NFC 보안 기술 분석 및 UICC 적용 효과 연구

정회원 임 선 희*, 전 재 우**, 준회원 정 임 진**, 정회원 이 옥 연***

Study on NFC Security Analysis and UICC Alternative Effect

Sun-Hee Lim*, Jae-woo Jeon** *Regular Members*, Jung Imjin** *Associate Member*,
Okyeon Yi*** *Regular Member*

요 약

NFC(Near Field Communication) 기술은 근접거리(Proximity) 무선 기술로서 다양한 모드에서의 서비스를 지원한다. 특히, NFC 기술은 유사한 RFID 기술에서의 단순한 태그 인식 서비스보다 복잡하고 상호연결 기술 지원으로 소액결제서비스, 티켓팅과 같은 금융서비스 지원이 가능하다. 그 결과로서 NFC 보안 기술은 보다 강력한 보안 기술을 정의하고 있다. 본 논문에서는 NFC 보안 기술에 대한 명세 및 분석하여 NFC 보안기술의 안전성 분석을 기반으로 NFC SE(Secure Element) 대안으로 UICC 카드의 가능성 및 효과에 대해 연구한다.

Key Words : NFC, Security, UICC, RFID, Secure Element

ABSTRACT

Near Field Communication is an emerging short-range wireless connectivity technology that offers proximity and different operating modes. Particularly, NFC technology has the potential to revolutionize mobile applications like payment and ticketing because NFC is more complex and mutual connectivity than RFID as the simple tag reader. Finally, NFC security technology defines the robust security protocols. This paper will specify and analyze the NFC security technology, and study the chance and its beneficial effect of the UICC card as the NFC Secure Element.

Ⅰ. 서 론

무선 네트워크 기술들의 도약적인 발전으로 통신, 금융, 유통 등 다양한 응용 서비스들이 활발하게 정의되고 있다. 각 무선네트워크 기술들의 특징에 따라 UMTS(Universal Mobile Telecommunications System), WiBro 같은 광대역 이동통신 망서비스, 로컬영역에서의 무선 네트워크 서비스인 무선랜 서비스뿐만 아니라 근거리 통신인 UWB(Ultra-wideband), Bluetooth, ZigBee 기술에 적합한 응용 서비스들이 모색되고 있다.

최근, NFC(Near Field Communication) 기술인 13.56Mhz 주파수 대역에서 10cm 이내의 근거리 통신을 기반으로 인식속도가 0.1초 이내로서 106Kbps~424Kbps 데이터 전송 속도를 지원하는 통신 기술이 정의되었다. NFC 기술은 ECMA, ISO, ETSI에서 표준을 진행하고 있다. 특히, ECMA-340(NFCIP-1)과 ECMA-352(NFCIP-2) 표준을 중심으로 NFC 기술에 대해 정의하고 있다.

근접통신(NFC) 기술은 지불, 티켓팅, 고객관리, 마케팅과 같은 다양한 응용서비스에 적용 가능한 잠재력을 가지고 있다[1]. NFC 기술이 탑재된 디바이스를 통해 스마트포스터(SmartPoster), 잡지나 상점의 물건

※ This paper has been supported by the Software R&D program of KEIT. [2010-10035257, Development of global collaborative integrated security control system]
* 한국전자통신연구원 지식정보보안연구부 인프라보호연구팀(capsunny@etri.re.kr),
** 고려대학교 정보경영공학전문대학원(jjwkma61@korea.ac.kr, ijjung@korea.ac.kr), *** 국민대학교 수학과(oyyi@kookmin.ac.kr)
논문번호 : KICS2010-10-488, 접수일자 : 2010년 10월 12일, 최종논문접수일자 : 2010년 12월 10일

들과의 상호작용을 통해 실시간으로 관련 정보를 검색하거나 요청이 가능하다. 또한 신용 카드와 유사한 전자 지갑 기능이 가능하다.

NFC 기술의 지원으로 사용자는 사용자의 핸드셋을 통해 새로운 응용서비스에 접할 수 있는 기회를 갖게 되었다. 즉, 각각의 물건을 인터넷상의 콘텐츠로 생각하여 각각의 콘텐츠 웹사이트로부터 실시간으로 정보를 추출 활용한다는 개념인 "The Internet of Things"를 NFC 기술의 지원으로 사용자가 적극적으로 정보 교류에 참여할 수 있는 서비스 모델이 가능하게 되었다[9].

본 논문에서는 NFC 기술의 특징 및 응용 서비스를 기반으로 안전한 서비스를 제공하기 위해 NFC 기술에서 정의하고 있는 보안 기술에 대해 분석한다. NFC 보안 기술은 NFC 기술의 금융 서비스 지원과 같은 응용성 때문에 타원곡선 공개키 방식의 인증 및 키 분배, 데이터 기밀성과 무결성을 지원을 위해 AES-CTR 모드 및 AES-CBC와 같은 강력한 보안 기술에 대해 정의하고 있다. 결과적으로, NFC 보안 기술에 대한 안전성 분석을 하고 UICC 카드에 보안 기술을 적용하였을 경우의 가능성과 그에 대한 효과에 대해 연구한다.

Ⅱ. NFC(Near Field Communication) 기술

NFC 기술은 다양한 근거리 무선 통신들의 다양한 성질들을 결합하여 다음과 같이 세 가지 모드로 작동 가능하다. 이 모드들은 각각 RFID와 같이 데이터를 읽고 수정할 수 있는 모드, 블루투스 등과 연결하여 데이터 통신 서비스 가능 모드, 카드에 탑재되어 비접촉식 카드의 성질을 지원하면서 스마트카드의 안전성을 기반으로 하는 안전한 서비스들이 지원 가능하다.

2.1 NFC 운영모드[9,10]

2.1.1 Reader/Writer 모드

NFC 디바이스는 NFC 트랜스폰더에 저장된 데이터를 읽고 수정할 수 있다. 사용자는 SmartPoster와 같이 NFC 디바이스가 스마트포스터의 태그를 읽어 추가 정보를 조회할 수 기술이다. URL 주소가 저장되어 있는 태그에서 NFC 디바이스를 터치(touch)하면 URL 주소를 읽고 그 주소의 웹사이트에 접근을 지원한다.

2.1.2 Card Emulation 모드

NFC 디바이스가 스마트 카드(ISO 14443)처럼 작동하는 모드이기 때문에 외부 NFC 리더기는 스마트카드와 NFC 디바이스를 구분할 수 없다. 이 모드에서는 비접촉식 지불, 티켓팅 서비스가 가능하다.

2.1.3 Peer-to-Peer 모드

Peer-to-Peer 운영모드(ISO 18092)는 두 개의 NFC 디바이스간의 링크 수준의 통신을 지원한다. 블루투스 페어링 절차를 NFC 기술로 대체하여 연결 초기 절차를 단순화한다. 연결 확립을 위해 클라이언트 (NFC peer-to peer initiator)는 호스트 (NFC peer-to-peer target)를 검색하고 NDEF(NFC Data Exchange Format) 메시지 형식을 통해 데이터를 전송한다.

2.2 NFC와 WPAN 통신 기술의 비교

NFC 기술은 다른 PAN 영역의 무선 통신과 비교하면 매우 짧은 거리에서의 통신 기술이다. 스마트카드 표준인 ISO 14443을 기반으로 약 10cm 정도의 거리에서의 통신 방법을 지원한다. 이러한 기술은 사용자가 모든 행위에 주체가 되는 사용자 중심의 서비스가 가능할 수 있다는 특징을 가지게 됨으로써 "Touch and Go"의 새로운 차원의 편리성을 추구할 수 있다[9]. 표 1은 NFC 기술과 단거리 무선 통신과의 기술의 비교이다[2,11]. 이는 NFC 기술이 RFID 기술과는 차별성을 가지고 있다. 특히, NFC 기술은 블루투스와 연동하여 데이터 전송을 위한 상호 보완 기술이 가능하다는 점 등 NFC 기술만의 특징으로 새로운 서비스 제

표 1. NFC와 다른 단거리 통신 기술의 비교

	NFC	RFID	IrDa	Bluetooth
초기절차	0.1ms이내	0.1ms이내	0.5s이내	6s이내
범위	약 10cm	3m	5m	30m
편리성	사용자중심, 쉽고, 직관적, 빠른 서비스	아이템중심, 편리	데이터 중심, 편리	데이터 중심
선택도	high, given, security	Partly given	Line of sight	식별 및 인증
사용처	지불, 접근허락, 공유, 초기서비스, 등록 편리	아이템 추적	데이터 제어 및 교환	데이터 교환을 위한 네트워크
소비자 측면	touch, wave, simply connect	get information	easy	configuration needed

안이 가능하다.

2.3 NFC 응용 서비스

NFC 기술은 실생활과 연계된 복잡한 정보활동에 대한 해결책으로 모든 타입의 사용자 기기에 대해서 “touch-and-start” 형식으로 직관적 연결이 가능하다[9]. 직관적 연결은 사용자가 두 개의 NFC 장치들을 가까이 접촉함으로써 각 환경에서 필요한 정보를 전송하고 복잡한 환경 설정 과정 동안 사용자 개입 없이 상호작용이 가능하다. 표 2는 NFC 기술에서 지향하는 목표 및 그에 대한 응용 서비스들을 분류한다[8]. 이러한 편리성으로 인해 NFC 기술은 단순 콘텐츠 캡처, 태그를 가진 포스터로부터의 URL 주소 획득 및 연결 등과 같은 응용 서비스들이 고려되고 있다. 특히, 가상쿠폰 서비스, 포스터 광고 및 티켓 구매 서비스, 자판기 서비스와 같은 소액 결제 서비스에서부터 의료 서비스까지 NFC 기술은 단순 태그 인식 서비스를 지원하는 RFID 기술보다는 보다 복잡하고 상호 데이터 통신을 요구하는 응용 서비스들에 적용가능하다.

표 2. NFC 응용 구분

구분	내용
접촉과 실행형 (Touch and Go)	접속제어나 물류, 이벤트 추적형, 티켓이 저장된 사용자 단말이나 접속코드를 리더 가까이 가져가면 자동으로 처리
접촉과 확정형 (Touch and Confirm)	암호입력이나 처리절차의 허용으로 확정되는 전자 지불 등의 응용으로, 사용자 암호 등의 정보가 저장된 사용자 단말이나 접속 코드를 리더 가까이 가져가면 자동으로 처리
접촉과 연결형 (Touch and Connect)	P2P(peer to peer) 데이터 전송이 가능한 두 NFC 장치의 연결을 통한 음악의 다운로드나 이미지 파일 혹은 주소록의 업데이트 처리
접촉과 발견형 (Touch and Explore)	사용자의 NFC 장치 스스로가 서비스 활용이 가능한 주변장치의 기능 파악

Ⅲ. NFC 보안 기술

NFC 보안 기술은 NFC Forum을 중심으로 ECMA 표준을 기반으로 데이터 교환 형식 및 태그 타입, 보안 프로토콜에 대해 정의하고 있다.

NFC 보안 프로토콜(NFC-SEC)은 그림 1과 같이 NFCIP-1(Near Field Communication Interface and Protocol)에 의해 NFC 디바이스간의 통신이 연결된 후에 서비스를 제공한다[6].

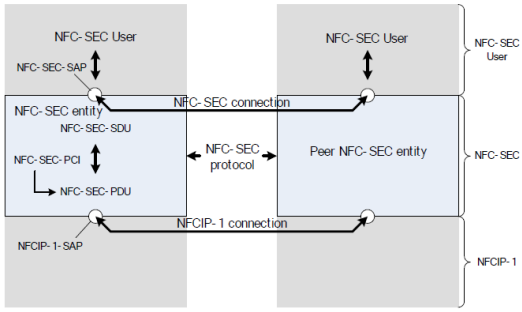


그림 1. NFC-SEC의 보안 계층 구조

NFC-SEC에서는 SSE와 SCH 보안 서비스를 제공한다.

3.1 보안 서비스[7]

3.1.1 SSE(Shared Secret Service)

NFC 디바이스간의 암호통신을 위한 공유 비밀(shared secret)을 생성하며, 이 과정에서 키 일치 및 확립 과정을 수행한다.

3.1.2 SCH(Secure Channel Service)

SSE 서비스를 통해 생성된 링크키를 통해 NFC 디바이스간의 통신 데이터에 대한 기밀성과 무결성을 제공한다.

3.2 보안 프로토콜 메커니즘

3.2.1 사전 요구사항

1) 각 NFC 디바이스는 EC(Elliptic Curve Diffie-Hellman) 공개키와 개인키를 가진다.
2) 식별자로서 연결 결합(association)과정에서 확립된 서로의 NFCID3(Random ID for transport Identifier) 값을 알고 있다.

NFCID3는 총 10octets 길이로 초기자(Initiator)의 랜덤 식별자(random identifier)로 정의된다. 이 값은 연결된 섹션동안에는 고정되어 있고 응용서비스에 따라 동적으로 생성된다.

3.2.2 SSE 과정

SSE는 그림 2와 같이 디바이스의 NFC-SEC에서 키 일치 및 확립 과정을 수행한다.

송신자, 수신자가 각각 생성한 난수값 NA, NB과 정수값 QA, QB를 통해 키 동의(Key Agreement) 과정

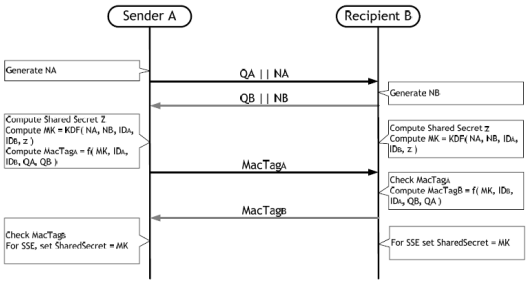


그림 2. 키 일치 및 확인 절차

① 송신자 A : 난수값 Nonce NA를 생성
② 송신자 A : 정수값 QA를 8자리 배열로 변환
③ 송신자 A → 수신자 B
ACT_REQ PDU의 Payload로 QA||NA를 B에게 전송
③' A로부터 ACT_REQ PDU의 Payload로 QA||NA를 수신
④ 수신자 B : 난수값 Nonce NB를 생성
⑤ 수신자 B : 정수값 QB를 8자리 배열로 변환
⑥ 수신자 B → 송신자 A
ACT_RES PDU로 QB||NB 를 A에게 송신
⑥' 송신자 A : B로부터 ACT_RES PDU로 QB'||NB' 수신
⑦ 송신자 A : QB로부터 EC 포인트 Q_B 추출
⑦' 수신자 B : QA로부터 EC 포인트 Q_A 추출
⑧ 송신자 A : Q_B이 타원 곡선에 유효한 키인지 ISO/IEC 15946-1의 표준에 따라 검증
IEEE 1363 ECSVDP-DH에 정의된 Diffie-Hellman primitive를 통해 z 값 생성
z를 8bit string(octet string) Z로 변환
⑧' 수신자 B
Q_A이 타원 곡선에 유효한 키인지 ISO/IEC 15946-1의 표준에 따라 확인
IEEE 1363 ECSVDP-DH에 정의된 Diffie-Hellman primitive를 사용하여 z값 생성
z를 8bit string(octet string) Z로 변환

키 확인(Key Confirmation) 과정
⑨ 송신자 A → 수신자 B
키 확인 과정을 위해 키 확인 태그를 계산하여 B에게 전송
$MK_{SSE}=KDF\text{-}SSE(NA,NB,Z,ID_A,ID_B)$
$=KDF(KDF(NA||NB,Z),Z||ID_A,ID_B||(01))$
$KDF(K,S)=AES\text{-}XCBC\text{-}PRF\text{-}128_K(S)$
$MacTagA=MAC\text{-}KC(MK,(03),ID_A,ID_B,QA,QB)$
⑨' 수신자 B
A로부터 수신한 MacTagA를 MAC-KC-VER를 통해 검증
$MK_{SSE}=KDF\text{-}SSE(NA,NB,Z,ID_A,ID_B)$
$MAC\text{-}KC\text{-}VER(MK,(03),ID_A,ID_B,QA,QB,MacTagA)$
⑩ 수신자 B → 송신자 A
키 확인을 위해 키 확인 태그를 계산하여 A에게 전송
$MacTagB=MAC\text{-}KC(MK,(02),ID_B,ID_A,QB,QA)$
⑩' 송신자 A
B로부터 수신한 MacTagB를 MAC-KC-VER를 통해 검증
$MAC\text{-}KC\text{-}VER(MK,(02),ID_B,ID_A,QB,QA,MacTagB)$

3.2.3 SCH 과정

SSE 과정에서 키 일치 및 확인을 성공적으로 수행되면 NFC 디바이스는 데이터의 기밀성과 무결성을 지원하기 위한 기밀성 키(KE), 무결성 키(KI)를 생성한다.

$\{MK_{SCH},KE_{SCH},KI_{SCH}\}=KDF\text{-}SCH(NA,NB,Z,ID_A,ID_B)$
$MK_{SCH}=KDF(KDF(NA||NB,Z),NA||NB||ID_A||ID_B||(01))$
$KE_{SCH}=KDF(KDF(NA||NB,Z),MK_{SCH}||NA||NB||ID_A||ID_B||(02))$
$KI_{SCH}=KDF(KDF(NA||NB,Z),KE_{SCH}||NA||NB||ID_A||ID_B||(03))$
$KDF(K,S)=AES\text{-}XCBC\text{-}PRF\text{-}128_K(S)$

생성된 기밀성 키(KE), 무결성 키(KI)를 가지고 NFC 디바이스간의 데이터를 AES-CTR 모드를 이용한 암복호화 및 AES-CBC 모드를 이용한 무결성 체크를 수행한다.

데이터 기밀성을 지원하기 위해 AES-CTR 모드의 초기벡터(IV Initial Vector)를 다음과 같이 정의한다.

$IV = MAC\text{-}IV(MK_{SCH},KI,NA,NB)$
$= AES\text{-}XCBC\text{-}PRF\text{-}128MK_{SCH}(KI||NA||NB||(04))$
$ENC_{KE}(DATA)=AES128\text{-}CTR_{KE}(DATA)$

데이터의 무결성 체크는 다음과 같다.

$MAC=AES\text{-}XCBC\text{-}MAC\text{-}96_{KI}(SN||DataLen||ENC_{KE}(DATA))$

SN(Sequence Number)은 데이터 송수신할 때 카운트를 체크함으로써 데이터 재생공격을 방지한다.

DataLen은 무결성을 체크할 데이터 길이를 나타낸다.

3.2.4 NFC-SEC 프리미티브(Primitive)

표 3은 NFC 디바이스에서 보안 서비스를 제공하기 위한 암호학적 함수들이다.

표 3. NFC-SEC 암호함수

보안 서비스	SSE(Shared Secret Service) SCH(Secure Channel Service)
키 일치	ECDH P-192
KDF	AES-XCBC-PRF-128
키 확인	AES-XCBC-MAC-96
데이터 기밀성	AES128-CTR IV init:AES-XCBC-PRF-128
데이터 무결성	AES-XCBC-MAC-96
재생공격 방지	SN(Sequence Number)

Ⅳ. NFC 보안 안전성 분석

NFC 보안 기술은 유사한 RFID 보안 기술과 비교하여 매우 강한 보안 서비스를 제공하고 있다. 이러한 강력한 보안 서비스 지원은 NFC 디바이스가 RFID와 같이 단방향의 태그 정보를 읽는 정보 수집의 목적보다는 양방향 통신이 가능한 근거리 무선 통신 기술로서 사용자 중심의 보다 안전하고 편리한 응용 서비스를 제공가능하기 때문이다. 특히, 소액결제 서비스 및 티켓팅과 같은 금융에 관련된 서비스가 가능하기 때문에 그에 적합한 강력한 보안 서비스를 제공하고 있다.

4.1 키 일치 및 확인

NFC 보안 프로토콜은 NFC 디바이스가 가지고 있는 공개키와 개인키를 기반으로 타원곡선암호알고리즘을 통해 키 일치 및 확인을 수행한다. 타 무선 네트워크에서 정의하고 있는 대칭키 공유 방식의 인증 및 키 일치 과정과는 차별된다. NFC 통신은 비밀키를 서로 공유하고 있는 디바이스들만 연결 가능한 서비스가 아니라 언제 어디서든 사용자가 연결을 원하는 NFC 디바이스와의 서비스가 가능해야 하기 때문에 공개키 기반의 키 일치 과정이 정의된다. 예를 들어, 스마트 포스터 서비스와 같은 사전의 비밀키 공유가 어려운 대상과의 연결이 요구 가능해야 한다.

키 확립을 체크하기 위해 타원곡선을 통해 생성된 비밀값을 기반으로 AES-XCBC-MAC-96 함수를 적용한다. 특히, 데이터의 기밀성 및 무결성을 제공하기 위해 기밀성 키(KE)와 무결성 키(KI)를 생성한다.

4.2 데이터 기밀성 및 무결성 제공

NFC 디바이스간에 키 일치 및 확립이 성공적으로 수행된 후에 통신되는 데이터를 보호하기 위해 AES-CTR 모드와 AES-CBC 모드를 적용한다.

데이터 기밀성 제공을 위해 AES-CTR 모드를 사용할 때 초기 벡터값의 추측을 어렵게 하기 위해 AES-XCBC-PRF-128 함수를 사용한다.

또한, 키의 상호 연결된 키 유도 과정을 요구한다. MK_{SCH} 키로부터 기밀성 키(KE)를 생성하고, 기밀성 키(KE)로부터 무결성 키(KI)를 생성한다.

데이터의 재생 공격 방지를 위해 SN(Sequence Number)를 체크하는데 SN는 최대 2^{24}-1까지 체크할 수 있는 충분한 길이를 가지고 있으므로 SN 값 추측을 통한 공격이 어렵다.

4.3 DoS 공격 및 중간자 공격 보호

NFC 물리적인 특성인 사용자 중심의 Proximity 통신을 지원하기 때문에 DoS 공격 및 중간자 공격(Man-in-the-Middle Attack)이 물리적 차원에서 어렵다.

4.4 UICC 카드에서의 NFC 보안 적용

NFC 컨트롤러는 신호의 변환 제어 및 근접통신(Proximity) 방식의 데이터 전송뿐만 아니라 안전한 스마트 카드 칩(Secure Smart Card Chip)을 포함한다. 통합 서킷(Integrated Circuit)은 태그 에뮬레이션 모드(Tag Emulation Operating Mode)에서의 Secure Element(SE) 역할을 한다. SE는 SWP(Single-Wired Protocol)로 근접처리를 위해 NFC 컨트롤러(controller)와 연결된다.

예를 들어, external 모드에서 구매 후 돈을 지불할 경우 호스트 컨트롤러는 SE와 데이터를 교환하여 결제 서비스를 지원한다. 반면 Internal 모드에서는 OTA(Over the Air)서비스로 SE에 충전 서비스가 가능하다. 이와 같이 SE는 지불 자산의 보호 및 응용 프로그램의 실행을 위해 안전 공간으로서 역할을 수행되어야 한다. 특히, 지불 응용 서비스를 사용할 경우 SE는 인증 과정 및 지불 서비스에 관련된 보안 메커니즘에 대한 저장 및 실행이 요구된다.

모바일 디바이스에 통합된 NFC 구조[10]인 그림 3과 더불어 NFC 기능을 적용한 차세대 스마트카드에서의 서비스 모드인 카드 에뮬레이션 모드 서비스에도 SE 역할을 수행할 수 있는 대안 보안 장치로서 UICC 카드를 제안할 수 있다.

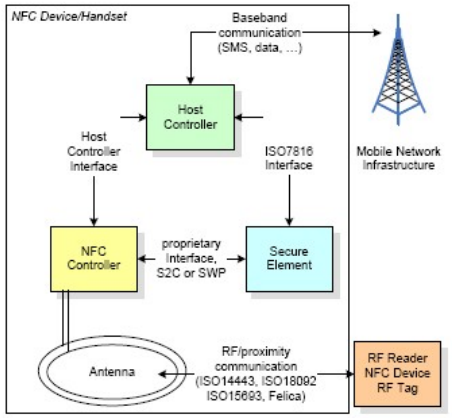


그림 3. 모바일 디바이스에 통합된 NFC 구조

4.4.1 SE(Secure Element) 대안

SE 역할을 수행할 수 있는 다양한 장치들이 장단점을 가지고 정의되고 있다. 하지만, 제안되고 있는 SE 장치들 중에 디바이스에 탈부착 가능, 보안, 재사용, 표준화 과정 단계로 분류하면 그림 4와 같이 4개의 대안책을 고려할 수 있다[12].

베이스밴드 프로세서는 이동통신 단말에서의 연결성 처리 및 응용 프로그램 운영을 관리하는 중요한 요소이다. SE 기능을 제공하기 위해 베이스밴드 프로세스를 이용하면 별도의 요소를 추가할 필요는 없지만 단말의 도난, 손실, 교환이 발생할 경우 문제가 된다. 또한 NFC 컨트롤러와 베이스밴드 프로세스간의 기본 프로토콜 정의에 대한 표준화가 진행되고 있지 않다.

임베디드 하드웨어 장치는 제조과정에서 사용자의 개인화 과정이 요구되어야 한다. 금융서비스를 위해 은행과 이동통신 사업자(Mobile Network Operator MNO)가 SE 공유를 지양하고자 할 경우 독립적인 방안으로 적합하다. 하지만, 대량 생산과정에서 개인화 과정을 거쳐야 하기 때문에 단말의 가격 상승의 요인이 될 수 있다. 또한 탈부착이 가능하지 않기 때문에 단말을 교체할 경우 재사용이 불가능하다.

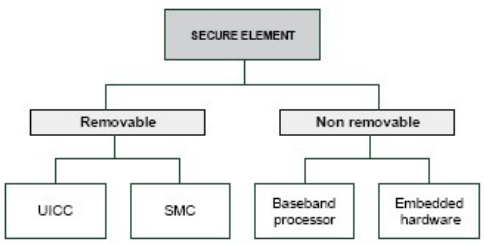


그림 4. Secure Element 대안들

SMC(Secure Memory Card)는 메모리, 임베디드 스마트카드(Embedded SmartCard Element), 스마트카드 컨트롤러(SmartCard Controller)로 구성되어 스마트카드와 같은 상위 레벨의 보안을 제공한다. 탈부착이 가능하고 대용량의 메모리를 제공 가능하기 때문에 수많은 애플리케이션이 탑재 가능하다. 또한, 단말기를 교체하여도 재사용이 가능하다. 하지만, NFC 컨트롤러와의 통신에 대한 표준화 작업이 미비하다.

반면, UICC(Universal Integrated Circuit Card)는 단말과의 탈부착이 가능하고 NFC 통신 뿐만 아니라 3G, WiBro와 같은 광대역 네트워크 서비스와 연동이 가능하다. 또한, 지불 서비스, 고객관리 서비스, 티켓팅, 전자 여권과 같은 다량의 애플리케이션 탑재가 가능하고 상위 레벨의 보안을 제공한다. 표준화 과정에서도 UICC와 CLF(Contactless Frontend)간의 데이터 링크와 물리계층의 표준 프로토콜로 SWP(Single Wire Protocol)을 정의하고 있다.

SE 대안책들에 대한 평가로 표 4와 같이 NFC 보안 서비스 및 다양한 응용 서비스에 대한 안전성을 제공하기 위해 현재 단계에서는 UICC 카드가 가장 적합하다.

표 4. SE 대안책 평가

	보안	재사용성	표준화	총합
Baseband Processor	1	-	-	1
Embedded HW	2	-	1	3
SMC	1	2	1	4
UICC	2	1	2	5

4.4.2 UICC에서의 NFC 보안 적용 및 효과성

그림 5는 UICC에 NFC 보안 메커니즘을 적용한 구조도이다. (1) NFC 단말에 UICC를 SE 기능으로 적용한다면 안전한 보안 서비스 기반의 지불 서비스가 가능하고 또한 3G 이동통신 서비스도 가능하다. (2) NFC 보안 메커니즘을 UICC 카드 애플리케이션에 탑재 가능하다. UICC는 SWP을 통해 NFC 컨트롤러와 통신한다. (3) 또한, NFC의 주요 서비스이면서 안전한 보안서비스를 제공해야 하는 지불 애플리케이션을 지원한다.

이는 사용자 중심에서의 근접거리(Proximity) 통신을 주축으로 하는 오프라인 형태의 서비스와 3G 이동통신의 광대역망 서비스와도 연동이 가능해짐에 따라 사용자 중심의 편이하면서 안전한 다양한 서비스 모

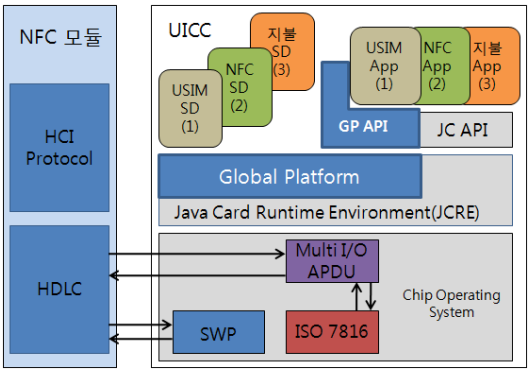


그림 5. NFC와 UICC간의 보안 연동 구조

델이 가능해진다.

HCI 프로토콜, HDLC(High Data Link Control), SWP 프로토콜은 각각 네트워크 계층, 링크 계층, 물리 계층의 역할을 수행한다.

현재 UICC 카드 주체는 대부분 이동통신 사업자인 MNO(Mobile Network Operator)를 중심으로 개발 및 보급화 되었다. MNO로부터 NFC 보안 서비스 및 지불 서비스와 같은 응용 서비스 애플리케이션 탑재를 위해[9] UICC에서의 공간 할당 및 애플리케이션으로 접근할 수 있는 SD(Security Domain)의 접근키를 부여받는다. SD 키에 의해 각 애플리케이션의 독립성을 지원한다. 또한, JVM(Java Virtual Machine)이 제공하는 소프트웨어 방화벽에 의해 (1)(2)(3)의 기능들은 서로 보호 될 것이다. 반면에 (1)(2)(3)간의 정보 공유가 필요할 경우 SIO(Shared Interface Objects) 기능을 사용한다.

자바카드 표준 2.2는 128비트 키 사이즈를 지원하는 AES(Advanced Encryption Standard) 및 타원곡선 암호 알고리즘으로 ECC-related crypto 알고리즘을 지원하고 있다[3]. 결과적으로, UICC 카드에 NFC 보안 메커니즘의 구현이 가능하다.

성능 측면을 고려하면 UICC 카드에서의 SSH 과정과 SCH 과정에서 AES기반의 CBC, CTR 모드 운용에 대한 수치는 식 (1)과 (2)와 같다.

- SSH 모드에서 KDF 함수 생성 및 MAC 계산을 위한 AES-CBC 모드

$$5*KDF\ 함수 + 2*MAC \quad (1)$$

- SCH 모드에서 키 생성 및 데이터 기밀성, 무결성 제공을 위한 AES 운영

$$1*IV+MAX_{AES}\{16*ENC+16*MAC\}*n\}+\alpha \quad (2)$$

KDF 함수 생성 및 데이터의 무결성, 기밀성을 제공하기 위해 AES 알고리즘 기반의 CBC, CTR 모드를 작동할 시에 NFC 데이터 길이가 2~255 octets[5]로서 한 섹션 당 최대 (2)와 같이 최대 AES 알고리즘을 작동한다. 이 수치는 UICC 기반에서도 빠른 성능을 기대 할 수 있다.

V. 결 론

NFC 기술은 근접 통신(Proximity) 기술로서 기존의 단방향 태그 인식 서비스를 지원하는 RFID 기술과는 차별적으로 보다 복잡하고 상호 연결 통신을 지원한다.

본 논문은 NFC 보안 기술에 대해 분석하고 SE 대안으로서 UICC 카드에 적용할 수 있는 가능성 및 효과성에 대해 연구한다. 그 결과 NFC 기술을 위한 UICC 카드 적용은 UICC 카드 제조사, 이동통신 사업자(MNO), 은행과 같은 서비스 제공자, 그리고 사용자들 모두 만족할 수 있는 가능성을 제시할 수 있다. 다양한 서비스의 가능성으로 UICC 카드의 다양성 제공 및 통신 서비스를 위한 UICC 카드를 활용함으로써 금융 서비스를 위한 UICC 카드 제작의 최소화, UICC 카드를 통한 NFC 기술과 이동통신망의 연동으로 온오프라인의 원활한 제공은 MNO의 이익 혜택 및 사용자 중심의 서비스 제공 시나리오가 가능해질 것이다.

참 고 문 헌

〔1〕 나준채, “차세대 USIM 기술”, *TTA Journal*, No.116 표준기술동향, 4, 2008.

〔2〕 전재우, 임선희, 윤승환, 이옥연, 진승헌, 김수형, “모바일 전자ID지갑 운용을 위한 NFC 기술 분석”, *한국정보처리학회 추계학술대회*, pp.619-620, 2009.

〔3〕 “Java card platform specification 2.2.1”, *Sun Microsystems*, Inc, 4150 Network Circle Santa Clara, CA 95054, Tech. Rep., Oct 2003.

〔4〕 Sun Microsystems Inc., Java Card 3 Platform White Paper, 2008.

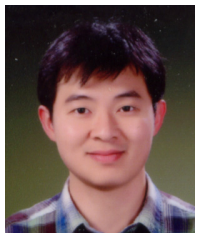
〔5〕 ECMA International: “ECMA-340 Near Field Communication Interface and Protocol (NFCIP-1),” Dec, 2004.

〔6〕 ECMA International: "ECMA-385 NFC-SEC NFCIP-1 Security Services and Protocol," 2008.
〔7〕 ECMA International: "ECMA-386_NFC-SEC-01 NFC-SEC Cryptography Standard using ECDH and AES," Dec, 2008.
〔8〕 M. PASQUET, J. REYNAUD, C. ROSENBERGER, "Secure Payment with NFC Mobile Phone in the SmartTouch Project", *IEEE,* The 2008 International Symposium on Collaborative Technologies and System.
〔9〕 G. Madlmayr, J. Langer, "Managing an NFC Ecosystem", *IEEE Computer Society*, 7th International Conference on Mobile Business, 2008.
〔10〕 G. Madlmayr, J. Langer, C. Kantner, J. Scharinger, "NFC Devices: Security and Privacy", *IEEE Computer Society*, 3th International Conference on Availability, Reliability and Security, 2008.
〔11〕 Lahtela, A., Hassinen, M., Jylha, V., "RFID and NFC in healthcare: Safety of hospitals medication care" 2008.
〔12〕 M. Reveilhac, M. Pasquet, "Promising Secure Element Alternatives for NFC Technology", I*EEE Computer Society*, First International Workshop on Near Field Communications, 2009.

임 선 희 (Sun-Hee Lim) 정회원

1999년 2월 고려대학교 컴퓨터학과 학사
2005년 2월 고려대학교 정보보호대학원 석사
2010년 8월 고려대학교 정보보호대학원 박사
2010년 9월~현재 한국전자통신연구원 선임연구원
<관심분야> 무선이동통신보안, 통합보안제어

전 재 우 (Jae-woo Jeon) 정회원



2005년 2월 육군사관학교 전산학과
2009년 3월~~현재 고려대학교 정보경영공학 전문대학원 석사과정
<관심분야> 무선이동통신보안

정 임 진 (Jung, Imjin) 준회원

2007년 8월 국민대학교 수학과 학사
2009년 3월~~현재 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 무선, 스마트카드

이 옥 연 (Okyeon Yi) 정회원

1988년 2월 고려대학교 수학과
1990년 2월 고려대학교 대학원 수학과 석사
1996년 8월 Univ. of Kentuchy 수학과 박사
1999년 7월~2001년 8월 한국전자통신연구원 팀장
2001년 9월~현재 국민대학교 수학과 교수
<관심분야> 무선이동통신보안, 암호알고리즘