

QR코드를 이용한 간편 결제 시스템

(시스템명 : Coconut Pay)

2019. 10. 29



지도 교수 : 이병천 교수님

1조 박종훈
권혁민
마민기
윤정민

1. **조원 편성**
2. **주제 선정**
3. **구 상 도**
4. **추진 경과**
5. **개발 환경 및 개발내용**
6. **개발 시스템 운영**
7. **결론 및 기대효과**

조원 편성

이름	역할
박종훈	데이터베이스 설계, 구축 및 관리, PPT 작성 [프로젝트 총괄]
권혁민	프론트엔드 설계 및 구현, 보고서 작성
마민기	백엔드 설계 및 구현, 보고서 작성
윤정민	데이터베이스 설계, 구축 및 관리, PPT 작성

주제 선정(1/2)

□ 전세계적으로 QR코드의 활용도가 높아지는 추세

아주경제 중국 정치 경제 산업 사회 국제 IT과학 오피니언 포토 연예스포츠 이슈 보도자료 | 아주TV

중국이 쏘아올린 QR 코드...아시아 개발 경쟁 불지피다

문은주 기자 | 입력 : 2018-08-22 08:02

중국, 올해 1분기 QR 코드 결제율 70%로 아시아 1위
인도·베트남·등 주요 국가 금융·관광 QR 코드 개발 집중
개인 정보 유출 우려 해소·인프라 연계 등은 과제로



[사진=바이두]

□ 우리 정부도 정책적으로 QR코드 활성화

삼성페이도 구식, 이젠 'QR코드'로 찍는다

돈이 보이는 **스페셜 뉴스 MoneyS**

서대웅기자 | 입력 : 2018.11.15 06:25

기사공유    

가 가 

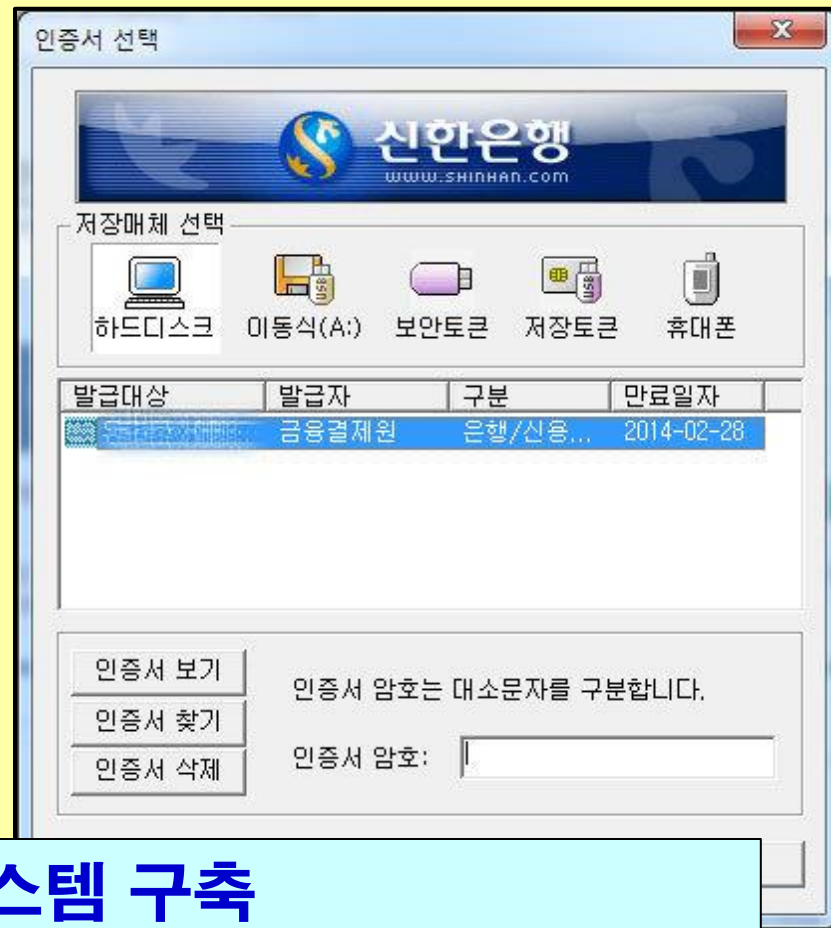
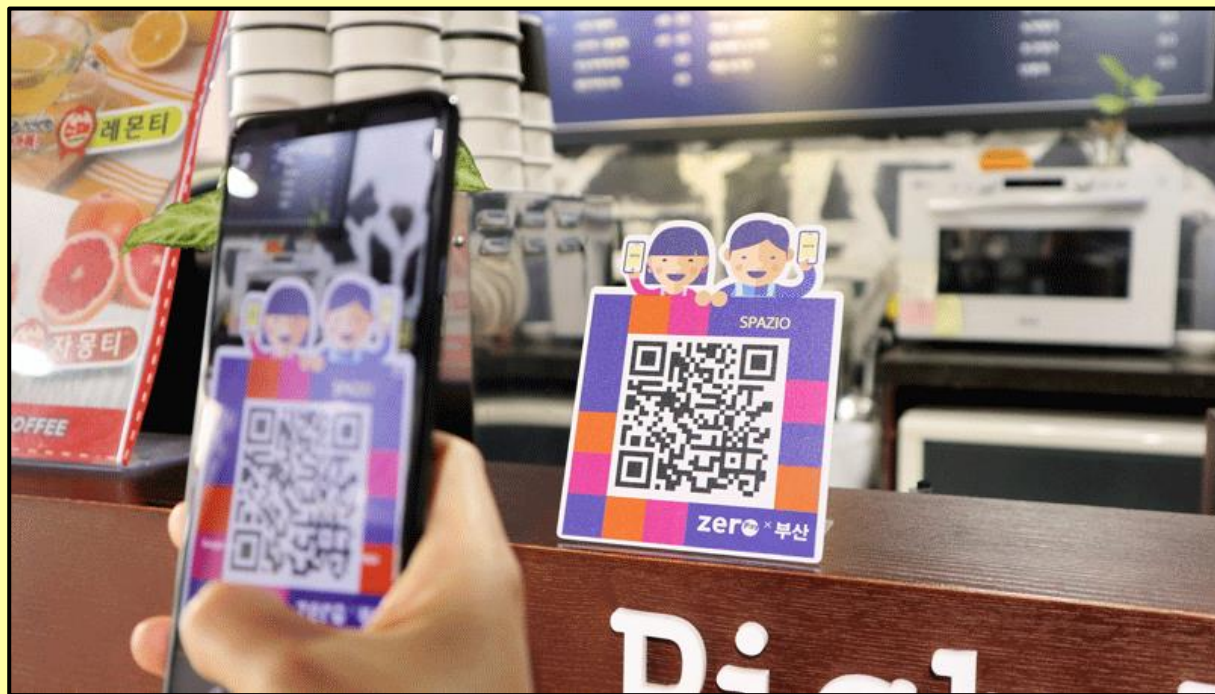
삼성페이, 카카오페이 등으로 대표되는 '간편결제'. 플라스틱 실물 카드를 소지하지 않고 스마트폰만으로 편리하게 결제할 수 있어 이처럼 불리지만 간편결제라고 다 같은 건 아니다. 최근까지 플라스틱 카드를 '긁는'(MST) 방법과 '꽂는'(IC칩) 방식이 있었던 것처럼 간편결제 역시 결제 구현방법에 따라 여러가지로 나뉜다. 대표적인 게 근거리무선통신(NFC)을 활용한 마그네틱 보안 전송(MST) 방식과 QR코드 입력 방식이다. 삼성페이가 전자를 대표하는 서비스라면 카카오페이는 QR코드 결제 서비스를 선도하고 있다.

공인인증서와 액티브X를 이용한 결제의 불편함에 대한 불만 폭증

주제 선정(2/2)

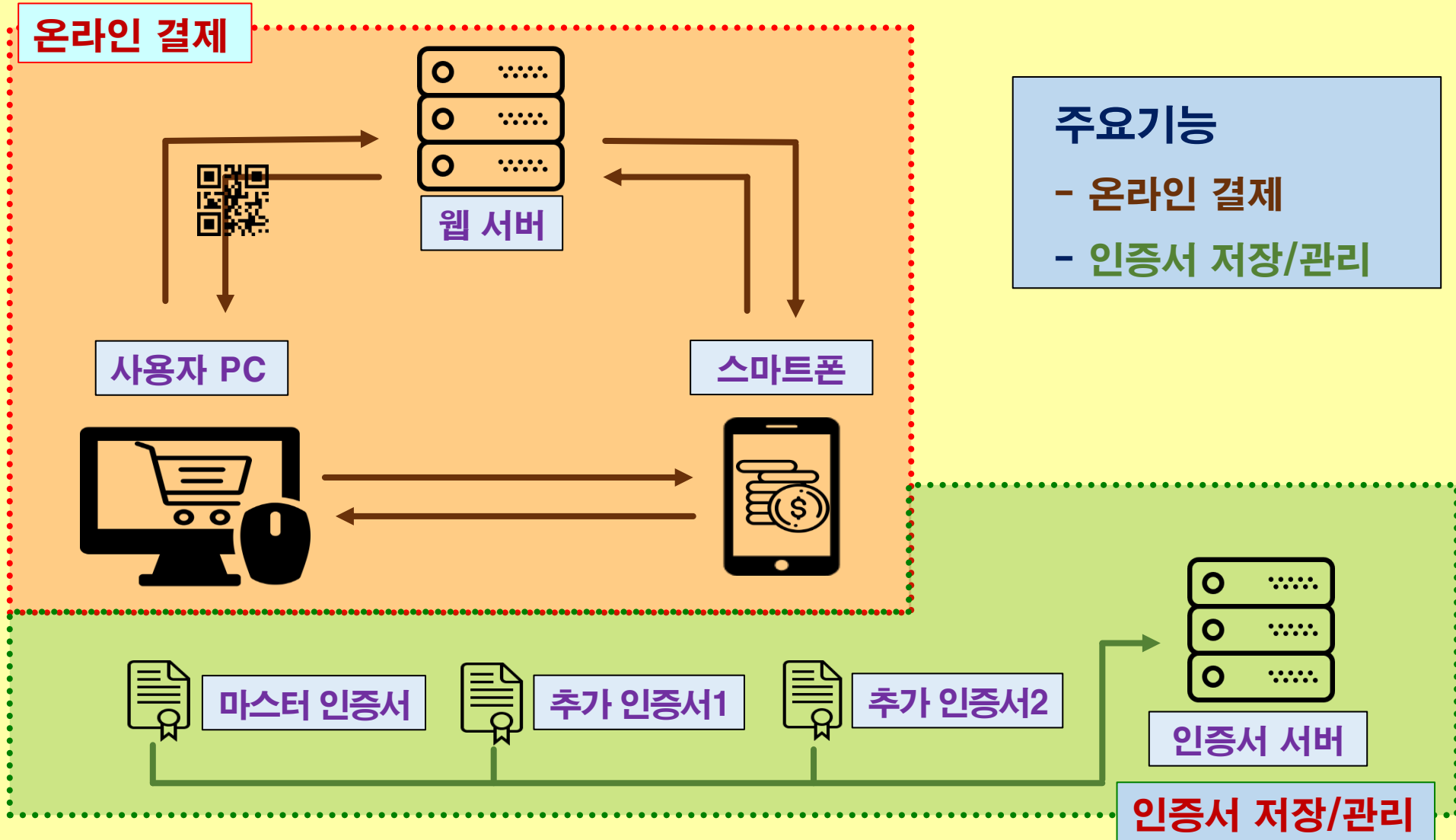
□ 스마트폰 카메라로 QR코드 촬영 후 즉시 결제 가능

□ 보안/기기 관리를 위한 마스터인증서/추가인증서 관리



QR코드를 이용한 간편 결제시스템 구축

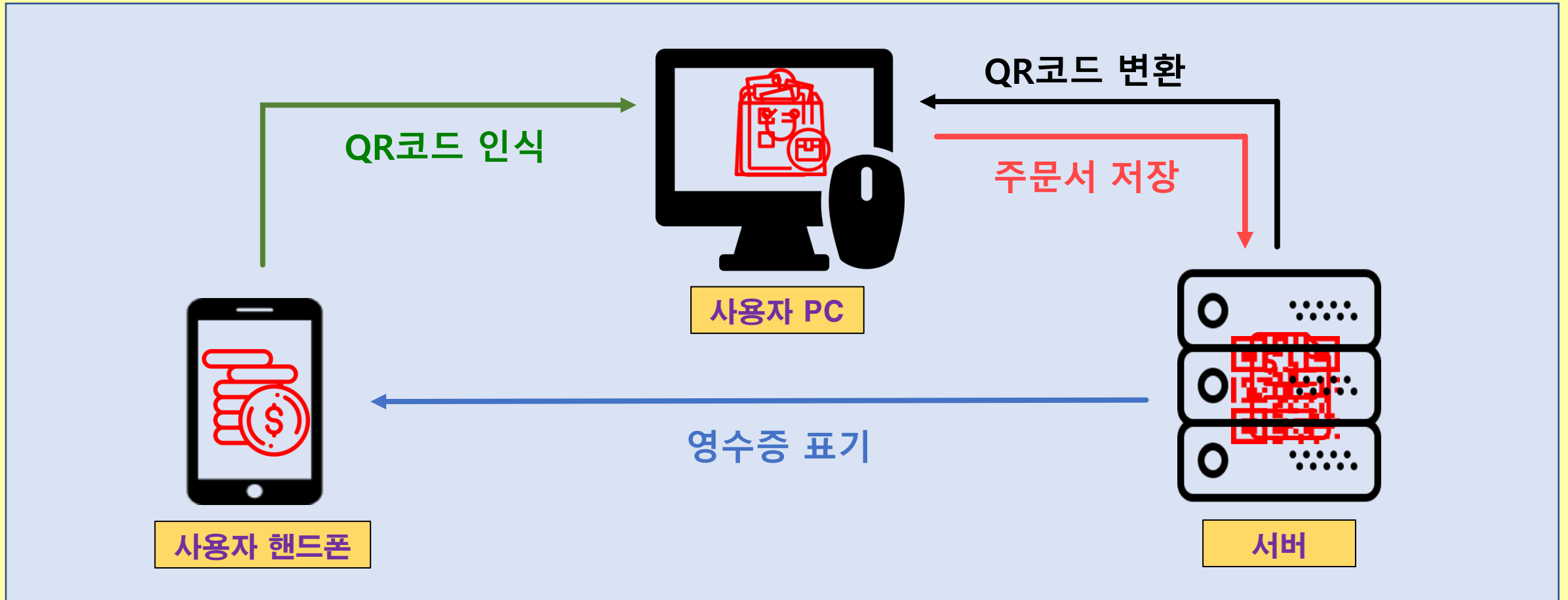
구상도(1/4)



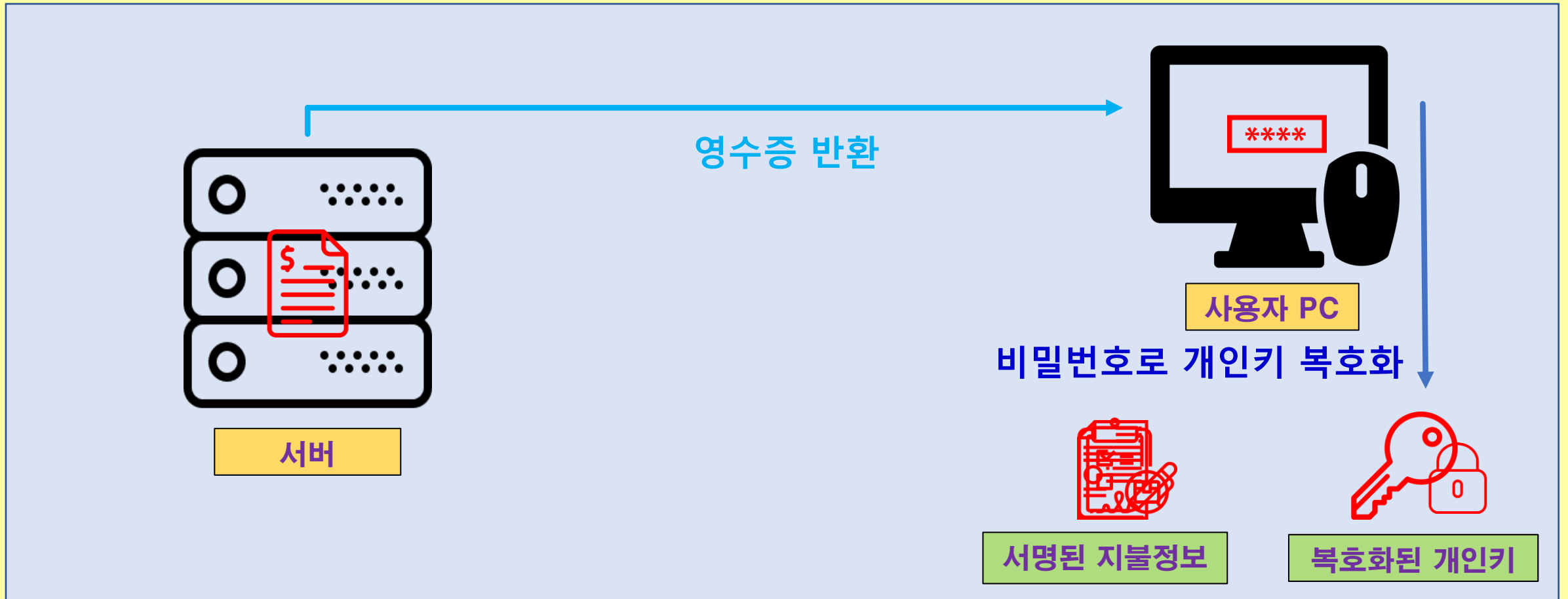
주요기능

- 온라인 결제
- 인증서 저장/관리

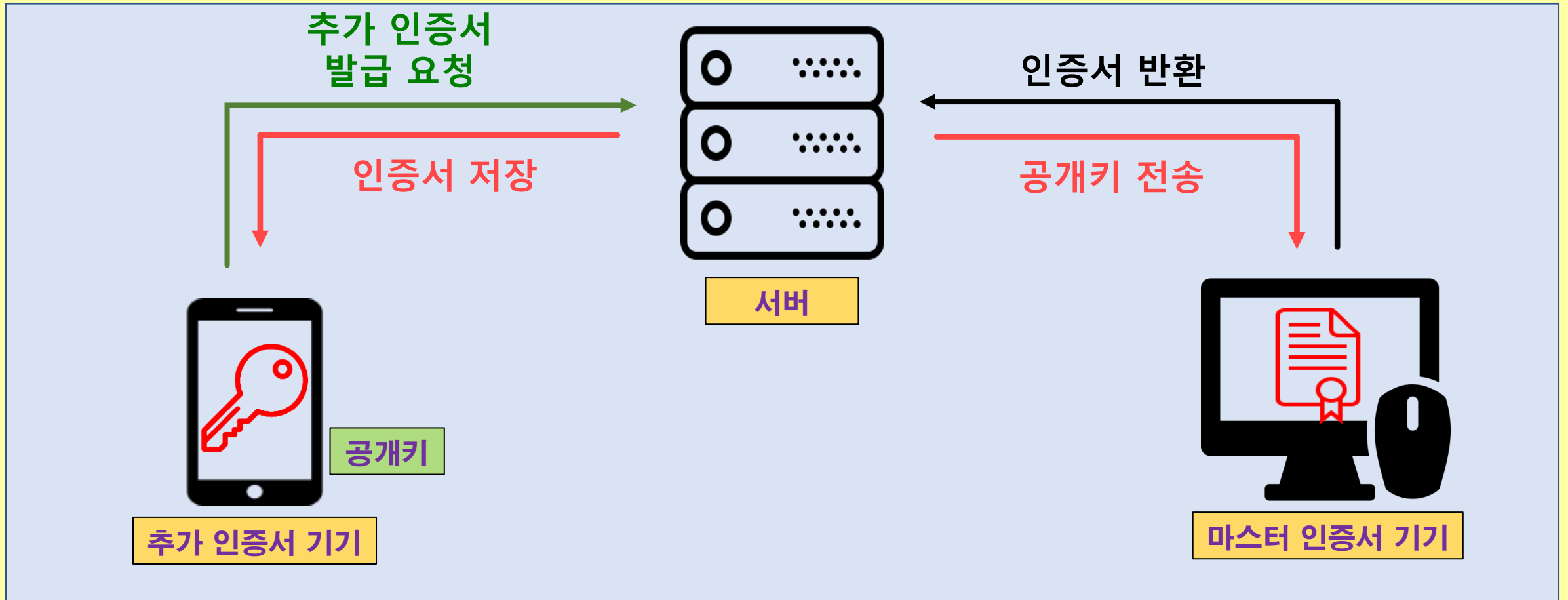
온라인 구매



결 제



추가 인증서 관리



추진경과

추진 내용		추진 기간 (2019년)							
		3월	4월	5월	6월	7월	8월	9월	10월
자료조사 및 설계		■							
시스템 설계 및 구현	기본 페이지		■	■					
	결제 시스템			■	■	■	■	■	
	송금 시스템							■	■
	인증서 발급/관리						■	■	■
웹 업로드 및 테스트			■	■	■	■	■	■	■

개발 환경

- 프론트엔드 : Vue.js
- 백엔드 : Node.js/Express
- 데이터베이스 : MySQL
- 개발언어 : Javascript



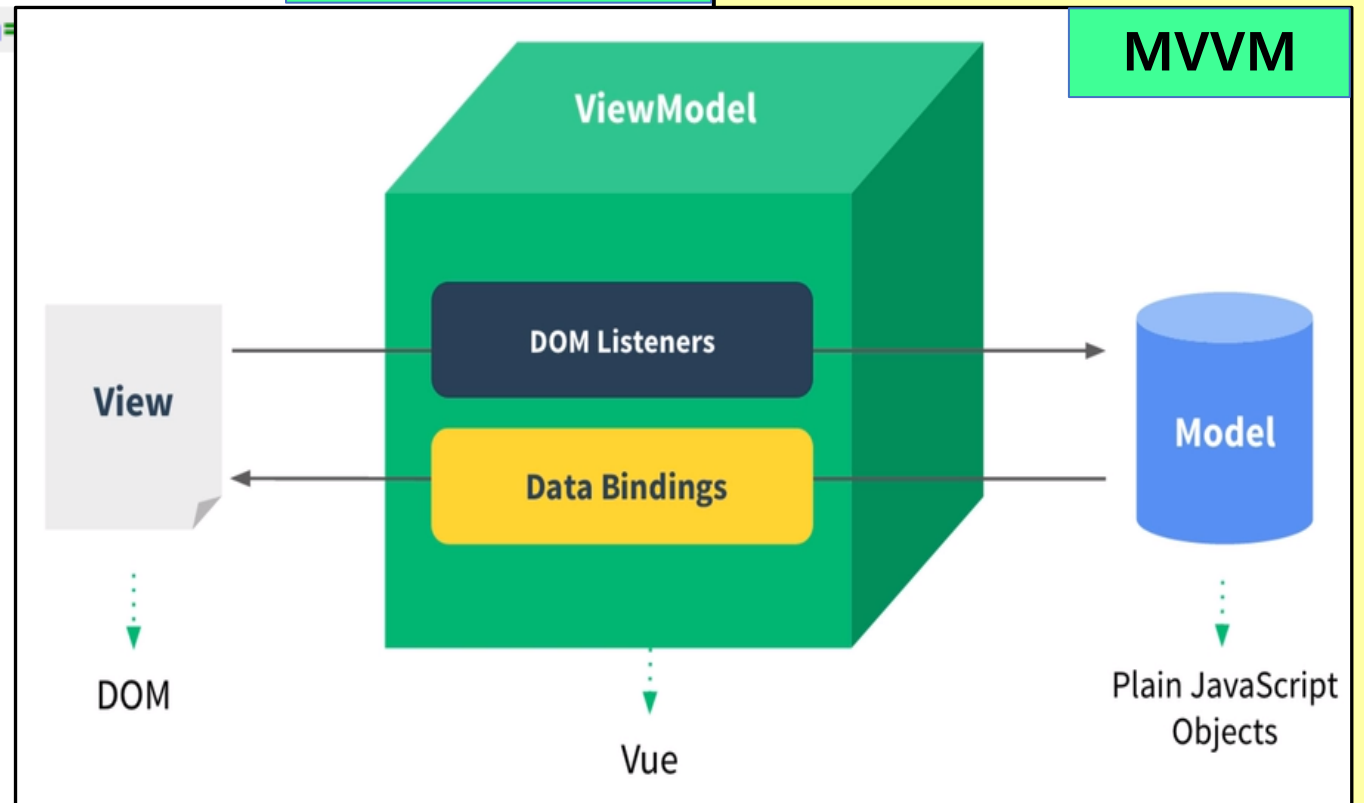
초기 화면 구현

```
<template>
  <div id="app" >
    <img alt="Vue logo" height="200px" width=
    <router-view/>
    <Navbar></Navbar>
  </div>
</template>

<script>
import Navbar from "./components/Navbar";

export default {
  name: "app",
  components: {
    Navbar
  },
  created() {
    this.$store.commit("GET_TOKENS");
  }
};
</script>
```

초기 화면 설정



MVVM(Model-View-ViewModel)패턴 지원

개발 환경 및 개발 내용(3/8)

회원 가입

```
function CreateSa
return new P
bcrypt.ge
if (sa
co
re
} else
co
re
});
```

```
function PasswordHash(salt, pass) { // 비밀번호 해시화 및 DB 등록
return new Promise( executor: function (resolve, reject) {
    bcrypt.hash(pass, salt, function (err, hash) {
        if (hash) {
            console.log("PasswordHash : "+hash);
            resolve(hash);
        } else {
            console.log("PasswordHash err : "+err);
        }
    });
});
```

number	name	id	password	role	status
▶ 31	개인회원1	개인회원1	\$2a\$10\$J.tOj7zGtheWRB57DxkjwtOZRfQMpZGaPvZsV7Td...	1	개인회원1
32	구매회원1	구매회원1	\$2a\$10\$U71XFVkrQ1tqIS7uo7rZsuWx4Plk4CHNKOUII2Tn...	구매회원1	구매회원1
33	판매회원1	판매회원1	\$2a\$10\$csuuQGV/TSsGFoCMYkY7SO4AOEFNrtgc8BMiaJo...	판매회원1	판매회원1
34	판매회원2	판매회원2	\$2a\$10\$y1e.0dOAW9tSdSSQljHFduB2YvWPiahDrpgLNs8...	판매회원2	판매회원2

등록된 회원정보

비밀번호 해시에 사용할 salt값을 생성

Bcrypt : 비밀번호전용 해시함수, salt값을 이용하는 해시함수로서 입력값이 같아도 매번 다른 해시값을 반환

해시 알고리즘인 bcrypt를 이용하여 비밀번호를 해시화하여 저장

개발 환경 및 개발 내용(4/8)

로그인

```

<div class="col-md-6">
  <div class="form-group row">
    <label for="id" class="col-sm-2 col-form-label">아이디</label>
    <div class="col-sm-10">
      <input type="text" id="id" v-model="User.id" class="form-control" placeholder="ID">
    </div>
    <br><br><br>
    <label for="password" class="col-sm-2 col-form-label">비밀번호</label>
    <div class="col-sm-10">
      <input type="password" id="password" v-model="User.password" class="
    </div>
  </div>
  <br>
  <button @click="onLoginSubmit" type="button" class="btn btn-primary">로그인</
</div>
  
```

로그인 정보 입력

공개/비밀토큰 발급

```

function CreateAuthToken
return new Promise(
  const ptoken = 'JWT '+jwt.sign(
    { data : User },
    config.secret,
    { expiresIn : 86400 * 7 } //유효기간 7일
  );
  console.log("공개 토큰값 : ", ptoken);

  const stoken = 'JWT '+jwt.sign(
    { data : ptoken },
    config.secret,
    { noTimestamp : true } //유효기간 무제한
  );
  console.log("비밀 토큰값 : ", stoken);
)
  
```

발급된 공개토큰/비밀토큰

Manifest	Key	Value
Service Workers	loglevel:webpa...	SILENT
Clear storage	pToken	JWT eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7Im51bWJlci...
Storage	sToken	JWT eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjoiSldlUGV5S...
Local Storage		
http://localhost:8080		

로그인 상태를 유지하기 위해 공개/비밀토큰의 생성 활용

개발 환경 및 개발 내용(5/8)

인증서 발급

```
router.post('/newCert', (req, res, next) => {
  console.log(JSON.stringify(req.body));
  var cert = pki.createCertificate({
    cert.publicKey = pki.getPublicKey(req.body.userNumber);
    cert.serialNumber = '00000000000000000000000000000000';
    cert.validity.notBefore = new Date(0);
    cert.validity.notAfter = new Date(0);
  });
```

유효기간 5년 설정

인증서 정보 입력

```
var userAttrs = [
  {
    name: 'commonName',
    value: req.body.userNumber
  }, {
    name: 'countryName',
    value: 'kr'
  }, {
    name: 'organizationName',
    value: 'Coconut'
  }, {
    name: 'shortName',
    value: req.body.deviceId
  }
];
```

서버키로 사용자 인증서 서명

```
cert.sign(caPrivateKey);
```

사용자가 입력한 정보로 인증서 생성 후 서버키로 서명

개발 환경 및 개발 내용(6/8)

서명 검증

```
for (var i=0; i<certPem.length; i++){
  let cert = pki.certificateFromPem(certPem[i].cert);
  console.log('cert : ' + JSON.stringify(cert));
```

PEM 파일을 인증서로 변환

```
var pss2 = forge.pss.create({
  md: forge.md.sha1.create(),
  mgf: forge.mgf.mgf1.create(forge.md.sha1.create()),
  saltLength: 20
// d
});
```

서명검증 객체 생성

```
var md2 = forge.md.sha1.create();
md2.update(sign, 'utf8');

var verifySignature = publicKey.verify(md2.digest().getBytes(), payload.signature[0], pss2);

console.log('Signature Verify : '+verifySignature);
```

사용자의 서명 검증

PEM 파일을 인증서로 변환 후 해당 인증서로 전자서명을 검증

개발 환경 및 개발 내용(7/8)

개인키 암호화

// 1. 공개키, 개인키 생성

사용자의 공개키쌍 생성

```
var keypair = pki.rsa.generateKeyPair( bits: 2048);
var publicKey = keypair.publicKey;
var privateKey = keypair.privateKey;
var privateKeyPem = pki.privateKeyToPem(privateKey);
var publicKeyPem = pki.publicKeyToPem(publicKey);
```

```
var encryptedPrivateKeyInfo = pki.encryptPrivateKeyInfo(
    privateKeyInfo, payload.pa, options: {
        algorithm: 'aes256', // 'aes128', 'aes192', 'aes256', '3des'
    });
```

사용자가 입력한 비밀번호를 대칭키로 사용하여 대칭키 암호화

개인키는 사용자가 입력한 비밀번호로 암호화하여 안전하게 저장

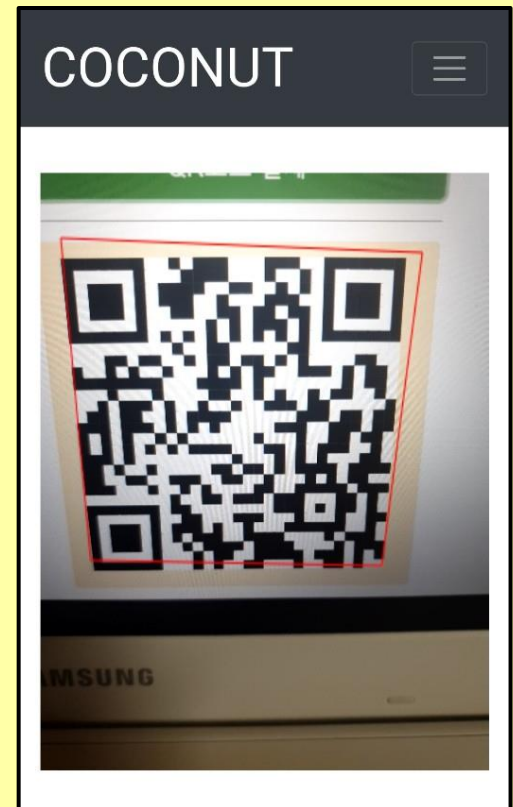
개발 환경 및 개발 내용(8/8)

QR코드 인식

```
Terminal: Local (2) × + NPM설치
C:\Users\gns14\WebstormProjects\Coconut>cd vue-coconut
C:\Users\gns14\WebstormProjects\Coconut\vue-coconut>npm install vue-qrcode-reader
```

NPM(Node Package Manger) : 자바스크립트 언어를 위한 패키지 관리자

```
import VueQrcodeReader from 'vue-qrcode-reader'
Vue.use(VueQrcodeReader); QR코드 인식 패키지 적용
```



QR코드 인식 패키지를 사용하여 QR코드 인식 시스템 구축

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.

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.

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.

회원가입

회원가입

개인 회원 가입

개인 구매회원
만 14세 이상

회원가입

사업자 회원 가입

사업자 구매회원

회원가입

사업자 판매회원

회원가입

개인/ 사업자 구분하여 가입
판매자/ 구매자 구분하여 가입

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

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

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

마이페이지

seller3님의 마이 페이지

잔액 : 1,000,000원

상품 관리

상품 등록

판매 내역

기업판매 회원만 상품 등록 표시

상품 등록

상품 등록

상품명: 액티브2 44mm 스테인리스

가격: 400000

수량: 300

카테고리: 가전디지털

설명: 삼성전자 갤럭시 워치 액티브2 44mm 스테인리스 스틸 케이스 (정품)

이미지: 9201189_2.jpg (126 KB) Upload complete tap to undo

상품등록

데이터베이스에 저장

가전디지털 삼성전자 갤럭시 워치 액티브2 44mm 스테인리스 스틸 케이스 (정품) 액티브2 44mm 스테인리스 400000 10 284 JO 20 1571313645130.jpg

상품 보기

카테고리별 정렬

모든 상품

의류

식품

생활용품

가전/디지털

스포츠/레저

자동차 용품

도서/음반/DVD

완구/취미

문구/오피스

반려동물용품

뷰티

출산/유아동

주방용품



액티브2 44mm 스테인
리스

400,000원

가전디지털

상품 상세 보기



갤럭시 워치

가전디지털



어메이징 워치

가전디지털



APPLE 워치

가전디지털



액티브2 44mm 스테인리스

남은 수량 : 300개

400,000원

- 1 +

총 상품금액 400,000원

장바구니

바로구매

결제

바로 결제는 인증서로 결제

QR코드 결제는 QR코드로 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



바로 결제

QR코드 결제

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

장바구니

장바구니

원하는 물품만 선택

상품정보	금액	수량	판매자	선택
 다용도 스퀴즈	7,000원	1개	JOONGBU3	<input checked="" type="checkbox"/>
 다우니 초고농축	9,000원	3개	JOONGBU3	<input checked="" type="checkbox"/>
 스타벅스 머그컵	10,000원	1개	JOONGBU3	<input checked="" type="checkbox"/>

바로구매

individual3님의 주문서

1. 주문상품 확인

상품정보	금액	수량	판매자
다용도 스퀴즈	7,000원	1개	JOONGBU3
다우니 초고농축	9,000원	3개	JOONGBU3
스타벅스 머그컵	10,000원	1개	JOONGBU3

2. 배송지 정보 입력

고객입력 상세주소	경기도 고양시 덕양구 원흥 1로 23
우편번호	10562
연락처	010-3333-3003

주문하기

주문/구매내역

individual3님의 마이 페이지
잔액 : -5,426,000원

장바구니
주문/구매내역

주문/구매내역

다용도 스퀴즈 포함 3종 5개 총 결제금액 : 26,000원
주문상세보기

주문번호 : 79 결제 완료

액티브2 44mm 스테인리스 포함 1종 2개 총 결제금액 : 800,000원
주문상세보기

주문번호 : 78 결제 완료

액티브2 44mm 스테인리스 포함 1종 2개 총 결제금액 : 800,000원
주문상세보기

주문번호 : 76 결제 완료

액티브2 44mm 스테인리스 포함 1종 2개 총 결제금액 : 800,000원
주문상세보기

주문번호 : 75 결제 대기

결제 대기 / 완료 확인

결제 내역 확인

주문번호 : 79

상품명	금액	수량	판매자	영수증
다용도 스퀴즈 3M 스키치브라이트 다용도 스퀴즈 (1개) 생활용품	7,000 원	1 개	JOONGBU3	미결제
스타벅스 머그컵 스타벅스 블랙 헤리티지 머그컵 355ml 생활용품	10,000 원	1 개	JOONGBU3	미결제
다우니 초고농축 P&G 다우니 초고농축 화이트티와 릴리향 1L (1개) 생활용품	9,000 원	3 개	JOONGBU3	미결제

주문자	12	구매자	12
배송 주소	경기도 고양시 덕양구 원흥 1로 23	전화번호	010-3333-3003
결제 시간	2019-10-18 / 23:50:60		

총 주문 상품수	3종 5개
총 결제금액	26,000원

영수증 발급

seller3님의 마이 페이지
잔액 : 7,439,000원

영수증은 판매자가 발급

상품 관리
상품 등록
판매 내역

판매내역

	다용도 스퀴즈 1개 3M 스키치브라이트 다용도 스퀴즈 (1개) 생활용품	상품 금액 : 7,000원 주문상세보기
	다우니 초고농축 3개 P&G 다우니 초고농축 화이트티와 릴리향 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
	엑티브2 44mm 스테인리스 2개 삼성전자 갤럭시 워치 액티브2 44mm 스테인리스 스틸 케이스 (정품) 가전디지털	상품 금액 : 800,000원 주문상세보기
주문번호 : 78		결제 완료

주문번호 : 78

판매 상품정보

 **엑티브2 44mm 스테인리스**
삼성전자 갤럭시 워치 액티브2 44mm 스테인리스 스틸 케이스 (정품)
가전디지털

주문자 : 12

배송 주소 : 경기도 고양시 덕양구 원흥 1로 23

결제 시간

주문 상품수	1종
결제 금액	800,000원

영수증 발급

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
엑티브2 44mm 스테인리스	400,000	2	800,000

영수증 서명값 : 2add54870a0c1469689bd18667a35870955bc
ae57dbb4dba574b7d7036c9bf7d5c5ca68557
15daad4ff90bfbff620bdc245059c14685edbb0
6ad921cce0cd6a7695cad1ee62447d33606dc
699dd515469af8cb2bac9074220f4460d25d83
4aa5e48ff5b55a6461bf0305ff7c5e7bcaacca4
5ca1a120bd8b6d2e45e9499d5636dd57143b9
59138963436ce1f4b0bd1d2b81d6a15755446
07bd983965e91fc68186fc1ae81cec665bbf9c
39c9f766c2db62645d3e9e22b57e9f9620d872
d135da92ff87306e5023076137368ca3a72911
5b7fac867a8d2c3c5e6c27ee424e93eec8a91
bedd6a40f60cabdcbc9fc6e16ac67f88242086
d4fc3cbae8d9044f997

영수증 서명 확인

영수증 발급

결론 및 기대효과

○ 결 론

- QR코드를 이용한 간편 결제 시스템 구축에 필요한 시스템 설계, 회원가입 및 로그인, 인증서 발급 등의 프로그램 개발을 정상적으로 완료하고 시스템 구축에 성공
- 특히 QR코드 인식처리 및 온라인/오프라인 결제 등 난이도가 높은 부분의 코딩에 많은 어려움이 있었으나 조원 간 기술공유 및 협동으로 난관을 극복

○ 기대효과

- 시스템 개발과정에서 어려운 기술이론 부분의 코딩 등을 직접 체험함으로써 기술 역량을 배가하고 성과에 대한 성취감
- 간편 결제 시스템은 소상공인 점포 등에서 운영할 경우 편의성과 보안성 측면에서 유용할 것으로 기대

- 끝 -

Q&A

감사합니다