ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

통합 아이디를 이용한 안전한 모바일 월렛 시스템☆

The secured mobile wallet system using by integrated ID

남 춘 성[1] 전 민 경[2] 신 동 렬[2*]
Choon-Sung Nam Min-Kyung Jeon Dong-Ryeol Shin

요 약

현대의 사회는 Single tapping, 단방향 통신, 통합 아이디 등 빠름, 간편함, 편리함을 위해 최대한 사용자의 행동 패턴을 줄이고 소모시간이 적게 걸리는 기술이 우선시 되고 있다. 스마트 웰렛 시장과 마찬가지로 사용자의 편의성, 신속성, 간편성을 적용하려는 분야는 통합 아이디 시장이다. 일반적으로 사용자들이 잊어버리기 쉬운 ID와 패스워드를 통합 관리하기 위한 시스템으로서 다수의 ID와 패스워드를 보유하고 있는 사용자가 보유한 다수의 정보를 시스템에 등록하여 한 번의 로그인에 의해 다수의 서비스를 받을 수 있는 기술이다. 하지만 OpenID 시대의 도래에도 다수의 서비스들에서 해당 기술이 적용되지 않는 이유가 각 사업자의 사이트에 일일이 가입해야 하는 등 서로의 이익을 위해 기술 적용을 꺼리는 경우가 많다. 또한, 다수의 포인트 사업자에 가입이 되어 있을 경우, 어떤 포인트의 적립이나 할인이 사용자 본인에게 더 유리한지 한눈에 확인할 수 없기 때문에 스스로 포인트 카드에 맞는 유리함을 계산해야하는 어려움이 있다. 따라서 본 논문은 사용자의 편의성을 위하여 단하나의 ID로 여러 가입된 사이트 및 카드 포인트 적립, 결제와 같은 서비스를 이용할 수 있도록 안전한 통신 아이디어를 제안한다. 또한, 통합 ID를 통하여 가맹점의 혜택 카드를 일일이 찾는 수고를 줄여 보다 간편하고 효율적인 적립이나 할인을 제공할 수 있는 시스템을 제안한다.

☞ 주제어 : 스마트 월렛, 지불 시스템, 통합 아이디, 싱글 태핑

ABSTRACT

Nowadays, Smart Wallet technology trend that is able to save users' consuming costs and also retain users' redundant behaviors such as Single-tapping, One-way communication, Integrated ID, has been issued in recent Mobile Industrial Fields. As one of Smart Wallet functions, Integrated ID is proposed for users' convenience, handiness, and immediate responses. It is designed for the effective management of users' IDs which are easy to be forgot because of its unusual structures. To be detail, instead of user, Integrated ID system can certificate users identification from various online sites (where user resisted) authorization requests via one-clicking, not putting identification data in each sites. So, this technology would be helpful much to a certain user who has lots ID and its Password in multiple Online shopping companies by establishing integrated ID. However, although Integrated ID has lots advantages to be used, most Mobile Service Companies has hesitated to apply Integrated ID service in their shopping systems because this technology requires them sharing their users' data. They have worried that this service would be not helpful to gain their profits. Furthermore, Users who join in multiple shopping companies and use Integrated ID services also are difficult to decide which company they have to save their points in before payment because this system could not show any financial benefit analysis data to their users. As following facts, via this paper majorly we propose the advanced Integrated ID system which concern shopping point management. Basically, this system has a strong security payment service and secure network services like other mobile Shopping systems. Additionally, this system is able to service (or to support) shopping -point -saving guide for customers' financial benefits and conveniences.

☞ keyword : Smart Wallet, Payment System, Integrated ID, Single Tapping

1. 서 론

현대의 신속성, 간소성, 편리성을 추구하는 IT 기술은 Single tapping, One-way, 통합 아이디 등과 같은 사용자 행동 패턴을 줄이고 소모시간이 적게 걸리는 기술발전하고 있다. 본 논문에서 제시하는 스마트 월렛 시장도 이러한 동향에 편승하고 있고, 이미 신용카드 3.0 시대로의 모바일 월렛을 제공하는 움직임을 보이고 있다[1, 2]]. 모바일 카드는 관리의 편의성을 제공하고 있다. 스마트 웰렛 시장과 마찬가지로 이러한 장점들을 적용하는 분야는 통합 아이디 시장이다. OpenID, I-PIN, 공인인증 등이 가장 대표적인 예이다[3]. 일반적으로 사용자들이 잊어버리기 쉬운 ID와 패스워드를 통합 관리하기 위한 시스템으

[1] School of Information, Yonsei University., Seoul, 120-7, Korea
[2] College of Information and Communication Engineering, SungKyunKwan University, Suwon, 440-746, Korea.
* Corresponding author (drshin@skku.edu)
[Received 10 May 2014, Reviewed 27 May 2014(R2 28 October 2014), Accepted 14 November 2014]
☆ 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2013R1A1A2063180)

로서 다수의 ID와 패스워드를 보유하고 있는 사용자가 이를 시스템에 등록하여 단 한 번의 로그인에 의해 다수의 서비스를 받을 수 있는 기술로 발전을 거듭하고 있다. 또한 개인정보 유출, 주민등록번호 대체 등 보안적인 이유로 이를 대체하기 위한 통합 아이디를 적용하는 사례가 많아지고 있다.

OpenID 시대의 도래에도 다수의 서비스들에서 해당 기술이 적용되지 않고 각 사업자의 사이트에 일일이 가입해야 하는 번거로움이 여전히 존재한다. 이는 서로의 이익을 위해 기술의 적용을 꺼리는 경우가 많다. 한 예로 카드, 포인트 적립 및 결제와 같은 서비스를 제공하는 사업자들이다. 그로인해, 현재 카드 포인트 적립이나 할인혜택을 적용하기 위해서는 사용자가 일일이 할인혜택을 알아보고 계산을 해야 하는 불편함이 있으며, 각 포인트 사업자의 사이트에 일일이 가입하여 그 혜택을 받아야 한다. 또한, 다수의 포인트 사업자에 가입이 되어 있을 경우, 어떤 포인트의 적립이나 할인이 사용자 본인에게 더 유리한지 한눈에 확인할 수 없기 때문에 일일이 포인트 카드를 찾아서 결제 시 적용해야 하는 불편함과 비효율성을 가지고 있다.

따라서 본 논문은 이와 같은 문제점을 해결하기 위해 사용자 편의성을 중심으로 단하나의 ID만으로도 여러 가입된 사이트 및 카드 포인트 적립, 결제와 같은 서비스를 이용할 수 있도록 안전한 통신 아이디어를 제안한다. 또한 통합 ID를 통하여 가맹점의 혜택 카드를 일일이 찾는 수고를 줄여 보다 효율적인 포인트 적립이나 할인을 선택적으로 이용하도록 하는 시스템을 제안한다. 2장에서는 기존 방식에 대한 설명과 문제점을 제시하고, 3장에서는 제안하는 시스템을 제시한다. 4장에서는 이를 검증하기 위한 분석을 하고, 마지막으로 5장에서는 결론을 맺는다.

2. 통합 ID 기술과 이전 기술 비교 및 요구사항

2.1 모바일 월렛(mobile wallet)

2.1.1 스마트 월렛(smart wallet)

대표적인 두 가지 모바일 웰렛은 스마트월렛과 구글월렛이다. 스마트월렛(smart wallet)은 신용카드, 상품권 및 멤버십 카드, 그리고 쿠폰 등을 편리하게 관리하고 사용할 수 있는 모바일 웰렛이다. 이는 다양한 제휴사의 멤버십 카드를 발급받고 실시간으로 포인트를 적립/조회/사용 가능하다[1]. 스마트월렛의 경우 결제는 해당 카드의 바코드를 읽히는 방법과 NFC를 이용하여 지불하는 방법이 가능하다.

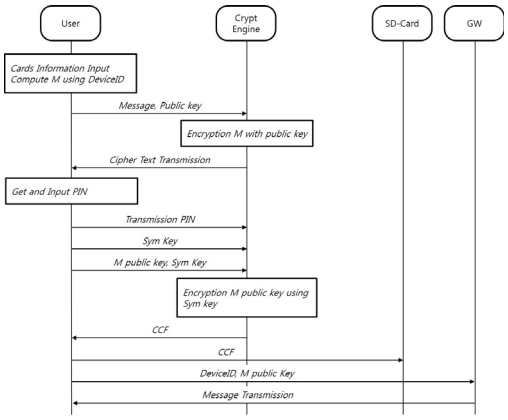
2.1.2 구글 월렛(google wallet)

구글 월렛은 single tapping NFC 방식을 지원하며 신용카드/체크카드, 쿠폰을 제공하는 모바일 서비스이다[2]. 각 사용자는 사용자 개인의 정보를 카드 발행 은행으로 전송하여 확인하는 작업을 거치고 TSM(Trusted Service Manager, Google의 경우 Frist Data에서 담당)에서 데이터를 관리하며, 시크릿 키(Secret key)를 통해 매번 구매 시, 사용자를 확인하고 NFC를 통하여 폰과 통신한다. 우리나라의 경우 사용을 위해 별도의 공인 인증서 발급의 절차가 필요하다. 가입 시 카드 번호, 유효기간, CVC 보안코드 등의 카드 정보를 입력하고 Single Tapping으로 결제 절차가 진행되지만, 포인트 카드 혹은 추가 할인 혜택은 동시에 사용이 가능하지 않으며 계산 시 따로 제시하는 방법을 사용하여야 한다.

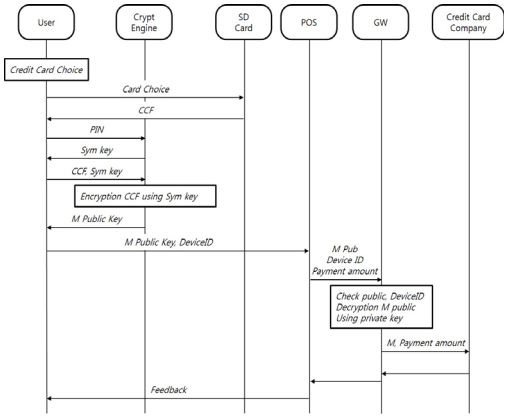
NFC Single Tapping 방식은 구글월렛 뿐만 아니라 선행 연구된 IDA-Pay 시스템 아키텍처에서도 마찬가지로 제안되고 있다[4]. 그림 1은 IDA-Pay 시스템의 카드 설정 통신 과정을 담은 시나리오이다. 사용자는 카드를 사용하기 전에 안드로이드를 통하여 카드의 정보를 입력하고 공용키와 PIN키를 이용하여 암호화 한 후 데이터를 주고받는 것을 볼 수 있다. 그림 2는 카드를 등록한 후 실제 결제를 하는 시나리오이다. 카드 등록 시나리오와 마찬가지로 사용자가 카드를 결정하고 NFC를 통하여 결제를 진행하게 되면 SD카드에 미리 저장된 CCF를 이용하고 결제의 과정에서도 공용키와 PIN키를 이용하여 결제를 제안하고 있다.

많은 연구들이 NFC를 이용하여 Single Tapping 방식을 적용하고 있으나 NFC 신호를 통하여 재사용 공격(relay attack)에 대한 피해가 다수 보고 되고 있다[5]. NFC신호를 모바일을 통하여 캡쳐하고 그 신호를 다시 흘려보냄으로써 재사용이 가능하게 되고 이를 통하여 사용자에게 손해를 입힐 수 있음이 실험을 통하여 증명되었다. 또한, 구글월렛의 안전성에 대한 논의 또한 발표되었다[6]. 즉, 선행 연구에서 문제가 되는 부분은 구글 월렛에서 PIN을 확인하는 과정에서 PIN 해쉬 값을 통하여 Known attack이 가능하다는 점과 On-card Component 의 경우 PIN값을 확인하지 않아 Unlock 명령에 해당하는 16진수 코드인 80 E2 00 AA 00 을 전송하였을 경우 구글 월렛이 unlock 모

드가 되어 보안에 취약하다는 점이다. 따라서 이를 보완하기 위한 방안이 필요하다.



(그림 1) IDA-Pay 시스템에서의 카드 설정 과정
(Figure 1) Card setup process in IDA-Pay system



(그림 2) IDA-Pay 시스템에서의 결제 과정
(Figure 2) Payment process in IDA-Pay System

2.2 통합 ID(integrated ID)

2.2.1 OpenID, OpenID 2.0

OpenID는 사용자 중심 아덴티티(identity)를 위한 분산형 공개 표준 기술로 개인정보 유출방지 및 관리, 주민등록번호 대체, 개인화 맞춤 서비스를 제공하기 위한 기술이다[3, 7]. 하나의 ID로 가입 절차 없이 OpenID를 지원하는 여러 사이트에서 로그인 서비스 제공한다. OpenID를 제공하는 방법은 사용자에게 ID로 URL 또는 XRI을 제공하여 OpenID 공급자의 서버에서 인증을 하여 다수의 사이트에 접속을 가능하게 한다. 이러한 기술의 강점은 일반적인 사업자 중심의 ID에서 고객 중심의 ID로 변화함에 따라 개인정보 노출을 최소화하고 사용자로 하여금 하나의 ID로 다수의 서비스를 이용하게 한다. 사업자의 입장에서는 컨텐츠 역량이 부족한 사업자의 고객에게 편의성 제공하여 컨텐츠 투자 비용 절감하는 동시에 ID 기반 결제로 추가 수익 창출하게 하여 기존 보유한 결제 시스템을 활용하여 수익 확대할 수 있다. 또한, OpenID 기반으로 수집된 고객 정보를 이용하여 고객 성향분석을 하고 개인 맞춤형 서비스 제공 하는 등 타겟 광고에 활용할 수 있다.

최근에는 OpenID의 단점을 보완하기 위해 OpenID2.0로 업그레이드된 기술이 발표되었다[8]. 기존의 OpenID는 하나의 OpenID 공급자에서 장애가 발생할 경우 대처할 방법이 없었다. 이를 해결하기 위해 하나의 아이디를 다수의 OP(OpenID Provider)에 등록해 특정 OP에 장애가 발생하면 다른 쪽을 선택할 수 있게 변형하여 OP 장애로 인해 서비스를 받지 못하는 상황을 최소화하였다. 또한, 악의적인 공격자가 가짜 OP를 진짜로 속이는 것을 방지하여 스니핑(sniffing)이나 스푸핑(snoofing), CSRF (Cross Site Request Forgery)공격을 막아 OpenID 사용을 좀 더 안전하게 제공한다[9].

하지만 일반적인 구조와 달리 특정 인증 메커니즘을 명시하지 않으므로 인증강도는 OpenID를 지원하는 사이트가 인증 정책에 대해 얼마나 많이 알고, 인증의 중요성을 인지하는데 따라 달라질 수 있다. 또한, ID를 검증해주는 서버를 통하여 매 순간 인증하게 되므로 시간적인 지연이 존재하며 사용자가 긴 URL로 된 OpenID를 암기해야 사용할 수 있는 불편함을 가지고 있다.

2.2.2 OpenID 기반 SSL 인증 스마트 카드

스마트 카드를 기반으로 한 솔루션 기술을 말하며, 스마트 카드는 SSL 인증서를 저장한다[10-11]. 스마트 카드는 키 물질을 전송하고 USB를 통하여 유효성을 검증하며 클라이언트가 유효성을 검증할 서버에 인증서를 전송하고 서버는 유효성을 검증할 클라이언트에게 인증서를 전송하여 서로를 인증하는 방법을 사용한다. 따라서 공격자는 HW/SW 모두를 알아야 공격 가능하다. 하지만, 안전을 위해 추가적으로 공용키 스트럭처(structure)가 필요하며 일반적인 인증서 기법과 마찬가지로 추가적인 저장 공간이 필요하게 된다. 인증서는 인증기관에서 발급을 받아야 하며 인증기관의 디지털 서명이 포함되어야 한다.

2.2.3 3GPP OpenID

네트워크 인증 및 접근제어 기술로써 클라우드 컴퓨팅(cloud computiing)과 같은 네트워크 환경에서 식별자 인증 및 접근을 제어한다. 모바일 환경에서의 클라이언트와 서버간의 상호인증 수행으로 GAA(Generic Authentication architecture), GBA(Generic Bootstrapping Architecture) 표준을 정의하고 있다. GAA는 인증서를 기반으로 상호인증을 수행할 수 있는 공통 아키텍처 환경을 말하고 GBA는 공유키를 생성하여 단말과 서버 간에 이를 공유, 인증 용도로 공유키를 사용할 수 있는 응용 독립적인 메커니즘 규정되어 있다[12-13]. 하지만 이 기술은 네트워크에서 해당 아키텍처의 능력과 장비의 기능, 스펙에 의존적이다. 또한, 네트워크에서 특정 기술을 구현하고 싶다면 장비에서도 해당 기능을 구현해야 하므로 현 시스템에서 바로 적용하기 어려운 단점을 가진다.

2.2.4 Liberty alliance(identity sharing)

동일 도메인 내에서 혹은 연계된 도메인들 내에서 사용자의 정보를 주고 받는 사업자 중심의 공유 기술이다. 사용자 정보는 해당 사용자를 거쳐 확인되어 전달한다. ID공유는 개인정보를 연계하는 매쉬업(mash-up) 서비스 등을 제공 하지만, ID공유 과정에서 생길 수 있는 보안문제나 위협에 대한 분석이 부족하여 아직은 추가적인 연구 필요하다고 전망되고 있다[14].

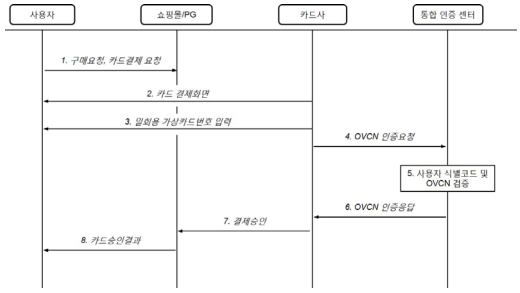
2.2.5 보안 토큰(security token)

서비스 요청 주체가 서비스 제공 주체의 서비스 이용을 지원하기 위해 ID 관리 주체가 서비스 요청 주체에게 발급하는 기술을 말하며 Kerberos, X.509 등의 기술들을 통해 생성한다. 보안 토큰은 주로 단일 인증 및 권한 관리 기술의 일부로 사용되므로 다수 인증을 하기에 적합하지 않으며 적용된 인증서 기술을 실시간 결제에 적용하기에는 사용자가 감수해야 되는 시간이 많아 실시간 시스템에는 적합하지 않다[15].

2.3 가상카드번호 생성 및 결제 방식

2.3.1 통합인증센터 일회용 가상카드번호 방식

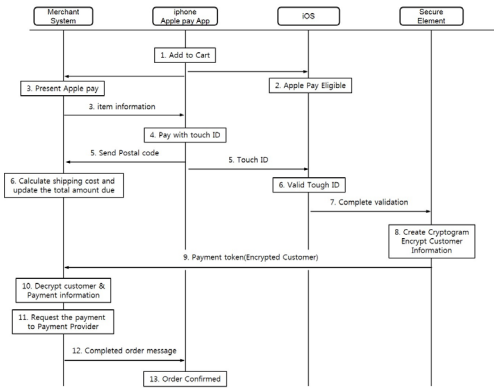
통합인증센터 일회용 가상카드번호 방식은 휴대단말기를 활용한 일회용 가상카드번호의 보안 요구사항을 만족하는 일회용 가상카드 번호 생성 스킴을 제안하고 있다. 이 방법을 사용하기 위해서는 사용자는 카드사로부터 통합인증센터에게 타기관 이용등록을 통한 이용등록을 완료하고, 사용자 단말에서 생성된 카드 번호를 카드사에 넘겨서 카드사가 통합인증센터로 이를 인증하기 위한 방법이다. 이는 제안된 시스템과 달리 카드사와 통합인증센터간에 협약이 되어 있어야만 가능한 방식으로 기존 시스템의 변경 없이는 이루어질 수 없다. 또한, 각 제휴 카드사가 각각의 인증센터(가상카드번호 생성 혹은 원타임 패스워드)를 갖는다면, 통합인증 센터가 필요없다. 이는 카드사의 제휴에 관련된 것이기 때문에 이 방법의 결제 서비스를 제공하는 것에 대한 확장성이 부족 할 수 밖에 없다[16].



(그림 3) 가상카드번호 결제 과정
(Figure 3) Payment process of virtual card number

2.3.2 애플페이(Apple Pay)

애플페이를 사용하기 위해서는 우선 신용카드를 등록해야 하는데 이는 iTunes에서 설정된 카드에 종속된 것으로 기존 iTunes에 종속된 카드나 혹은 'Passbook' 어플로 카드를 등록하여 사용가능하다. 이는 간단히 카메라를 통한 캡쳐로 등록될 수 있지만, 신용카드 정보는 'Passbook' 있지 않고, iTunes에 남아있기 때문에 어떠한 카드의 트랜잭션(transaction) 정보를 기기가 저장하지 않는다. 따라서 결제과정에서 어떠한 신용카드 정보도 노출될 위험이 적다. 결제는 사용자의 기기 계정 번호를 이용한 일회성 고유번호로 승인되고, 카드 뒷면의 보안 코드 대신에 동적 보안 코드를 생성하여 이를 결제에 이용한다. 이와 같은 방식은 카드 정보를 암호화 하고 사용하는데 편리함은 제공될 수 있으나, 이 역시 기존의 시스템을 유지하면서 이용할 수 없다. 즉, 각 카드사와의 결제를 위한 제휴를 통해서만 이루어질 수 있다[17].



(그림 4) 애플페이 결제 과정
(Figure 4) Payment process of Apple Pay

2.4 통합 ID를 위한 요구사항

본 논문에서 효율적인 통합 결제/적립시스템을 만들기 위해 위 연구를 분석하여 아래 몇 가지 조건을 만족시켜야 한다[18-19].

- 사용자가 시스템을 로그인/로그아웃 허용 시간만족.
- 결제 과정에서 사용자 입장에서 쉽고 편리.
- 통합을 위한 보안문제는 처리.
- 현 시스템에서 적용 가능한 시스템.
- 현 결제/적립 시스템에서 최소 변경요소.

일반적으로 시스템을 사용하는 사용자들은 많은 시간을 기다려주지 않는다. 그것이 보안적으로 적당히 안전하다하더라도 복잡한 인터페이스 조작과 잦은 지연 시간은 사용자로 하여금 시스템을 사용하지 않게 하는 결과를 초래한다. 그러므로 로그인부터 결제 완료까지의 과정은 쉽고 편리하되 빠른 시간을 보장해야만 한다. 하지만, 빠른 시간과 통합이란 단어는 보안과 반비례한다. 안전한 시스템 통신을 위해서는 신뢰가능한 제 3자 기관을 통하여 각자를 인증하고 암호화를 한 후 데이터를 주고받는 것이 정석이나 이 방법은 지연된 시간을 소요하기 때문에 실시간 결제를 하기엔 적합하지 않다. 반면에 빠른 시간을 중점으로 두고 시스템과 1:1통신을 하게 된다면 서로의 인증하기에 많은 과정이 필요하고 그 인증은 대체적으로 안전하다고 평가하기 어렵다. 따라서 제3자를 통한 인증과 1:1 인증을 적절하게 사용한 인증을 통하여 시간과 보안의 적정선을 찾아 낼 필요가 있다.

3. 통합 아이디 이용 안전한 이동형 지갑 시스템

3.1 카드 등록 단계

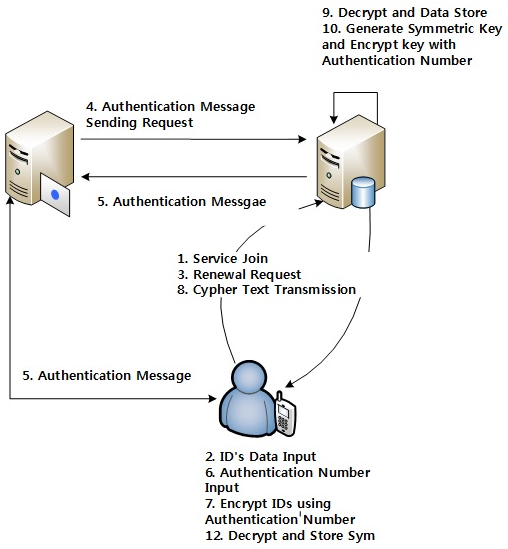
사용자는 결제/적립을 위해 소지한 카드들을 등록하는 사전작업이 필요하다. 카드 등록에 안전함을 위하여 사용자의 휴대폰 통신사를 인증기관 CA로 두고 인증을 진행한다. 사용자는 자신의 카드를 등록하기 위해 IID서버에 등록을 요청하게 되는데 사용자의 ID들은 신용카드의 경우 카드번호, 유효기간, CVS 등이 포함되며, 포인트 카드의 경우 카드번호, 아이디 등이 될 수 있다. 사용자가 자신의 스마트폰 앱에서 자신의 ID들을 입력하고 갱신을 누르게 되면 서버로 갱신 요청이 온다. 이 후 서버는 사용자의 휴대폰 통신사의 서버로 확인 인증 문자 전송을 요구한다. 그와 동시에 사용자의 앱 화면에서는 인증번호를 입력할 수 있는 팝업 창이 뜨게 되고 사용자는 인증번호를 탑재한 문자를 기다려야 한다. 통신 3사는 임의의 문자+숫자 조합으로 사용 가능 시간제한을 둔 인증번호를 만들어 IID서버에 알려주며, 사용자에게 문자로 인증번호를 전송하게 되고, 인증번호를 입력하는 팝업창에 문자로 전송받은 인증번호를 입력하면 사용자의 ID정보들은 인증번호를 통하여 암호화되어 IID서버로 전송한다.

E authenticateNum (IDs)

IID서버는 통신사를 통하여 전송받은 인증번호를 이용해 사용자의 ID를 복호화하여 데이터베이스에 저장하고 추후의 정보 교류를 위하여 Symmetric Key(Sym)값을 선정하여 저장하고 전송받은 인증번호를 통해 암호화하여 사용자에게 암호화된 메세지를 전송한다. Sym을 이용하여 전달되는 정보들은 사용자의 신상, 카드정보, 바코드 등이 될 수 있다.

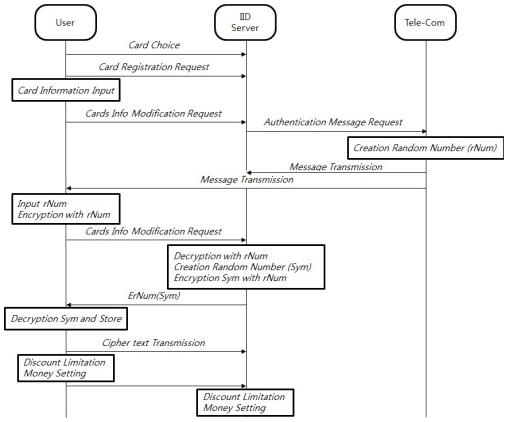
E authenticateNum (sym)

사용자는 기본으로 사용할 카드와 포인트 카드를 등록할 수 있으며, 할인금액이 사용자가 지정한 일정금액이 넘지 않을 시 기본으로 지정한 카드를 자동으로 사용할 수 있도록 한다. 이에 대한 그림은 그림 5과 6에서 알 수 있다.



(그림 5) 서비스 인증 구조도

(Figure 5) The proposed architecture for service authentication

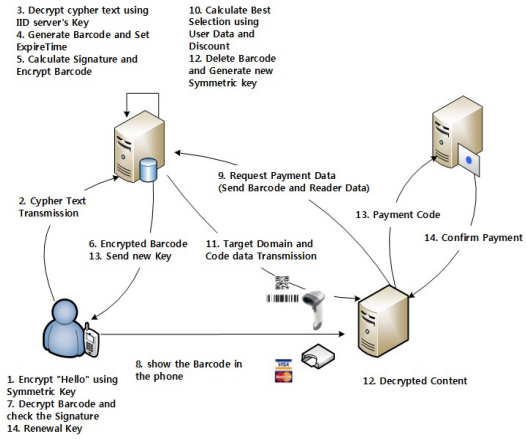


(그림 6) 서비스 인증 흐름도

(Figure 6) Service authentication process of the proposed system

3.2 카드 사용 단계

사용자가 스마트폰의 앱(app)에 접속하면 저장된 대칭키(symmetric key)를 이용하여 'Hello'라는 문자열이 암호화 되어 전송되고, IID서버는 전송된 암호문을 자신이 들고 있는 대칭키를 가지고 복호화하여 해당 키가 유효함을 인증한다. 대칭키로 암호화 된 구문이 복호화가 되지 않으면 사용자 휴대폰의 통신사를 통하여 인증번호를 발급 후 다시 암호화 키를 발급받는다.



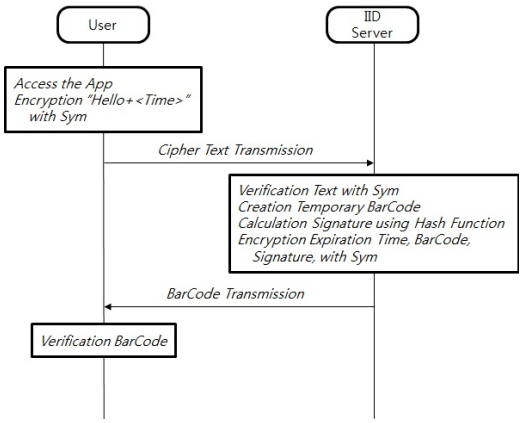
(그림 7) 카드 사용 전체 구조도

(Figure 7) The proposed architecture for card use

대칭키의 유효함이 입증되면, IID서버는 사용자가 쓸 임시적인 바코드 하나를 생성하고 임시적으로 사용하기 위해 만료 시간을 설정한다. 임시적으로 발급된 바코드는 일회용 패스워드(one time password)로 사용되며 만료시간을 두어 안전하게 설계되어있다. 일시적으로 발급된 바코드를 통하여 사용자는 다수의 카드를 물리적으로 제시하지 않고 한 번에 결제와 적립을 받을 수 있다. 앱을 구동하면 사용자의 별다른 수고 없이 자동적으로 발급되어 보이는 바코드로 한 번의 인식만으로 결제/적립이 되므로 사용자 편의성이 높아진다. 사용자에게 생성된 바코드를 전송하기 전에 바코드에 대한 시그니처(signature) 값을 계산하고 바코드와 함께 암호화 하여 만료시간과 전송한다.

$$E\ sym\ (\ BarCode\ ||\ Signature\ )\ ||\ ExpirationTime$$
$$Signature\ =\ H\ (\ BarCode\ )$$

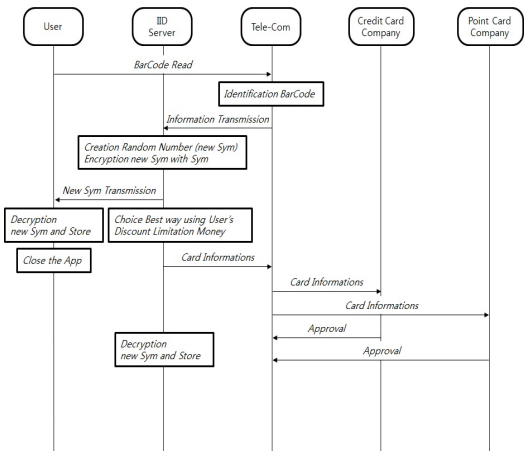
시그니처는 바코드가 전송 상에서 훼손되거나 악의적인 타인에 의해 교환될 경우를 대비하여 설계되었다. 사용자의 앱에서 저장하고 있던 대칭키를 이용하여 전송된 바코드를 복호화 한 후, 유효한 바코드인지 시그니처를 확인하고 화면에 띄워 사용자가 결제 및 적립을 할 수 있게 한다.



(그림 8) 통합 ID와 앱간 인증 흐름도
(Figure 8) Authentication process between Integrated ID and the application

3.3 카드 결제 단계

사에서 제시하는 바코드 결제는 사용자가 등록한 신용카드나 포인트 카드를 한 번의 바코드 읽기와 사용자의 다른 수고스러움을 없애기 위해 단 방향(one-way)로 진행한다. 앱에서는 사용자가 미리 할인고려 금액을 설정해 놓을 수 있는데, 할인 고려 금액을 통해 계산하여 각 카드사의 할인과 적립률을 자동적으로 계산해 최선의 방법으로 최대의 효과를 누릴 수 있는 카드가 결제 및 적립될 수 있다.



(그림 9) 카드 결제 흐름도
(Figure 9) The payment process of the proposed system

사용자는 물건 구매를 위해 점원에게 화면을 공개하고 점원을 해당 바코드를 바코드(barcode) 리더기를 이용하여 읽고 리더(Reader) 서버는 해당 바코드의 정보를 식별하여 IID 서버에 전송한다. IID 서버는 전송된 바코드에 대한 정보를 전송 받아 해당 가게에서 사용자가 이용할 수 있는 할인과 적립에 관한 데이터를 이용하여 최저가를 계산한다.

- 기본으로 설정된 신용카드와 포인트 카드로 결제 및 적립 : 기본 설정된 IDs의 가격 - 할인이 계산된 최저가 < 할인받기를 거부한 금액
- 최대로 할인된 가격의 신용카드와 포인트카드로 결제 및 적립 : 기본 설정된 IDs의 가격 - 할인이 계산된 최저가 >= 할인받기를 거부한 금액

타겟 도메인(target domain : 신용 혹은 체크카드회사, 포인트회사 등)이 결정되었으면 리더서버에 타겟 도메인들과 카드 Code를 전송한다. 결제를 위한 바코드가 사용이 완료되었으므로 만료시간이 남았더라도 임시 생성된 바코드를 삭제하여 악의적인 타인의 결제를 제한한다. 또한, 추후 사용될 Sym을 갱신하여 보안을 견고히 할 수 있다.

$$E\ sym\ (\ newSym\ )$$

사용자가 인식하지 못하는 사이 보내진 새로운 대칭키(new Sym)는 기존의 대칭키(Sym)를 삭제한 채 저장된다. 결제가 완료되기 전에 미리 키를 업데이트 하는 이유는 일반적인 사용자는 바코드가 찍히는 순간 결제가 완료되었다고 인식하고 앱을 꺼버리기 때문이다. 그 후, 리더서버는 카드 회사에 결제 및 적립 처리를 요청하고, 카드 회사, 타겟 도메인,들은 카드 정보를 기반으로 사용자의 정보를 식별하고 결제 및 적립을 처리 한 후 리더 서버에 결제 완료를 통보한다.

4. 제안한 시스템 분석

다음은 제안하는 시스템의 보안 공격에 대해 서술한다. 보안 공격은 중간자 공격, 추측 공격, 위장공격, 재전송 공격이 있다.

4.1 중간자 공격 분석

중간자 공격 (Man-in-the-middle attack)이란, 네트워크에서 두 노드의 통신 내용을 조작하여 도청하는 보안 공격 기법이다. 만약 두 노드가 서버와 클라이언트 통신일 경우, 공격자가 두 노드의 통신 사이에 침입하여 서로 연결되어 있지만 공격자를 통해 연결 되어 있으며, 공격자는 주고받는 통신 내용을 변조하거나 도청할 수 있다. 제안하는 시스템에서는 사용자와 IID Server 간의 통신인 경우, 반드시 Tele-Com 과의 인증이 필요하다. 그러므로 중간자 공격을 성공할 수 없다.

4.2 추측 공격 분석

추측 공격(Guessing attack)이란, 공격자가 통신 내용을 이용하여 사용자의 인증정보의 추측하는 것이다. 사용자의 인증정보는 패스워드, 개인 키, 인증 답변 등이 될 수 있다. 제안된 시스템에서의 인증정보는 바코드이다. 이 바코드는 일시적으로 발행하여 일회용 비밀번호를 사용하므로, 인증정보인 일시적인 바코드 정보를 추측 할 수 없다. 그러므로 공격자는 추측 공격을 할 수 없다.

4.3 위장 공격 분석

위장 공격 (Impersonation attack)이란, 공격자가 통신상에서 도청하거나 변조한 메시지를 이용하여 정당한 사용자로 위장하여 공격하는 기법이다. 제안하는 시스템에서는 이전 세션에서 사용된 인증 메시지를 훔치거나 변조하더라도, 공격자는 다른 세션에서 사용할 수 없다. 왜냐하면 인증정보인 바코드는 인증 요청하여 생성될 때 만료시간을 설정하며, 사용한 후에는 만료시간 시간이 지났으므로 지난 세션에서 이용한 인증 정보는 다시 재사용할 수 없다. 그러므로 제안된 시스템에서는 공격자가 위장공격을 할 수 없다.

4.4 재전송 공격 분석

재전송 공격 (Replay attack)이란, 공격자가 현재 세션에서 메시지를 저장한 후, 나중에 메시지를 다시 보내 정당한 사용자로 가장하는 공격방법이다. 제안된 시스템에서 인증 정보인 바코드는 무결성을 위해 해쉬 함수를 이용하여 바코드의 시그니처를 만들고 일시적으로 만료시간을 설정하여 생성된 세션에서만 유효하도록, OTP(One Time Password)와 같은 역할을 한다. 만약 이미 만료시간이 경과된 바코드의 시그니처를 포함된 메시지를 이용하여 사용자가 시도(challenge)를 할 경우, 서버는 받은 메시지가 해당 세션에서 유효하지 않기 때문에 거절(reject)한다. 그러므로 제안된 시스템에서는 재전송 공격을 할 수 없다.

4.5 제안한 시스템 요구 시간 분석

요구사항에서 언급하였듯이 통합적인 시스템으로 보안적으로 안정되어야 하며 그와 동시에 일반적으로 시스템을 사용하는 사용자들은 많은 시간을 기다려주지 않는다. 하지만 반대로 복잡한 인터페이스 조작과 잦은 지연시간도 사용자로 하여금 시스템을 사용하지 않도록 하는 결과를 초래한다. 제안하는 시스템은 이러한 시간적인 문제와 보안 문제를 적절히 해소하고 있다.

일시적인 바코드의 발행과 일회용 비밀번호를 사용함으로써 프로그램의 보안성을 높이는 한편, 통신사를 통한 신뢰성 있는 제 3자 파티(party)를 결성하여 빠른 시간과 보안성을 동시에 충족하고 있다. 매 통신시마다 일회용 비밀번호인 대칭키 키 값을 갱신함으로써 연관성 없는 키 체인이 만들어지고, 키가 일치하지 않을 경우 보안을 위하여 통신사와의 재인증 과정을 거쳐 통신의 무결성을 만족하고 있다.

또한, 일시적인 바코드의 무결성을 인증하기 위하여 해쉬 함수를 통하여 바코드의 시그니처를 만들고 일시적인 바코드의 만료시간을 설정하여 통신상의 스니핑, 스푸핑을 방지하고 사용자의 신용정보가 타인에 의해 재사용되는 경우를 막았으며 전송되는 바코드 또한 일회용 비밀번호로 암호화되어 이중적으로 보안을 강화하고 있다.

그뿐만 아니라, 일반적으로 공인된 제 3자를 통해 인증서를 발행하고 서로의 인증서를 확인하는 방법 대신 모바일에서 사용하는 통신사를 제 3자로 두어 USIM을 가지고 사용자를 바로 식별하는 방법을 사용하여 적은 시간으로 안전한 보안을 이끌어냈다. 또한, 신용카드와 포인트카드의 결제와 적립에 드는 다수의 시간과 사용자 측에서 부담하였던 여러 번의 번거로운 작업 대신 한 번의 바코드 읽기를 통하여 결제까지 단 방향(One-way)으로 진행되는 일련의 과정을 통해 사용자의 시간적, 물리적 번거로움이 크게 해소될 것이다.

(표 1) 평균 암호 연산 경과 시간

(Table 1) The average operation time code

암호적 연산	표기	소요 시간(㎲)
AES-256 Encryption	E.AES	156
AES-256 Encryption	D.AES	118
Hash Function - HMAC-SHA-256	H	20
RSA-1024 Public Key Encryption	E.RSA	110,000
RSA-1024 Public Key Dncryption	D.RSA	2,070,000
ECDSA-160 Sign Generation	G.ECDSA	930,000
ECDSA-160 Sign Verification	V.ECDSA	1,105,000

(표 2) 연산 오버헤드 비교

(Table 2) Compared to operation time code of IDA-Pay and the proposed method

시스템		암호적 연산	평균오버헤드(㎲)
Proposed	Card Reg. Step	2E.AES 2D.AES 2E.RSA 2D.RSA	4,360,548
	Access App Step	2E.AES 2D.AES 2H 1G.ECDSA 1V.ECDSA	2,035,588
	Payment Step	5E.AES 5D.AES	1,370
IDA -Pay	Card Reg. Step	1E.RSA 1D.RSA 1E.AES 1D.AES	2,180,274
	Access App Step	1E.AES 1D.AES	274
	Payment Step	2E.AES 2D.AES 2E.RSA 2D.RSA	4,360,548

(표 3) 결제 시스템 복잡성

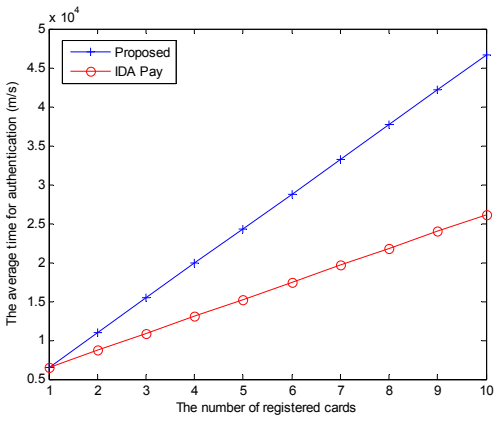
(Table 3) Complexity of payment system

		제안시스템	IDA-Pay	Smart Wallet
Card Reg.	SMS 인증	O(1)	O(n)	O(n)
	통신	O(n)	O(n)	O(n)
Access App	사용자 조작	O(1)	O(1)	O(1)
	통신	O(1)	O(1)	O(1)
Payment	사용자 조작	O(1)	O(1)	O(1)
	통신	O(1)	O(1)	O(1)

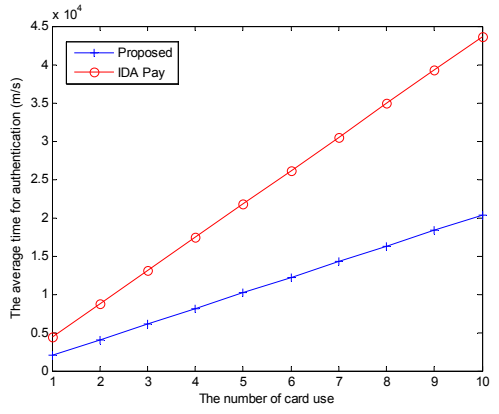
표 1은 암호적인 연사 경과 시간을 수치로 나타낸 값을 보여준다[20]. 우리는 이 값을 이용하여 제안한 시스템과 IDA-Pay와의 비교를 표 2에서 나타내었다. 제안한 시스템은 카드 등록 절차에 소요되는 시간이 IDA-Pay보다 2배 이상의 시간을 소요하고 있다. 하지만, 일반적으로 카드 등록은 사용자가 카드 등록을 위해 허용 할 수 있는 시간이 준비되어 있다고 가정하기 때문에 이러한 시간 차이는 충분히 보안할 수 있는 방안이다. 반면에 앱 접근 시간은 제안된 방법이 소요시간이 길다. 이유는 앱에 접근할 경우 새롭게 암호화된 통합카드를 위한 바코드 생성에 소요되기 때문이다. 하지만 실제 결제 단계에서는 제안한 방법이 3,000배 이상 빠른 결과 값을 보이는 것을 알 수 있다. 즉, IDA-Pay 같은 경우 카드 등록과 같은 시간의 결제 단계가 필요하기 때문이다.

그림 10에서와 같이 카드 등록에 소요되는 시간이 제안된 시스템 보다 IDA 방식이 카드 등록 수에에 비례하여 소요시간이 짧다. 하지만 충분한 시간적 여유를 가지고 미리 진행되는 작업인 카드 등록의 경우를 고려하면 사용자는 실제 카드 사용에 있어서 이러한 시간을 감수할 수 있다. 따라서 어플리케이션의 실행과 결제까지 걸리는 시간을 비교하면 그림 11과 같이 그림 10의 결과와는 반대로 시간적인 차이가 발생하고 이는 카드 사용의 빈도가 높을 경우에 그 차이가 더욱 더 벌어지는 것을 알 수 있다.

제안한 시스템, IDA-Pay 그리고 스마트 월렛과의 복잡도를 살펴보면 모든 부분에서 동일한 복잡도를 가지지만 sms 인증을 통한 방법에서 보다 나은 복잡도를 보임을 볼 수 있다.



(그림 10) 카드 등록에 따른 소요시간 비교
(Figure 10) Compared to the average time for authentication by card registration



(그림 11) 카드 사용에 따른 소요시간 비교
(Figure 11) Compared to the average time for authentication by card use

5. 결 론

시스템은 안전하고 편리한 단방향 결제/적립 시스템에 대해서 제안하고i 있다. 이러한 시스템을 이용하게 되면 한 번의 바코드 발급으로 결제와 적립을 모두 처리하고 최적의 경우로 결제가 되므로 사용자의 편의성을 효과적으로 높여준다. 또한 통신사를 인증기관으로 사용하여 별다른 인증서 발급이나 확인 없이 서로 비밀키를 생성하고 갱신할 수 있으므로 보안성을 보장할 수 있다. 또한 바코드에 대한 만료시간(expiration time)을 설정하여 결재될 때마다 새로운 바코드를 다시 생성함으로 결제에 대한 재사용 공격이 및 무작위 공격(Brute Force Attack)이 불가능하고, 공격자는 만료시간 내에 키 값을 계산할 수 없기 때문에 시간적으로 보안을 보장할 수 있다. 이러한 이유로 제안하는 메커니즘은 위에서 요구되는 조건을 만족하는 시스템을 제공한다.

참 고 문 헌 (Reference)

[1] Smart wallet : Google Patent
http://www.google.com/patents/US20110320345

[2] C. Benninger, “A Brave New Wallet – First look at decompiling Google Wallet,” Intrepidus Group Insight,Sep. 2011,
http://intrepidusgroup.com/insight/2011/09/a-brave-new-wallet-first-look-at-decompiling-google-wallet/

[3] OpenID.net: OpenID Specifications,
http://openid.net/developers/specs/

[4] Luca Mainetti, Luigi Patrono, and Roberto Vergallo, “IDA-Pay: a secure and efficient micro-payment system based on Peer-to-Peer NFC technology for Android mobile devices”, Journal of Communications Software & Systems. Vol. 8 Issue 4, Dec2012, pp 117-125.
http://connection.ebscohost.com/c/articles/87531092/ida-pay-secure-efficient-micro-payment-system-based-peer-to-peer-nfc-technology-android-mobile-devices

[5] Lishoy Francis, Gerhard Hancke, Keith Mayes, Konstantinos Markantonakis, “Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones”. Radio Frequency Identification: Security and Privacy Issues, 2010. pp. 35-49.
http://dx.doi.org/10.1007/978-3-642-16822-2_4

[6] Michael Roland, Josef Langer, Josef Scharinger, “Applying relay attacks to Google Wallet”, IEEE 5th NFC International Workshop, 2013.
http://dx.doi.org/10.1109/NFC.2013.6482441

[7] Andreas Leicher, Andreas U. Schmidt, Yogendra Shah, “Smart OpenID: A Smart Card Based OpenID Protocol”, 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete,

Greece, June 4-6, 2012. Proceedings, pp 75-86. http://dx.doi.org/10.1007/978-3-642-30436-1_7

[8] David Recordon, Drummond Reed, “OpenID 2.0: a platform for user-centric identity management”, DIM ’06 Proceedings of the second ACM workshop on Digital identity management, 2006, pp. 11-16. http://dx.doi.org/10.1145/1179529.1179532

[9] Tsyrklevich, E., Tsyrklevich, “V.: Single Sign-On for the Internet: A Security Story, BlackHat Conference Las Vegas, 2007. http://amifan.googlecode.com/svn-history/r94/trunk/bh-usa-07-tsyrklevich-WP.pdf

[10] Urien, P.: Convergent identity: Seamless OpenID services for 3G dongles using SSL enabled USIM smart cards. In: Consumer Communications and Networking Conference (CCNC), 2011, pp. 830 – 831. http://dx.doi.org/10.1109/CCNC.2011.5766616

[11] Pascal Urien, “An OpenID Provider based on SSL Smart Cards”, CCNC’10 Proceedings of the 7th IEEE conference on Consumer communications and networking conference, 2010, pp 444-445. http://dl.acm.org/citation.cfm?id=1834318

[12] 3GPP TS 33.220; “Generic Authentication Architecture (GAA). Generic Bootstrapping Architecture(GBA)”, 2006. http://www.etsi.org/deliver/etsi_tr/133900_133999/133919/06.02.00_60/tr_133919v060200p.pdf

[13] 3GPP: 3G security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP), 2009. http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/old_vsns/33102-3b0.pdf

[14] Liberty Alliance: ID-WSF Advanced Client Implementation and Deployment guidelines for SIM/UICC Card environment. Technical report, 2007. http://www.projectliberty.org/resource_center/specifications/?f=resource_center/specifications

[15] Rao, T. Venkat Narayana, and K. Vedavathi. ″Authentication Using Mobile Phone as a Security Token.″ International Journal of Computer Science and Engineering Technology, IJCSET 1.9, 2011, pp. 569-574. http://ijcset.net/docs/Volumes/volume1issue9/ijcset2011010908.pdf

[16] Seung-Hyun Seo, ″One-Time Virtual Card Number Generation & Transaction Protocol using Integrated Authentication Center″,Journal of the Korea Institute of Information Security and Cryptology, Vol 20, no 3. 2010, pp. 9-21. http://www.koreascience.or.kr/article/ArticleFullRecord.jsp?cn=JBBHCB_2010_v20n3_9

[17] Apple Inc, “Getting Started with Apple Pay – Version 1.0”, 2014. https://developer.apple.com/apple-pay/Getting-Started-with-Apple-Pay.pdf

[18] Félix Gómez Mármol, Marcus Quintino Kuhnen, Gregorio Martínez Pérez, “Enhancing OpenID through a Reputation Framework”, 8th International Conference, ATC 11’, Banff, Canada, Proceedings, Sep 2011, pp. 1-18. http://dx.doi.org/10.1007/978-3-642-23496-5_1

[19] Supakorn Kungpisdan, Bala Srinivasan, Phu Dung Le, “Lightweight Mobile Credit-Card Payment Protocol”, 4th International Conference on Cryptology in India, New Delhi, India, Dec 2003, pp. 295-308. http://dx.doi.org/10.1007/978-3-540-24582-7_22

[20] Martínez-Peláez, Rafael, et al. ″Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network.″ 6th COLLECteR Iberoamerica (2008). https://scholar.google.co.kr/scholar?q=Performance+Analysis+of+Mobile+Payment+Protocols+over+the+Bluetooth+Wireless+Network&btnG=&hl=en&as_sdt=0%2C5

◐ 저 자 소 개 ◑

남 춘 성 (Choon-Sung Nam)
2005년 상명대학교 소프트웨어학과(이학사)
2007년 숭실대학교 대학원 컴퓨터학과(공학석사)
2011년 성균관대학교 대학원 전자전기컴퓨터학과(공학박사)
2014년 ~ 현재 연세대학교 IT정책전략연구소 박사후연구원
관심분야 : 센서네트워크, VANET, IoT etc.
E-mail : namgun99@gmail.com

전 민 경 (Min-Kyung Jeon)
2011년 경성대학교 컴퓨터공학과(공학사)
2014～현재 성균관대학 대학원 전자전기컴퓨터학과 석사과정
관심분야 : 네트워크 보안, 유비쿼터스 컴퓨팅, etc.
E-mail : mkjeon031@gmail.com

신 동 렬 (Dong-Ryeol Shin)
1980년 성균관대학교 전자공학과(공학사)
1982년 KAIST 대학원 전기 및 전자공학과(공학석사)
1992년 Georgia Tech, 대학교 전기 및 전자공학과(공학박사)
1994년～현재 성균관대학교 정보통신공학과 교수 .
관심분야 : 유비쿼터스 컴퓨팅, 센서 네트워크 etc.
E-mail : drshin@skku.edu