

QR코드와 추가인증서를 이용한 간편결제 웹서비스

2019. 11. 30



중부대학교 정보보호학과

윤정민, 권혁민, 박종훈, 마민기, 이병천



<https://coconutpay.herokuapp.com/>

1. 서론

2. 관련연구

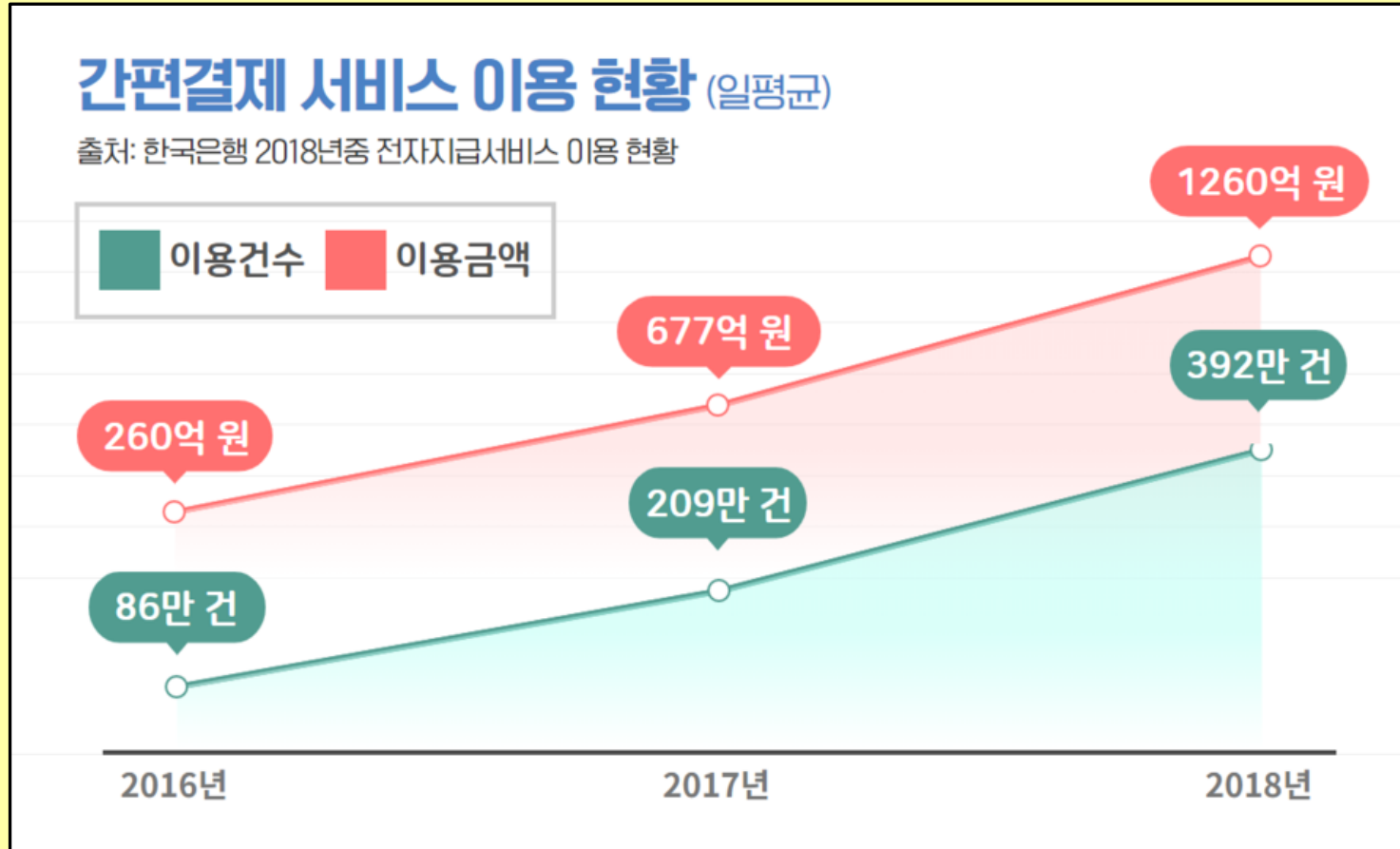
- 기존의 간편결제 서비스
- 이중토큰을 이용한 인증유지
- 추가인증서를 이용한 인증확장

3. 간편결제 웹서비스 개발

- 시스템 개요
- 서비스의 활용성 분석

4. 결론 및 향후과제

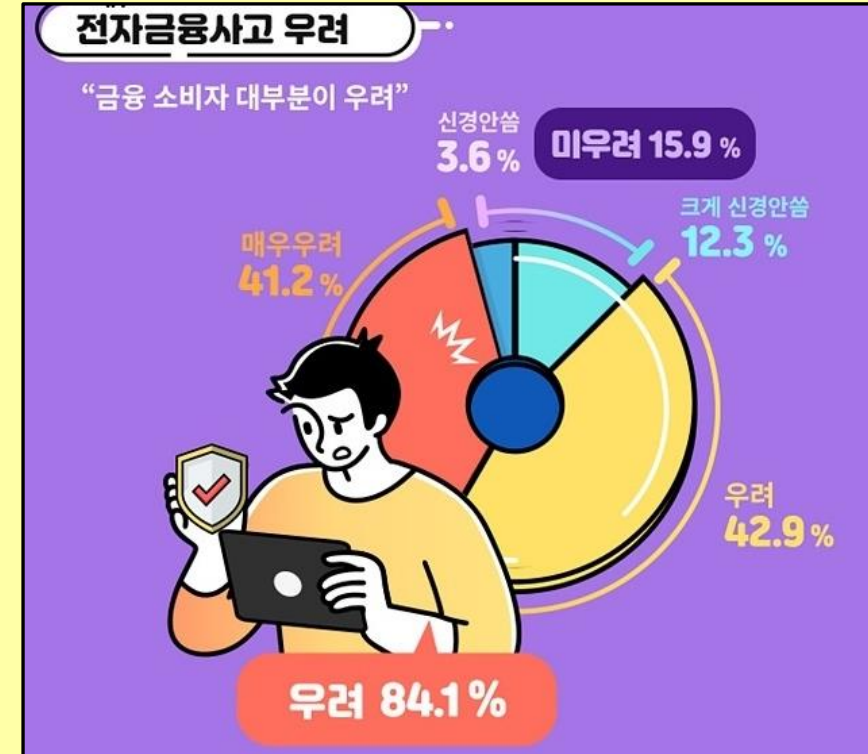
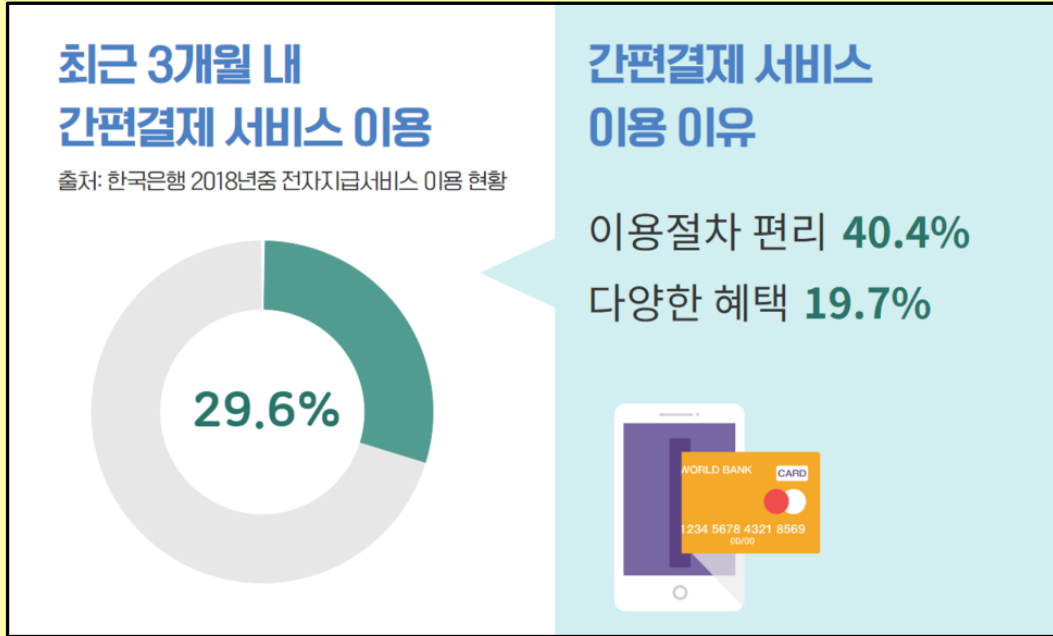
간편 결제 서비스의 급격한 성장



2016년 대비 2017년 이용금액
143.4% 증가

2018년 이용건수 329만건
87.5% 성장

이용절차의 편리함을 고려한 부인방지 불가



온라인 간편결제 서비스 이용 이유에 대해 40.4% 소비자가 편리한 이용절차 선택

그러나, **84.1%**의 소비자가 **전자금융사고 우려**

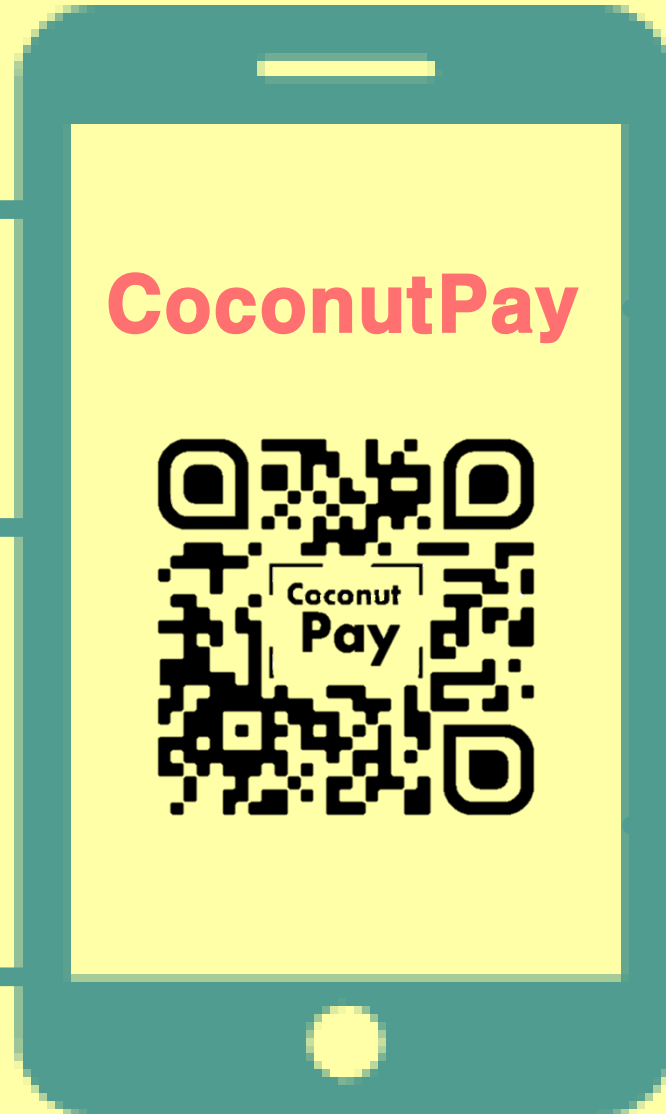
	공인인증서 전자서명 결제	휴대폰 간편결제
장점	<ul style="list-style-type: none">• 부인방지 기능• 위조불가• 사용자 검증	<ul style="list-style-type: none">• 소비자들의 사용 편리성
단점	<ul style="list-style-type: none">• Active-X 사용• 인증서 관리의 어려움	<ul style="list-style-type: none">• 부인방지 불가

두가지 기능을 모두 제공하는 **통합 결제서비스** 필요
(**사실인증서** 활용 가능)

인증서의 **안전한 관리**

인증서 기반
간편결제 **웹서비스**

추가인증서를 이용한
복수기기 인증서 활용 환경



이중토큰을 이용한
인증유지

인증기관에 의존하지 않는
사실인증서 활용

최근 많은 QR코드 사용 서비스 증가



카카오페이



BC카드 QR코드 결제

편의성 향상, 그러나
부인방지 서비스 불가

이중토큰을 이용한 인증유지

공개토큰 $t_p = HMAC(\text{사용자정보}, K)$

공개토큰은 사용자정보에 대한 서버의 서명값

공개토큰 - 서명된 ID

비밀토큰 $t_s = HMAC(t_p, K)$

비밀토큰은 사용자 공개토큰에 대한 서버의 서명값

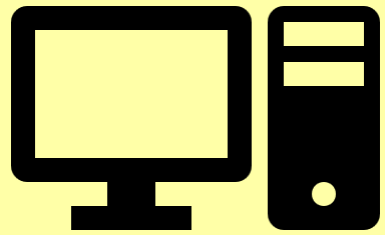
비밀토큰 - 서명된 패스워드

현재시간 ctime
auth = H(ctime, t_s)

$\langle \text{ctime}, \text{auth}, t_p \rangle$

$t_s = HMAC(t_p, K)$
auth = ? H(ctime, t_s)

추가인증서를 이용한 인증 확장



메인 PC



마스터인증서

사용허가



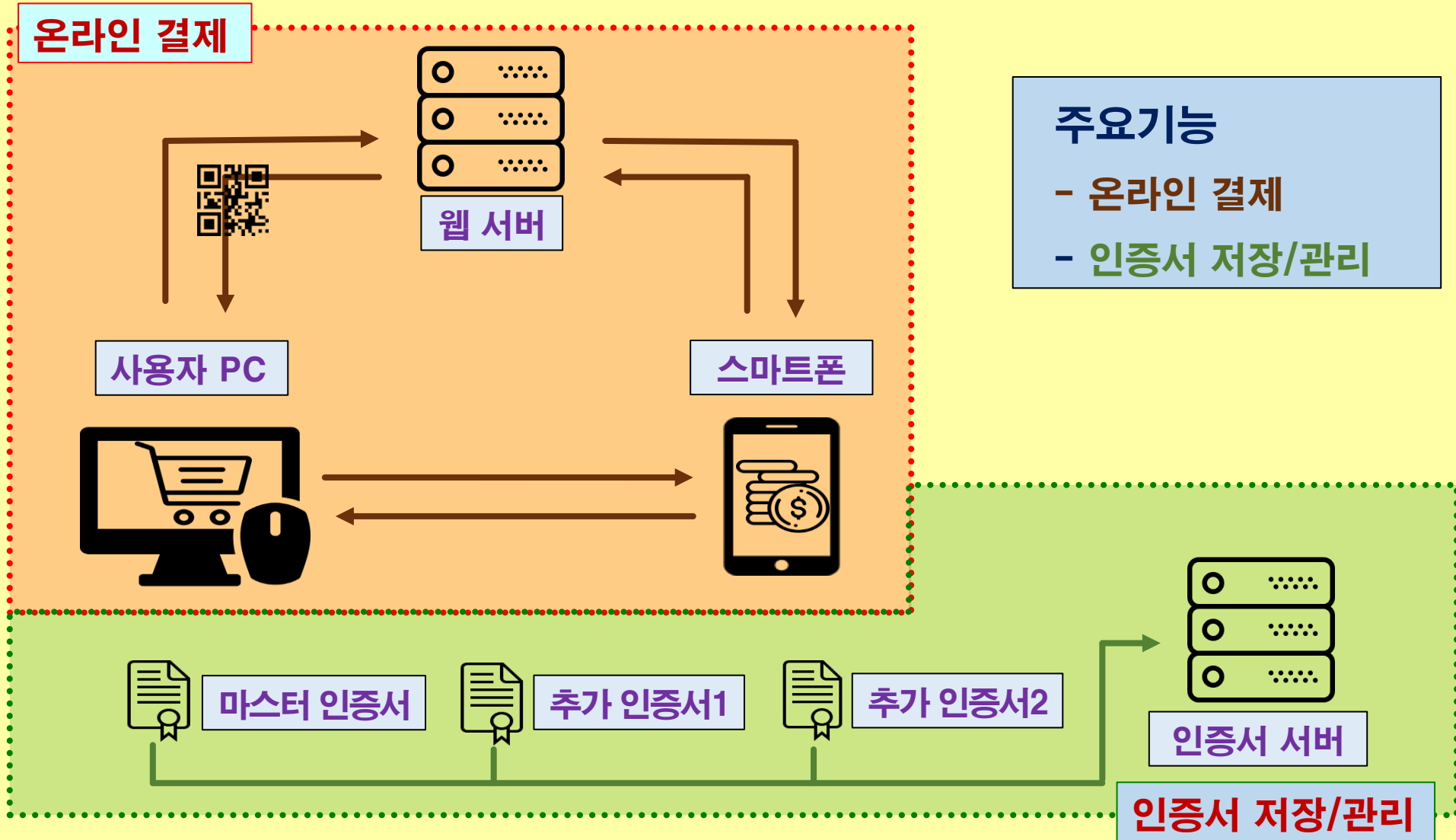
발급된 추가인증서

사용허가 ❌



모바일 기기

시스템 개요



주요기능

- 온라인 결제
- 인증서 저장/관리

개발 환경

- 프론트엔드 : **Vue.js**
- 백엔드 : **Node.js**
- 데이터베이스 : **MariaDB**
- 개발언어 : **Javascript**



1. 초기화면

COCONUT 마이페이지 인증센터 모든 상품 QR결제 로그아웃

QR코드 간편결제 시스템



QR코드를 이용한 모바일 웹 애플리케이션
인증서를 사용한 안전한 거래
JSON Web Token기반의 무상태 서비스 제공

Express Backend

Express는 웹 및 모바일 애플리케이션을 위한 일련의 강력한 기능을 제공하는 간결하고 유연한 Node.js 웹 애플리케이션 프레임워크입니다.

자유롭게 활용할 수 있는 수많은 HTTP 유틸리티 메소드 및 미들웨어를 통해 쉽고 빠르게 강력한 API를 작성할 수 있습니다.

X.509 인증서

X.509는 PKI에서 사용하는 표준 인증서 형식이다. PKI에서 사용하는 공개키, 개인키 같은 비대칭 키를 X.509 인증서로 관리한다.

X.509(V1)은 1993년 디렉터리 접근 제어를 위한 두 가지 내용을 추가하기 위해 X.509(V2) 형식으로 개정되었다. 그리고 e메일의 보안 요소 등 새로운 개념이 포함된 X.509(V3)가 1996년에 발표되었다.

Vue JS

Vue.js는 뷰(View)에 최적화된 프론트엔드 프레임워크입니다. 컨트롤러 대신 뷰 모델을 가지는 MVVM(Model-View-ViewModel) 패턴을 기반으로 디자인되었으며, 컴포넌트를 사용하여 재사용이 가능한 UI들을 쉽고 뷰 레이어를 정리하는 것이 가장 강력한 기능입니다.

Vuex

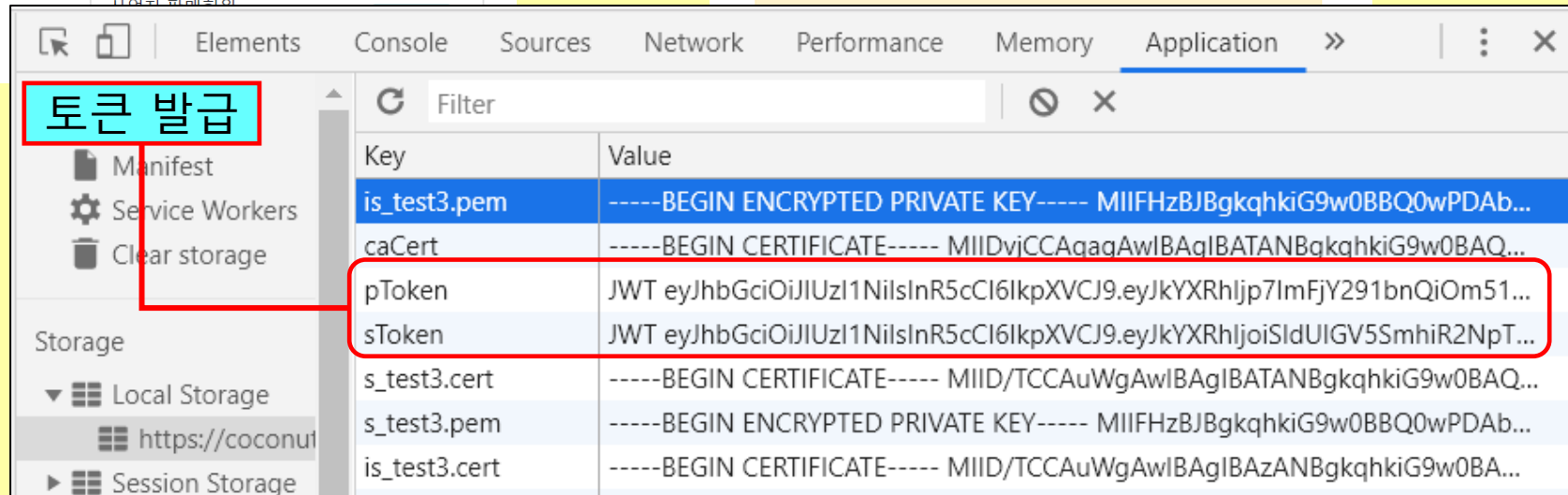
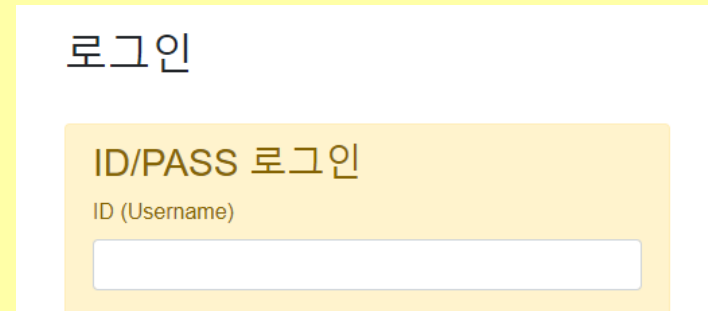
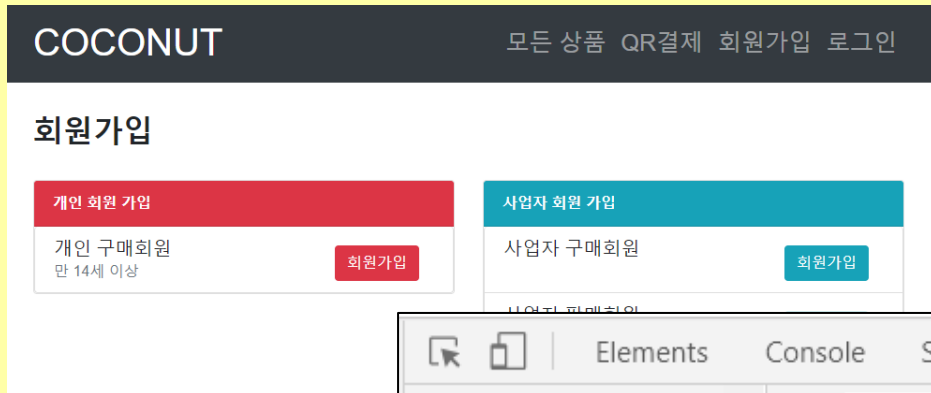
Vuex는 Vue.js 애플리케이션에 대한 상태 관리 패턴 + 라이브러리입니다. 애플리케이션의 모든 컴포넌트에 대한 중앙 집중식 저장소 역할을 하며 예측 가능한 방식으로 상태를 변경할 수 있습니다. 또한 Vue의 공식 확장 프로그램과 통합되어 설정 시간이 필요 없는 디버깅 및 상태 스냅 샷과 같은 고급 기능을 제공합니다.

JWT Tokens

JSON Web Token은 정보를 안전하게 전송하기 위해 정의된 공개된 표준(RFC 7519)입니다. JWT은 자체적으로 필요한 모든 정보를 포함합니다. 헤더 정보와, 실제 전달할 데이터, 검증할 수 있는 서명 데이터를 모두 포함하고 있습니다.

디지털 서명에 의해 검증할 수 있으며 신뢰할 수 있습니다. 비밀 값을 사용하는 HMAC 알고리즘이나 RDS or ECDSA와 같은 공개키, 개인키 쌍으로 서명될 수 있습니다.

2. 사용자 등록, 로그인, 인증유지



3. 인증 센터

인증 센터

마스터 인증서 / 추가 인증서란?

- **마스터 인증서** : 사용자당 **하나만** 소유가 가능한 인증서로, 해당 사용자의 **모든 추가 인증서**를 관리할 수 있습니다. 결제, 영수증 발급에 사용이 가능합니다.
- **추가 인증서** : 사용자의 **마스터 인증서로 발급**한 인증서로, 발급 요청시 마스터 인증서가 저장된 기기에서 **승인**을 받아 사용할 수 있습니다. 결제, 영수증 발급에 사용이 가능합니다.

마스터 인증서 발급

- 처음 인증서를 발급받으려는 사용자
- 마스터 인증서 유효기간이 만료된 사용자

마스터 인증서 발급

추가 인증서 발급

- 마스터 인증서를 발급받은 사용자
- 추가 인증서 유효기간이 만료된 사용자

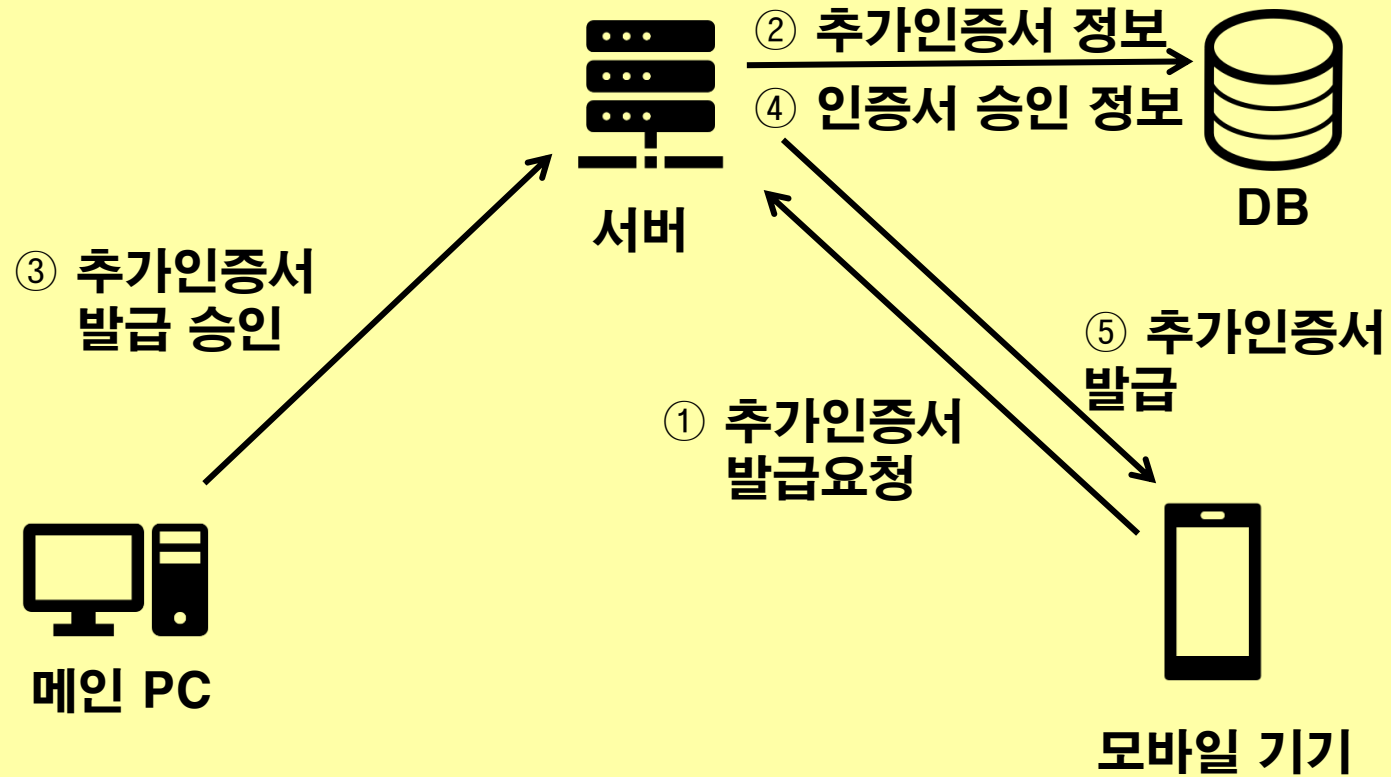
추가 인증서 발급

인증서 관리

- 마스터 인증서를 사용해 추가 인증서를 승인, 폐기하려는 사용자

인증서 관리

5. 추가 인증서 발급



5. 추가 인증서 발급

추가 인증서 발급

추가 인증서는 발급 요청 후, 마스터 인증서 기기에
서 승인을 받은 뒤 사용이 가능합니다.
추가 인증서는 제한없이 소유가 가능합니다.

발급 승인 완료된 추가 인증서

▶ 기기명 : 한성 노트북12

발급

기기 이름 입력
한성 노트북12
현재 사용하는 기기의 별명이나 명칭을 입력하세요. 다른 인증서와의
구분에 사용됩니다.

추가 인증서 비밀번호 입력
....

추가 인증서 비밀번호 확인
.... ✓

추가 인증서 발급

별도의 기기로 인증서 발급 신청

6. 인증서 관리

인증서 관리		마스터 인증서로 발급승인	
기기 이름	발급 승인	상태	작업
한성 노트북01	발급 승인	발급 승인 필요	
한성 노트북02	발급 승인	발급 승인 필요	

인증서 비밀번호 입력

Password

....

[발급 승인](#)

7. 결제

바로 결제는 인증서로 결제

QR코드 결제는 리다이렉트 결제

바로 결제

인증서 비밀번호 입력

Password

결제

금액	수량	판매자
800,000 원	2 개	JOONGBU
액티브2 44mm 스테인리스		
정전자 갤럭시 워치 액티브2 44mm 스테인리스		
스탈 케이스 (정품)		
현디지컬		
총 주문 상품수	1종 2개	
총 결제 예상 금액	800,000원	

QR코드 결제



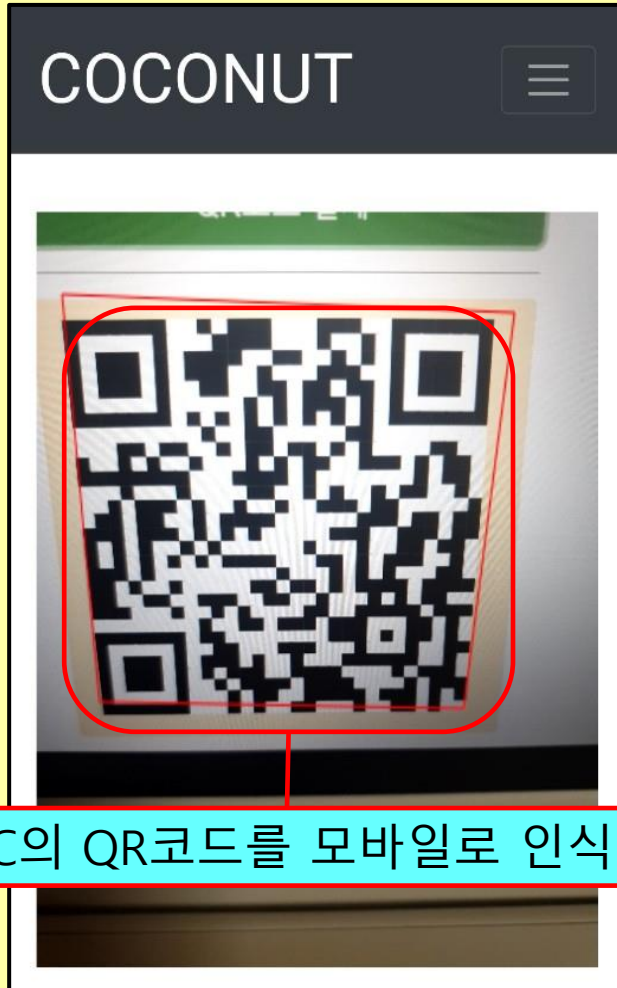
인증서를 보유한 경우

바로 결제

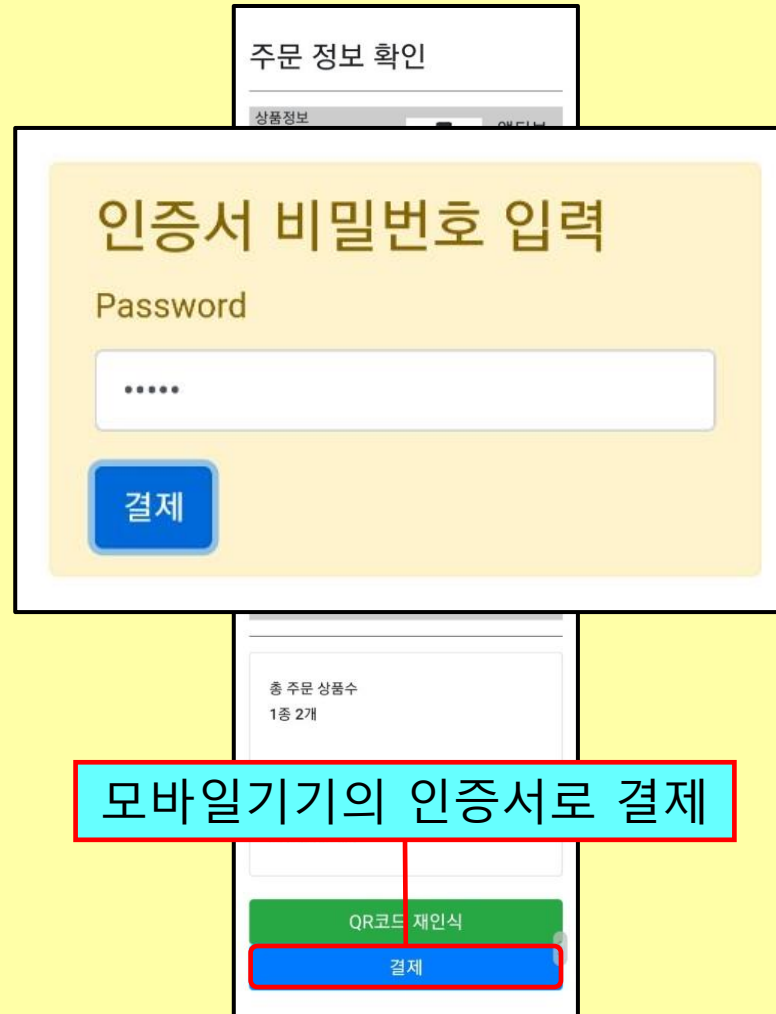
QR코드 결제

인증서가 없는
공용컴퓨터의 경우

8. QR코드 결제



PC의 QR코드를 모바일로 인식



모바일기기의 인증서로 결제

결제 완료	
결제 금액	결제일
800,000원	2019-10-18 / 23:45:07
구매자	주문자
individual3	individual3
배송 주소	주문자 전화번호
경기도 고양시 덕양구 원흥 1로 23	010-3333-3303
주문번호	
78	

9. 서명 검증

seller3님의 마이 페이지
잔액 : 7,439,000원

영수증은 판매자가 발급

상품 관리
상품 등록
판매 내역

판매내역

	다용도 스퀴즈 1개 3M 스카치브라이트 다용도 스퀴즈 (1개) 생활용품	상품 금액 : 7,000원 주문상세보기
	다우니 초고농축 3개 P&G 다우니 초고농축 화이트티와 밀리향 1L (1개) 생활용품	상품 금액 : 9,000원 주문상세보기
	스타벅스 머그컵 1개 스타벅스 블랙 헤리티지 머그컵 355ml 생활용품	상품 금액 : 10,000원 주문상세보기
주문번호 : 79		결제 완료
	액티브2 44mm 스테인리스 2개 삼성전자 갤럭시 워치 액티브2 44mm 스테인리스 스틸 케이스 (정품) 가전디지털	상품 금액 : 800,000원 주문상세보기
주문번호 : 78		결제 완료

주문번호 : 78

영수증 확인

영수증

상호 : JOONGBU3
사업자 번호 : 2147483647
주소 : 경기도 고양시 덕양구 원흥 3로 23
대표자 : seller3
전화번호 : 010-3333-00
매출일 : 2019-10-18 / 23:45:07
번호 : 78

상품명	단가	수량	금액
액티브2 44mm 스테인리스	400,000	2	800,000

영수증 서명값
2add54870a0c1469689bd18667a35870955bc
ae57dbb4dba574b7d7036c9bf7d5c5ca68557
15daad4ff90bf620bdc245059c14685edbb0
6ad921cce0cd6a7695cad1ee62447d33606dc
699dd515469af8cb2bac9074220f4460d25d83
4aa5e48ff5b55a6461bf0305ff7c5e7bcaacca4
5ca1a120bd8b6d2e45e9499d5636dd57143b9
59138963436ce1f4b0bd1d2b81d6a15755446
07bd983965e91fc68186fc1ae81cec665bbf6c
39c9f766c2db62645d3e9e22b57e9f9620d872
d135da92ff87306e5023076137368ca3a72911
5b7fac867a8d2c3c5e6c27ee424e93eec8a91
bedd6a40f60cabdcbc9fc6e16ac67f88242086
d4fc3cbae8d9044f997

영수증 서명 확인

영수증 발급

- **이중토큰을 이용한 인증유지**
 - ✓ 보안통신을 사용하지 않고도 인증이 안전하게 유지됨
- **인증서 기반 간편결제 웹서비스**
 - ✓ 표준 웹기술을 이용하여 전자서명 결제를 구현. 부인방지 기능 제공
 - ✓ 브라우저의 로컬 스토리지를 이용한 인증서 자동 관리
- **추가인증서를 이용한 복수기기 인증서 활용 환경 제공**
 - ✓ 사용자가 추가인증서를 직접 발행하여 사용
 - ✓ 자신의 추가인증서 발행 현황을 직접 관리

전자결제 서비스의 편의성 및 안전성 제공

결론 및 기대효과

○ 결론

- 전자서명 결제와 QR코드 결제 기능의 통합결제 방법론 제시
- 복수기기 환경에서 사용자 자신에 의한 인증서 관리 기능을 제공하여 사용자의 편의성과 보안성을 향상
- 이중토큰을 이용한 인증유지 기술로 보안통신에 의존하지 않는 안전한 인증

○ 향후 과제

- 실제 지불서비스에서 요구되는 각종 기능들의 설계 및 구현
- 상용 지불서비스와의 연계 검토

Q&A

감사합니다