전통시장 활성화를 위한 소액 결제 모델의 인증 및 프라이버시 지원하기 위한 개념 설계

Concept Design to support Authentication and Privacy of Micropayment Model for Traditional Market Activation

차병래*, 박봉구**, 김대규***

Byung-Rae Cha*, Bong-Goo Park**, and Dae-Gue Kim***

요 약

본 논문에서는 광주광역시의 전통시장 활성화를 위한 노력과 현황에 대해서 알아본다. 그리고 전통시장 활성화를 위한 물리적인 인프라와 환경 개선 사업보다 IT 측면에서의 소상인의 소액결제를 지원하기 위한 안드로이드 NFC 기반의 소액 결제 모델과 토큰화 기술을 제안한다. 소액결제 모델은 NFC 기반의 스마트폰을 이용하여 결제의 편리성을 제공하며, 암호화 및 토큰화 기술에 의한 사용자들의 간접 인증과 프라이버시를 제공한다.

Abstract

In this paper, we find out about the effort and status of GwangJu metropolitan city to reinvigorate traditional market. And we propose the micro payment model based on Android NFC and tokenization technique to support the small trader's micro payment in aspect of information technology more than the physical infrastructure and environmental improvement projects 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 indirection authentication and privacy of users.

Key words : Traditional Market, Micro Payment, NFC, Token, Small Trader

I. 서 론

광주광역시의 지역유통업은 대부분이 중소유통업체로 광주광역시 인근의 생산자와 소비자들의 생산과 소비를 연결하는 유통의 중추적 역할을 담당하고 있다. 그러나 최근 대형 판매시설의 확산으로 중소 소매업체와 전통시장의 매출액이 감소해 가는 추세이며, 심지어 소상인들의 폐업이 증가하고 있는 실정이다. 이러한 문제를 해결하기 위하여 다각적인 노력의 결과로는 기존에 전통시장이 갖고 있던 이동의 불편함, 주차공간 부족 등의 물리적인 인프라와 환경개선 사업에 의해서 단점들이 많이 개선되었으며, 이에 머물지 않고 전통시장 활성화를 위한 IT 측면의 접근이 필요하다. 전통시장의 소매상들의 현금 또는 상

* 광주과학기술원(GIST.): brcha@nm.gist.ac.kr
** 호남대학교 교양학부: bgpark@honam.ac.kr
*** (주)아젠텍: afoxkim@ajantech.com
· 제1저자 (First Author) : 차병래
· 투고일자 : 2012년 6월 5일
· 심사(수정)일자 : 2012년 6월 8일 (수정일자 : 2012년 8월 21일)
· 게재일자 : 2012년 8월 30일

품권 결제방식에 대한 IT 측면의 새로운 접근법으로 스마트폰의 NFC 기반 소액 결제 모델을 제안하여 전통시장의 활성화 가속화에 협력하고자 한다.

Ⅱ. 관련 연구

2-1 NFC(Near Field Communication)

NFC 개념은 13.56MHz의 HF 대역을 이용한 기존의 비접촉식 카드 결제 방식을 접목시켜 휴대폰이 결제 장치에 근접하면 인증과 결제가 진행되며 소액결제, 인터넷뱅킹, 인터넷 쇼핑몰에서의 결제 등을 SMS 방식 아니라 NFC를 통해 가능하다. 자판기나 편의점의 POS 시스템에 휴대폰을 가까이 대면 자동결제가 가능하며, 공항, 지하철, 영화관 등에서도 e-티켓으로 활용할 수 있다. 또한 휴대폰끼리의 저장된 사진 또는 동영상 데이터 교환이 가능하다.

NFC 응용 분야에로는 NFC의 시작은 통신화의 개인화에 초점이 맞춰지며, 사용자 기기를 근접시킴으로써 모든 종류의 데이터를 완벽한 보안 환경에서 서로 교환이 가능하며, 저전력, 저비용의 통신 솔루션이다.

NFC 시장은 크게 커뮤니케이션 분야와 인포테인먼드(Infotainment) 분야로 구분할 수 있다. 커뮤니케이션 분야는 개인화를 위한 근거리 통신 용도와 저용량이나 저속에 적합한 데이터 통신에 사용될 수 있다. 저용량의 데이터를 공유하거나 WIFI 혹은 블루투스 초기 설정을 자동으로 수행하는 프로토콜을 주고받는 용도로 적합하다. 인포테인먼드 분야는 정보성과 엔터테인먼트적인 요소가 강한 데이터를 얻기 위한 단말기로 사용되며, 구입 제품의 온라인 등록, 신분 확인, 교통카드와 같은 소액결제 기능, 홈쇼핑 및 인터넷쇼핑의 개인 인증 및 결제 등에 활용될 수 있다.

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.

NFC 포럼의 논리적 구조 표준화는 NDEF(NFC Data Exchange Format), RTD(NFC Record Type Definition), NFC Text RTD, 그리고 NFC URI RTD 기술스펙이 정의되었다. NDEF 기술 스펙은 장치와 태그에 대한 공통의 데이터 포맷을 규정하고, NDEF 메시지 조합을 위한 규정한다. 그리고 NDEF 레코드에 포함된 애플리케이션 데이터 형식을 정의하는 메커니즘 제시하였다. RTD 기술 스펙은 장치 또는 태그 간에 주고받는 NDEF 메시지의 표준 레코드 형식을 규정한다. NFC Text RTD 기술 스펙은 장치가 읽을 수 있는 평문을 포함하는 레코드를 규정하며, 태그 상의 다른 오브젝트의 자유형식 평문을 기술하며, Text RTD는 URI와 같은 것에 메타데이터의 추가 목적을 지닌 평문 필드이다. NFC URI RTD 기술 스펙은 NFC를 지원하는 장치에 저장된 인터넷 리소스를 참고하는 NDEF 요소에 관한 레코드를 규정한다. [1]

2-2 소액결제 모델

소액지불시스템은 기존의 상거래에서는 쓸 수 없었던 것으로 그 출현자체가 많은 새로운 비즈니스 분야를 창출하고 있으며, Millicent, SubScrip, Payword, MicroMint 등의 소액지불시스템에 대해서 간략하게 정리한다. [2]

Millicent는 Digital Equipment Corporation이 1/10 센트(0.001 달러) 정도의 소액지불도 가능하도록 설계한 분산 소액지불시스템이다. Millicent 지불은 제 3자와의 접촉없이도 상인의 사이트에서 효율적으로 확인할 수 있는데, 이러한 분산적 접근법은 어떤 추가적인 통신, 값비싼 공개 키 암호화 또는 오프라인 처리없이 반복되는 소액지불을 효율적으로 가능하도록 한다. Millicent 시스템은 스크립이라는 전자통화(Electronic Currency)를 이용하고 있는데, 이것은 특정 상인에게만 가치가 있는 상인 종속형 통화이다.

SubScrip은 오스트레일리아의 University of Newcastle이 인터넷 상에서 효율적인

PPV(Pay-per-View) 지불을 위해 개발한 간단한 소액 비줄 프로토콜이며, 이용자 인식이 필요 없는 선불식 시스템이다. 기본적으로 특정 상인에 대해 고객을 위한 임시적인 선불 계정이 생성되면 고객은 이 계정을 이용해 소액지불 구매를 하게 된다. 계정이 임시적이고 선불식이기 때문에 가입 서비스와 관련된 일반적인 부담은 지지 않는다. 이 SubScrip 시스템은 자체의 과금 또는 뱅킹 위계를 필요로 하지 않는 반면, 선불 계정을 설정하기 위해 상인에게 초기 지불을 할 때, SET 이나 ECash와 같은 기존의 소액지불시스템이 이용될 수 있다.

PayWord는 MIT Laboratory for Computer Science의 Ron Rivest와 이스라엘 Weizmann Institute of Science의 Asi Shamir가 개벌한 크레딧-기반의 소액지불시스템이다. 이 시스템은 좀 더 빠른 해쉬 함수를 이용하여 지불 당 소용되는 공개 키 동작의 수를 감소시키고자 하였다. PayWord는 시스템 내에서 이요자 크레딧을 나타내기 위해 해쉬 값 체인을 이용학 있는데, PayWord라고 불리는 각 해쉬 값이 자불수단으로 상인에게 보내질 수 있다. 하나의 PayWord 체인은 특정 상인에게만 통용되며, 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 PayWord 보다는 낮지만 다른 많은 상인과의 소액지불에 더 효과적이다. MicroMint 시스템 내에서는 브로커는 코인을 발행하여 고객에게 판매하며, 소액 비줄을 위해 설정될 수 있는 고객과 상인의 계정을 유지한다.

Ⅲ. 광주광역시의 전통시장 활성화 현황

광주광역시 지역유통업의 대부분은 중소유통업체로 생산과 소비를 연결하는 유통의 중추적 역할을 담당하고 있다. 그러나 최근 대형 판매시설의 확산으로 중소 소매업체와 전통시장의 매출액이 감소해 가는 추세에 있다. 현재 광주광역시 지역유통업 판매시설은 총 55개소로 전통시장 27개소(시장 20, 상점가 7), 대형마트 13개소, 전문점 5개소, 쇼핑센터 6개소, 백화점 4개소가 있다.

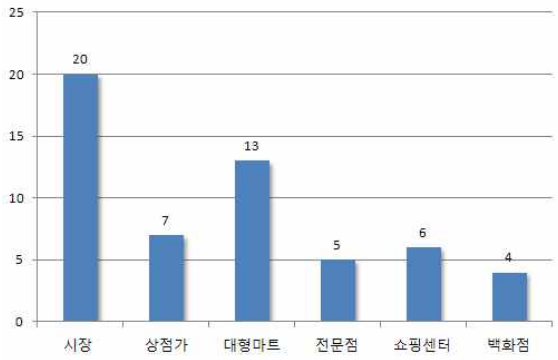

그림 1. 광주광역시의 지역유통 판매시설
Fig. 1. Local Distribution Sales Facilities in Gwangju Metropolitan City

그림 2. 전통시장 현대화 사업의 추진 비용의 비율
Fig. 2. Promote Cost Ratios to Traditional MArket Modernization

광주광역시에서는 전통시장 등 지역상권 활성화 사업을 위해 2002년부터 현재('12년)까지 1,062억원(국비643, 지방비 379.37, 민자 39.63)을 투자하여 전통시장 현대화 사업을 추진하고 있으며, 그 결과 대인시장, 말바우시장 등 18개 시장에 주차장이 조성되었고, 양동시장, 두암시장 등 3개 시장내 점포 리모델링, 하남시장, 상무시장 등 6개 시장 내에 화장실을 신축정비하였다.

정부·중소기업청과 연계하여 대규모 점포, 대기업 슈퍼마켓(SSM) 지역 진출 확대, 방문판매, 인터넷 쇼핑몰 등으로 다각화된 유통환경에 대응하여 전통시장 온누리 상품권을 발행·유통하여 지역상인의 매출 증대를 지원하고 있으며, 전통시장의 정겨움과 변화된 모습을 TV를 통해 홍보하여 소비자 인식을 개선하고, 전통시장과 관련된 축제 등에 관한 정보제공을 위해 지역 민영방송사(KBC광주방송)와 연계하여 홍보 프로그램을 제작 방영하고, 월 2만부의 시장신문을 발행하고 있다.

그리고 전통시장 상인들의 영업 활성화를 위해 점포당 5백만원의 소액대출을 지원하고 있으며, 전통시장 내 문화이벤트를 개최하고 우수 박람회 참가를 지원하는 등 전통시장 경영현대화 사업을 추진하고 있다.

이러한 다각적인 노력의 결과로 기존에 전통시장이 갖고 있던 이동의 불편함, 주차공간 부족 등의 단점들이 많이 개선된 것이 사실이다.

그리고 지역상인의 의식개선을 위한 상인대학 등 다양한 교육프로그램 지원으로 전통시장 소상인들의 의식에도 많은 변화가 있었다. 그러나 전통시장이 광주에 맞는 전통문화, 먹거리 등 종합공간으로서 역할을 위해 지역·위치적 특성에 맞는 특성화를 도모해야 하며, 과거 속에서 뿐만 아니라 젊은 신세대의 접근성을 높이기 위해서는 좀 더 체계화되고 다각적인 변화와 노력이 수반되어야 할 것이다.

광주광역시는 최근 두 번째와 네 번째 일요일을 대형마트와 SSM 의무 휴업일로 정하여 대기업 판매시설 규제를 통해 지역내 전통시장의 활성화를 도모하고 있다. 이러한 의무규제는 전국적인 기조로서 의무 휴업일에 마트의 고객을 전통시장으로 끌어들이기 위해서는 지역상인회의 자발적인 노력과 의식변화가 필수적이라 할 것이다. 최근 남광주 시장에서는 “으랴차차 남광주”라는 제목으로 판촉이벤트를 개최하였으며, 행사당일 호박죽 무료 나눔행사와 봄나물 파격할인 행사를 열어 지역주민의 큰 호응을 얻었으며, 남광주시장을 시작으로 말바우시장, 양동시장, 무등시장, 봉선시장, 대인시장 등이 대형마트 대신 전통시장을 찾는 고객들에게 다양한 판촉행사를 개최해 양질의 물품을 저렴하게 공급할 예정이다. 또한 정부에서도 중소기업청, 시장경영진흥원, 농식품부와 연계하여 정부가 보관해온 냉동 고등어, 깐마늘 등을 소매가 보다 최대 반값까지 할인된 가격으로 전통시장에 공급할 계획에 있어, 어느 때보다 전통시장 활성화를 위한 적기라 볼 수 있다.

Ⅳ. 안드로이드 NFC 기반 소액 결제의 개념 설계

4-1 전통시장을 위한 소액결제 모델

전통시장 활성화를 위한 소상인과 구매자간의 소액 결제 절차는 크게 소상인, 구매자, 은행으로 구분할 수 있으며, 그림 3과 같이 나타낼 수 있다.

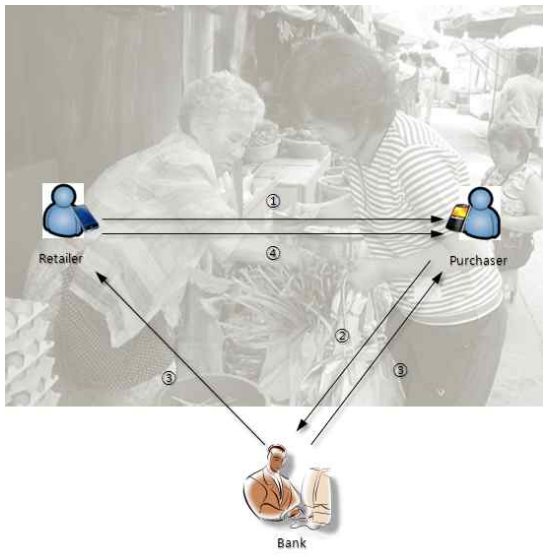

그림 3. 전통시장의 안드로이드 NFC 기반 소액결제 모델
Fig. 3. Micro-Payment Model based on Android NFC of Traditional Market

거래 절차는 그림 3의 ①에서 구매자는 소액결제를 위한 정보와 소상인의 정보를 NFC 기반으로 안드로이드 빔(Android Beam)[3]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 않

기 때문에 공개된다.

그림 3의 ②에서 구매자는 구매자 계좌의 인증과 소상인의 계좌 정보로 구입 물품에 대한 소액 결제를 진행하게 된다. 은행은 이를 복호화 및 토큰화에 의한 계좌번호를 알아낼 수 있다. 또한 은행은 소액 결제를 위한 인증 및 간접 인증을 수행하게 된다.

그림 3의 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 3의 ④에서 소상인과 구매자 간의 계약 성립에 따라 구매 물품을 구매자에게 인도하면 된다.

4-2 NFC 기반의 소액 결제 모델의 절차 및 기능

안드로이드 개발 사이트에서 제공하는 NFC 시나리오 2: 블루투스 페어링의 기본 개념을 이용한다. NFC가 근접식으로 장치 동작은 모바일폰의 개인화에 유리한 기능을 갖으며, 특히 개인화로 무선 네트워크의 동작 범위가 WPAN의 영역보다 작아야 하며, WPAN이 10m 이내인 것에 비해 NFC는 WBAN(Wireless Body Area Network)이 된다. 블루투스/WiFi를 처음 동작하기 위해서는 초기설정 과정으로 주변의 블루투스/WiFi 장치를 검색하며, 검색된 장치를 선택하여 과정이 필수이며, 블루투스/WiFi 장치를 설정하기 위해서는 블루투스/WiFi의 어드레스 정보가 장치 간에 교환이 필요하며, 페어링이 진행된다. 페어링이 진행되는 동안에 소상인의 사업자 정보와 계좌 번호 등의 정보를 스캔하여 저장하게 된다. 안드로이드 NFC 기반의 소액 결제 모듈의 기본 설계는 그림 4와 같이 기본 절차를 플로우챠트로 나타낸다. 모바일 장치에 기본적으로 개인 정보와 결제 정보가 등록되었다는 가정 하에서 결제를 진행하면 보안 모듈이 호출되면서 결제 프로세스의 모든 절차를 진행하게 되며, 보안 모듈이 호출되지 않으면 다음의 모든 절차는 진행되지 않으며, 결제를 위한 초기화 상태 또는 결제 모듈의 종료로 전환된다.

그림 4에 나타낸 것처럼, 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 리포팅된다. 이를 위한 각 모듈의 라이프사이클은 그림5와 같이 나타낸다.

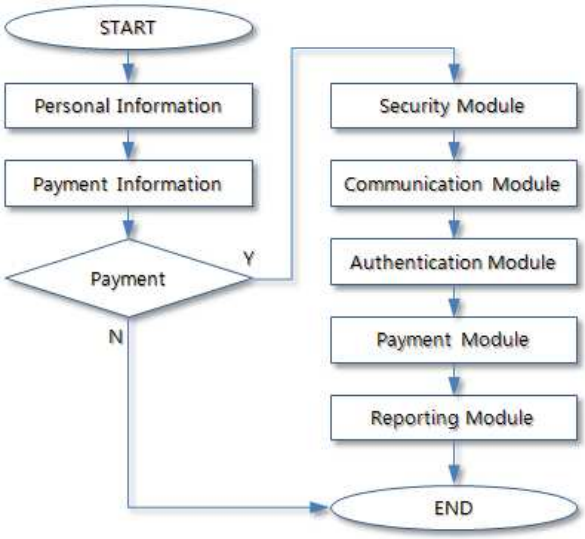

그림 4. 제안된 소액 결제의 수행 절차
Fig. 4. Processing Procedure of proposed Micro-payment

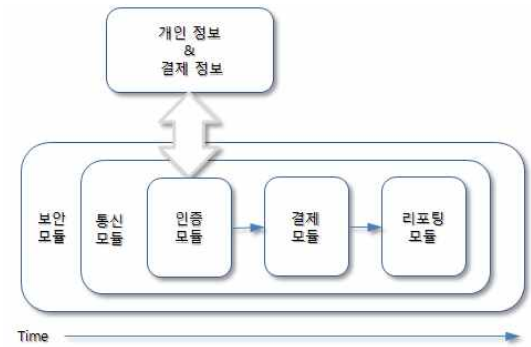

그림 5. 모듈들의 라이프 사이클
Fig. 5. Life Cycle of modules

• 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.

4-3 인증 기술

NFC 기반의 전자결제를 위한 보안 인증 기능을 설계하며, 인증은 크게 직접 인증과 간접 인증에 의한 결제의 안전성과 부인방지 기능을 제공할 수 있다. 직접 인증은 일반적인 인증을 의미하며, 간접 인증은 직접 인증을 증명할 수 있는 정보를 제공하는 것이다.

(1) 보안 인증

JAAS(JavaTM Authentication and Authority Service)[4]는 플러그인 구조의 프레임워크이며, 자바 인증과 권한 부여 서비스를 제공한다. JAAS는 특정 작업을 하는데 권한이 있어야 실행할 수 있도록 제한되어 있는 프로그램을 개발한다. JAAS는 사용자를 인증하는 클래스이며, 사용자가 특정 작업을 할 수 있도록 권한 부여를 할 수 있게 하는 클래스이다. JAAS에서 특정 사용자에게 부여된 권한은 시스템 관리자가 관리한다. JAAS 지원 애플리케이션은 다음과 같이 동작한다:

• 소액 결제 모듈은 사용자에게 로그인을 요청하면서 사용자 로그인 객체를 받아온다. 프로그램에서 LoginContext 객체를 생성하고, 그 객체에 메소드를 호출한다. 이 클래스는 솔라리스 NIS 또는 NIS+, 윈도우 NT 로그인 서비스, LDAP 서버 또는 다른 인증 시스템을 통해서 인증을 한다.

• 소액 결제 모듈은 사용자 로그인 객체와 사용자 대신에 실행되어야 할 코드를 매개변수로 메소드를 호출한다(doAs() 또는 doAsPrivileged() 메소드)

JAAS의 LoginContext 클래스는 사용자를 인증할 수 있는 환경을 만든다. 사용자 인증은 login(), logout(), getSubject()의 3가지 메소드가 존재한다. 또한 Subject 클래스는 인증된 사용자를 표현하며, 각 사용자는 이 클래스에 저장되어 있는 Principal 객체 배열로 표현된다.

JAAS 정책 파일의 구현은 Policy 클래스의 하위 클래스이다. JAAS 정책 클래스의 기본 구현은 PolicyFile 클래스이며, 이 클래스는 JAAS 정책 파일을 파싱하고 요청에 대한 알맞은 권한을 리턴한다. 또한 JAAS Policy 클래스에는 getPolicy(), setPolicy(), getPermissions(), 그리고 refresh()의 4가지 메소드가 있다.

(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. MongoDB[4]는 기본 데이터 유형으로 12바이트 크기의 ObjectIds를 제공하며, 이러한 자료형에 의해서 비구조적 DB의 Primary key 역할을 수행하게 된다. 간접 인증을 위한 결제 트랜잭션에 대한 ObjectIds는 그림 6과 같이 자료 구조를 설계한다.

NFC 기반의 전자 결제의 간접 인증을 위한 ObjectIds의 구조는 그림 6과 같으며, Machine 필드가 4바이트로 확장되고, Flag라는 1바이트의 필드가 추가된 14 바이트로 구성된다. 추가된 Flag 필드에 의해서 결제를 위한 인증 절차의 모든 상황 및 절차에 대

한 점검이 가능하게 된다.

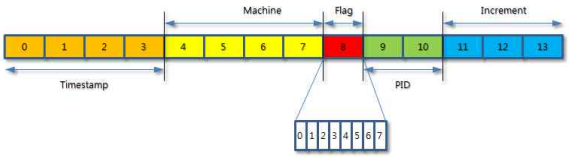

그림 6. 간접 인증을 위한 ObjectIds의 구조
Fig. 6. Structure of ObjectIds for indirection authentication

4-4 프라이버시를 위한 암호화 및 토큰화 기술

IT 분야의 프라이버시(privacy)는 개인의 정보를 인터넷과 컴퓨터에 있는 자기의 자료를 보호하는 행동이다. 프라이버시 보호는 제 3자에 대해서 정보의 공개를 방지하며, 개인 정보의 오용을 사전에 차단하는 것이며, 유선 네트워크 환경에서 무선 네트워크 환경으로 프라이버시 보호의 영역을 확장하고 있는 상황이다. 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.

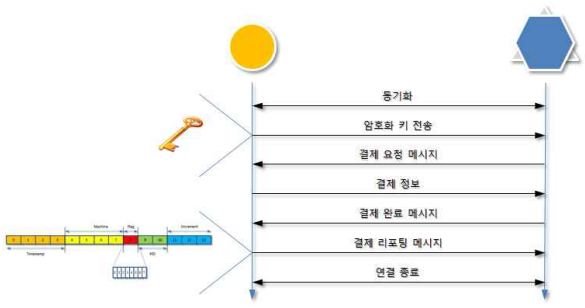

그림 7. 암호화에 의한 프라이버시 보호 및 ObjectIds의 간접 인증 절차
Fig. 7. Encryption to protect privacy and indirection authentication procedure of ObjectIds

(1) 암호화 기술

자바 암호 아키텍처(JCA: Java Cryptography Architecture)[5]와 자바 암호 확장(JCE: Java Cryptography Extension)[6]은 자바에서 구현에 무관한 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.

(2) 토큰화 기술

토큰화(Tokenization)[7] 기술은 금융 거래 정보를 보호하기 위해 2005년에 제안되었으며 최근에는 개인정보 보호를 위한 DB암호화 기술로 많은 주목을 받고 있다. 토큰화 기술은 유출되지 않도록 보호되어야 하는 데이터를 토큰(token)으로 치환한 뒤에 원본 데이터를 대신하여 토큰을 사용하는 기술이다. 유출로부터 보호되어야 하는 데이터는 주민등록번호, 은행 계좌 번호나 신용 카드 번호 등의 금융 거래 정보, 의료 기록, 범죄 기록, 운전면허나 차량 등록번호 등의 자동차 관련 정보, 주식 거래 정보 등이 이에 해당된다. 이러한 정보들은 개인정보를 담고 있기 때문에 통신 과정에서 유출되거나 혹은 서버 내부에 저장된 데이터가 유출되었을 경우에 큰 피해를 가져올 수 있다. 토큰화 기술은 개인 정보의 유출 위험이 있는 전송 과정과 저장 단계에서 개인정보 데이터를 치환한 토큰 데이터만을 전송하고 저장함으로써 개인 정보를 보호하는 접근법이다. 그림 3의 1 ~ 4에서 소액 결제 모듈의 등록은 프라이버시를 위한 암호화된 정보의 교환이지만, 등록 이후에는 교환되는 정보들이 토근으로 교체되어 나타나게 된다. 토큰화 기술의 보안성은 크게 3가지 측면에서 주장한다. 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.

V. 결 론

본 논문에서는 광주광역시의 전통시장 활성화를

위한 10여년의 노력과 현황에 대해서 알아보았으며, 소액지불시스템에 대한 고찰을 수행하였다. 이를 기반으로 전통시장 활성화를 위한 IT 측면에서의 소상인의 소액결제를 지원하기 위한 NFC 기반의 소액 결제 모델과 간접 인증 및 토큰화 기술을 제안하였다. 소액결제 모델은 NFC 기반의 스마트폰을 이용하여 결제의 편리성을 제공하며, 암호화 및 토큰화 기술에 의한 사용자들의 간접 인증과 프라이버시를 제공한다. 또한 간접 인증에 의한 결재 진행에 대한 로그 정보를 제공한다. 향후 연구로는 모바일 전자 결제의 보안측면에서 좀더 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]

참 고 문 헌

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

[2] 김정환, 이윤철, 이동일, “전자지불시스템 및 시장 동향”, *정보통신연구진흥원*, 2011년 4월 24일.

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

[4] JavaTM Authentication and Authorization Service (JAAS), http://http://docs.oracle.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html

[5] JavaTM Cryptography Architecture (JCA), http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

[6] JavaTM Cryptography Extension (JCE), http://docs.oracle.com/javase/1.4.2/docs/guide/security/jce/JCERefGuide.html

[7] 심상규, “토큰화 기술에 대한 보안성 고려”, http://www.boannews.com/media/view.asp?idx=31476&kind=0

차 병 래 (車炳來)

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

박 봉 구(朴奉求)

1968년 ~ 1973년: 공주사범대학 수학교육학과
1980년 ~ 1982년: 원광대학교 대학원 수학과(이학석사)
1982년 ~ 1987년: 조선대학교 대학원 수학과(이학박사)
1984년 ~ 현재: 호남대학교 수학과 및 교양학부 교수
관심분야: 수학교육, 복소해석학, 정보보안

김 대 규 (金大圭)

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