	277	282	197	278	538	153	92
18	277	281	196	278	536	153	92
19	277	282	194	278	539	153	92

20	277	282	194	278	535	153	92
21	277	282	197	278	539	153	92
22	277	282	197	278	539	153	92
23	277	282	197	278	539	153	92
24	277	283	197	278	539	153	92
25	276	281	197	278	535	153	92
26	277	282	196	278	544	153	92
27	279	282	196	278	539	153	92
28	277	282	196	278	536	153	92
29	278	282	194	278	539	153	92
30	277	282	197	278	539	153	92
31	278	282	197	278	539	153	92
32	277	282	197	278	539	153	92
33	277	282	196	278	539	153	92
34	277	283	194	278	539	153	92
35	277	281	197	278	539	153	92
36	277	282	197	278	539	153	92
37	277	282	197	278	539	153	92
38	277	282	197	278	536	153	92
39	277	282	194	278	539	153	92
40	277	282	194	278	539	153	92
41	277	282	197	278	539	153	92
42	277	282	197	278	539	153	92
43	276	283	196	278	535	153	92
44	278	282	196	278	539	153	92
45	278	282	197	278	544	153	92
46	277	282	196	278	535	153	92
47	277	282	196	279	543	153	92
48	278	282	196	278	531	153	92
49	277	282	194	278	539	153	92
50	277	282	197	278	543	153	92
51	277	282	197	278	535	153	92
52	277	281	197	278	539	153	92
53	277	282	197	278	543	153	92
54	277	282	194	278	535	153	92
55	277	281	197	278	544	153	92
56	277	282	197	278	535	153	92
57	277	282	196	278	539	153	92
58	277	282	196	278	540	153	92
59	277	282	194	278	535	153	92
60	277	282	194	278	543	153	92
61	277	282	197	278	535	153	92
62	277	282	197	278	539	153	92
63	277	282	196	278	543	153	92
64	277	283	196	278	535	153	92
65	277	282	197	278	544	153	92
66	277	282	197	278	535	153	92
67	277	281	197	278	539	153	92

68	277	282	196	278	540	153	92
69	277	282	194	278	535	153	92
70	277	282	197	278	539	153	92
71	278	282	197	278	535	153	92
72	277	282	197	278	535	153	92
73	276	283	196	278	543	153	92
74	277	282	194	278	535	153	92
75	277	282	197	278	539	153	92
76	277	281	197	278	544	153	92
77	277	282	197	278	535	153	92
78	277	282	196	278	540	153	92
79	276	282	194	278	535	153	92
80	277	281	194	278	539	153	92
81	277	282	197	278	543	153	92
82	277	282	197	278	535	153	92
83	277	282	196	278	543	153	92
84	278	282	197	278	535	153	92
85	277	282	197	278	539	153	92
86	277	283	197	278	544	153	92
87	277	282	197	278	534	153	92
88	277	282	197	278	540	153	92
89	277	283	194	278	535	153	92
90	277	282	197	278	539	153	92
91	277	282	197	278	543	153	92
92	277	282	197	278	535	153	92
93	277	283	196	278	539	153	92
94	276	282	194	278	539	153	92
95	277	281	197	278	539	153	92
96	277	282	197	278	540	153	92
97	276	282	197	278	539	153	92
98	277	282	196	277	536	153	92
99	277	282	194	278	539	153	92
100	277	282	194	278	539	153	92
합계	277.04	282.04	196.12	277.99	538.51	153	92

표 2의 결과를 얻을 수 있었다. 위 결과는 정리하여 평균치를 취한 값은 표 3과 같다.

표3. 결과 평균치

	평균속도(ms)	카드
1	92	"A"사 후불
2	153	"B"후불
3	196.12	"A" 선불
4	277.04	"C"선불
5	277.99	"D"사 후불
6	282.04	"E"사 선불
7	538.51	"F"사 선불

결과를 얻을 수 있었고, "A"사 후불카드가 가장 빨랐음을 알 수 있고. 최대 538[msec]와 최소 90[msec]의 카드처리 응답의 속도를 보이고 있음을 알 수 있다. 이는 각 카드사마다의 요청 키 값과 그에 따른 소요시간이 다르고, 대상이 되는 태그의 상태(질)에 따라 응답의 속도가 달라짐에 따라 생기는 차이라고 생각된다. 향후 보완해야 될 것으로 생각된다. 그리고 카드 처리 알고리즘의 개선으로 더욱 빠른 속도를 기대할 수 있다.

IV. 결론

1. 다중 키 값의 사전 탐색으로 인하여 수행 시간의 감소를 얻을 수 있다. 처리 결과의 도표에서도 알 수 있듯이 1개의 사용 시 와 다중 키의 사용 시 의 값의 차이가 적어 다중 키의 사용에서도 별다른 어려움이 없이 사용 할 수 있는 알고리즘을 개발하였다. 본 논문에서는 최대 8개의 키값을 얻을 수 있었으나, 최대 확장이 가능한 16개의 키값을 삽입하였을 경우는 알고리즘의 개선이 요망된다. 본 설계는 현재 국내에서 유통되는 비접촉 시 카드를 중심으로 이루어졌으므로 다른 카드의 대응 시 에 유용 할 것으로 생각된다. UART 및 NIC의 적용으로 인터페이스의 확장이 용이함은 실지로 사용되어지는 현장의 특성을 생각하면 유용하게 사용이 가능하다고 생각된다.

최대거래시간은 각각의 카드사의 서버 능력과 현지의 망사용 능력에 따라 아주 많은 차이를 가진다. 90~500[msec] 이상의 차이를 가지는 것으로 판단되며, 이는 사용자의 편의를 생각해서라도 하루 빨리 개선되어야 한다고 생각된다.

2. 다중 키 적용된 단말기의 개발로 인하여 키가 추가된 단말기의 빠른 적용을 할 수 있었다. 이미 적용된 단말기와 이중의 키가 적용되는 시점에서 키만 추가 되면 개발 작업에 상관없이 사용이 가능하여서 이중의 단말기나 카 사용이 많이 요구되는 단말기에서의 사용이 용이 하게 되었다. 아울러 사용 환경 또한 별다른 구애를 받지 않는다는 것은 이 단말기의 가장 큰 강점이 될 수 있다.

3. 위에서 언급하였으나 더 많은 키의 사용 시, 즉 16가지 이상의 키의

사용은 이번 논문에서는 언급하지 않았다. 이를 적용하기 위해서는 더욱 빠른 스캔 알고리즘이 필요하고 이는 차후의 논문에서 다루도록 한다.



참고 문헌

- [1] Klaus Finkeneller, RFID Handbok, John Wiley&Sons Ltd., 2003
- [2] Jerry Banks, David Hanny, Manuel A. Pachano, and Les G Thompson, RFID Applied, John Wiley&Sons Inc., 2007.
- [3] ISO/ICE 18000-6 : 2039(E) "Information technology automatic identification and data capture techniques - Radio Frequency Identification for item management air interface
- [4] ISO/IEC 14443 Identification cards- Contactless integrated circuit(s) cards - Proximity cards : PART1, PART2, PART3, PART4.
- [5] Wren L. stutzman, Gary A. Thiele, Antenna theory and design, John Wiley&Sons. inc., 1998.
- [6] 남상엽, 변상기, 정교일, RFID 구조 및 응용, 상학당, 2006.
- [7] 최길영, 성낙선, 모희숙, 박찬원, 권성호, "RFID 기술 및 표준화 동향", 전자통신동향 분석, 제22권, 3호, 한국전자통신연구원, 2007.
- [8] 정보통신단체표준 TTAS.KO - 12.0022/R1, "비접촉식 전자화폐 관독 기용 지불 SAM 규격", 한국정보통신기술협회. 2003.
- [9] ISO 10126-2(1991) : Banking - Procedure for message encipherment (wholesale) - Part 2 : DEA algorithm
- [10] ISO 8372(1987) : Information processing-Modes of operation for a 64-bit block cipher algorithm
- [11] ISO/IEC 10116(1997) : Information technology-Security techniques - Modes of operation for an n-bit block cipher

감사의 글

본 논문이 완성되기까지 부족한 저에게 학문에 임하는 자세와 열정을 가르쳐 주시고, 아낌없는 지도와 격려로 보살펴 주신 이형기 지도교수님께 진심으로 감사드립니다.

바쁘신 와중에도 학위 과정동안 부족한 점을 지적해 주시고 많은 가르침을 주신 변기식 교수님, 이경창 교수님, 안영주 교수님께도 감사드리며, 평소 많은 지도를 받은 최연욱 교수님, 김남호 교수님, 황용연 교수님, 김만고 교수님께도 감사의 말씀을 드립니다.

많은 어울림을 가지지는 못하였으나 많은 도움과 격려를 아끼지 않았던 시스템 제어연구실의 동료분들에게도 감사의 말씀을 전합니다.

본 논문의 많은 도움을 준 삼원FA(주)의 정필규 선임연구원과 윤현성 선임 연구원에게도 진심으로 감사의 말을 전합니다.

오늘이 있기까지 헌신적인 사랑과 믿음으로 용기와 희망을 주신 부모님과 우리 가족, 사랑으로 나의 길을 지켜주는 든든한 아내에게 이 논문을 바치며, 항상 따뜻한 격려와 관심을 아끼지 않으셨던 처가 가족에게도 진심으로 감사를 드립니다.

도움을 주신 고마운 분들께 일일이 찾아뵙지 못하고, 지면을 통해서나마 감사의 마음을 전하고자 이 글을 올립니다. 지금까지 부족한 저에게 크고 작은 관심을 가져준 모든 분들의 기대에 어긋나지 않도록 앞으로 더욱 노력할 것을 다짐하며 이 글을 마칩니다.

2009년 02월

유상영 올림