情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

보안성이 강화된 모바일 지급결제 수단으로써의 금융microSD 프레임워크 연구

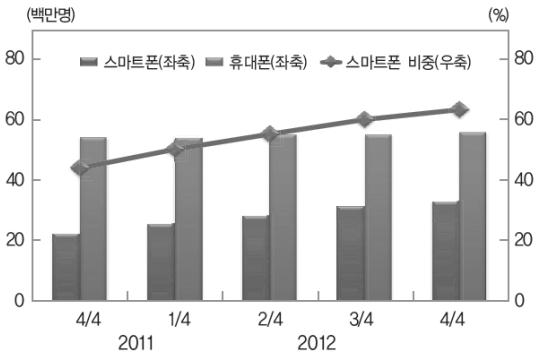
이 정 규*, 황 희 성**, 김 학 범***

요 약

최근 새로운 지불결제 플랫폼인 스마트폰의 등장으로 모바일 금융 결제 비중이 지속적으로 증가하고 있다. 특히 금융microSD는 기존에 사용해오던 USIM의 불편함을 해소하고 보안성을 강화하여, 새로운 모바일 지불결제 수단으로써 IT업계와 금융업계의 지대한 관심을 받고 있다. 이에 금융microSD를 통해 모바일 지불결제가 또 다른 제2의 서비스로 융합하는 단초가 될 것으로 기대하고 있다. 본고에서는 모바일 지급결제 시장 현황 및 서비스 동향과 모바일 지급결제 서비스의 핵심 플랫폼으로 기능하는 Secure Elements(SE)를 유형별로 나누어 살펴보고, 금융microSD 프레임워크를 분석하여 보안사항 및 활용방안 등에 대해 기술하고자 한다.

Ⅰ. 서 론

2012년중 전세계 휴대폰 판매량 가운데 스마트폰이 차지하는 비중은 38.8%이며 국내의 경우 전체 휴대폰 이용자 가운데 스마트폰 이용자 비중이 61.0%(2012년 말 기준)에 이르고 있다[1]. 스마트폰이 빠르게 보급되면서 이를 활용한 스마트폰 뱅킹, 모바일 신용카드 등 모바일금융서비스가 확산되고 있다.



〔그림 1〕 국내 스마트폰 가입자 현황[2]

특히 스마트폰 뱅킹의 경우 서비스 이용 등록 고객수가 2012년말 기준으로 2,395만명(중복계좌 합산)을 넘어서고 일평균 거래량이 8,611억원을 초과하는 등 모바일기기를 활용한 금융서비스 사용량이 빠르게 증가하는 추세이다.

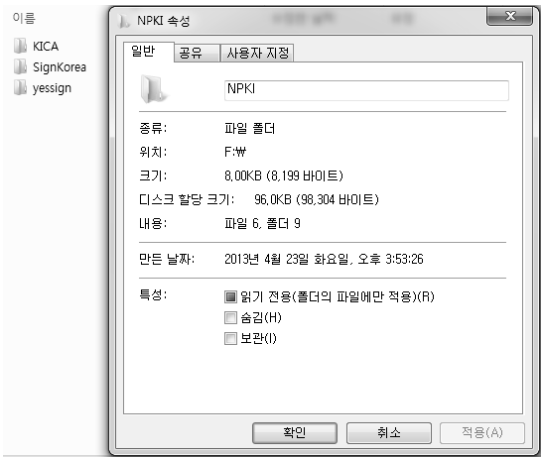
하지만 스마트폰 내에 들어있는 금융정보는 이에 비해 안전하게 관리되지 못하고 있다는 지적이 일고 있다. 금융정보를 저장·관리하기 위한 저장 매체가 통신정보를 관리하는 USIM에 국한되어 다양한 금융정보를 관리하기에 적합하지 않기 때문이다. 특히 스마트폰 뱅킹 등을 위한 공인인증서가 모바일 기기의 일반 메모리 영역에 저장되고 있어 악성 어플리케이션, 스마트폰 분실 등으로 유출될 경우 쉽게 복제되어 악용될 소지가 있다[3].

지금까지는 금융정보를 저장하는 매체로 USIM을 활용해 왔지만 이동통신사마다 USIM의 규격이 다름으로 인해, 사용자가 이동통신사를 변경하면 기존에 발급받았던 금융정보들 역시 다시 발급받아야하는 불편함이 있어왔다.

또한 결제 서비스 업계에 따르면, 우리나라의 근거리

* 동국대학교 국제정보대학원 (secure.gyu@gmail.com)
** 동국대학교 국제정보대학원 (heediyo@naver.com)
*** 동국대학교 국제정보대학원 / ㈜이너버스 (khb0305@dongguk.edu)

비접촉 결제 플랫폼은 이동통신사가 독점하는 구조로, 이동통신사 USIM과의 제휴를 통해서만 모바일 카드, 결제 기능 등을 구현할 수 있으며 이 외의 모듈은 사용할 수 없다고 한다. 모바일 비자카드 등의 혁신기술 역시 이러한 구조 때문에 국내에서 사용할 수 없는 실정이기도 하다(2013년 4월 기준). 이런 측면에서 봤을 때도 금융microSD가 모바일 금융결제 시스템의 대안으로 자리 잡을 가능성은 크다. 시장의 흐름이 이를 반증하고 있는 것이다.



〔그림 2〕 스마트폰의 일반 메모리 영역(F:\NPKI\)에 저장된 공인인증서

금융microSD는 기존의 보안성이 낮은 일반 메모리 영역에서 관리되던 공인인증서를 포함한 금융정보를 논리적, 물리적으로 보안성이 강화된 금융microSD에 저장함으로써 보다 안전한 관리가 가능하도록 설계한 모바일 지급결제 수단이다. 또한 모바일 기기에서만 사용할 수 있는 USIM과는 달리 태블릿 등의 모든 스마트 기기에서 사용이 가능하다는 점에서도 차별성을 가진다. 이러한 범용성 또한 기존의 모바일 지급결제 수단을 대체할만한 수단으로 금융microSD가 급부상하고 있는 이유 중의 하나다.

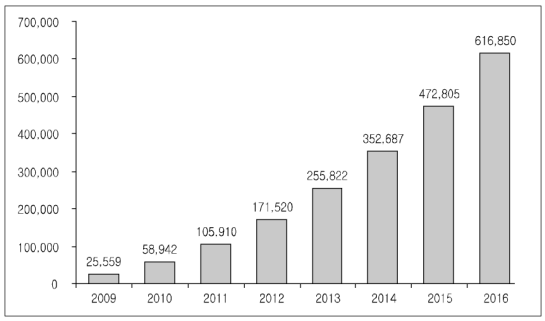
이에 한국은행은 금융정보화추진협의회를 통한 표준화 사업에 의해 2012년 10월, 모바일 금융서비스 이용 고객들이 금융정보를 안전하게 관리하고 다양한 서비스를 편리하게 이용할 수 있도록 microSD에 공인인증서, 전자지갑 등의 금융정보를 수록·관리하는 금융microSD 표준을 제정하기에 이르렀다[3].

Ⅱ. 모바일 지급결제 시장 현황 및 서비스 동향

2.1 세계시장

2.1.1 세계 모바일 지급결제 시장 현황

Gartner에 따르면 전세계 모바일 지급결제 거래액은 2011년말 1,059억 달러로 전년대비 44.3% 증가하였으며, 2016년에는 6,169억 달러에 이를 것으로 예상하고 있다.



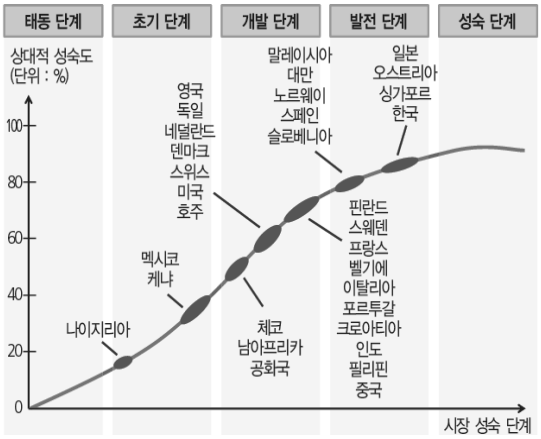
(단위: 백만달러)

〔그림 3〕 전세계 모바일 결제 시장규모 추이[4]

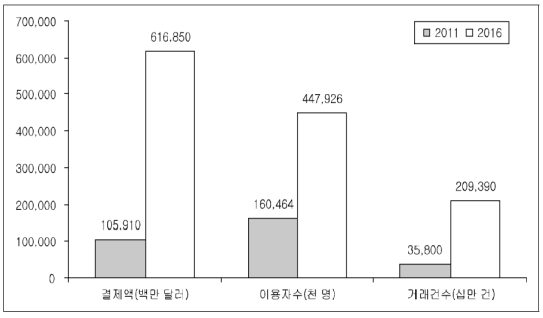
지역별로는 2011년 기준 아프리카(37.9%)가 401억 달러로 가장 규모가 컸는데, 주로 Money transfer 형태였다. 그 다음으로는 아시아－태평양 지역(34.9%)이었는데, 아시아－태평양 지역의 모바일 결제 이용자수는 1억 6,364만명으로 아프리카의 1억 134만명보다 1.6배 더 많았다[5].

특히 한국, 일본, 호주를 포함한 아시아 지역은 전세계의 모바일 지급결제 시장 가운데 가장 큰 규모를 차지한다. 2008년 결제 금액 기준으로 아시아 지역은 전세계(약 290억 달러)의 53%, 서유럽, 북미 및 남미 지역은 각각 13%, 12% 및 11%를 차지하였다[1].

전세계 모바일 결제 시장은 향후 5년간 연평균 42.2%를 기록하며 꾸준한 성장세를 보일 것으로 기대되며, 2016년에는 거래액이 6,169억 달러, 이용자수가 4억 4,793만명, 거래건 수가 209억건에 달할 것으로 전망되고 있다[5].



〔그림 4〕 전세계 모바일 지급결제 서비스 발전 추이[6]



〔그림 5〕 전세계 모바일 결제 시장 전망

2.1.2 세계 모바일 지급결제 서비스 동향[1]

미국은 높은 휴대폰 보급률에도 불구하고 모바일 지급결제 서비스 시장의 성장이 다소 늦은 편이다. FRB (Federal Reserve Bank) Boston이 2009년 실시한 조사에 따르면 응답자중 모바일뱅킹 이용자는 10.2%, 모바일카드 등 대금지급 서비스 이용자는 3%에 불과했다.

그러나 스마트폰의 등장 이후 서비스 개발 등의 시장 활성화 노력이 이어지고 있다. 모바일기기 플랫폼 사업자 구글은 2011년 9월, MasterCard와 제휴하여 NFC 기반의 모바일지갑 서비스인 구글월렛을 제공하였고, 이동통신사 진영도 2012년 10월부터 모바일지갑 서비스 Isis를 시작하였다.

미국에 비해 유럽 각국은 비교적 일찍부터 다양한 기술방식과 비즈니스 모델을 개발하여 모바일 지급결제 서비스 이용을 촉진해 왔다. 핀란드의 Nordea 은행은

〔표 1〕 미국의 모바일 지급결제 서비스 이용도[7]

(단위 : %)

	2008	2009
은행 계좌 보유	93.0	93.8
휴대폰 보유	-	89.5
모바일뱅킹 이용	8.2	10.2
모바일 대금지급 이용	-	3.0

1999년부터 Nokia와 공동으로 모바일뱅킹 WAP Solo를, 프랑스는 2000년부터 모바일카드 서비스 Payment CB sur mobile을 제공하였으며, 스페인도 2002년부터 모바일지갑 서비스 Mobipay를 시행하였다. 최근 들어서는 미국과 마찬가지로 NFC 기반의 모바일 지급결제 서비스 활성화를 추진중이다. 프랑스에서는 2010년 5월 이동통신사 Orange가 Cityzi 프로젝트를 출범하였고, 영국의 경우 2012년 9월 Everything Everywhere 등의 주요 이동통신사들이 합작하여 Project Oscar를 설립, 모바일 서비스 확산을 위해 노력하고 있다.

일본에서는 미국 및 유럽과 달리 비접촉 통신기술을 이용한 지급결제 서비스가 활발히 이용되어 왔다. 일본의 이동통신사 NTT DoCoMo는 2004년 7월 플라스틱 카드에만 사용되던 FeliCa 기술을 모바일기기에 접목시켜 오사이후케이타이라는 휴대폰 지갑 서비스를 시작하였다. 아울러 오프라인 결제 단말기의 보급 확대 등을 통해 시장을 활성화하는 데도 상당한 성과를 거두었다.

2010년 7월말 현재 일본의 모바일 전자화폐와 신용카드 발급장수는 각각 1,000만장과 2,000만장을 넘어섰으며 결제용 단말기도 90만대 이상 보급되었다.

〔표 2〕 일본의 주요 모바일 지급결제 수단 발급 현황

(만장, 만대)

구 분	서비스명	발급장수	단말기수
모바일 전자화폐	Edy	830	24
	MobileSuica	122	11
	Nanaco Mobile	92	2
모바일 신용카드	iD	1,459	44
	Quickpay Mobile	486	2
	Visa Touch	110	8

오사이후케이타이는 모바일 지급결제 분야의 대표적 성공사례로 회자되고 있지만 핵심기술인 FeliCa는 국제 표준이 아닌 특정 사업자 주도의 기술로서 글로벌 표준과 연동되지 않는다는 문제점도 있다. 이러한 한계를 극복하기 위해 NTT DoCoMo는 NFC 전환 입장을 공식화하는 한편 우리나라의 SK텔레콤, KT와 국가간 결제 연동 계획도 발표하였다.

2.2 국내시장

2.2.1 국내 모바일 지급결제 시장 현황[3]

2012년 말 17개 국내은행, 우체국 등에 등록된 인터넷뱅킹 및 모바일뱅킹 고객은 전년대비 각각 15.5%, 56.2% 증가하였다. 이 중 2009년 12월 도입된 스마트폰 기반 모바일뱅킹 서비스의 등록고객 수는 전년말 대비 131.3% 증가한 2,395만명을 기록하였다.

〔표 3〕 인터넷뱅킹 및 모바일뱅킹 등록고객 추이

(연말기준, 천명, 천개, %)

		2010	2011	2012	증감률
인터넷뱅킹	개 인	62,952	70,625	81,384	15.2
	법 인	3,550	4,192	5,046	20.4
	합 계	66,502	74,817	86,430	15.5
모바일뱅킹	IC칩방식	4,579	4,434	4,376	-1.3
	VM방식	8,561	8,928	8,718	-2.4
	스마트폰	2,609	10,358	23,954	131.3
	합계	15,748	23,720	37,048	56.2

2012년중 인터넷뱅킹 및 모바일뱅킹을 이용한 일평균 자금이체 규모(금액기준)는 전년대비 각각 4.1% 및 47.3% 늘어났다. 특히 모바일뱅킹 서비스 이용금액은 스마트폰 보급 확산에 따라 전년대비 131.1% 증가한 8,611억원을 기록하였다.

〔표 4〕 인터넷뱅킹 및 모바일뱅킹 자금이체 규모

(일평균, 천건, 십억원, %)

		2010	2011	2012	증감률
인터넷뱅킹	건 수	33,355	39,023	45,728	17.2
	금 액	29,571	31,917	33,239	4.1
모바일뱅킹	건 수	3,736	7,697	12,946	68.2
	금 액	416	653	962	47.3
	(스마트폰)	47	373	861	131.1

2.2.2 국내 모바일 지급결제 서비스 동향

현재 국내 모바일 지급결제 서비스 제공업체는 이동통신사업자, 단말기 제조업체, 카드사, 은행권 및 백화점이 모두 참여하여 경쟁하고 있는 상황이다[5].

〔표 5〕 사업자군별 모바일 지급결제 서비스 현황

	서비스명	제공업체
통신사	스마트월렛	SKT
	스마트월렛	LG U+
	올레마이월렛	KT
금융사	하나N월렛	하나은행
	주머니	신한은행
제조사	삼성월렛	삼성
	구글월렛	구글
	아이월렛	애플
	패스북	애플
유통사	S월렛	신세계백화점
	캐시비	롯데그룹
	팝티머니	GS리테일

최근에는 일반 microSD에 금융정보를 저장한 금융 microSD가 금융기관을 중심으로 새로운 결제 플랫폼으로 부상하고 있다[5]. 한국은행은 금융정보화추진협의회를 통해 금융microSD 표준 기반 모바일금융 서비스가 상용화되도록 노력하고 있다.

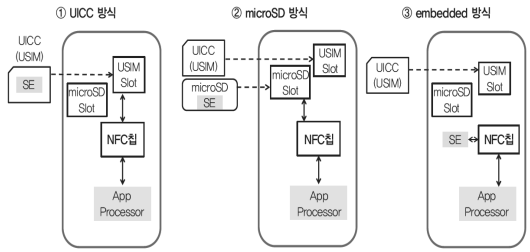
2012년 10월 한국은행, 금융결제원, 주요 금융사 및 IT 기업 등 총 43개의 유관기관 등이 참여하여 금융microSD 표준을 제정하였고, 2012년말 금융microSD 시제품을 금융기관 등에 배포하여 자사 어플리케이션과 금융microSD를 연동시키는 시험을 할 수 있도록 지원하였다. 또한 2013년중에는 금융microSD에서 스마트폰 뱅킹 어플리케이션과 모바일 신용카드 어플리케이션 활용 사례를 안내하기 위한 시연회를 개최하였으며, 빠르면 2013년말 내에 시범서비스가 실시될 예정이다[3].

Ⅲ. Secure Elements(SE) 유형[1]

Secure Elements(SE)란 지급결제 서비스에 필요한 지급수단 정보, 계좌 정보, 인증 정보 등의 각종 개인정보가 저장되는 보안영역으로써, 모바일 카드 등의 서비스에 있어서 핵심적이고 소비자들의 안전한 서비스 이용을 보장하는 역할을 담당한다.

SE가 모바일 지급결제 서비스의 핵심 플랫폼으로 기

능함에 따라 통상 SE를 발급·관리하는 주체가 서비스 제공의 주도권을 갖게 된다. 현재 국내외 대부분의 모바일 지급결제 서비스는 UICC 방식의 SE를 이용하고 있으나 SE 유형의 선택 문제를 두고 사업자간 논쟁을 지속하고 있다. 이동통신사는 UICC를 SE로 활용하는 방식을 선호하는 반면 제조회사는 SE 내장 방식을, 금융기관은 microSD 방식을 선호한다.



〔그림 6〕 Secure Elements의 분류

3.1 UICC 방식

UICC는 3세대 또는 4세대 이동통신 환경의 모바일 기기를 구성하는 주요 장비로써 가입자 식별 모듈(SIM)을 포함하고 있으며, 흔히 USIM이라고 불린다.

UICC를 SE로 활용하는 경우 SE를 관리하는 마스터 키는 이동통신사가 보유하게 된다. UICC 방식을 계속 사용하게 되면 이동통신사의 USIM 인프라를 활용할 수 있다는 장점이 있다. 하지만 USIM은 표준화가 되어 있지 않고 이동통신사 별 규격의 차이로 인해 사용자가 불편할 수 있으며, 또한 통신정보를 관리하는 USIM에서 금융정보를 포함한 개인정보가 다뤄지기 때문에 보안 측면에서도 위험이 높다는 논란이 계속되고 있다.

3.2 embedded 방식

embedded 방식은 SE가 모바일기기 제조 단계에서부터 내장되는 방식으로, 모바일기기 제조사나 플랫폼 사업자가 서비스의 주도권을 갖게 된다. 모바일기기 제조사는 SE에 개별 이용자의 정보를 저장한 후 기기를 판매하게 되는데, 금융기관이 모바일기기 제조사에게 SE 이용 수수료를 지급하고 SE에 대한 통제권을 획득하는 경우도 있다.

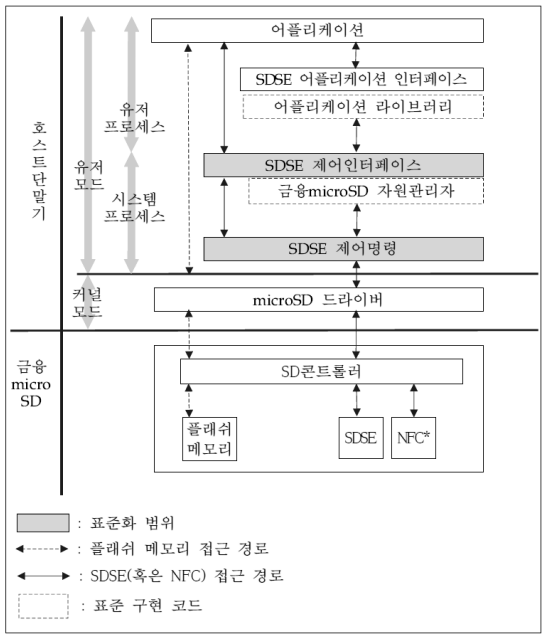
embedded 방식은 제조 단계에서부터 내장되기 때문에 탈부착이 어렵다는 단점이 있는데, 이로 인해 가격이 상승되고 기기 교체 시 재사용이 불가능하다는 어려움이 있다.

3.3 microSD 방식

microSD는 모바일기기의 메모리 확장 시 이용되는 소형 플래시 메모리카드를 말한다. microSD는 데이터를 저장하는 낸드 플래시칩과 전력 및 신호처리를 담당하는 SD컨트롤러로 구성되는데, 여기에 금융정보 및 보안모듈 등이 탑재, 모바일기기에 장착되어 금융정보를 안전하게 보관하도록 고안된 것이다. 이 경우 금융기관은 이동통신사의 개입 없이 독립적으로 지급결제 서비스를 제공할 수 있다.

또한 UICC에 비해 저장용량이 커서 microSD 내에 다양한 어플리케이션의 설치가 가능하며, 공인인증서를 휴대폰 내부메모리가 아닌 SE에 저장함으로써 보안성을 강화할 수 있다. 또한 UICC와 달리 표준화가 이루어져 있어 사용자의 이동통신사 변경 시에도 금융정보가 포함된 종전의 SE를 계속 사용할 수 있다는 이점이 있다.

Ⅳ. 금융microSD 프레임워크 분석 및 활용



〔그림 7〕 금융microSD 구성 및 표준화 범위

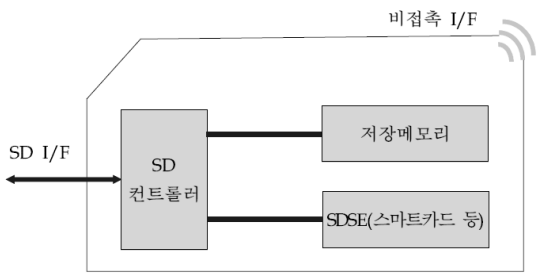
본 고에서의 금융microSD의 프레임워크 분석은 2012년 10월 제정된 금융microSD 표준을 기반으로 한다. 금융microSD 표준은 모바일 금융서비스를 이용할 수 있는 금융정보를 저장하는 매체 규격에 대한 것으로 기본요구사항을 포함하여 총 5부로 구성되어 있다[3].

〔표 6〕 금융microSD 표준 구성

번 호	제 목	구 분
제1부	기본 요구 사항	공통사항
제2부	SDSE 제어인터페이스	기술부문
제3부	SDSE 제어명령	기술부문
제4부	금융microSD 식별번호 부여체계	관리부문
제5부	금융microSD 발급기관 식별번호 관리체계	관리부문

4.1 금융microSD 내부 구성

금융microSD의 내부 구성은 SD 표준화 단체인 SDA(Secure Digital Association)에서 정의한 SD카드의 내부 논리 구성구조를 기반으로 설계되었다. 따라서 금융microSD는 내부에 필수 사항인 SDSE(microSD Secure Elements)를 탑재하여, 호스트단말기와는 SDA에서 제정한 호스트단말기와 SD간의 통신규격인 Common SD I/F(Interface) 및 비접촉 I/F를 이용하여 통신하는 금융 서비스를 지원하는 매체를 말한다[8].

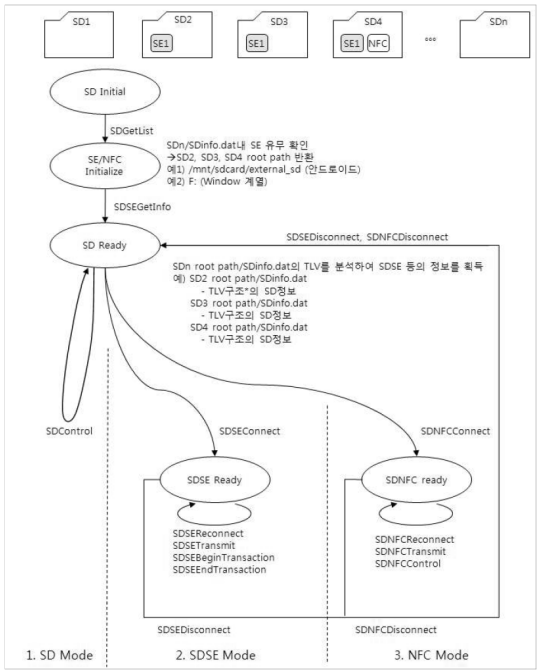


〔그림 8〕 금융microSD 내부 구성

4.2 금융microSD 동작절차[8]

4.2.1 접근 계층도

장착된 모든 microSD를 검색하여 SDSE가 존재하는 microSD에 대해서만 드라이브 목록을 획득하고, 획득된 드라이브에 root path에서 SD 정보파일(SDinfo.dat)을 획득한다. SD 정보파일은 TLV(Tag Length Value) 구조로 되어 있으며, TLV구조를 분석하여 SDSE 접근파일을 획득 후, SDSE 접근파일을 입출력버퍼로 사용하여 SDSE에 접근한다.



〔그림 9〕 금융microSD 접근 계층도

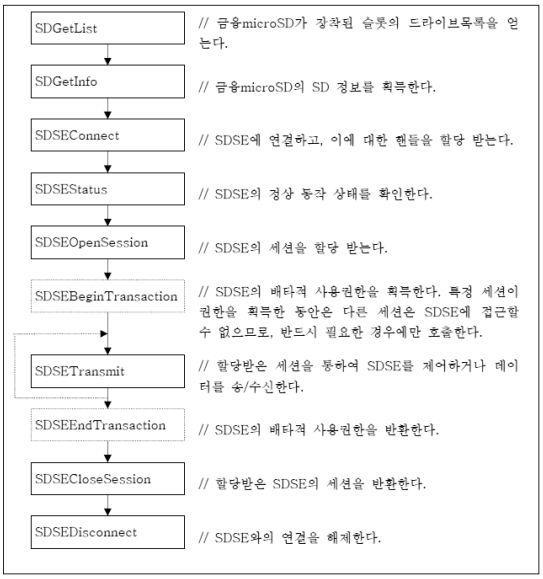
4.2.2 금융microSD 인식

리눅스 또는 유닉스 계열의 운영체제를 사용하는 호스트단말기의 경우 마운트되는 디렉토리 이름 또는 디바이스 파일을 통하고, 윈도우즈 계열의 운영체제를 사용하는 호스트단말기의 경우 영문자 기반의 드라이브명(E:\, F:=\ 등)을 통하여 접근하게 된다.

또한 금융microSD내에 있는 SDSE와 SDNFC는 파일을 통해 접근이 가능한데, SDSE(NFC) 접근파일은 금융microSD 내부에 하나의 SDSE(SDNFC)와 논리적으로 연결되어 있으며, 이는 파일처리용 함수(open(), close(), read(), write())를 사용하는 방식으로 SDSE(SDNFC)와 통신하게 된다. 이때 파일에는 실제 데이터가 쓰여 지지는 않고 SDSE에 데이터를 전달하기위한 통로 역할만을 하게 된다.

호스트단말기에서 금융microSD 내부에 있는 SDSE(NFC)에 접근하기 위한 SDSE 접근파일명은

SDSE.dat(SDNFC.dat)이며, 파일명은 GetInfo를 통해서 획득할 수 있다. 또한 해당 파일명은 비휘발성으로, 포맷되지 않는 한 같은 파일명을 유지하게 된다. 따라서 전원이 켜져있는 상태에서 서로 다른 어플리케이션에서 획득되는 파일명은 동일하다.



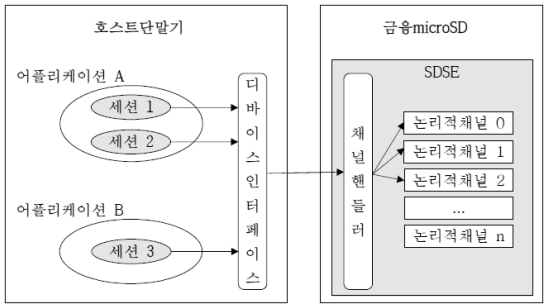
〔그림 10〕 SDSE 인터페이스 처리 흐름도

어플리케이션에서는 SDGetList를 통하여 SDSE가 내장되어 있는 모든 microSD의 드라이브 목록을 획득하게 되는데, 이때 금융microSD 자원관리자는 SDSE를 내장하고 있는 모든 microSD의 드라이브 목록을 가지고 있다가 어플리케이션에 반환하여 드라이브 목록을 획득하게 된다. 이후 SDGetInfo를 통하여 TLV구조와 SD 정보를 획득하여 TLV를 분석, SDSE 접근파일명과 NFC 접근파일명을 파악하게 된다.

4.2.3 세션 연결

세션은 어플리케이션과 SDSE 내의 어플리케이션간의 논리적인 연결을 제공한다. 세션은 SDSEOpenSession으로 회득하고, SDSECloseSession으로 반환하게 된다. 이 때 세션은 SDSE에서 논리적 채널로 할당되는데, 세션과 논리적 채널이 1:1로 대응되어 할당된다.

이후 호스트단말기에서 SDSE를 내장하고 있지 않은 일반 microSD를 제외한 금융microSD만을 조회목록에 포함하여 조회하게 된다.

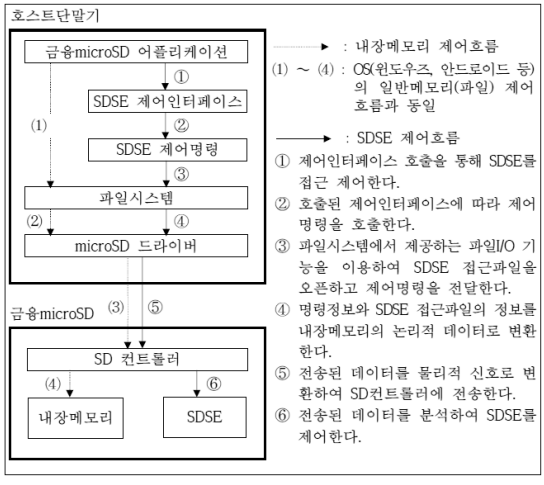


〔그림 11〕 세션 연결 구조

4.2.4 SDSE 접근 및 제어

어플리케이션에서 SDSE를 제어하는 방식은 명령 송수신을 통하여 이루어진다. 어플리케이션과 SD컨트롤러 사이의 명령 송수신은 저장메모리의 SD 정보파일(SDinfo.dat)을 읽어 금융microSD에 장착된 SDSE을 확인하고, SDSE 접근파일(SDSE.dat)을 통하여 제어명령을 송수신하게 된다. 또한 어플리케이션 및 SD컨트롤러 간 명령 송수신은 상기 SDSE 접근파일에 일반적 파일 I/O 함수를 이용하여 읽기·쓰기 방식으로 수행하게 된다.

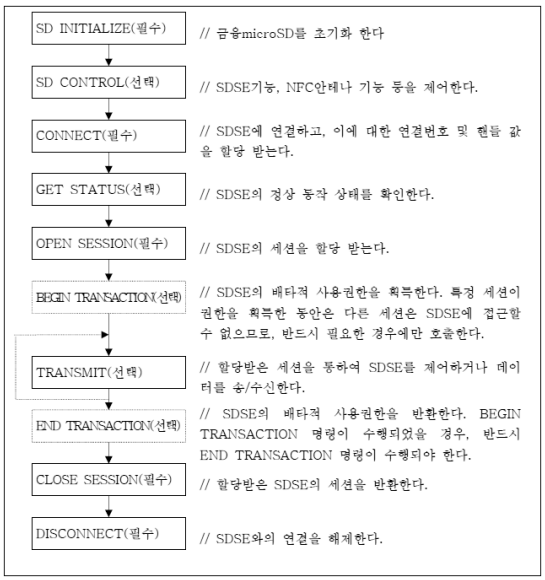
금융microSD 내의 SDSE에 접근하기 위해 1단계로 어플리케이션은 SD정보파일(SDinfo.dat)를 읽어 장착된 SDSE를 확인하고, 2단계로 SDSE 접근파일



〔그림 12〕 SDSE 접근 및 제어 방식

(SDSE.dat)을 통하여 어플리케이션과 SD컨트롤러 간 명령전문을 송수신한다.

이 때, SD컨트롤러 또는 금융microSD 자원관리자는 SD정보파일과 SDSE 접근파일을 생성하고 관리하게 되는데, 동시에 SD정보파일 및 SDSE 접근파일의 삭제를 방지하고, 삭제될 경우 재생성시킨다.



〔그림 13〕 SDSE 제어 명령 흐름

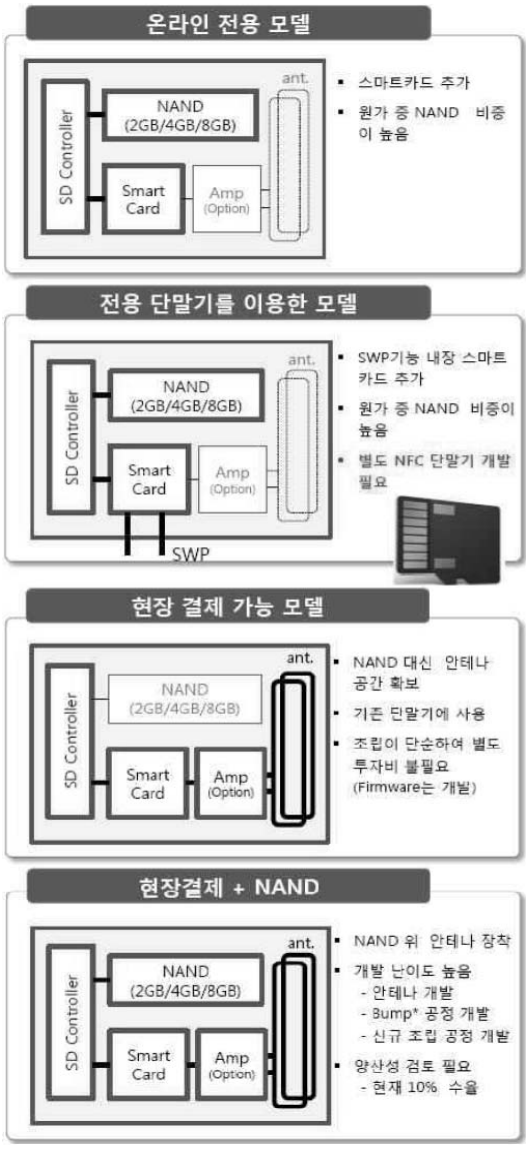
4.3 금융microSD 표준 적용 및 활용방안[9]

4.3.1 금융microSD 표준 적용 제품 유형

금융microSD 표준을 기반으로 구현이 가능한 제품 유형은 크게 온라인 전용 모델, 전용 단말기 이용 모델, 현장 결제 가능 모델, 현장결제 + NAND 모델로 나누어 볼 수 있다.

4.3.2 금융microSD 활용방안

금융microSD의 활용방안은 다양하다. 금융정보화추진협의회는 2013년 4월 금융microSD 표준 기반 모바일금융서비스 시연회를 개최하였는데, 우리은행, 농협카드, 외환카드, 하나SK카드, BC카드, 드림시큐리티, 크루셜텍, 유니온터뷰니티, 코나아이, 티모넷, SK C&C 등의 기업들이 시연기관으로 참여한 바 있다.

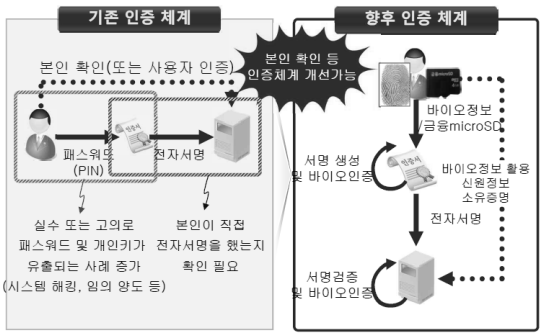


〔그림 14〕 금융microSD 표준 적용 유형별 제품

〔표 7〕 금융microSD 시연회 참가기관 및 시연 내용

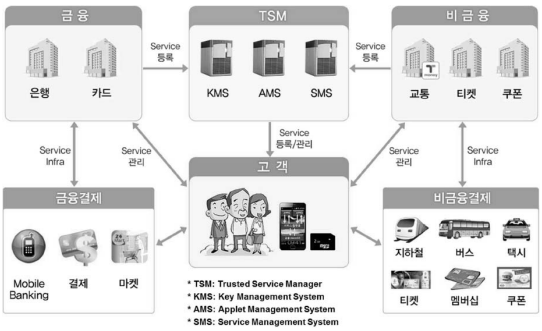
구분	기관명	시연 내용
은행사 (1)	우리은행	— 모바일 뱅킹서비스 · 모바일보안토큰 발급 · 모바일보안토큰 기반 로그인 및 이체
카드사 (4)	농협카드, 외환카드, 하나SK카드, BC카드	— 모바일 신용카드서비스 · 모바일신용카드 오프라인 결제 · 신용카드 앱에서 사용내역 조회
IT업체 (5)	드림시큐리티, 크루셜텍	— 지문인식기반 모바일보안토큰
	유니온커뮤니티	— 지문인식기반 보안솔루션
	코나아이	— 모바일 OTP
	티모넷	— 모바일 교통카드서비스 · 모바일 티머니 온라인·오프라인 결제
	SK C&C	— 모바일 지급결제 생태계 솔루션 · TSM, 카드 발급 시스템 등

시연회에서는 금융microSD를 기반으로 한 모바일뱅킹, 모바일신용카드, 모바일교통카드 등 다양한 모바일 금융서비스 활용 방안과 함께 모바일보안토큰, 모바일 OTP, 생체인증 등의 IT솔루션 서비스도 함께 선보여졌다.



〔그림 15〕 생체인증 모바일토큰을 이용한 모바일뱅킹

이외에도 모바일신분증, 지문인식기반 도어락 등 금융microSD의 활용 영역은 비단 금융 부문에만 그치지 않고 비금융 부문에도 적용할 수 있어 그 영역은 점차 확대될 것으로 보인다.



〔그림 16〕 금융microSD의 활용 영역

4.4 금융microSD의 기대효과

금융microSD는 사용자 입장에서 금융정보 저장 매체가 다양화됨으로 인해 선택권이 향상되고, 스마트폰 변경 시 자유로운 이동 장착이 가능함에 따라 금융정보를 재발급 받아야하는 불편함이 해소될 수 있다. 또한 금융microSD 표준이 국제표준의 초석이 됨으로써 외국 업체의 특허 공세도 방어할 수 있을 것으로 기대된다.

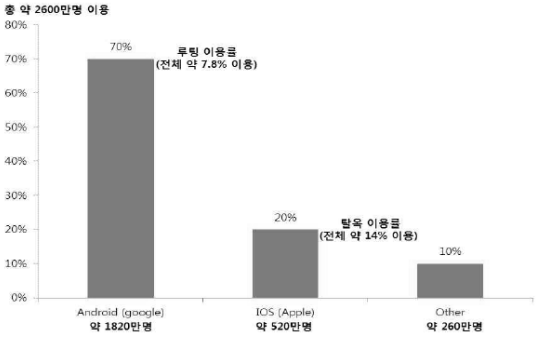
금융기관은 이동통신사의 개입 없이 독자적인 모바일지급 결제서비스를 제공함에 따라 다양한 응용서비스를 제공할 수 있으며, 서비스제공자 역시 자유로운 독자 서비스의 제공을 통해 다양한 지불 응용 사업과 접목이 가능하게 되어 업체 간 선의의 경쟁을 펼칠 수 있는 장이 되리라 기대한다[9].

한국은행에서는 금융microSD가 확산되면 모바일금융서비스를 위한 금융정보들이 안전하게 관리되어 유출에 의한 금융 사고를 예방할 수 있을 것으로 예상하며, 통신기반 금융서비스의 안전성 제고에도 크게 기여할 것으로 기대하고 있다[3].

4.5 금융microSD의 보완점

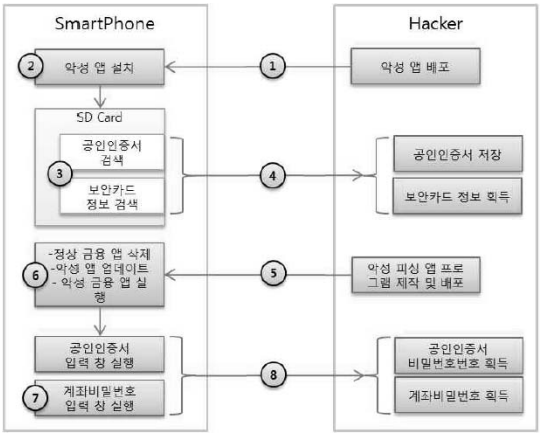
4.5.1 기술적 측면

금융microSD는 탈착이 용이하여 이동 장착 시 편리하다는 장점이 있지만, 반대로 그로 인해 분실가능성이 높아져 결제정보 등의 유출 위험이 존재한다. USIM의 경우, 분실 시 스마트폰의 주요 기능(통화 등)이 마비되어 분실 여부를 즉각 인지할 수 있지만, 금융microSD를 분실했을 때는 즉각적인 확인절차가 없어 분실을 인지하는데 시간이 걸릴 수 있다. 만약 그 사이 금융정보 등의 개인정보가 유출된다면 그 피해는 더욱 확산될 것이다.



〔그림 17〕 국내 스마트폰 사용 및 루팅(탈옥) 현황[10]

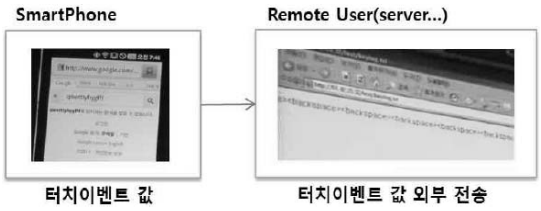
또한 microSD의 해킹 가능성도 무시할 수 없다. 2012년 2월 기준, 국내 스마트폰 이용자 2,600만 명 가운데 안드로이드폰과 아이폰 사용자는 90%에 달했고, 이들 중 루팅(탈옥)으로 스마트폰 해킹을 시도한 사용



〔그림 18〕 스마트폰 뱅킹 해킹 시나리오

자는 사용기간이 길수록 그 비율이 높았다.

2010 국제정보보호컨퍼런스에서 소개된 스마트폰 뱅킹 해킹 시연에서는 SD에서 금융 정보를 수집하는데 성공한 바 있고, 2011 POC(Power of Community)에서 소개된 스마트폰 해킹 시연에서는 공격자가 스마트폰에 Kernel Rootkit을 설치하여 터치이벤트값을 절취 및 위·변조하고 이를 외부에 전송하는데 성공했다[10]. 그렇다면 스마트폰의 터치이벤트값과 공인인증서 비밀번호 또는 보안카드 캡춰화면 등이 공격자에게 전송될 가능성은 충분하다.



〔그림 19〕 스마트폰 터치이벤트 값 절취 시연

이러한 불법 루팅(탈옥) 등의 해킹에서 스마트폰을 보호하기 위해서는 스마트폰의 운영체제를 업데이트하는 것이 한 방법이 될 수 있는데, 운영체제 업데이트 시 iOS의 경우 애플에서 모든 것을 관장하는 반면, 안드로이드는 각 단말제조사에서 개별적으로 관리하기 때문에 업데이트 운영체제에 대한 배포속도가 느려져 제로데이 공격(Zero-day Attack)에 더욱 취약할 수 있다는 것 역시 문제점으로 지적된다.

더불어 안드로이드 운영체제에서 스마트폰 뱅킹을 이용하는 경우 은행 공인인증서를 복사하여 사용하게 되는데, 스마트폰에 공인인증서를 복사하기 위해 특정 절차를 거쳐야만 하는 것처럼 눈속임하는 일은 다시는 없어야겠다. 단순 Copy&Paste로 공인인증서의 복사가 가능하다는 것은 이미 많은 이들이 인지하고 있는 사실이다. 이러한 기존 공인인증서 허술한 복제 문제도 극복해야할 과제로 남아있다.

4.5.2 경제적 측면

금융microSD는 스마트폰에 탑재된 NFC 기능과 연동되어 결제서비스를 이용하거나, microSD 자체에 NFC 기능을 내장하여 NFC 기능 미탑재 단말기(iOS 단말, 피쳐폰 등)로도 NFC 기반 결제가 가능하다는 장점이 있다. 하지만, 금융microSD 자체가 기존에 사용되어오던 USIM에 비해 가격이 높아(25~50달러) 가격상승의 요인이 된다는 문제가 제기된다,

또한 금융microSD를 NFC와 연동하여 활용하고자 할 경우 NFC 인식단말기 설치 등 인프라 구축에 대한 부담과 낯선 기술에 대한 거부감 등으로 성장이 더딜 수 있다[5].

4.5.3 법률적 측면

관련법의 정비도 필요하다. 현재의 법률 및 규정은 모바일 지급결제의 범주를 뚜렷이 특정하고 있지 않아 모바일 서비스를 효과적으로 규제·감독하기 어려운 측면이 있다. 원칙적으로 2007년 1월 시행된 전자금융거래법이 각종 전자적 금융거래를 규율하고 있으나 모든 모바일 지급결제 서비스에 적용하는 데는 한계가 있다. 전자금융거래법은 전자지급대행업자(PG사)의 영업대상을 온라인으로 한정하고 있으나 PG사들은 점차 오프라인으로 서비스 영역을 확장하고 있기 때문이다. 아울러 Apple, Google, Paypal과 같이 해외에 서버를 둔 글로벌사업자들이 국내에서 지급결제 서비스를 제공하는 경우 국내법을 적용하기 어렵다[1].

4.5.4 기타

NFC 탑재 단말에 비해 이용자들의 인식도가 낮은 것과 더불어 모바일 지급결제에 대한 이용자들의 보안 우

려도 금융microSD가 대중화되는데 걸림돌이 된다. MasterCard의 설문조사(2011)에 따르면 응답자의 62%가 모바일 지급결제 수단 이용 시 금융정보 유출을 우려하고 있다고 한다[1].

이 외에도 금융microSD는 microSD슬롯이 존재한다는 가정 하에 사용되는데, microSD슬롯이 없는 일부 단말의 경우 사용이 불가하여 이러한 단말을 사용하는 사용자들에게 금융microSD는 선택권 확대가 아닌 선택권 축소 내지는 역차별이 될 수 있다.

Ⅴ. 결 론

모바일 혁신의 영향으로 국내는 물론 세계에서도 모바일 지급결제 서비스 분야에 큰 변화가 나타나고 있다. 특히나 최근에는 스마트폰의 등장으로 인해 모바일 지급결제가 더욱 활성화되면서 모바일뱅킹이 자금이체 부문에서 상당한 비중을 차지하고 있다.

이러한 상황에서 최근 보안성과 편리성을 무기로 한 모바일 지급결제 수단으로써 금융microSD가 새롭게 떠오르고 있다. 기존의 USIM 방식에 비해 공인인증서를 포함한 금융정보 및 개인정보를 논리적, 물리적으로 보다 안전하게 저장함으로써 보안성을 강화할 수 있고, 탈부착이 가능하여 편리하게 사용할 수 있으며, 금융microSD의 국제 표준 초석 등의 여러 가지 이점이 있기 때문이다. 하지만 이러한 장점들에도 불구하고 분실 및 해킹으로 인한 정보의 유출, 가격 상승 및 인프라 구축에 대한 거부감으로 인한 대중화 저해 가능성, 모바일 지급결제 관련법의 미비로 인한 분쟁 가능성 등 해결해야 할 과제도 적지 않다.

금융microSD는 특정 이해당사자의 필요에 의해 만들어진 것이 아니라 정책기관, 금융계, 산업계, IT업계가 함께 필요성을 공감하여 탄생된 결과물이다. 이러한 금융microSD가 기존 모바일 지급결제 서비스뿐만 아니라 신규 서비스 창출의 촉매제로도 활용될 수 있도록 하기 위해서는, 업계는 사용자를 만족시킬 수 있는 서비스를 계속 개발하며 경쟁하는 동시에 기술 표준화와 인프라 구축에 힘써야 하고, 정부는 신규서비스에 대해 관련법 규정의 미비로 인해 규제 사각지대가 발생하거나 피해구제가 어려워지는 등의 문제를 해결하기 위해 관련법을 면밀히 검토할 필요가 있다.

본고에서는 금융microSD 표준과 동 표준 기반 시연회에서 각 기업들이 제시한 Prototype을 중심으로 금융microSD의 프레임워크를 분석하고 활용방안 및 보완점에 대해 짚어보았다. 이후 연구에서는 금융microSD를 적용하여 출시되는 제품들과 기존 방식의 장단을 비교하여 보다 안전하고 편리한 지급결제 수단으로 기능할 수 있도록 해야 할 것이다.

참고문헌

[1] 이동규, 모바일 지급결제 혁신 동향 및 시사점, BOK 이슈노트, 2013-7, 2013년 5월.

[2] 한국방송통신위원회, 2012 유무선 통신서비스 가입자 현황, 2013년 3월.

[3] 한국은행, 2012년도 지급결제 보고서, 2013년 3월.

[4] Gartner, "Forecast: Mobile Payment, Worldwide, 2009~2016", May 2012.

[5] 이주영, "최근 NFC 및 비 NFC 기반 모바일 결제시장 현황", 방송통신정책, 25(7), pp. 67-80, 2013년 4월.

[6] Arthur D.Little, Global M-Payment Report Update, Apr. 2009.

[7] Federal Reserve Bank of Boston, Survey of Consumer Payment Choice, Apr. 2011.

[8] 금융정보화추진협의회, 금융microSD 표준(안), 2012 10월.

[9] 유희준, 금융microSD 표준 기반 모바일금융서비스 시연회 발표자료, 한국은행 금융결제국, 2013년 4월.

[10] 금융보안연구원, 금융 스마트폰 주요 보안 이슈 및 동향보고서, 2012년 7월.

[11] 공영일, "NFC기반 모바일 결제시장의 이해관계 분석과 시사점", 정보통신정책연구원, 23(6), pp. 55-63, 2011년 4월.

[12] 김남훈, "모바일 지급결제의 현황 및 경쟁구도", DIFIECO FOCUS, 2012년 9월.

[13] 김남훈 외 1명, 스마트폰이 모바일 금융시장에 미치는 영향, 하나산업정보, 13, 2010년 2월.

[14] 김서영, "국내외 신유형 지급결제서비스 현황과 시사점", 지급결제와 정보기술, 51, 2013년 1월.

[15] 김진백, "스마트폰 기반 모바일 뱅킹에서의 연구과제: 국내 모바일 뱅킹 사례 연구 및 논문 리뷰", Entrue Journal of Information Technology,

10(2), pp. 223-238, 2011년 7월.
[16] 김필수, "스마트폰의 확산이 지급결제시스템에 미치는 영향 및 대응전략", 지급결제와 정보기술, 42, pp. 29-58, 2010년 10월.
[17] 이수미 외 3명, "모바일 NFC 기반 보안 동향", 한국정보통신기술협회, 136, pp. 52-57, 2011년 8월.
[18] 조진만 외 4명, "모바일 지급결제의 시장 현황 및 표준화 동향", 전자통신동향분석, 20(1), pp. 33-42, 2005년 2월.
[19] 최필주 외 2명, "모바일 지급결제 및 바이오인식 융합기술 동향", 정보보호학회논문지, 22(4), pp. 21-28, 2012년 6월.
[20] 강동호 외 6명, "스마트폰 보안 위협 및 대응기술", 전자통신동향분석, 25(3), pp. 72-80, 2010년 6월.
[21] "금융microSD 기고문 - 이중식 한국은행 금융결제국장", 전자신문, 2010년 5월. <http://www.etnews.com/news/economy/finance/2761774_1492.html>

〈著者紹介〉

이 정 규 (Jung-Gyu Lee)
학생회원

2013년 2월 : 한세대학교 경찰행정학과/정보통신공학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일 보안, 금융 보안, DB 보안

황 희 성 (Hee-Sung Hwang)
학생회원

2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 보안컨설팅, 감리

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
<관심분야> 통합로그 시스템, K-ISMS, PIMS, 클라우드컴퓨팅 보안, 개인정보보호