한국항행학회 논문지 제17권 제1호 2013년 2월 (JKONI 17(1): 47-55 Feb. 2013)

NFC 기반 모바일 소액 결제를 위한 MD 인증과 프라이버시 설계

Design of MD Authentication and Privacy for Mobile Micro-payment based on NFC

김용일*, 김대규**, 차병래***

Yong-Il Kim*, Dae-Gue Kim**, and Byung-Rae Cha***

요 약

본 논문에서는 전통시장 활성화를 위한 IT 측면에서의 소상인의 소액결제를 지원하기 위한 NFC 기반의 소액 결제 모델과 소액결제를 위한 인증 및 프라이버시 기술을 제안한다. 모바일 소액결제 모델은 NFC 기반의 스마트폰을 이용하여 결제의 편리성을 제공하며, 암호화 및 토큰화 기술에 의한 사용자 결제의 MD 인증과 간접 인증, 그리고 프라이버시의 기능을 설계한다.

Abstract

In this paper, we propose the micropayment model based on NFC, authentication, and privacy technique to support micro-payment in aspect of information technology to reinvigorate the traditional market. The micropayment model supports facilities of payment using smart phone based on NFC, and the encryption and tokenization support the functions of MD authentication, indirection authentication, and privacy of user's payment.

Key words : Traditional Market, Micro Payment, NFC, Token, MD(Message Digest) Authentication

I. 서 론

핸드폰의 이용이 단순한 음성통화 중심에서 데이터 통신 서비스를 거쳐 스마트폰 기반의 '생활편의' 서비스로 진화 중이다. 최근에 NFC(Near Field Communication) 기능을 탑재한 스마트 폰이 출시되면서 NFC를 이용한 다양한 응용분야가 연구 중이다. 특히, NFC 기반의 모바일 결제 서비스가 모바일 비즈니스의 핵심으로 인식되고 있다. NFC는 RFID 기술보다 보안성이 높고 데이터를 교환하기 위해 통신 대상 기기에 이용자가 직접 스마트폰을 터치해야 한다. 또한, 기존 근거리 무선 데이터 교환 기술이 '읽기' 중심이었으나 NFC는 양방향 서비스를 제공한다. 미국의 경우 이동통신 3사가 ISIS라는 모바일 전자결제 합작사를 설립하여 관련 사업을 추진 중이며, 유럽의 경우 '스마트 전자결제 서비스'를 제공하기 위해 2011년 이후 출시되는 휴대폰의 절반 이상에 NFC 기능 탑재를 유도하고 있다[1].

* 호남대학교 인터넷 콘텐츠학과(Honam Univ., Dept. of Internet Contents): yikim@honam.ac.kr
** (주)아젠텍(Ajantech): afoxkim@ajantech.com
*** 광주과학기술원(GIST.): brcha@nm.gist.ac.kr
· 제1저자 (First Author) : 김용일(Yong-Il Kim, tel: +82-62-940-5595, email : yikim@honam.ac.kr)
· 접수일자 : 2012년 11월 23일 · 심사(수정)일자 : 2012년 12월 3일 (수정일자 : 2013년 2월 23일) · 게재일자 : 2013년 2월 28일
http://dx.doi.org/10.12673/jkoni.2013.17.01.047

NFC은 13.56MHz의 HF 대역을 이용한 근거리 데이터를 교환할 수 있는 비 접촉식 무선통신 기술로 스마트폰 등에 내장되어 교통카드, 신용카드, 멤버쉽 카드, 쿠폰, 신분증 등의 역할을 대체할 수 있다. ‘NFC 기반 Mobile Smart Life 서비스’는 이용자가 자신의 휴대 단말을 인식장치(결제기 등)에 가져다 대는 것만으로 쉽고 편리하게 정보를 교환할 수 있는 서비스로 모바일 결제 서비스와 응용서비스로 구분된다. NFC의 동작은 NFC 비접촉 컨트롤러와 전자기기 응용 프로세서 간의 통신에서 출발하였으며, NFC에는 RF와 베이스밴드를 포함하는 호스트 프로세서가 내장된다. 호스트와 호스트 프로세서 간의 프로토콜 통신을 대개 펌웨어 레벨에서 구현되며, 호스트의 호환성을 위한 가상의 인터페이스 HCI가 있다. NFC 프런트엔드 부분은 휴대폰, PDA, PC 등의 프로세서와 직접적으로 통신할 수 있는 기반 갖추었으며, NFC HCI의 3가지 모드는 리더/라이터 모드, P2P 모드, 그리고 카드 에뮬레이션 모드가 존재한다[2].

ABI Research가 발표한 근거리 무선 통신(Near field Communication)시장 전망에 따르면 ’12년 약 2억 9,200만 대의 모바일 기기에 근거리 무선통신 기능이 탑재되어 출시될 예정이며, 이는 전 세계 모바일 기기 시장의 약 20%를 상회한다. 또한 Ovum[3]에서 발표된 자료에서도 ’08년 400만 대의 NFC폰 출하대수가 ’12년 약 3억 6,400만 대로 크게 증가하는 등 NFC 기술을 탑재한 단말기 시장의 성장으로 모바일 RFID 기기 및 서비스 시장 영역도 더욱 확대될 전망이다. 그림 1에서 지역별로 살펴보면 서유럽이 가장 두드러진 증가세를 보이며 높은 비중을 차지하고, 그 다음 순으로 미국&캐나다와 아시아가 높은 증가를 보였다. 또한 Juniper Research에서는 모바일 결제 시장 규모가 2010년에 1,700억 달러에서 2014년에는 6,300억 달러 수준으로 확대 및 급성장할 것을 전망하고 있으며, 모바일 금융 서비스 분야에 대한 새로운 비즈니스 모델과 표준화에 대한 연구를 수행하고 있다.

본 논문에서는 전통시장 등에서 소액 결제를 할 수 있도록 NFC를 기반으로 한 소액 결제 모듈의 MD 인증과 프라이버시에 대한 연구를 수행하였다.

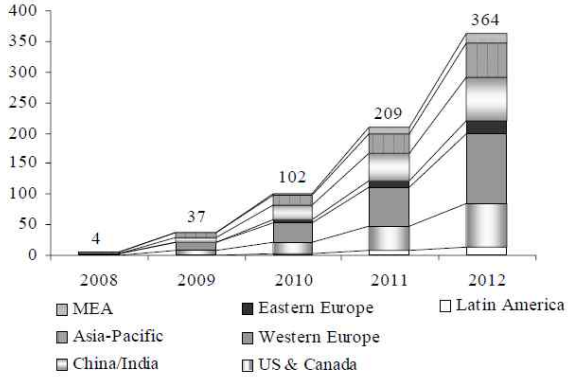

그림 1. 지역별 NFC폰 시장 전망
Fig. 1. Market prospects of regional NFC Phone

Ⅱ. 관련 연구

2-1 전자 현금지불 시스템

전자 현금지불 시스템은 수용성(Acceptability), 보장된 지불(Guaranteed payment), 무거래비용(No transaction charges), 익명성(Anonymity) 이라는 현금의 특성을 실현하는데 초점을 두고 있으며, 이와 유사한 속성을 가진 시스템으로 ECash, CAFE, NetCash, 그리고 CyberCoin 등을 살펴본다[4].

ECash는 DigiCash사가 인터넷 상에서 완전한 익명성을 가지고 사용할 수 있도록 개발한 보안 전자화폐이며, 정보, 상품에 대한 지불과 과금 서비스도 가능케 하는 온라인 소프트웨어 솔루션이다. ECash는 1995년 10월 Mark Twain 은행에서 처음 발행한 이후 인터넷 상에서 실제 화폐와 동일한 가치로 이용되고 있으며, 대칭 및 비대칭 암호화를 이용한 강력한 보안성을 제공한다. CAFE(Conditional Access for Europe)는 European Community의 ESPRIT 프로그램으로 진행되었으며, 추적 불가능한 전자화폐와 계산기가 있는 수표의 개념에 기반을 두고 있다. CAFE는 익명성이 있는 전자화폐의 모든 장점을 제공하면서 동시에 특정 금액에 대한 수표에 이용자가 서명하는 하이브리드 구조를 가지고 있다.

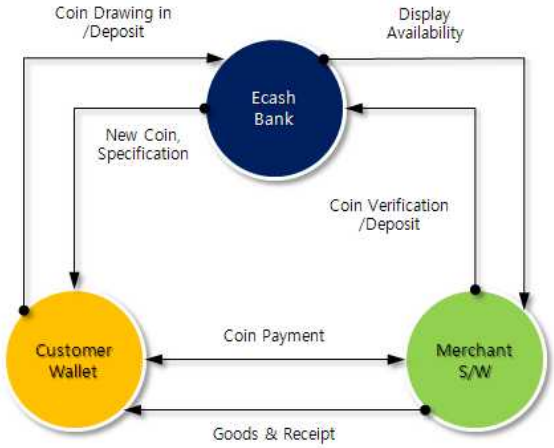

그림 2. ECash 시스템의 구성요소와 기능
Fig. 2. Components and function of ECash SystemPhone

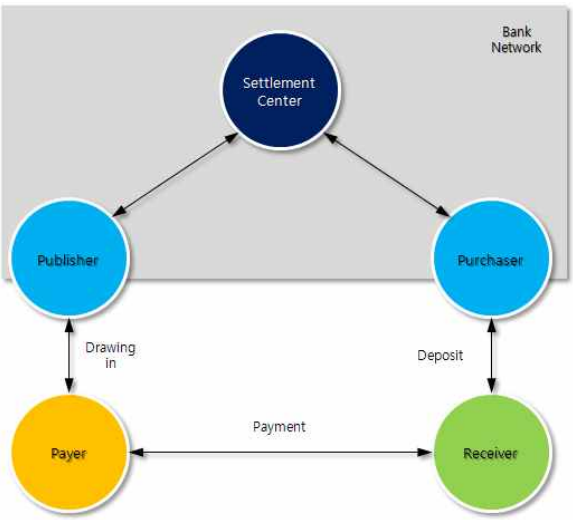

그림 3. CAFE 아키텍처
Fig. 3. Architecture of CAFE

NetCash 시스템은 온라인 전자현금 시스템으로 전자 코인을 만들고 시스템 사용자에게 이 코인을 발행하는 통화 서버로 구성된다. NetCash는 상품, 정보 또는 다른 망 서비스를 파는 데 적합한 고액지불 시스템으로 이용자는 지불을 할 수도 받을 수도 있다. CyberCoin은 신용카드로 지불하기 너무 적은 금액의 거래에 이용하도록 설계된 전자현금 시스템이다.

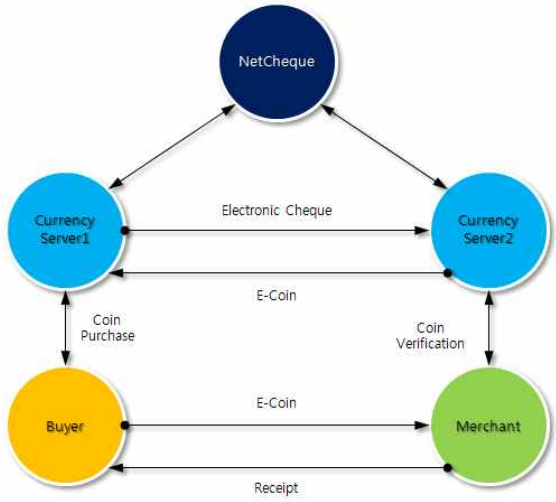

그림 4. NetCash 시스템
Fig. 4. System of NetCash

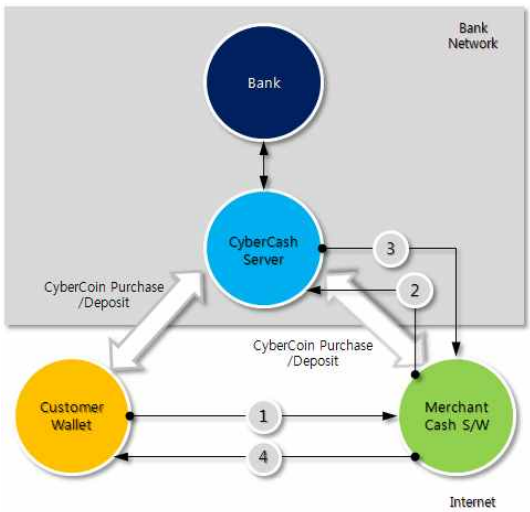

그림 5 CyberCoin에 의한 구매 절차
Fig. 5. Purchasing process by CyberCoin

2-2 소액결제 시스템

소액지불시스템은 기존의 상거래에서는 쓸 수 없었던 것으로 출현자체가 많은 새로운 비즈니스 분야를 창출하고 있으며, Millicent, SubScrip, Payword, MicroMint 등의 소액지불시스템에 대해서 간략하게 정리한다[4]. Millicent는 Digital Equipment Corporation이 1/10 센트(0.001 달러) 정도의 소액지불도 가능하도록 설계한 분산 소액지불시스템이다. Millicent 시스템은 스크립이라는 전자통화(Electronic Currency)를 이용하고 있는데, 이것은 특정 상인에게만 가치가 있는 상인 종속형 통화이다. SubScrip은 오스트레일

리아의 University of Newcastle이 인터넷 상에서 효율적인 PPV(Pay-per-View) 지불을 위해 개발한 간단한 소액지불 프로토콜이며, 이용자 인식이 필요 없는 선불식 시스템이다.

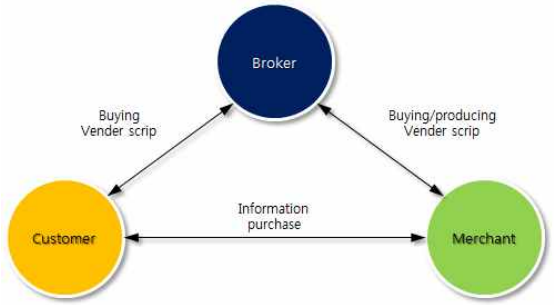

그림 6. Millicent 모형
Fig. 6. Model of Millicent

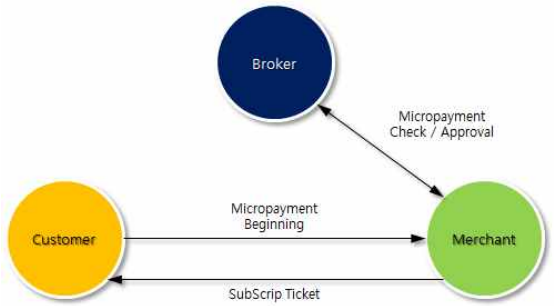

그림 7. Subscrip의 계정 설정
Fig. 7. Account setting in Subscrip

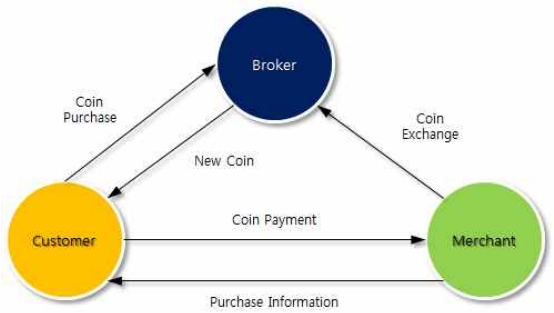

그림 8. Microminit 시스템의 구성
Fig. 8. System configuration of Microminit

PayWord는 MIT Laboratory과 이스라엘 Weizmann Institute of Science에서 개발한 크레딧-기반의 소액지불시스템이다. PayWord는 시스템 내에서 이용자 크레딧을 나타내기 위해 해쉬 값 체인을 이용하며, PayWord 체인은 특정 상인에게만 통용된다. 이용자는 그 체인을 지불하기 위해 디지털 서명을 하게 된다. 브로커는 고객이 PayWord를 생성할 수 있도록 PayWord 보증서를 발부하고, 상인으로부터 지불된 PayWord 체인을 고객의 계정으로부터 상인의 계정으로 사용한 액수를 이체시킨다. MicroMint는 PayWord를 개발하였던 Ron Rivest와 Asi Shamir의 두 번째 소액지불시스템으로 공개 키 암호화를 필요하지 않는 독특한 형식의 전자화폐에 기반을 두고 있다. MicroMint 코인은 구매시 인증을 위해 은행이나 브로커를 접촉하지 않고 어떤 상인에게도 효율적으로 이용할 수 있다. 제공되는 보안 레벨은 PayWord보다는 낮지만 다른 많은 상인과의 소액지불에 더 효과적이다.

Ⅲ. NFC 기반 소액 결제의 개념 설계

3-1 전통시장을 위한 소액결제 모델과 기능

전통시장에서 소액 결제는 소상인, 구매자, 은행 간에 이루어지며, 소액 결제 절차는 그림 9와 같이 나타낼 수 있다[5].

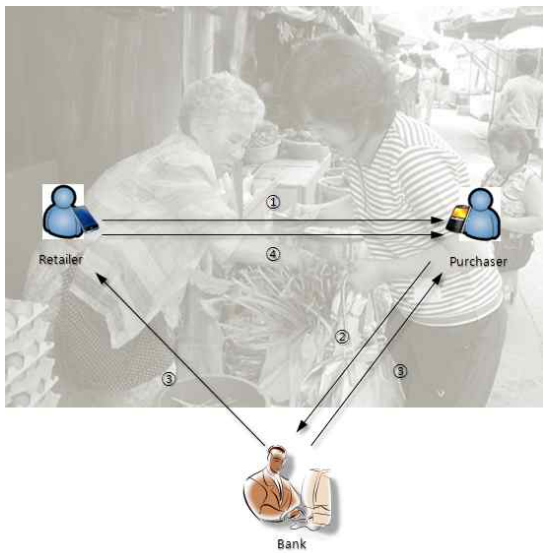

그림 9. 전통시장의 NFC 기반 소액결제 모델
Fig. 9. Micro-Payment Model based on NFC of Traditional Market

거래 절차는 그림 9의 ①에서 구매자는 소액결제를 위한 정보와 소상인의 정보를 NFC 기반으로 안드

로이드 빔(Android Beam)[6]을 통해 얻음으로써 거래를 시작하게 된다. 소액 결제를 위한 계좌 정보는 프라이버시를 제공하기 위하여 암호화와 토큰화에 의해서 소상인과 구매자의 계좌 정보를 서로 간에 알 수 없으며, 사업자 정보는 프라이버시가 필요하지 않기 때문에 공개된다. 그림 9의 ②에서 구매자는 구매자 계좌의 인증과 소상인의 계좌 정보로 구입 물품에 대한 소액 결제를 진행하게 된다. 은행은 이를 복호화 및 토큰화에 의해 계좌번호를 알아낼 수 있다. 또한 은행은 소액 결제를 위한 인증 및 간접 인증을 수행하게 된다. 그림 9의 ③에서 은행은 상인을 인증하고 구매 금액에 대한 계좌 이체를 승인하며, 동시에 구매자는 은행으로부터 계좌 이체 정보를 받게 된다. 소상인은 거래를 완료에 의한 계좌 이체 정보와 물품에 대한 비용이 소상인의 계좌로 이체된다.

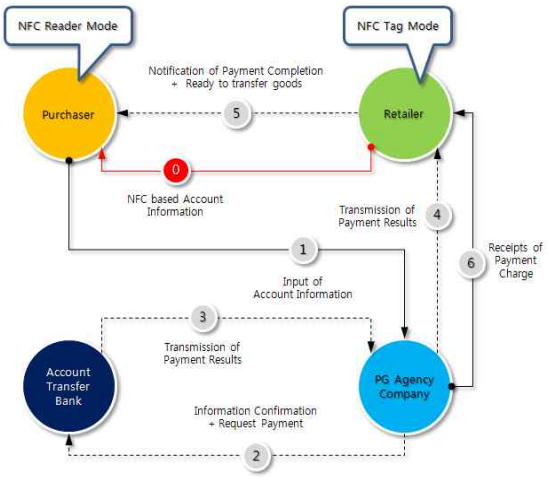

그림 10. 제안된 NFC기반의 소액결제 시스템
Fig. 10. Proposed Micro-Payment System based on NFC

그림 9의 ④에서 소상인과 구매자 간의 계약 성립에 따라 구매 물품을 구매자에게 인도하면 된다. 그림 9의 NFC 기반의 소액결제 모델에 대한 실제적인 트랜잭션의 흐름을 그림 10과 같으며, 안드로이드 NFC 기반의 소액 결제의 절차는 그림 11에 흐름도로 나타낸다.

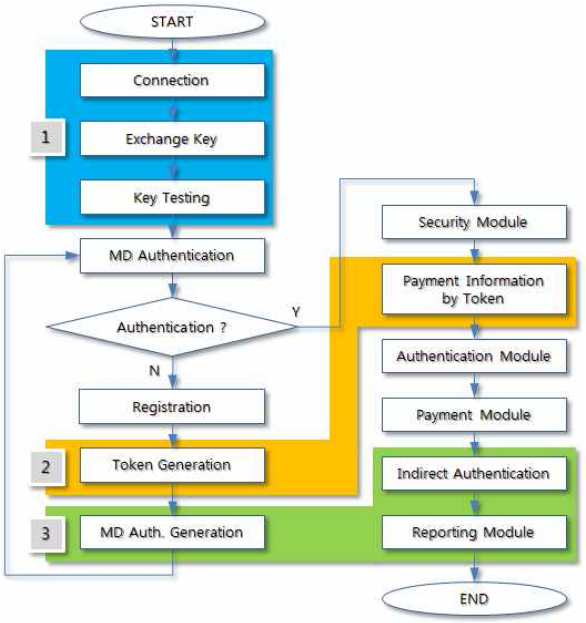

그림 11. 제안된 소액 결제 시스템의 수행 절차
Fig. 11. Processing Procedure of proposed Micro-payment system

제안된 모바일 소액 결제를 진행하기 위해서는 모바일 장치에 기본적으로 개인 정보와 결제 정보가 등록되어 있다고 가정한다. 결제를 진행하려면 보안 모듈이 적재되고, 통신 모듈에 의해서 다양한 통신 인터페이스를 제공하고, 사용자 인증과 결제 정보의 확정에 의해서 결제가 진행된다. 마지막으로 결제에 대한 모든 정보가 리포팅 되며, 이를 위한 각각의 모듈의 기능은 다음과 같다.

- 보안 모듈 - 모바일 장치의 보안 모듈은 모바일 내부의 다양한 정보에 대한 접근 제어 기능을 제공한다. 통신 모듈 호출하기 전에 필요한 정보 외의 모바일 장치 내부 데이터의 접근을 차단하며, 샌드박스 기능을 제공한다.
- 통신 모듈 - 보안 모듈이 사전에 호출되어야만 통신 모듈이 호출되는데, 3G, WI-FI, 블루투스, NFC 등의 다양한 통신을 제공하기 위한 추상화된 모델을 제공한다.
- 인증 모듈 - 특히 전자결제의 경우와 데이터의 전송에 대해서는 사용자의 인증 절차를 거치게 되며, 인증 절차가 완료가 되어야만 결제 및 데이터의 전송이 승인된다.
- 결제 모듈 - 결제 모듈이 호출되기 위해서는 보안 모듈과 인증 모듈에 대한 플래그 정보를 확인한

후에 결제가 진행되게 된다. 플래그 모듈에 보안 과 인증 모듈의 체크 정보가 없으면 결제가 진행되지 않는다.

• 리포팅 모듈 - 결제와 데이터의 전송에 대한 모든 정보는 ObjectIds에 의한 간접인증 정보가 보안 정보의 저장소에 저장된다. 결제 및 데이터 전송 정보를 상대방에게도 전송하고 상대편의 ObjectIds를 요구하고 저장한다.

3-2 소액결제 프로토콜 설계

NFC기반의 소액결제를 위한 프로토콜의 기능들은 다음의 그림 12, 그림 13, 그리고 그림 14에 간략하게 나타낸다. 소액결제를 위한 구성 요소로는 그림 12와 같이 PG Server와 Client 1과 Client 2 로 이루어지며, 각각의 구성요소의 기능은 암/복호화 기능, DB, 네트워크, 난수, 그리고 MD(Message Digest) 기능을 갖게 된다.

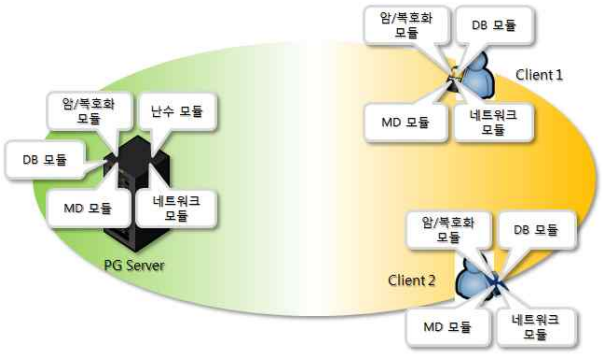

그림 12. 구성 요소와 기능
Fig. 12. Components and features

그림 13은 Client 1과 PG Server의 초기화 및 공개 키 교환을 나타낸 것이다. Client 1은 PG Server에 접속하면, Client 1과 PG Server는 서로의 공개 키를 교환한다. 그리고 Client 1과 PG Server는 교환된 서로의 공개 키를 테스트한다. 테스트가 실패하면 성공할 때까지 2번과 3번 절차를 반복하여 수행한다. 테스트가 3~5회 연속적으로 실패하면 연결을 초기화하며, 키 교환과 테스트를 재 수행한다.

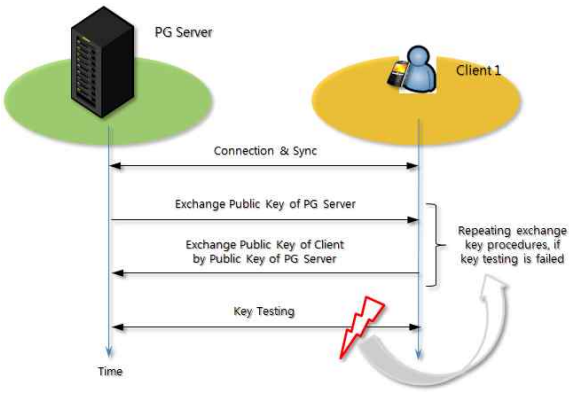

그림 13. 소액결제 프로토콜의 기능 1
Fig. 13. Protocol function of Micro-Payment 1

그림 14는 Client 1과 PG Server의 대칭 키 교환을 나타낸다. Client 1과 PG Server는 서로의 공개 키 교환이 완료된 상태에서 PG Server는 대칭 키를 발급하여 Client의 공개 키로 암호화하여 Client에게 전송한다. Client 1은 암호화된 대칭 키를 Client 1의 개인 키로 복호화를 수행한다. 그리고 복화화된 대칭 키를 이용하여 모든 전송 메시지를 암호화 및 복호화를 수행한다.

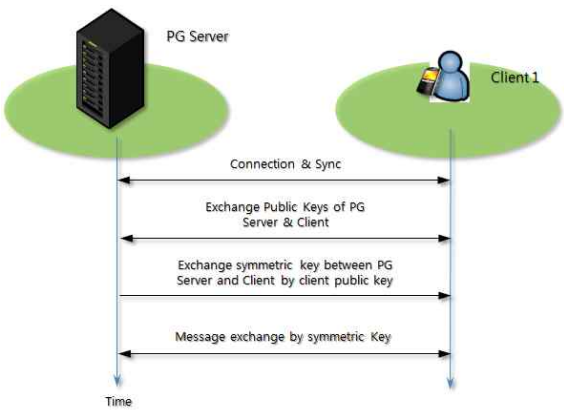

그림 14. 소액결제 프로토콜의 기능 2
Fig. 14. Protocol function of Micro-Payment 2

3-3 인증 기술

NFC 기반의 전자결제를 위한 보안 인증 기능을 설계하며, 인증은 크게 MD(Message Digest) 인증과 간접 인증에 의한 결제의 안전성과 부인방지 기능을 제공할 수 있다. MD 인증은 일반적인 인증이며, 빠른 전자 결제를 제공하기 위한 인증 방법을 제안한다. 간접 인증은 직접 인증을 증명할 수 있는 Flag 정

보를 제공한다.

(1) MD 인증

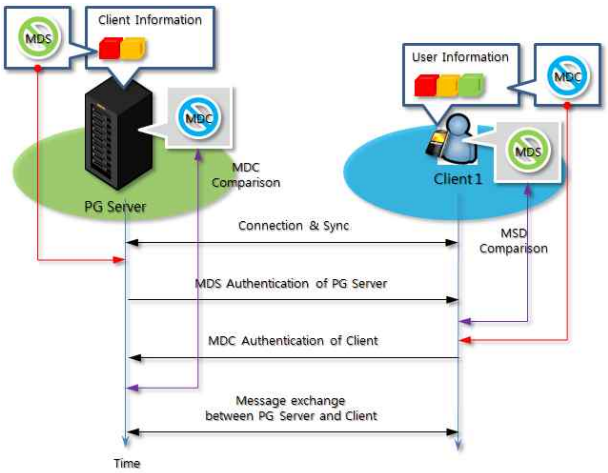

그림 15. MD 인증의 절차
Fig. 15. Authentication process of MD

Client 1과 PG Server의 MD 인증을 위해서는 임의의 비트 크기의 ID, Realm, Password 정보를 이용하여 MD를 생성한다. 그림 15는 생성된 MD를 이용하여 인증을 수행하는 과정을 나타내었다. PG Server와 Client 1 간의 모든 인증은 MD 정보를 이용하여 단순하게 처리한다. PG Server는 Client 1의 MDS = Hash(ID:Realm)을 산출 및 비교하여 Client를 인증한다. 그리고 Client 1은 Server의 MDC = Hash(ID:Realm:Hash(Password))을 산출 및 비교하여 Server를 인증한다.

(2) 간접 인증

직접 인증은 사용자 정보와 결제 정보, 핸드폰 정보에 의해서 일반적인 결제를 위한 인증 절차를 의미한다. 간접 인증을 위해서는 결제 모듈에서 ObjectIds와 같은 특별한 구조체에 의해서 각 상태에 대한 정보를 제공하는 것이다. MongoDB는 기본 데이터 유형으로 12바이트 크기의 ObjectIds를 제공하며, 이러한 자료형에 의해서 비구조적 DB의 Primary key 역할을 수행하게 된다. NFC 기반 전자 결제의 간접 인증을 위한 ObjectIds의 구조는 그림 16과 같으며, Machine 필드가 4바이트로 확장되고, Flag라는 1바이트의 필드가 추가된 14 바이트로 구성된다. 추가된 Flag 필드에 의해서 결제를 위한 인증 절차의 모든 상황 및 절차에 대한 점검이 가능하게 된다.

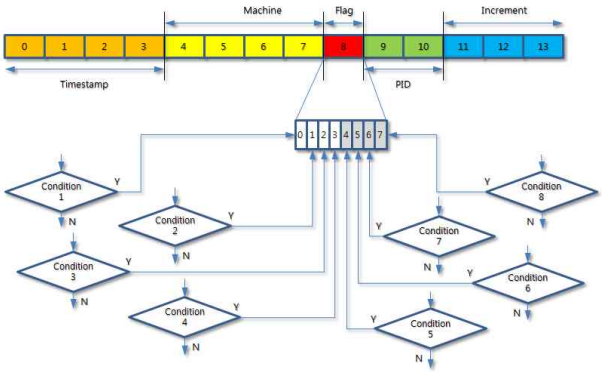

그림 16. 간접 인증을 위한 ObjectIds의 구조
Fig. 16. Structure of ObjectIds for indirection authentication

간접 인증을 위한 ObjectIds 클래스는 전자 결제에 필요한 정보들과 결제의 진행 상황을 저장하는 플래그 정보를 포함한다. ObjectIds에 의한 결제 정보와 결제 상황에 대한 리포팅을 수행하여 사후 감사 정보를 제공한다. ObjectIds는 Client 1에서 생성하여 PG Server에 전송하고, 복사본을 전자결제 DB에 저장한다. PG Server는 Client들로부터 전송된 ObjectIds의 정보를 수집하며, 이상 징후를 점검한다.

3-4 프라이버시를 위한 암호화 및 토큰화 기술

결제의 진행 절차 중에서 전반부에는 동기화에 이어서 곧바로 암호화 키의 전송이 이루어지는데, 암호화 키는 모바일 단말에서 생성된 키가 전송된다. 모든 정보는 암호화되어서 전송 및 수신되며, 서로 공유한 암호화 키에 의해서 정보의 복호화가 진행된다. 자바 암호 아키텍처(JCA)와 자바 암호 확장(JCE)은 암호 API를 제공한다. JCA는 Java 2 Run-time environment의 일부이고, JCE는 JDK에 들어있지 않은 JCA의 확장팩이다. JCE는 JCA에서 간단한 암호화와 복호화 API를 제공한다. 암호 관련 함수를 사용할 때마다 JCA와 JCE API를 사용함으로써 다른 자바 라이브러리를 사용하는 다른 환경에서도 애플리케이션을 이식할 수 있다.

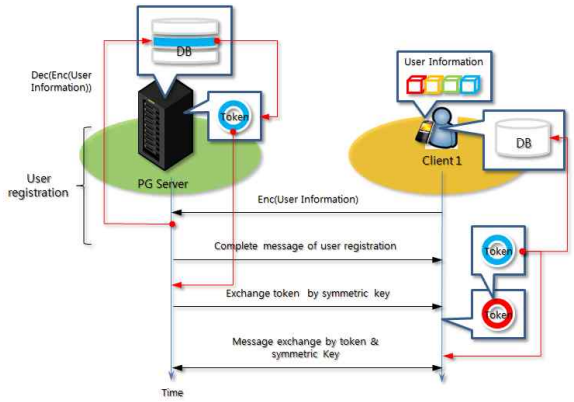

그림 17. 토큰화 절차
Fig. 17. Tokenization process

토큰화(Tokenization)[7] 기술은 금융 거래 정보를 보호하기 위해 2005년에 제안되었으며, 최근에는 개인정보 보호를 위한 DB암호화 기술로 많은 주목 받고 있다. 토큰화 기술은 유출로부터 보호되어야 하는 데이터(주민등록번호, 은행 계좌 번호, 신용 카드 번호, 금융 거래 정보, 의료 기록, 범죄 기록 등)의 정보를 보호하기 위해 데이터를 토큰(token)으로 치환한 뒤에 치환한 토큰 데이터만을 전송하고 저장함으로써 개인 정보를 보호하는 접근법이다. 그림 9의 ① ~ ④에서 소액 결제 모듈의 등록은 프라이버시를 위한 암호화된 정보의 교환이지만, 등록 이후에는 교환되는 정보들이 토큰으로 교체되어 나타나게 된다. 토큰화 기술의 다음 3가지 측면에서 보안성을 강조한다. 첫째, 토큰화 기술이 PCI-DSS가 명시한 보안 요구사항에 부합하는 기술이기 때문에 안전할 수 있으며, 둘째, 개인정보는 토큰 서버에서 안전하게 보관되고 관리되기 때문에 안전하다. 마지막으로, 토큰이 난수로 얻어지는 값이기 때문에 토큰으로부터 노출되는 개인정보가 없으므로 안전할 수 있다.

그림 17의 토큰화 절차는 전자결제를 위한 암호화 키 교환 절차가 완료된 후에 모바일 디바이스 Client 1의 전화번호 또는 모바일 디바이스의 시리얼 번호를 간접 정보로 등록한다. 사용자 Client 1은 사용자 정보를 암호화하여 PG Server에 전송하여 등록을 완료한다. PG Server는 암호화된 Client 1의 사용자 정보를 수신하여 복호화하고 사용자 DB에 등록한 후에 Client에게 완료 메시지를 전송한다. PG Server는 Client 1을 위한 토큰을 생성하여, 이를 암호화한 후에 Client 1에게 전송한다. Client 1은 PG Server로부터 암호화된 토큰을 수신하고 복호화를 수행한다. 그리고 토큰 정보를 전자 결제 DB에 등록 및 저장한다. 이후의 모든 전자결제는 이 토큰 정보를 이용하여 진행한다.

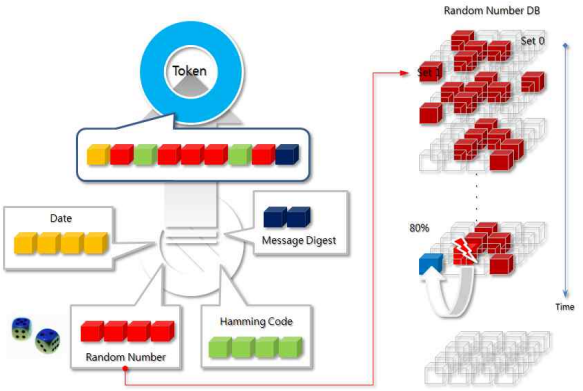

그림 18. 토큰 생성을 위한 무작위 수 생성과 등록 절차
Fig. 18. Process of random number generation and registration for token generation

그림 18은 토큰 생성을 위한 무작위 수 생성과 등록 절차를 나타낸 것이다. 토큰 클래스는 크게 난수 부분과 헤밍 (Hamming) 코드로 구성되며, 난수의 크기는 결제 시스템에 따라 임의적으로 결정되며, 헤밍 코드의 크기는 난수의 크기에 따라 결정된다. 헤밍 코드는 난수와 헤밍 코드의 에러를 복구하는 역할을 수행한다. 생성된 난수는 난수 DB에 사용여부를 기록한다, 생성된 난수가 DB에 0으로 설정되어 있으면, 생성된 난수를 이용하여 토큰을 구성한다. 생성된 난수가 DB에 1로 설정되어 있으면, 생성된 난수를 버리고 난수를 재생성 한다. DB가 80% 이상 사용되었고, 생성된 난수가 연속적으로 30번 이상(CLT를 근거) 1로 설정되어 있으면, DB를 새로 생성한다. 새로 생성된 DB를 이용하여 앞의 절차를 수행한다.

V. 결 론

본 논문에서는 전통시장 활성화를 위한 전자 현금결제와 전자 소액지불시스템에 대한 해외 사례를 연구하였다. 이를 기반으로 전통시장 활성화를 위한 IT 측면에서의 소상인의 소액결제를 지원하기 위한 NFC 기반의 소액 결제 모델과 인증 및 프라이버시를

제공하기 위한 방법을 제안하였다. 소액결제 모델은 NFC 기반의 스마트폰을 이용하여 결제의 편리성을 제공하며, 암호화 및 토큰화 기술에 의한 사용자들의 MD 인증, 간접 인증, 그리고 프라이버시 기능을 제공한다. MD 인증은 전자 소액결제를 위한 빠른 인증을 제공하며, 간접 인증에 의한 결제 진행 과정을 플래그 형태로 로그 정보를 제공한다. 제안된 토큰화 기술에 의해서 실질적인 정보 대신에 토큰에 의한 색인 정보를 제공하므로써 사용자의 프라이버시 기능을 제공한다. 향후 연구로는 모바일 전자 결제의 보안측면에서 샌드박스 모델과 접근 제어 측면에서의 추가적인 연구가 필요하며, 특히 인증과 프라이버시 문제를 해결하기 위한 다양한 기법들에 대한 모색이 필수적으로 필요하다.

감사의 글

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업 (정보통신)의 일환으로 수행하였음[10041057, 휴대단말 기반의 RFID 서비스 산업 활성화를 위한 모바일 RFID/NFC 융합형 기술 개발]. 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012R1A1A2041274)".

Reference

[1] JinYong Yang, “Vitality method of Mobile Smart Life Services based on NFC,” *Telecommunications Technology Association*, July 2011.

[2] NFC Forum, http://www.nfc-forum.org/

[3] Ovum, “NFC-enabled phones: forecast analysis”, 2007. 10. 31

[4] JeongHwan Kim, YoonCheol Lee, and DongIl Lee, “Electronic Payment System and Market Trend,” *National IT Industry Promotion Agency,* April 24, 2011.

[5] Byung-Rae Cha, Bong-Goo Park, and Dae-Gue Kim, “Concept Design to support Authentication and Privacy of Micropayment Model for Traditional Market Activation,” Journal of The Korea Navigation Institute, *Vol. 16, No. 4,* pp.665~pp.672, August 2012..

[6] Android Beam, http://developer.android.com/guide/topics/nfc/nfc.html

[7] SangGyu Sim, “Security Consideration about Tokenization Techniques”, http://www.boannews.com/media/view.asp?idx=31476&kind=0

김 용 일 (Yong-Il Kim)

1984년 3월 : 전남대학교 계산통계학과(이학사)
1986년 2월 : 한국과학기술원 전산학과(공학석사)
1986년 3월~1994년 2월 : 한국원자력연구소 선임연구원
1994년 3월~2000년 2월 : 초당대학교 컴퓨터학과 조교수
2002년 3월~현재 : 호남대학교 인터넷콘텐츠학과 조교수
관심분야 : 지능형정보검색, 클라우드 컴퓨팅, 지능형 에이전트 등

김 대 규 (Dae-Gue Kim)

1998년 ~ 2001년: 밀레니엄 버그 전산 전문가
1999년 ~ 2001년: 해양수산연구정보센터 개발실장
2008년 ~ 현재: ㈜ 아젠텍, 수석연구원
2009년 ~ 현재: M-RFID 표준화 및 관련 기술 개발
2010년 ~ 현재: 감성ICT산업협회, 정회원
현재 : (주)아젠텍 S/W 개발실 실장
관심분야 : 모바일-RFID 기술 개발, 클라우드 컴퓨팅

차 병 래 (Byung-Rae Cha)

2004년 2월 : 국립 목포대학교 컴퓨터공학과(공학박사)
2005년 3월 ~ 2009년 2월 : 호남대학교 컴퓨터공학과 전임강사
2009년 9월~현재 : 광주과학기술원(GIST), 정보통신공학부 연구조교수
관심분야 : 정보보안, Intrusion Detection System, 신경망, 클라우드 컴퓨팅, Future Internet 등