QR코드와 추가인증서를 이용하는 간편결제 웹서비스

윤정민, 박종훈, 권혁민, 마민기, 이병천

중부대학교 정보보호학과

Easy Payment Web Service Using QR code and Additional Certificates

Jeongmin Yoon, Jonghun Park, Hyukmin Kwon, Mingi Ma, Byoungcheon Lee

Division of Information Security, Joongbu University

요 약

현재 널리 사용되는 결제방식은 공인인증서 기반의 전자서명 결제와 휴대폰에 모바일 간편결제 앱을 설치하여 사용하는 등의 방법이 이용되는데, 편의성 때문에 모바일 간편결제로 시장이 이동하고 있다. 공인인증서 기반의 전자결제는 사용자가 다수의 결제서비스를 이용하거나 복수의 컴퓨팅 기기들을 사용하게 되는 실제 환경에서는 인증서 관리가 복잡하다는 단점이 있고, 모바일 간편결제는 부인방지 서비스의 기본인 인증서를 사용하지 않고 앱과 서비스의 신뢰성에 크게 의존한다는 단점이 있다. 본 논문에서는 이 두 가지 접근방법을 모두 포괄하는 인증서 기반 간편결제 모바일 웹서비스를 개발하였고 이의 상용화 타당성을 검토하였다. 이 서비스에는 이중토큰을 이용한 인증유지, 추가인증서를 이용한 인증서 발급 및 관리, QR코드를 이용한 리다이렉트 결제 등의 기능을 포함하여 사용자는 어떤 환경에서도 표준 웹브라우저만을 이용하여 편리하게 간편결제를 사용할 수 있도록 하였다.

I. 서론

현재 널리 사용되는 결제방식은 공인인증서 기반 전자서명 결제와 모바일 간편결제의 두 가지 방식으로 나누어 볼 수 있는데, 사용자 편의성 문제로 공인인증서 사용을 지양하고 모바일 간편결제로 시장이 크게 이동하고 있다.

첫째, PC 환경에서 공인인증서를 이용한 전자서명 결제방식에서는 인증서를 활용할 수 있도록 인증서 관련 플러그인 프로그램을 브라우저에 설치하여야 하는데 이 경우에는 비표준 플러그인 프로그램을 설치해야 한다는 점, 인증서를 관리하기 어렵다는 점에서 많은 불편함이 있다. 특히 사용자가 하나의 공인인증서를 여러 컴퓨터에 복사하여 사용하는 것이 불편하기도 하고 보안성이 취약하다는 점이 비판되고 있다. 이런 이유로 인증서를 사용하지 않는 모바일 간편결제 서비스로 시장이 이동하고 있다.

둘째, 모바일 앱을 이용하는 모바일 간편결제 방식은 부인방지 서비스의 기본인 인증서를 사용하지 않고 앱과 서비스의 신뢰성에 크게 의존해야 한다는 단점이 있다.

한편 사용자가 여러 대의 컴퓨팅 기기, 모바일 디바이스를 사용하는 경우에는 인증서 및 인증키의 관리에 불편함이 있다. 이를 해결하기 위한 방식으로는 첫째, 하나의 디바이스에 인증키를 안전하게 관리하고 다른 컴퓨터를 이용하게 될 때는 결제를 안전한 디바이스로 리다이렉트 하여 결제하도록 하는 방식이 금융권을 중심으로 널리 개발되고 있다. 두 번째 방식으로는 하나의 마스터 디바이스에 마스터인증서를 인증기관으로부터 발급받고 추가 기기에는 사용자가 직접 추가인증서를 발급 및 관리하여 복수의 디바이스로도 인증서 기반의 결제를 수행하도록 하는 방식이 제안되었다[2,3].

이 논문에서는 QR코드를 이용하여 결제를 리다이렉트하여 수행하는 방식과 추가인증서를 이용하여 어느 디바이스를 사용하더라도 인증서 기반의 결제를 가능하도록 하는 기능을 함께 웹서비스로 구현하는 사례를 제시한다. 사용자는 모바일 디바이스에 특정 앱을 설치하지 않고도 표준 웹브라우저를 이용하여 인증서 기반의 결제를 진행할 수 있게 되었다. 이

러한 서비스의 운영 사례를 기반으로 이러한 기술의 상용화 타당성을 검토한다.

II. 관련연구

2.1 기존의 간편결제 서비스

현재 국내외적으로 많은 간편결제 서비스들이 개발 및 서비스되고 있다. 국내 서비스로는 카카오페이, 삼성페이, 네이버페이, 페이코 등이 있고 국외 서비스로는 애플페이, 알리페이, 위챗페이 등이 있다. 이들 서비스는 사용 기술 및 기능들이 각기 다르지만, 부인방지의 기반이 되는 기술인 인증서를 사용하지 않고 사용자에게 편의성을 제공하는 간편결제 서비스를 추구하고 있다는 공통점이 있다.

2.2 이중토큰을 이용한 인증유지 [1]

OAuth2.0, JWT(JSON Web Token) 방식의 토큰 인증은 서버가 인증된 클라이언트에게 발급하는 토큰을 서비스 요청 시 서버에 반복해서 전송하여 인증상태를 유지하는 방식을 사용하는데 이것은 도청 공격에 취약하므로 HTTPS와 같은 보안통신 기술과 함께 사용되어야 한다는 제약이 있다.

이중토큰을 이용한 인증유지 기술은 보안통신 채널을 이용하지 않고도 안전한 무상태 인증을 제공할 수 있도록 개선한 토큰인증 기술이다. 사용자가 서버에 초기인증에 성공하면 서버는 추후 인증을 위해 사용자에게 공개토큰과 비밀토큰의 쌍을 발급한다. 공개토큰은 사용자 정보 및 유효기간에 서버의 HMAC 서명 값을 포함하는 토큰인데 이것은 인증된 사용자임을 나타내기 위해 서버에 반복적으로 전송하는 정보로서 서명된 ID와 같은 역할을 한다. 비밀토큰은 사용자의 공개토큰에 대해 서버의 HMAC 서명이 포함된 토큰으로 외부로 노출되지 않고 일회용 인증정보 계산에만 사용하는 정보로서 서명된 패스워드와 같은 역할을 한다.

클라이언트가 서버에 인증요청 시 현재 시각과 비밀토큰을 이용하여 일회용 인증정보를 계산하고 <공개토큰, 현재시간, 일회용 인증정보>를 서버로 전송하게 된다. 서버는 사용자의 공개토큰으로부터 사용자의 비밀토큰을 계산하게 되고 일회용 인증정보의 유효성을 검증하여 클라이언트를 인증하게 된다. 이러한 방식은 서버가 사용자의 비밀토큰을 유지, 관리할 필요가 없어서 무상태 인증이 가능하고 현재 시각에 기반한 일회용 인증정보는 재사용할 수 없어서 보안통신을 사용하지 않아도 안전하다는 장점이 있다.

2.3 추가인증서를 이용한 인증확장 [2,3]

사용자가 복수의 컴퓨팅 기기들을 사용하게 되는 경우 인증서 기반의 전자서명을 사용하기 위해서는 하나의 인증서를 여러 대의 컴퓨팅 기기들에 복사하여 사용하는 것이 지금까지의 일반적인 방법이었으나 인증서와 개인키를 복사하여 사용하는 것은 불편하기도 하고 매우 위험한 일이다. 추가인증서를 이용한 인증확장 방식은 사용자가 하나의 인증기관으로부터 발급받은 하나의 마스터인증서를 기반으로 스스로 필요한 만큼 추가인증서를 발급하여 사용할 수 있도록 하는 방식이다.

마스터인증서는 서버가 인증된 사용자의 마스터 컴퓨터에 최초로 발급해주는 인증서이다. 다른 컴퓨터에서도 인증서를 사용할 필요가 있는 경우 사용자는 자신의 마스터인증서로 추가인증서를 직접 발급 및 배포하여 사용할 수 있다. 사용자는 자신이 발행하여 사용하고 있는 추가인증서의 현황을 확인하고 삭제 및 비활성화할 수 있어야 한다.

2.4 QR코드를 이용한 결제정보 리다이렉트

QR코드는 1차원 바코드와는 다르게 숫자로는 최대 7098자의 많은 데이터를 담을 수 있고, 오류 정정 기능 및 디자인 분야에서도 많은 이점을 가지고 있어서 직접 대면한 환경에서 정보를 직접 전달하는 용도에 매우 유용하다. 중국의 Alipay, Wechatpay에서는 QR코드를 카메라로 인식하면 결제로 연동되도록 하여 간편결제 서비스로 크게 성공하였다.

III. 간편결제 웹서비스 개발

3.1 시스템 개요

우리는 QR코드를 이용하여 결제페이지를 리다이렉트 하는 간편결제 기능, 인증서를 사용한 전자서명 결제, 복수의 기기들을 이용하는 때도 추가인증서를 이용한 인증서 관리 기능, 이중토큰을 이용한 인증유지 기능을 가지는 전자결제 웹서비스를 개발하는 것을 목표로 하였다. 사용자는 여러 대의 컴퓨터에 발급한 추가인증서를 이용하여 직접 전자서명 결제를 할 수도 있고, QR코드를 이용하여 결제정보를 다른 모바일 디바이스로 리다이렉트하여 전자서명 결제를 하도록 할 수도 있다.

이러한 웹서비스를 구현하기 위하여 다음의 [표 1]에 표시한 것과 같은 기술들을 사용하였다.

[표 1] 사용된 구현 기술

분야	기술
back-end	node.js, express
front-end	vue.js
DB	MySQL
cloud service	Heroku
암호 라이브러리	node-forge, bcrypt
토큰인증	jwt

현재 구현된 모델 서비스에서는 MySQL DB에 다음과 같은 테이블들이 운영된다.

- 사용자정보 테이블: 등록된 사용자 정보 관리
- 인증서 테이블: 사용자에게 발급하는 마스터인증서 및 추가인증서를 저장
- 장바구니 테이블: 사용자가 선택하는 상품을 저장
- 결제정보 테이블: 사용자가 결제한 정보를 저장
- 영수증 테이블: 판매자가 결제정보에 대해 서명한 영수증을 저장

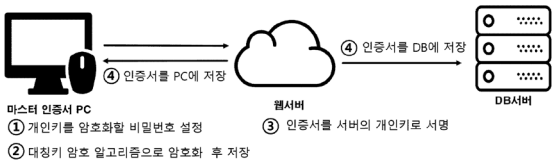
3.2 사용자등록, 로그인 및 인증유지

사용자는 서버에 계정을 등록할 수 있다. 사용자는 가입된 계정으로 아이디, 패스워드를 입력하고 로그인에 성공하게 되면 서버는 향후의 인증유지에 사용하기 위한 공개토큰과 비밀토큰의 쌍을 발급한다. 사용자의 컴퓨터는 브라우저의 로컬스토리지에 공개토큰과 비밀토큰을 저장한다. 이때 서버는 사용자에게 발급한 토큰들을 저장할 필요가 없다.

로컬스토리지에 공개토큰과 비밀토큰이 저장되어 있으면 로그인된 상태가 유지된다. 로그인된 상태에서 클라이언트가 서버에 서비스를 요청할 때에는 비밀토큰과 현재 시각을 이용하여 일회용 인증정보를 생성하고 이것을 현재시간, 공개토큰과 함께 서버에 전송한다. 서버는 공개토큰으로부터 비밀토큰을 계산하고 일회용 인증정보의 유효성을 검증한 이후 유효한 경우에만 서비스를 제공한다. 이 토큰은 유효기간이 설정되어 있는데 유효기간 이내에는 다시 로그인할 필요 없이 로그인된 상태를 유지하는데 토큰의 유효기간이 지나면 서버는 다시 로그인할 것을 요구하게 된다.

3.3 마스터인증서와 추가인증서 발급과 관리

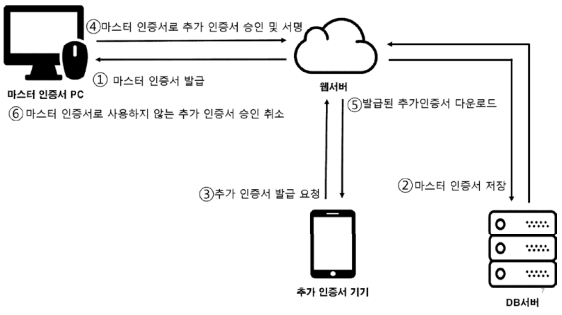
회원가입 후 처음 로그인에 성공하면 사용자는 서버에게 마스터인증서 발급을 요청할 수 있다. 마스터인증서를 발급받은 기기는 사용자의 마스터기기가 되며 사용자는 이것을 안전하게 관리하여야 한다. 마스터인증서는 브라우저의 로컬스토리지에 저장되며 개인키는 패스워드로 암호화하여 로컬스토리지에 저장된다.



[그림 1] 마스터인증서 발급

사용자가 또 다른 추가 컴퓨팅 기기에 추가인증서를 발급하여 사용하고자 하는 경우 추가 기기에서 로그인한 후 추가인증서 발급 신청을 할 수 있고 신청내역은 서버의 DB에 저장된다. 이때 사용자 아이디 이외에 기기를 구별하기 위한 기기 아이디 정보를 입력하게 된다. 이후 동일 사용자는 마스터기기로 로그인하여 신청내역을 검색할 수 있고 추가인증서 발급을 승인하여 추가인증서를 발급한다. 추가인증서는 마스터인증서의 개인키로 서명한 개인용 인증서가 된다. 동일 사용자는 추가 기기에서 서비스에 다시 접속하면 추가인증서 발급 내역을 검색할 수 있고 기기에 인증서를 다운로드하게 된다. 추가인증서 및 개인키는 브라우저의 로컬스토리지에 저장된다.

사용자는 서버에 로그인하면 인증서 관리 메뉴를 통해 자신의 인증서 발급 내역을 검색할 수 있고 기기 분실 및 고장 등으로 인해 추가인증서를 사용하지 못하게 되는 경우 해당 추가인증서를 삭제 또는 비활성화할 수 있다. 그러므로 사용자는 자신이 사용하는 마스터인증서 및 추가인증서의 내역을 언제든지 검색해볼 수 있고 직접 관리할 수 있어서 관리의 편의성과 안전성을 확보할 수 있다.



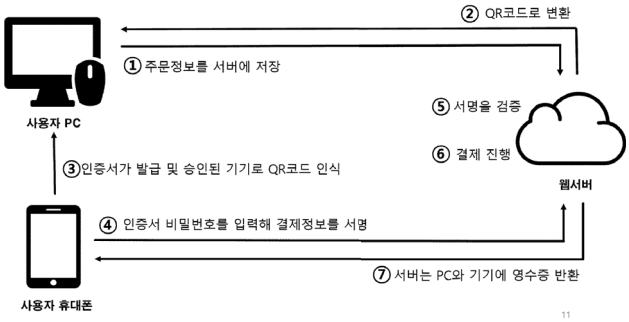
[그림 2] 추가인증서 발급 절차

3.4 상품 구매 및 결제 절차

사용자는 구매할 상품들을 선택하여 구매 버튼을 누르면 클라이언트는 구매요청 정보를 웹서버로 전송하고, 서버는 지불요청 페이지를 표시하게 된다. 사용자는 현재 사용 중인 기기에서 마스터인증서 또

는 추가인증서를 이용하여 직접 전자서명 지불을 할 수도 있고 또 다른 추가인증서가 장착된 휴대폰으로 QR코드를 스캔하여 지불정보를 휴대폰으로 리다이렉트하여 전자서명 지불을 할 수도 있다.

[그림 3]은 QR코드를 이용하여 결제를 휴대폰으로 리다이렉트하여 수행하는 대표적인 결제 시나리오를 보여준다.



[그림 3] QR코드 방식의 결제 시나리오

사용자가 상품을 선택해 구매요청을 하면 주문정보를 서버로 보내 서버에서는 DB에 주문정보를 만들고 결제 여부에 False를 넣는다. 서버에서는 주문정보에서 주문번호를 추출하여 <주문정보, 현재시간>을 전달하기 위한 QR코드를 만들어 화면에 표시한다. 사용자는 로그인된 스마트폰으로 해당 쇼핑몰의 모바일 페이지의 결제페이지로 이동하여 카메라를 활성화하고 QR코드를 인식하면 주문정보와 결제정보가 스마트폰의 화면에 나타난다. 사용자가 결제승인 버튼을 누르면 스마트폰에 발급된 추가인증서를 이용하여 결제정보에 서명하고 서버에 전송한다. 서버가 결제를 검증하여 정상으로 판정되면 결제 완료 페이지로 리다이렉트한다.

3.5 구현 및 데모

1) 서비스 운영: 현재 구현된 모델 서비스는 클라우드 PaaS인 Heroku에 포팅하여 다음의 주소에서 서비스되고 있다.

https://coconutpay.herokuapp.com/

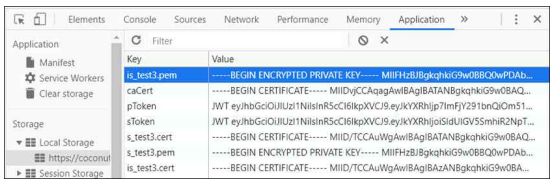
2) 인증 및 로그인: 사용자 가입 후 성공적으로 로그인하면 [그림 4]에 보인 바와 같이 서버가 발급한 이중토큰이 브라우저의 로컬스토리지에 저장된다. 이 상태가 되면 사용자는 다시 로그인할 필요 없이 토큰의 유효기간(현재 7일) 동안 로그인된 상태로 유지되며 서버를 이용할 수 있다.

[그림 4] 로컬스토리지에 저장된 이중토큰

3) 인증서 발급 및 관리: 로그인한 사용자는 '인증센터'를 통해 마스터 PC에서 마스터인증서를 발급받을 수 있고, 동일한 아이디로 다른 기기에서 로그인하면 '추가인증서 발급'을 신청할 수 있다. [그림 5]에 보인 바와 같이 추가인증서 발급 신청을 하면 동일한 사용자는 마스터 PC에서 '인증서 관리' 메뉴를 통해 승인 버튼을 누르면 추가인증서가 발급되며, 동일 사용자는 추가 기기에서 이것을 다운로드하여 사용하게 된다. 또한, 이미 발행하여 사용하던 추가기기의 추가인증서를 사용하지 않고자 할 때는 [그림 6]의 '인증서 관리' 메뉴를 통해 해당 인증서를 비활성화할 수 있다. [그림 7]는 브라우저의 로컬스토리지에 저장된 인증서를 보여준다.

[그림 5] 인증서 발급, 관리를 위한 인증 센터

[그림 6] 인증서 관리 기능



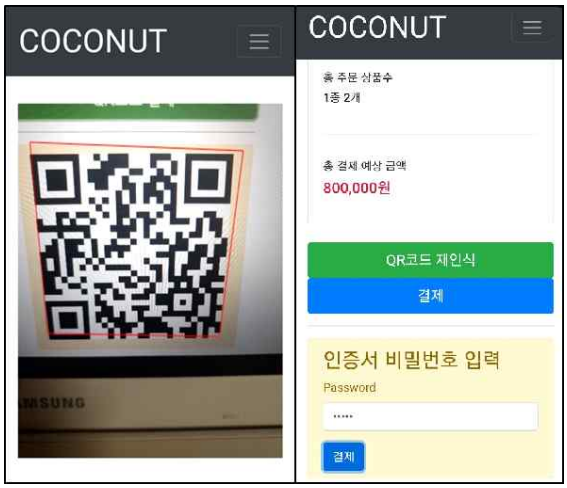
[그림 7] 로컬스토리지에 저장된 인증서

4) 주문 및 결제: 결제 단계에서는 현재 사용 중인 기기에 발급되어 설치된 추가인증서를 이용하여 직접 전자서명 결제를 하는 '바로 결제'와 QR코드를 이용하여 휴대폰으로 리다이렉트하여 결제를 진행하는 'QR코드 결제' 중에서 선택하여 결제할 수 있다. '바

로 결제'의 경우 현재의 기기에 마스터인증서 또는 추가인증서가 있는 경우 진행할 수 있으며 바로 인증서의 비밀번호를 입력하여 전자서명을 통해 결제가 진행된다. 'QR코드 결제'를 진행하는 경우 화면에 주문정보와 현재 시각이 담긴 QR코드를 화면에 표시하게 되며, 이 QR코드를 인증서가 보관된 모바일 기기의 카메라로 인식해 결제를 진행하게 된다.

휴대폰으로 QR코드를 인식하게 되면 QR코드에 담긴 주문정보를 화면에 표시하게 되며, 결제버튼을 클릭하고 인식한 기기의 인증서의 비밀번호를 입력하여 결제를 진행하게 된다.

[그림 8] 인증서 유무에 따라 결제방식 선택



[그림 9] 모바일 기기를 통한 QR코드 리다이렉트 결제

5) 영수증 발행: 사용자의 지불이 완료되면 판매자가 서명한 영수증을 발급하며 이것은 DB에 저장된다. 사용자는 거래 내역 페이지에서 판매자의 영수증 정보를 확인, 검증할 수 있다.

3.6 서비스의 활용성 분석

현재 구현된 서비스가 제공하는 특징적인 기능들은 간편결제 서비스에서 활용하기에 매력적인 기능들이라고 생각된다.

1) 이중토큰을 이용한 인증유지: 한번 로그인되면 토큰의 유효기간 동안 다시 로그인할 필요 없이 인증이 유지된다. 더구나 이러한 인증상태는 비밀토큰을 이용한 일회용 인증정보를 검증하므로 https 보안통신을 사용하지 않고도 인증이 안전하게 유지된다.

2) 인증서 기반 간편결제 웹서비스: 특정 앱을 설치하지 않고도 표준 웹브라우저를 이용하여 결제할 수 있도록 표준 웹서비스 기술들을 이용하여 전자서명 지불을 구현하였다. 기존의 간편결제 서비스에서는 제공하지 못했던 부인방지 가능한 인증서 기반 간편결제 기능을 제공한다.

3) 추가인증서를 이용한 복수기기 인증서 활용 환경: 사용자가 필요한 추가 기기의 수량만큼 추가인증서를 스스로 발행하여 사용할 수 있다.

4) 인증기관에 의존하지 않는 사설인증서 활용: 인증기관이 발행하는 공인인증서를 여러 서비스에 통용하여 사용하도록 시도하는 것은 경로검증 등이 복잡하고 인증서 관리에도 많은 어려움이 있다. 여기에서는 현재 로그인된 서버에서 자동으로 발급하고 브라우저에서 자동으로 관리되는 사설인증서를 해당 서비스에서만 이용하는 것이므로 인증모델이 간단하고 사용자의 이용도 편리하다.

5) 인증서의 안전한 관리: 여러 서비스에 통용하여 사용되는 것을 목표로 하는 공인인증서를 안전하게 관리하는 것은 매우 어려운 문제이며 개인키의 안전한 보관장소가 필요하다. 현재 구현된 서비스에서는 브라우저의 로컬스토리지에 패스워드 암호화하여 개인키를 보관하는데 이것은 해당 서비스에서만 접근하고 지불에 사용할 수 있다. 로컬스토리지에 저장되는 정보가 여러 가지 공격에 취약한 것은 사실이다. 그러나 이 방법은 브라우저에 의해 자동으로 관리되며 해당 서버에서만 사용될 수 있는 특수 인증서이고 사용자가 직접 관리할 수 있다. 사용자는 서버에 로그인하여 마스터인증서를 새로 발급받을 수도 있고 추가인증서도 직접 갱신할 수 있다. 무엇보다도 사용자가 자신의 인증서 사용 현황을 직접 파악하고 편리하게 관리할 수 있는 기능을 제공하여 편의성 및 안전성을 높일 수 있다.

IV. 결론

본 논문에서는 이중토큰을 이용한 인증유지, 추가인증서를 이용하는 복수기기 환경의 인증서 관리, 표

준 웹서비스 기술을 이용하는 인증서 기반 간편결제, QR코드를 이용한 리다이렉트 결제 등의 특징을 가지는 간편결제 서비스를 구현하였고 서비스의 활용성을 분석하였다. 이러한 특징적인 기술들은 간편결제 서비스 운영에 매우 유용하게 사용될 수 있다고 판단된다. 향후 실제 지불서비스에서 요구되는 여러 가지 기능들을 분석하고 구현하여 활용성을 더욱 높이는 연구개발이 필요하다.

[참고문헌]

[1] 이병천, “OAuth 2.0 MAC 토큰인증의 효율성 개선을 위한 무상태 난수화 토큰인증”, 정보보호학회논문지, Vol. 28, No. 6, pages 1343-1354, Dec. 2018.

[2] 이병천, “복수 K-FIDO 기기 환경에서의 인증키 관리”, 정보보호학회논문지, Vol. 27, No. 2, pages 293-303, Apr. 2017.

[3] 이병천, “하이브리드 인증을 위한 키관리서버 모델”, 보안공학연구논문지, Vol.13, No.1, pages 27-40, 2016.