# NFC 결제 서비스 환경에서 결제정보보호를 위한 Signature RTD 기반 거래 인증 기법+

박성욱*, 이임영*
*순천향대학교 컴퓨터소프트웨어공학과
e-mail : swpark@sch.ac.kr, imylee@sch.ac.kr

# Transaction Authentication Scheme based on Signature RTD for Payment Information Protection in NFC Payment Service Environments

Sung-Wook Park*, Im-Yeong Lee*
*Dept of Computer Software Engineering, Soonchunhyang University

요 약

최근 NFC를 이용한 모바일 결제 서비스가 국내·외에서 널리 주목받음에 따라 모바일 결제 시장이 더욱 활성화 될 것으로 전망되고 있다. 이에 따라 지식경제부 기술표준원에서는 2012년 3월 모바일 지급결제를 위한 표준으로 KS X 6928을 제정하였으며, 관련 학계 및 업체들은 안전하고 효율적인 결제 서비스 환경을 위한 다양한 연구를 진행하고 있다. 본 연구에서는 기존 모바일 지급결제 표준이 갖는 문제점을 제시하고 이를 해결하기 위해 기존에 제공되는 표준 기술과 NFC의 Signature RTD를 활용하여 안전한 거래 인증 기법을 제안한다.

## 1. 서론

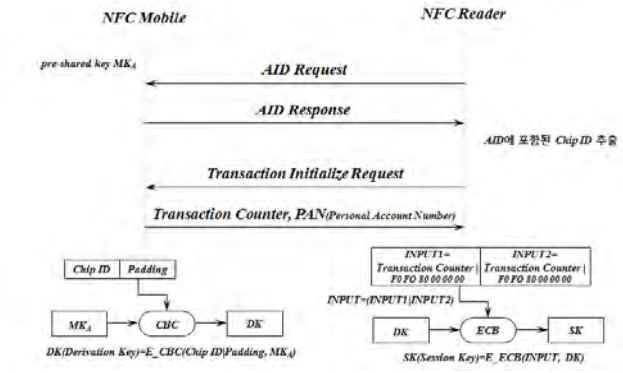
NFC(Near Field Communication)는 13.56MHz대역의 Short range high frequency를 이용한 전자태그의 일종으로 최근 모바일과 결합된 다양한 비즈니스 모델로 인해 관련 시장을 확대시키는 추진력을 불러일으키고 있다. NFC모바일은 모바일 쿠폰 서비스, 결제 서비스, 출입통제 서비스, 스마트 포스터 등 다양한 응용 서비스가 가능한데 특히, NFC와 모바일을 이용한 결제서비스가 관련 시장에서 각광받고 있다. NFC 서비스 활용의 대표 주자인 Google사에서는 NFC를 이용한 "Google Wallet"이라는 서비스를 이미 발표한바 있으며, 국내에서도 다양한 전자 지갑 앱 서비스를 출시하며 서비스 활성화에 노력하고 있다. 그러나 이와 같은 NFC 서비스 활성화 동향을 쫓기 바쁜 국내 업체들은 검증되지 않은 다양한 서비스를 내놓으며 서비스 활성화에만 열을 올리고 있으며 이는 NFC 기반 결제 서비스 사용의 증가에 따른 다양한 보안상 침해요소에 대해 대처하기 힘들 것으로 예상된다. 이에 따라 지식경제부 기술표준원에서는 2012년 3월 모바일 지급결제를 위한 표준으로 KS X 6928을 제정한바 있다[1,2,3]. 그러나 해당 표준 기술을 통해 현재까지도 발생하고 있는 보안상의 문제점을 원천적으로 해결하는 것이 어렵다. 한국인터넷진흥원에서 발표한 "NFC 개인정보보호 대책 최종보고서"에 통해 NFC 모바일 신용카드 결제 단계에서 결제에 사용되는 정보가 네트워크를 통해 상점과 VAN사, 카드사에 각각 수집 및 저장됨을 알 수 있다. 이러한 방식은 상점에 있는 POS 단말기를 해킹할 경우 개인 금융정보를 빼내는 것이 가능하며, 실제 사례로 앞서 언급한 공격 방식으로 10만 건에 달하는 신용카드 정보가 유출되었다[4].

본 연구에서는 기존 모바일 지급결제 표준 방식을 변형하지 않고 NFC 표준에서 제공하는 Signature RTD(Record Type Definition)를 이용하여 기존 결제정보가 다른 개체에 의해 노출되어도 실제 거래에는 사용이 불가능한 거래 인증 기법을 제안한다. 2장에서는 모바일 지급결제 표준과 관련 연구에 대해 분석한다. 3장에서는 기존연구를 기반으로 NFC 기반 모바일 결제에 대한 보안 요구사항에 대하여 분석한다. 4장에서는 보안요구사항을 만족하는 제안방식을 기술하며, 5장에서는 보안요구사항에 의한 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

## 2. 관련연구

본 장에서는 지식경제부 기술표준원에서 제정한 지급결제 표준에 대해 설명하고 기존에 제안된 NFC 지급 결제 관련 연구와 Signature RTD에 대해 설명한다.

+ 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A1A2012940)




(그림 1) 대면 거래 세션키 생성 과정(KS X 6928)

2.1 KS X 6928 - 모바일 지급결제 표준

KS X 6928는 통신과 금융이 융합된 모바일 지급결제 시장이 급성장함에 따라 사업자 간의 주도권 경쟁이 가열되고 있는 상황에서 중복투자를 방지하고 향상된 기술개발을 유도하기 위해 지식경제부 기술표준원에 의해 제정된 모바일 지급결제표준이다.

모바일 결제 서비스의 상호운영성을 확보하기 위해 기본적인 플랫폼을 국가표준으로 제시하며, 이해관계별로 다양한 요소기술을 적용해 신규 비즈니스 모델을 창출하는 방식으로 3개 분야를 선정해 중점 선행표준화가 추진되었다[1,2,3]. KS X 6928은 총 3부로 구성되어 있으며, 1부에서는 모바일 카드 발급 단계와 데이터 관리를 위한 요건을 규정하고 있다. 또한, 2세부와 3세부에서는 대면 거래와 비대면 거래 결제 절차와 요구사항을 각각 규정하고 있다. 본 연구에서 사용되는 대면거래 요구사항을 살펴보면 KS X 1S0/IEC 14443과 ISO/IEC 18092, ISO/IEC 21481의 호환을 모두 지원하고 있어 NFC의 운용모드인 Peer-to-Peer 모드와 NFC-SEC에서 제공하는 보안서비스인 SSE(Shared Secret Service)와 SCH(Secure Channel Service)의 활용이 가능할 것으로 판단된다[2,5,6]. (그림 1)은 KS X 6928-2의 대면거래 의 세션키 생성 과정이다.

2.2 Signature Record Type Definition

Signature RTD(Record Type Definition)은 NFC 포럼에 의해 처음 발표되었다. Signature RTD는 NDEF(NFC Data Exchange Format) 메시지에 디지털 서명과 인증서를 추가하여 NDEF의 무결성과 신뢰성을 제공한다.

Signature Record의 페이로드 내용은 Version, Signature, Certificate Chain 세 부분으로 구성된다. Version Field는 서명이 준수하는 사양의 버전을 나타내는 단일 바이트 필드로써 현재 유효한 버전은 한 가지만이 존재한다. Signature Field는 실제 서명 또는 서명에 대한 URI(Uniform Resource Identifier) 참조 중 하나를 포함한다. Certificate Chain Field는 인증서 포맷, 인증서의 총 개수, 인증서의 목록과 URL 참조(선택적)를 포함하고 있다.

## 3. 보안요구사항

NFC 모바일 결제 환경은 결제를 위한 기본적인 보안요구사항을 만족해야하며, NFC 태그 특성 상 발생할 수 있는 보안 취약점으로부터 안전성을 제공할 수 있어야 한다. 따라서 본 논문에 보안요구사항은 다음과 같다.

• 기밀성 : 통신에 사용되는 데이터들은 민감한 결제정보를 포함하고 있어, 정당한 통신객체들만이 공유되어야 하며 통신 중간에 노출되더라도 그 데이터의 값을 유추하지 못해야 한다.
• 무결성 : 통신상에서 제공되는 데이터들은 과금과 같은 금전 거래의 근거가 되므로 통신 중간에 위조 및 변조되지 않아야 한다.
• 안전성 : 기존 NDEF 구조상에 존재하는 Signature RTD의 보안상 취약점들(Record Composition Attack, Record Hiding & Composition Attack)에 의한 위협으로부터 안전성을 제공해야 한다.

## 4. 제안 방식

이 장에서는 3장의 보안요구사항을 만족하는 NFC 결제 서비스 환경에서 결제정보보호를 위한 Signature RTD 기반 거래 인증 기법을 제안한다. 본 제안 방식에서는 별도 OTA 인증 프로토콜과 CA와 상점간의 세션키 획득 단계는 범위 외로 간주하며, 상점과 사용자 간의 세션키 확립 단계는 기존에 제공되는 KS X 6928 모바일 지급 결제 표준을 기반으로 한다. 본 제안방식은 기본적으로 인증레코드 생성단계와 검증 단계로 구성되며, 결제 흐름 상 발생하는 주문정보 전달 단계와 결제정보 전달 단계에서 인증레코드를 각각 사용한다. 본 장에서는 사용자가 상품에 대한 결제 정보를 상점에게 전달하는 단계만을 기술한다. 각 단계의 수행절차는 다음과 같다.

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

- $*$ : 각각의 개체 (U : *User*, T : *Merchant* A : *CA*)
- *User* : NFC 모바일 사용자
- *Merchant* : 상품 또는 서비스를 제공하는 상점
- *CA* : 모바일 카드를 발행하며 상점으로부터 전달받은 결제 정보를 검증하는 인증 기관
- *PI* : 결제정보(카드정보, CVC정보 등)
- *OI* : 주문정보(제품명, 가격 정보, 제품번호 등)
- *TPI* : 상점에게 가시적으로 표시되는 결제정보
- *TOI* : 사용자에게 가시적으로 표시되는 주문정보
- *AID* : 모바일에 저장된 모바일 카드의 식별자
- *Chip ID* : 모바일 카드의 고유 식별자
- *TS* : 타임 스탬프
- *MK* : 카드사 마스터 비밀키

- $SK$ : KS X 6928 표준에 의해 생성된 세션키
- $PR_*$ : Signature RTD에 정의된 *의 개인키
- $PU_*$ : Signature RTD에 정의된 *의 공개키
- $R1$ : $TPI$ 또는 $TOI$가 표시되는 임의 레코드
- $R2$ : $PI$ 또는 $OI$가 표시되는 임의 레코드
- $AR$ : $R1$과 $R2$를 이용한 인증 레코드
- $H()$ : 암호학적 해시 함수

4.2 인증 레코드 생성 단계

***Step 1***: 결제정보 검증에 필요한 데이터 레코드 $R1$과 $R2$에 대해 아래와 같은 형태의 서명을 수행한다.

$$U: AR_{TPI} = H(R1 \| H(R2))$$
$$U: AR_{Auth} = H(R2 \| H(R1))$$

***Step 2***: 생성된 서명을 각 레코드와 연관된 서명 레코드에 삽입한 후 상점이 요청 시 해당 정보를 전송한다.

$$U: AR_{TPI} = H(R1 \| H(R2)) \rightarrow Signature\ Field$$
$$U: AR_{Auth} = H(R2 \| H(R1)) \rightarrow Signature\ Field$$

***Step 3***: 이후 사용자는 결제에 필요한 정보 $M$을 생성하고, 상점간의 세션키와 사용자의 개인키를 이용하여 결제 정보를 전송한다.

$$U \rightarrow T: (TPI \ || PR_U(TPI||AR_{TPI}) \ || \ (SK(M)||PR_U(H(M)|| AR_M))$$

4.3 검증 단계

***Step 1***: 상점은 수신된 메시지로부터 $TPI$를 확인하고 사용자의 공개키 $PU_U$를 이용하여 각각의 데이터 레코드의 해당하는 서명 레코드를 복호 및 검증한다.

$$T: PU_U(PR_U(TPI||AR_{TPI})$$
$$T: TPI = ?TPI'$$
$$T: H(M) = ?H(M)'$$

***Step 2***: 상점은 각 데이터 레코드 $R1$과 $R2$의 해쉬 값 $H(R1')$과 $H(R2')$를 생성하여 아래와 같이 무결성 검사를 수행한다.

$$T: AR_{TPI} = ?AR_{TPI}' \ , \ AR_M = AR_M'$$
$$T: H(R1 \| H(R2)) = H(R1' \| H(R2'))$$
$$T: AR_{TPI} = ?H(TPI||H(SK(M))$$
$$T: H(R2 \| H(R1)) = H(R2' \| H(R1'))$$
$$T: AR_M = ?H(SK(M)||H(TPI))$$

위 과정을 통해서 각 데이터 레코드에 대한 무결성과 연관된 데이터 레코드 간의 무결성을 동시 검증하는 것이 가능하다.

## 5. 제안 방식 분석

본 제안방식은 3장에서 도출된 보안요구사항을 다음과 같이 만족한다.

• 기밀성 : 통신에 사용되는 결제정보들은 KS X 6928 지급결제 표준기반의 세션키 확립 프로토콜로 안전하게 전송되므로 통신 중간에 노출되더라도 그 데이터의 값을 유추하기 어렵다.

• 무결성 : NFC Signature RTD에 정의된 서명 기술을 사용하므로 통신 중간에 데이터의 위조 및 변조가 어렵다.

• Record Composition 공격 : 두 개의 연관레코드에 따른 서명 검증이 이루어지므로 안전성을 제공한다.

• Record Hiding 공격 : Record 값이 숨겨질 경우 초기에 생성한 해쉬 값과 일치하지 않으므로 두 개의 연관 레코드 해시 값 검증을 통해 안전성을 제공할 수 있다.

• Record Hiding & Composition 공격 : 두 방식을 연계한 공격이라도 제안된 방식은 필드를 구별하지 않고 페이로드 전체의 값을 검증하는 방식이므로 안전하다.

## 6. 결론

본 논문에서는 기존에 상점 단계에서 유출되던 개인 금융 정보를 보호하기 위한 수단으로 Signature RTD 기반 거래 인증 기법을 제안하였다. 본 방식에서는 금융 거래 시 사용되는 결제 정보에 Signature RTD 기반의 서명정보가 없을 경우 거래가 불가능하기 때문에 직접적으로 신용정보가 노출된다 하더라도 사용자는 금전적인 손해를 입을 수 없다. 또한 기존 Signature RTD의 알려진 취약점을 레코드 인증 기법을 통해 보안함으로써 더욱 안전성을 향상시켰다. 마지막으로 아직까지 알려지지 않은 다양한 보안위협을 대처하기 위한 추가적인 연구가 필요할 것으로 예상된다.

## 참고문헌

[1] 지식경제부 기술표준원, KS X 6928-1 "모바일 지급결제-모바일 신용카드, 제1부 : 일반" 2013. 3. 28.

[2] 지식경제부 기술표준원, KS X 6928-2 "모바일 지급결제-모바일 신용카드, 제2부 : 대면거래" 2013. 3. 28.

[3] 지식경제부 기술표준원, KS X 6928-3 "모바일 지급결제-모바일 신용카드, 제3부 : 비대면거래" 2013. 3. 28.

[4] 동아일보, "POS 단말기 해킹…신용카드 정보 또 '탈탈'털렸다", http://news.donga.com/East/3/all/20140411/62462956/1, 2014. 4. 11

[5] ECMA International: "ECMA-385 NFC-SEC NFCIP-1 Security Services and Protocol", 2008.

[6] ECMA International: "ECMA-386_NFC-SEC-01 NFC-SEC Cryptography Standard using ECDH and AES", Dec, 2008.