QR코드와 추가인증서를 이용한 간편결제 웹서비스

2019. 11. 30

중부대학교 정보보호학과

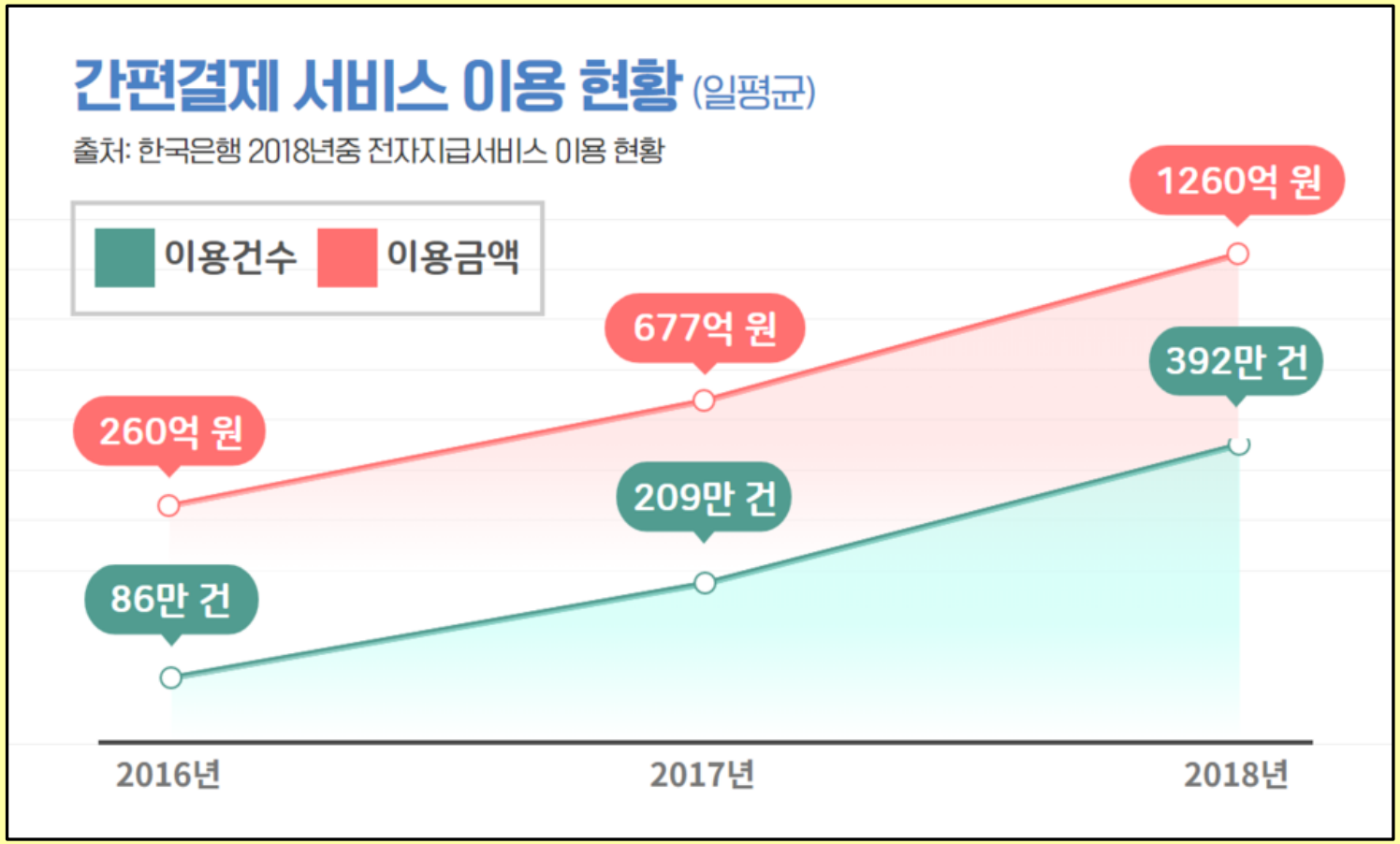
윤정민, 권혁민, 박종훈, 마민기, 이병천

https://coconutpay.herokuapp.com/

목차

서론

간편 결제 서비스의 급격한 성장

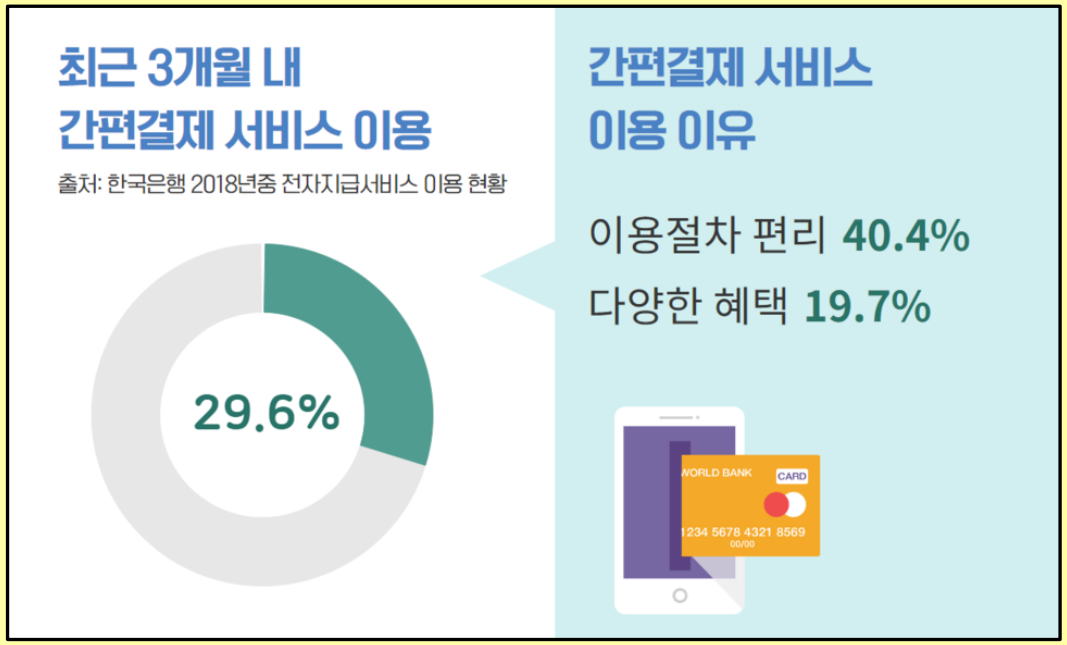


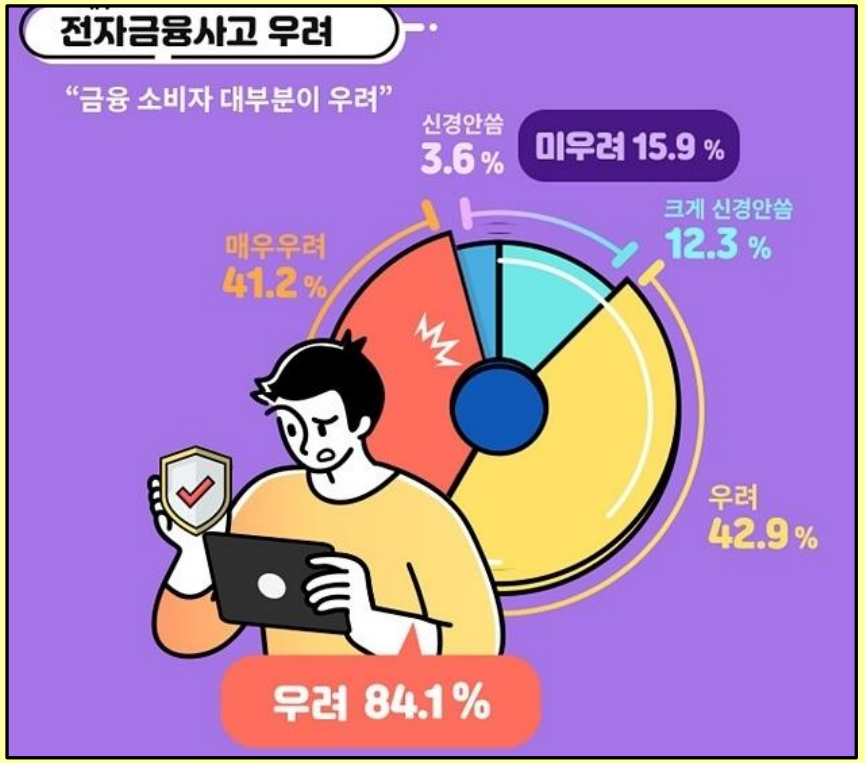
2016년 대비 2017년 이용금액
143.4%증가

2018년 이용건수 329만건
87.5% 성장

서론

이용절차의 편리함만을 고려한 부인방지 불가





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

그러나, 84.1%의 소비자가 전자금융사고 우려

서론

	공인인증서 전자서명 결제	휴대폰 간편결제
장점	• 부인방지 기능 • 위조불가 • 사용자 검증	• 소비자들의 사용 편리성
단점	• Active-X 사용 • 인증서 관리의 어려움	• 부인방지 불가

두가지 기능을 모두 제공하는 통합 결제서비스 필요
(사설인증서 활용 가능)

서론

인증서의 안전한 관리

인증서 기반
간편결제 웹서비스

추가인증서를 이용한
복수기기 인증서 활용 환경

이중토큰을 이용한
인증유지

인증기관에 의존하지 않는
사설인증서 활용

관련 연구

최근 많은 QR코드 사용 서비스 증가

카카오페이

BC카드 QR코드 결제

편의성 향상, 그러나
부인방지 서비스 불가

관련 연구

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

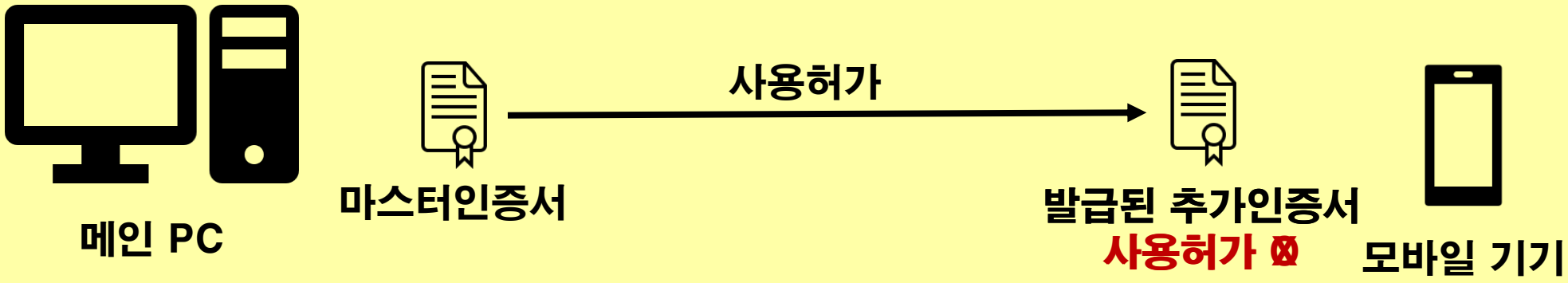
현재시간 ctime
auth = H(ctime, t_S)

<ctime, auth, t_P >

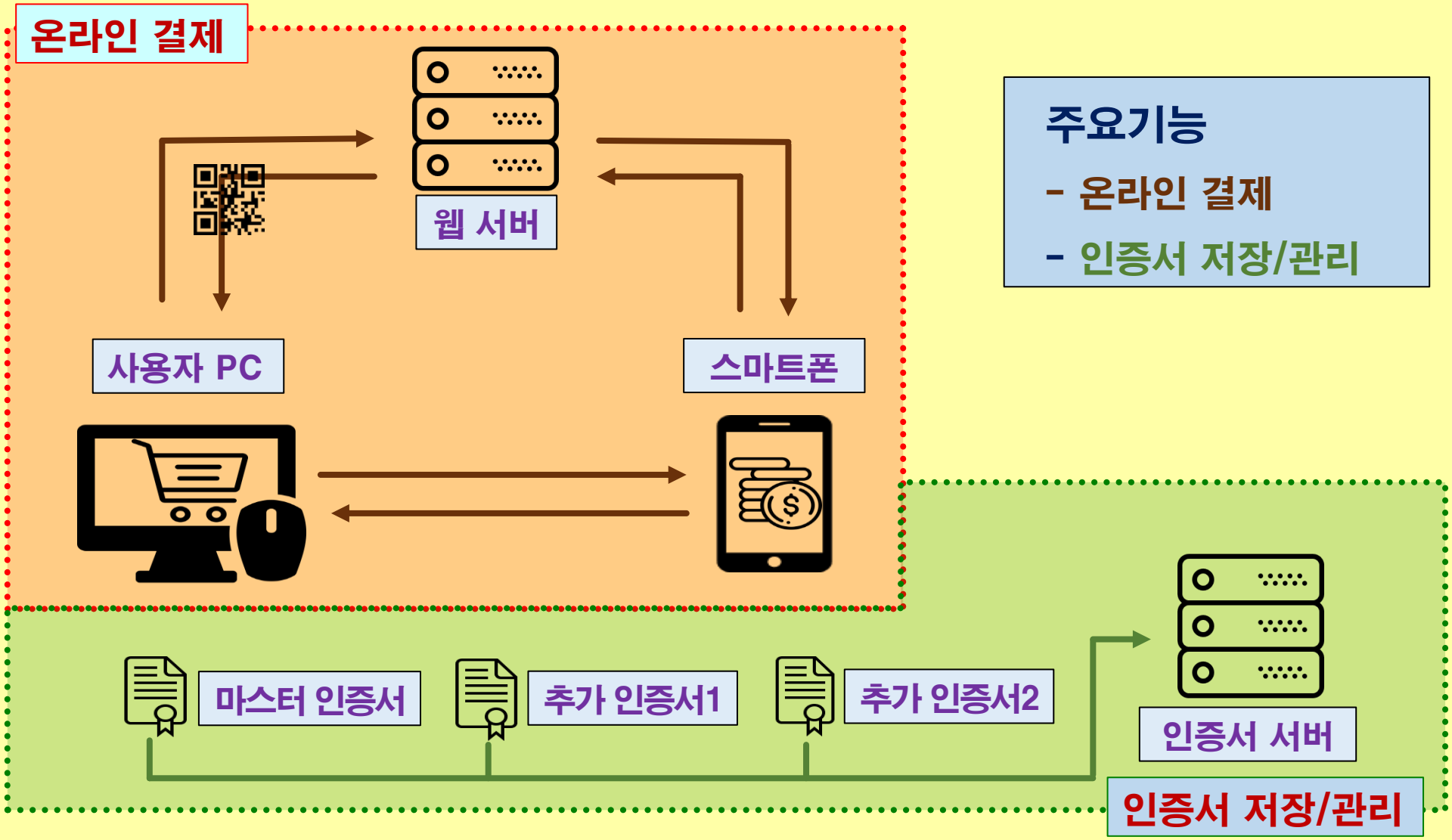
$t_S = HMAC(t_P, K)$
auth =? H(ctime, t_S)

관련 연구

추가인증서를 이용한 인증 확장



시스템 개요


온라인 결제
웹 서버
사용자 PC
스마트폰
주요기능
- 온라인 결제
- 인증서 저장/관리
마스터 인증서
추가 인증서1
추가 인증서2
인증서 서버
인증서 저장/관리

시스템 개요

개발 환경

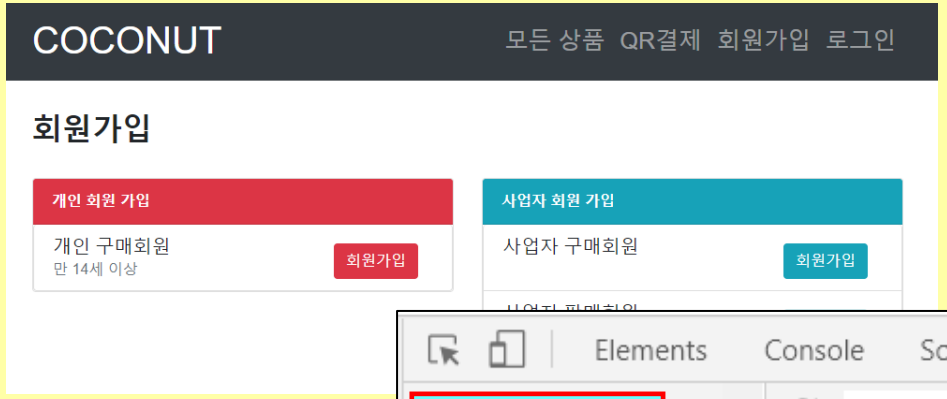
- 프론트엔드 : Vue.js
- 백엔드 : Node.js
- 데이터베이스 : MariaDB
- 개발언어 : Javascript

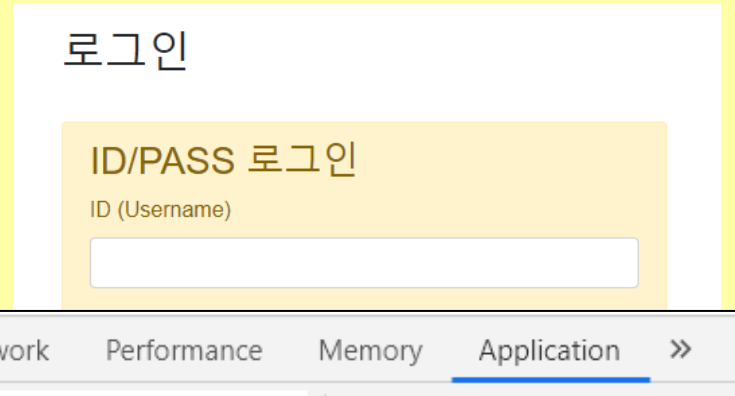
개발 시스템 (1/10)

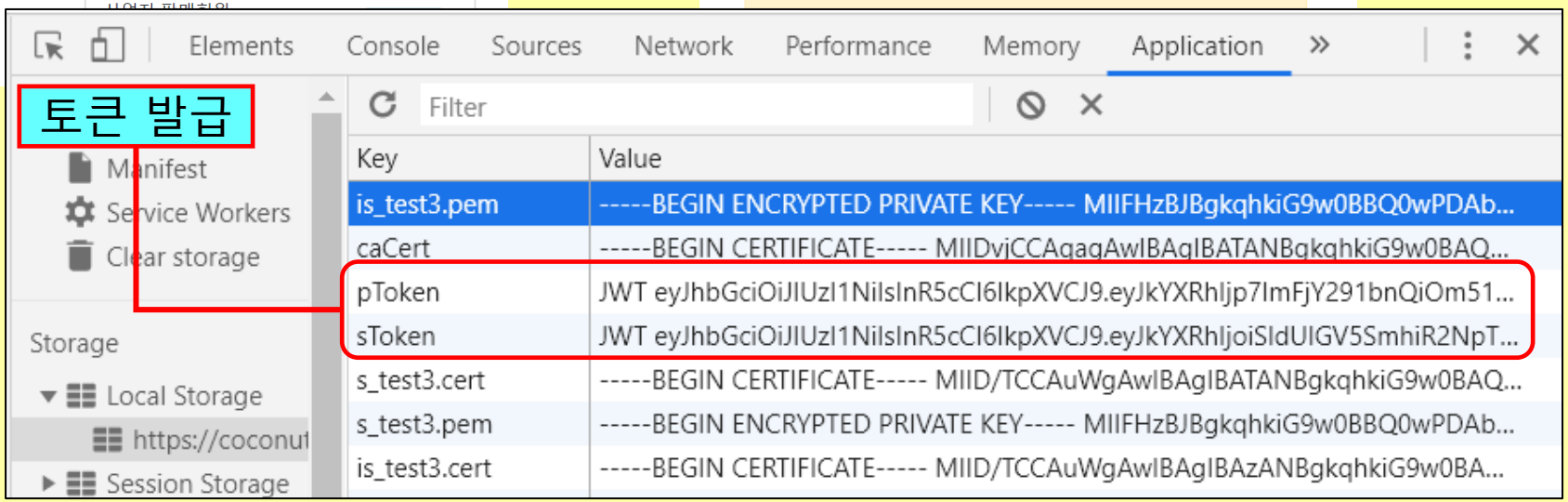
1. 초기화면

개발 시스템 (2/10)

2. 사용자 등록, 로그인, 인증유지

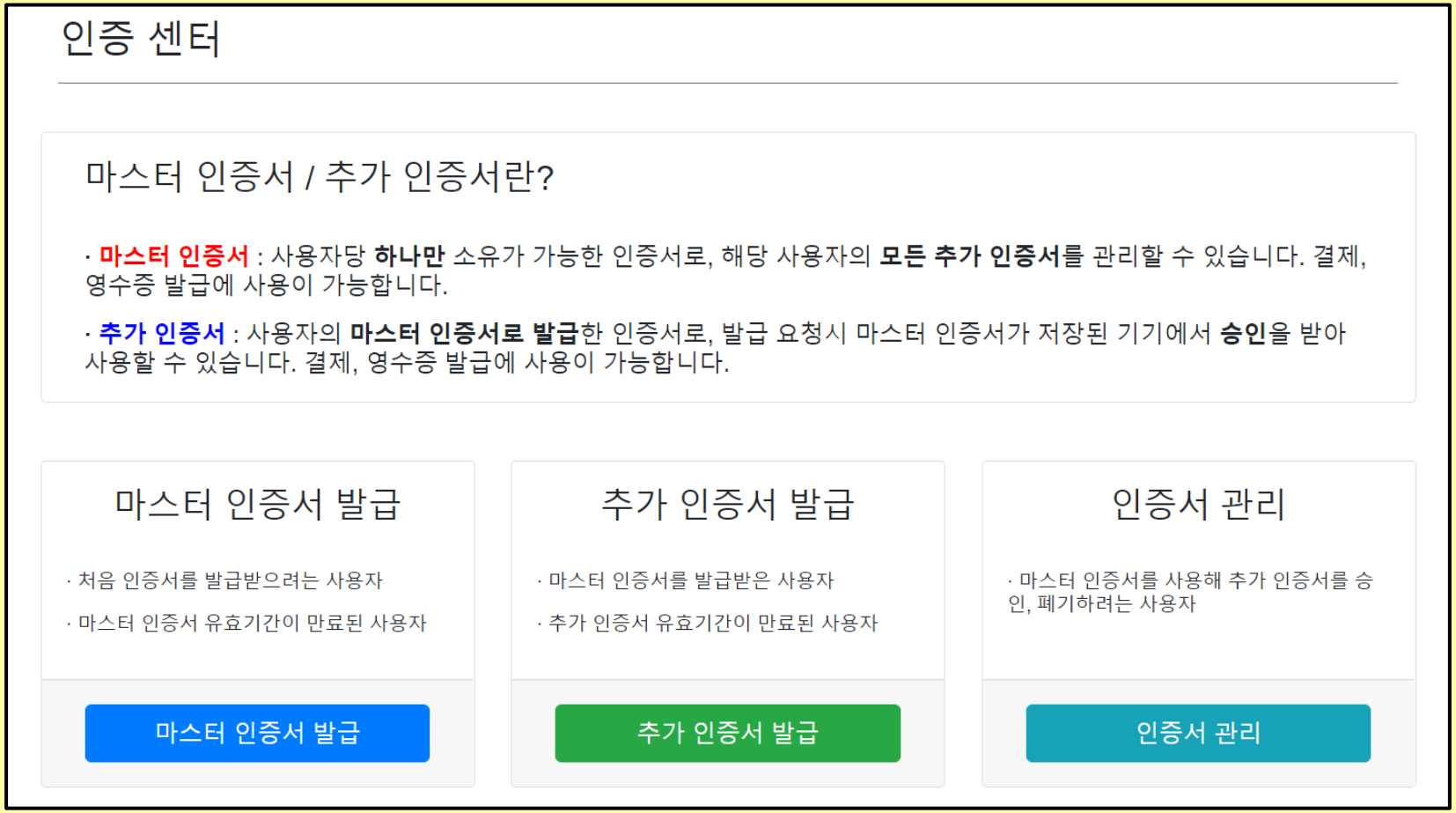






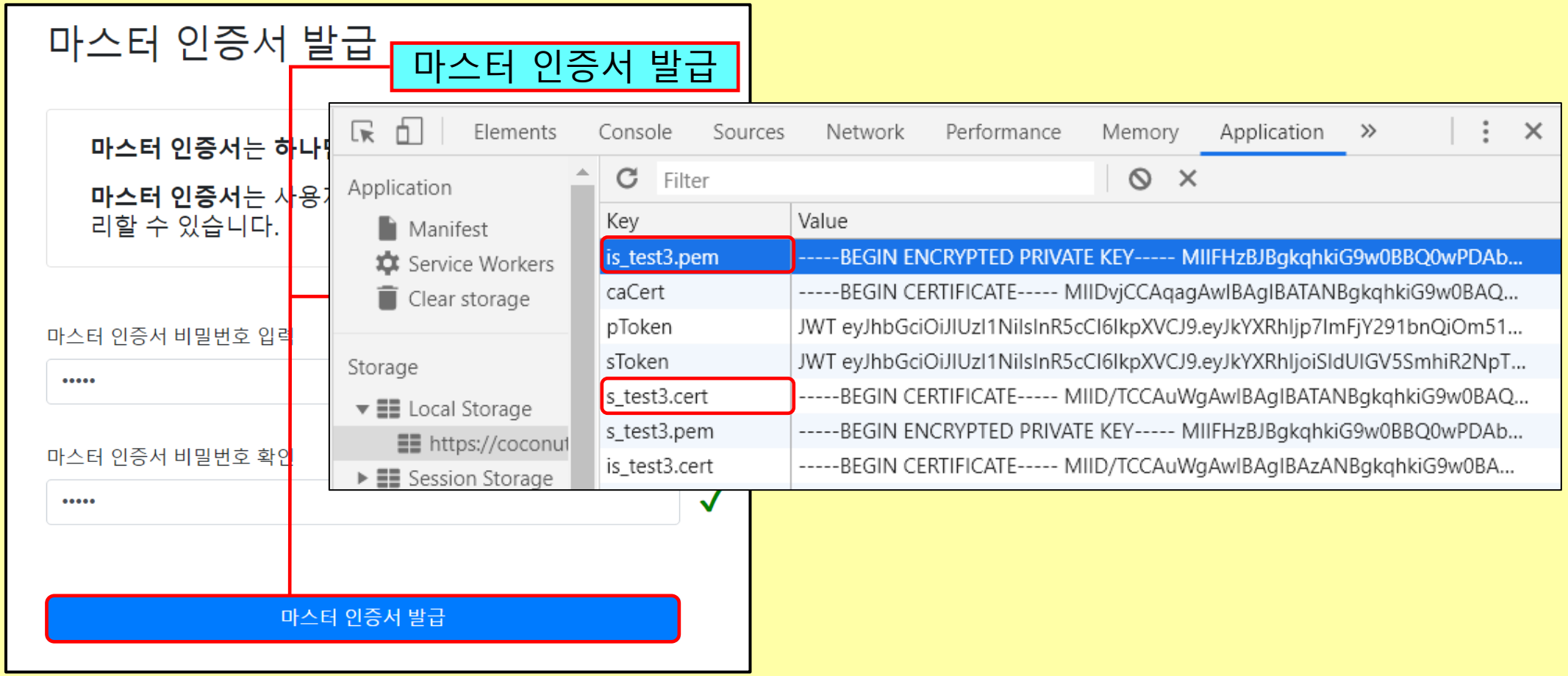
개발 시스템 (3/10)

3. 인증 센터



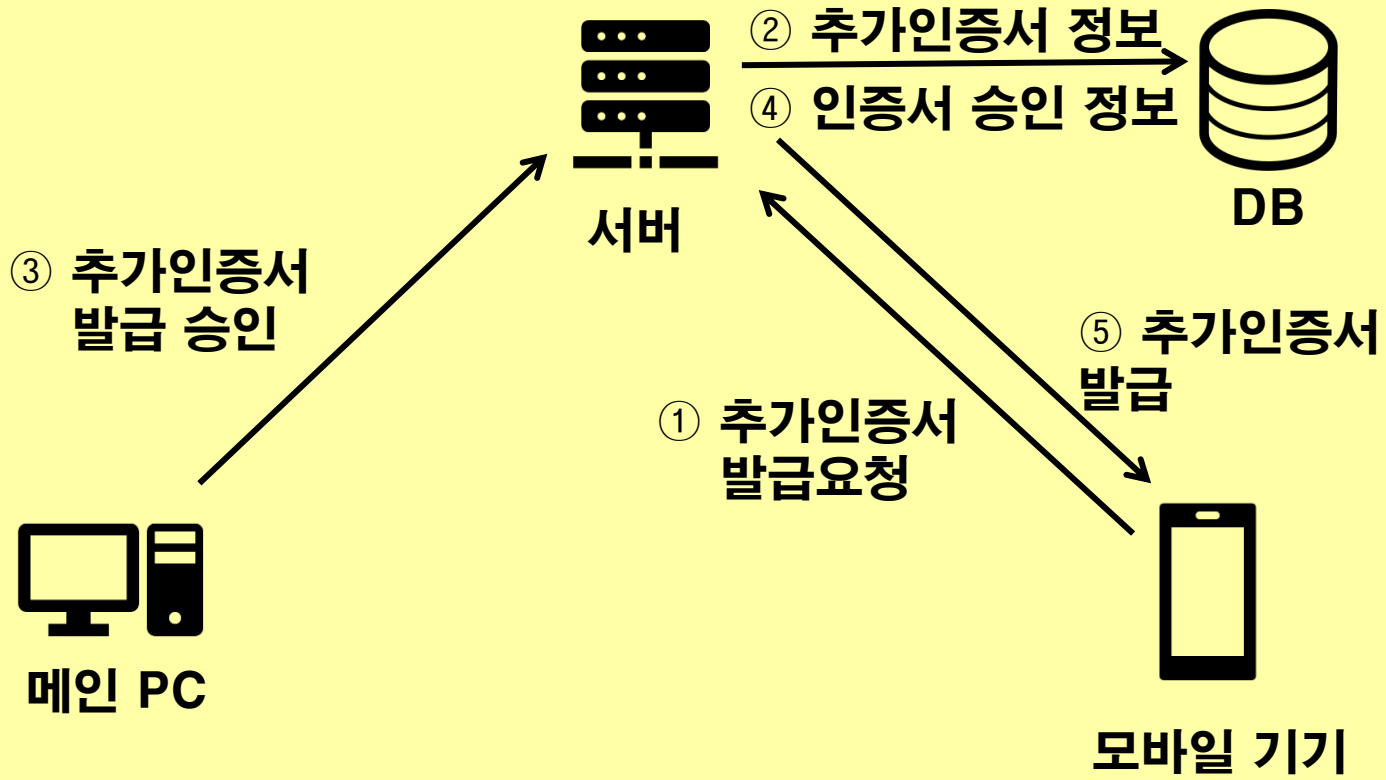
개발 시스템 (4/10)

4. 마스터 인증서 발급



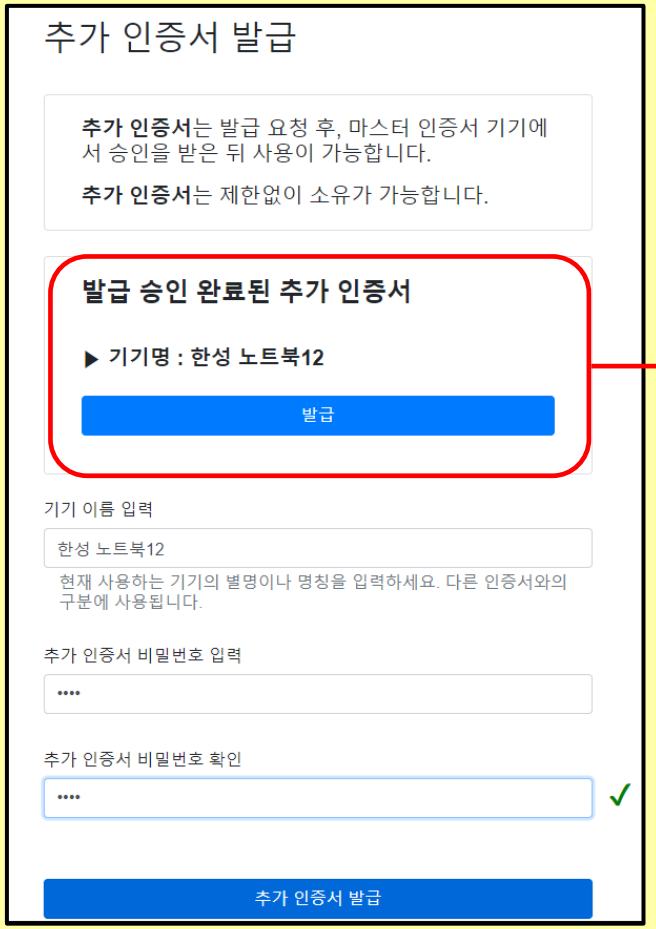
개발 시스템 (5/10)

5. 추가 인증서 발급



개발 시스템 (6/10)

5. 추가 인증서 발급



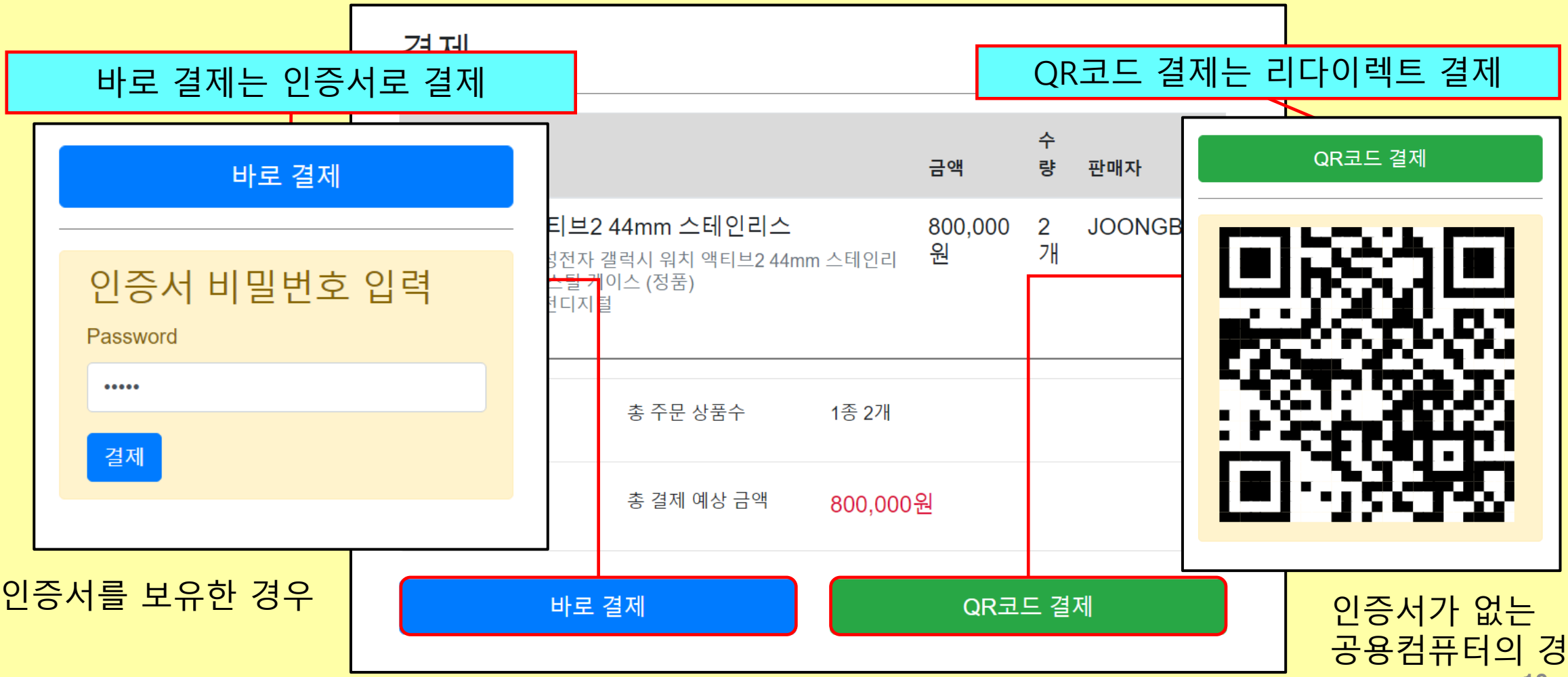
별도의 기기로 인증서 발급 신청

개발 시스템 (7/10)

6. 인증서 관리

개발 시스템 (8/10)

7. 결제

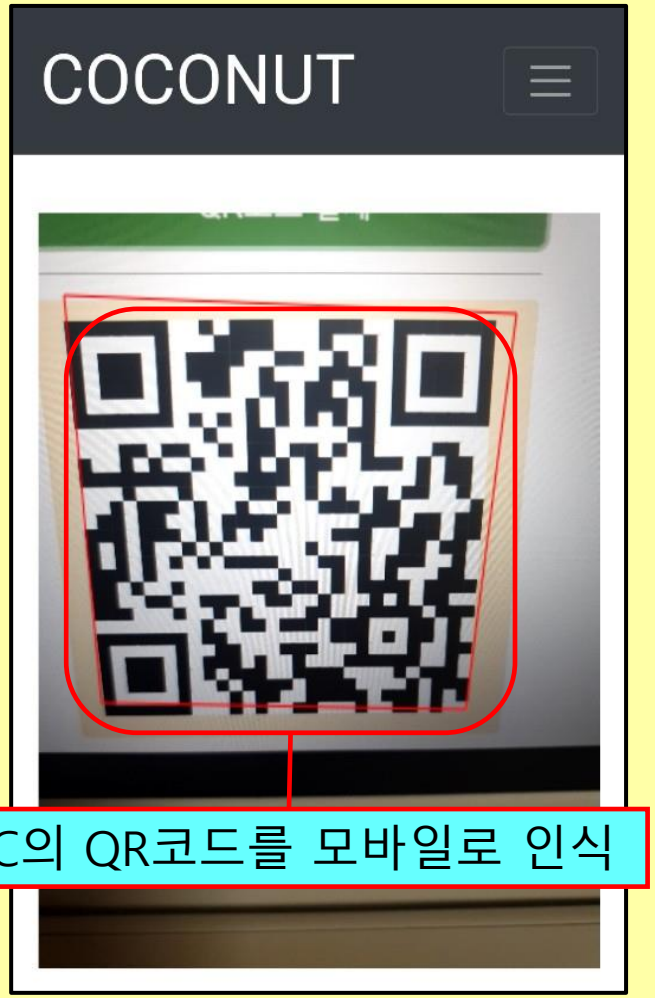


인증서를 보유한 경우

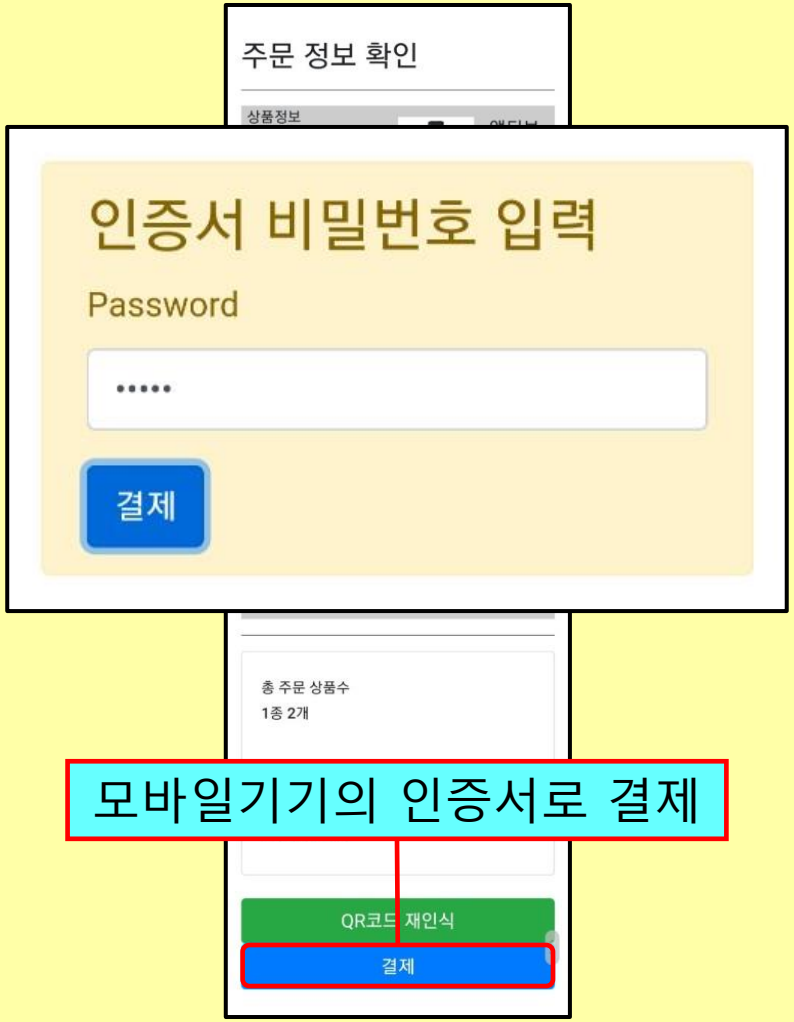
인증서가 없는 공용컴퓨터의 경우

개발 시스템 (9/10)

8. QR코드 결제



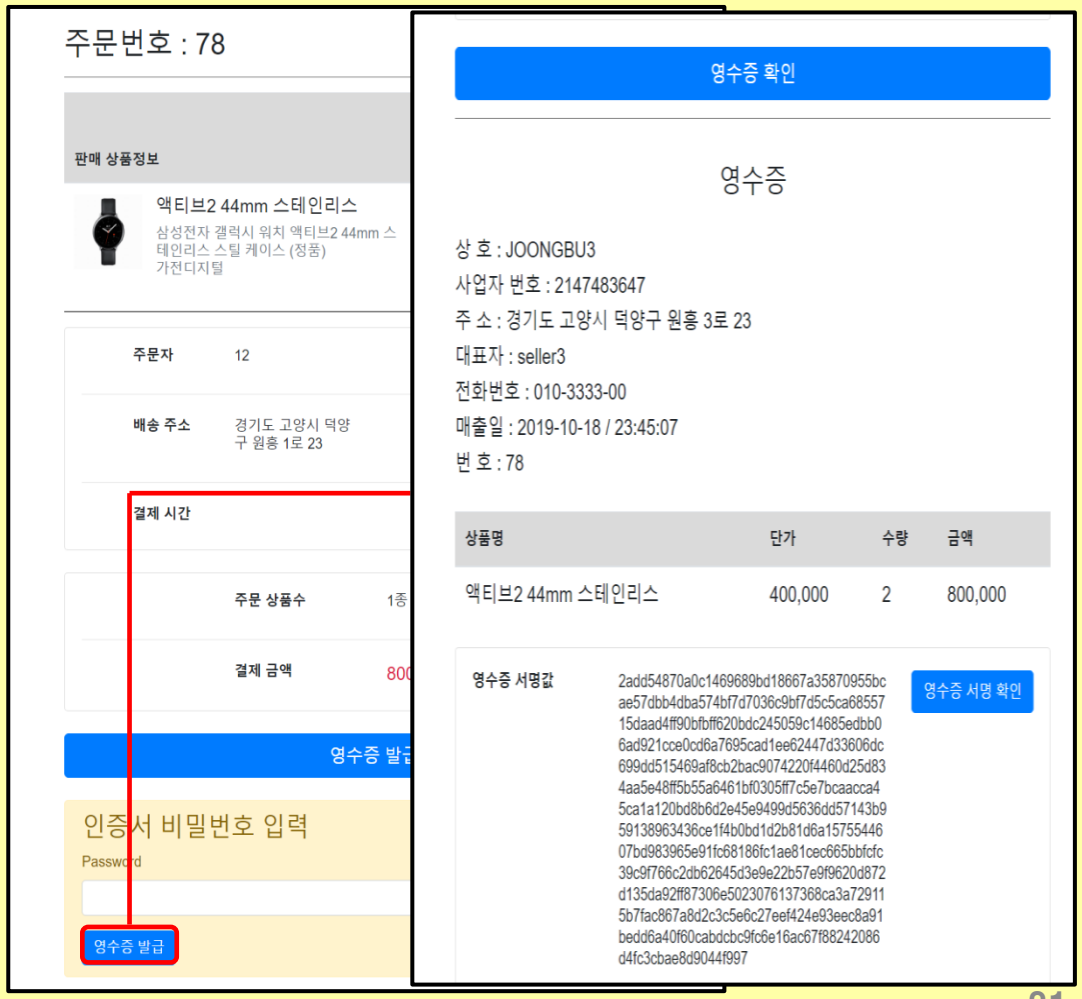
PC의 QR코드를 모바일로 인식



모바일기기의 인증서로 결제

개발 시스템 (10/10)

9. 서명 검증



서비스 활용성 분석

- **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

○ 결 론

- 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