Stylus Pen을 활용한
소유 및 속성 기반 본인 인증 방식 제안

김현지

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

01. 제안 배경

01. 제안 배경

❖ 최근 신용카드 사용 비중 및 결제 건수 증가 → 보안 위협 또한 증가 추세

- 카드 분실, 도난, 제3자 범죄 → 부정사용 연간 약 3만 8000건 (금융감독원, 지난 5년간 신용카드 부정사용 현황)
- 카드사의 지나친 영업 & 온라인 및 모바일 카드 발급 증가 → 명의 도용 가능성 늘어날 전망

❖ 개인정보 알고 있는 경우, 명의도용 발생 쉬움

❖ 그러나 인증 필요한 과정에서 형식적 인증 절차를 거치는 것이 관련 범죄의 원인 중 하나

01. 제안 배경 : 현재 본인 인증 방식의 한계점

빈번히 발생하는 부정사용 및 명의 도용 방지 위해

추가적 보안 절차 필요

새로운 본인 인증 기법 제안

➢ **사실상 보안 절차가 없는 것과 같음**

02. 관련연구

2.1 SET protocol

❖ Secure Electronic Transaction

- 안전한 신용카드 거래를 위해 개발된 프로토콜
- 신용카드 번호 등 중요 결제정보를 암호화하고, x.509 공개키 인증서 발급 통한 상호간 인증
- Dual signature 사용
- 디지털 서명과 해시함수에 의해 메시지 무결성 보장

❖ 장점

- 사기 방지
- 기존 신용카드 시스템 활용 가능
- SSL의 단점(상인에게 지불정보를 노출) 해결

❖ 단점

- 암호화 과정 복잡 & 속도저하(RSA로 인해)
- 별도의 하드웨어, 소프트웨어 요구

2.1 SET protocol

❖ Dual signature 목적

- 고객의 **지불 정보가 판매자에게 노출될 가능성 있음**
- 판매자에 의한 **지불 정보의 위/변조의 가능성 있음**
- 하나의 거래 정보에서 부분적으로 정보를 가리기 힘든 점 보완

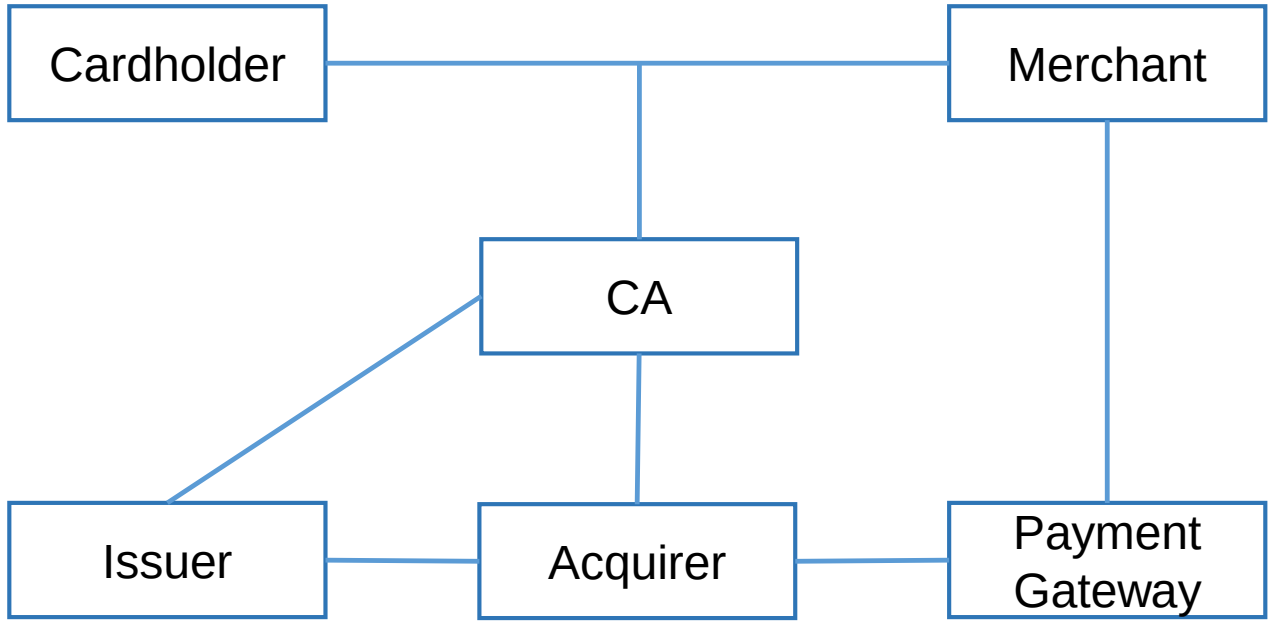
- 판매자에게 지불 정보를 노출시키지 않으면서도 구매자 및 거래내용의 **정당성 확인** 가능

  → **실제 사용자가 의뢰한 전문인지 확인하기 위해** 도입

2.1 SET protocol

❖ 참여주체

- 카드사용자 (Cardholder)
- 상인 (Merchant)
- 지급정보 중계기관 (PG, VAN)
- 인증기관 (CA)
- 카드사 (Issuer)
- 매입사 (Acquier)



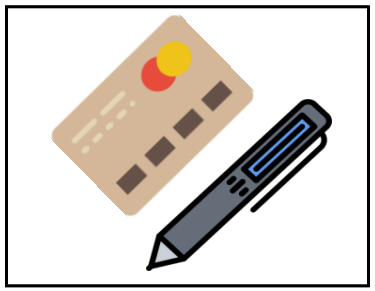
*Payment Gateway : 상점이 전달한 카드로 금융기관에 결제요청
*CA : X.509 시스템에서 규약에 따라 SET 참여자에게 공개키를 가진 인증서 발급

2.1 SET protocol

❖ 수행 단계

1. 판매자, PG,카드사, 매입사는 CA로부터 인증서 발급 받음
2. 구매자는 전자지갑 실행하여 신용카드 등록 후, CA로부터 인증서 발급 받음
3. 상품 구매시 전자지갑 작동하여 판매자에게 지불정보 전달
4. 판매자는 PG에게 결제정보 전달
5. 카드사, 매입사는 판매자에게 대금 결제

2.1 SET protocol : 구성도



카드사용자

카드사의 승인까지
관련 데이터 보관

Server

각 참여기관에
전자 인증서 발급

CA

① 카드 결제

⑧ 서명

⑦ 서명 요청

⑨ 거래 완료

② 카드 읽은 후 데이터 저장

구매 정보만 확인

판매자

⑤ 정당한 결제인지
확인 후 승인

② 지불 정보

지불 정보 확인
정당성, 위/변조 여부
확인

PG/VAN

③ 카드 조회

카드사용자의 계좌가
개설된 금융기관

카드사

판매자의 계좌가
개설된 금융기관

매입사r

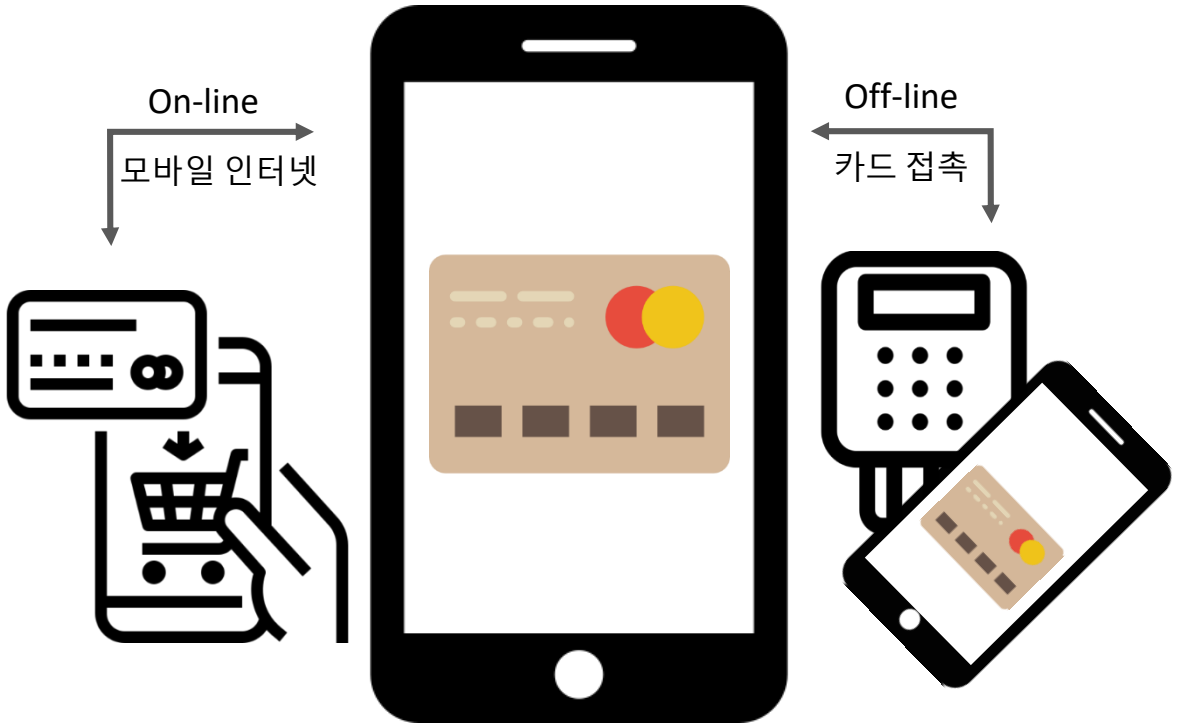
2.2 KS X 6928

❖ **국내 모바일 지급결제 표준** : 모바일 기기에 신용 카드 저장하여 결제하는 방식

- **스마트폰에 내장된 모바일 신용카드 (KS X 6928-1)**
- **대면 거래 (KS X 6928-2)**

  → RF 통신모듈에 모바일 신용카드를 접촉시켜 거래
- **비대면 거래 (KS X 6928-3)**

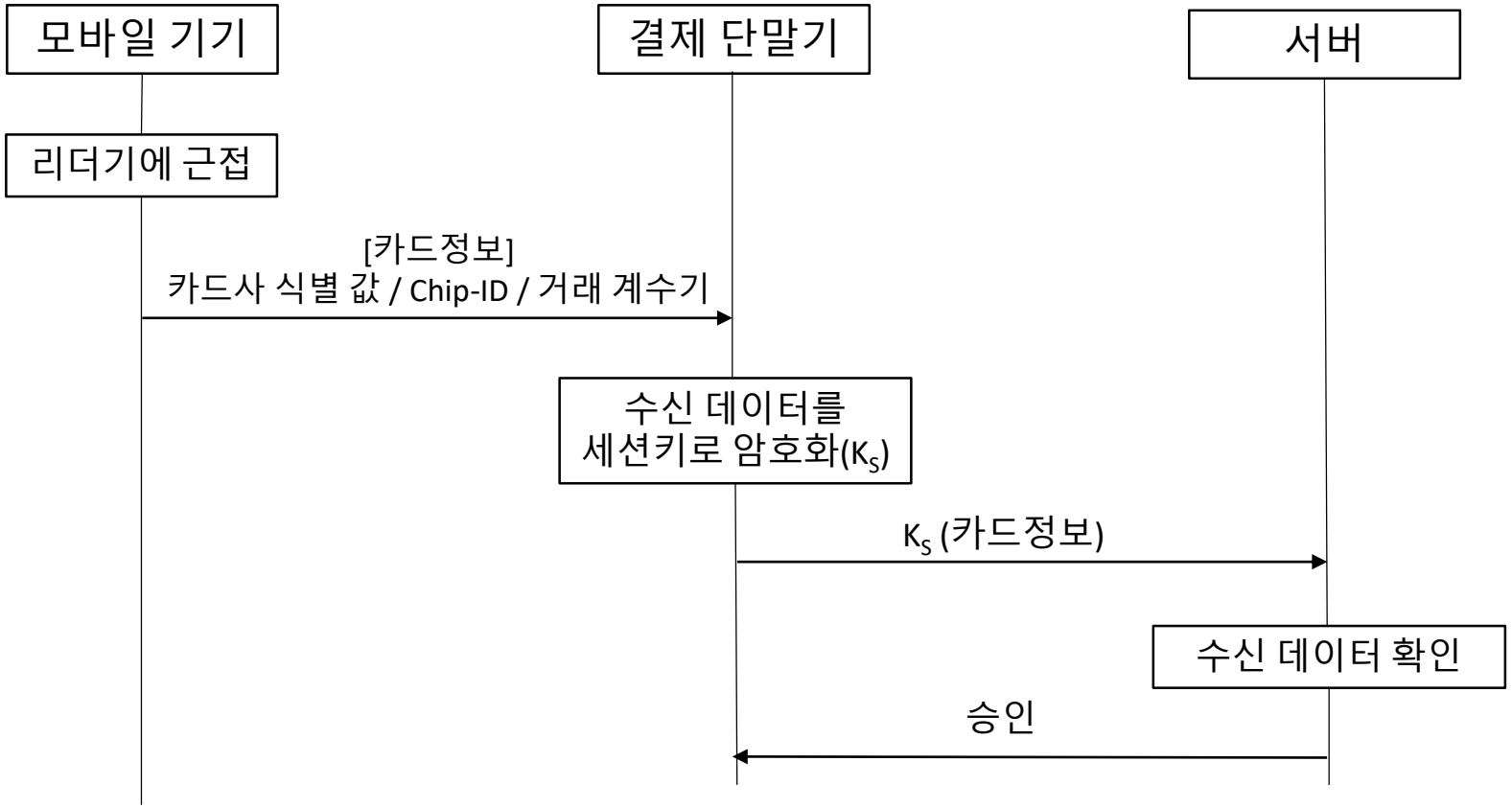
  → 모바일 인터넷 통해 결제



2.2 KS X 6928

❖ 대면 거래

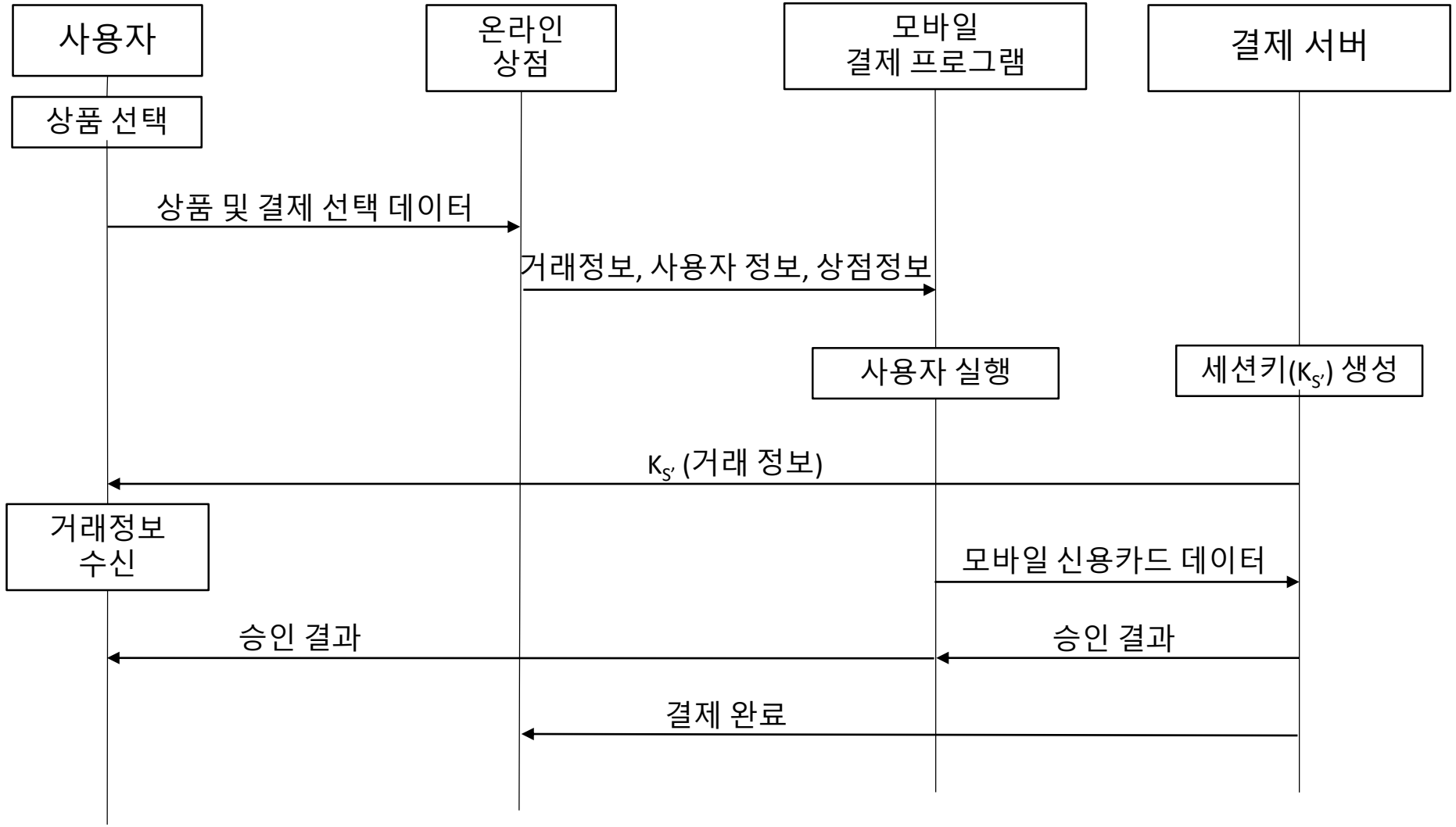
- NFC 이용 → 모바일 카드가 저장된 모바일 기기에서 결제 단말기로 데이터를 전송하여 온라인으로 거래



2.2 KS X 6928

❖ 비대면 거래

모바일 결제 프로그램 통한 온라인 결제



2.3 가속도 및 자이로센서를 활용한 동작인식

❖ 센서

- 가속도, 각 속도, 빛 등의 주변의 상황, 변화를 감지하는 감지기

❖ 가속도 센서

- 움직임의 방향과 세기 측정
- 정적인 상태에서 정확한 측정 가능 → 움직임 발생 직후 측정값 : 부정확

❖ 자이로스코프 센서

- 회전 운동 측정
- 각 속도를 적분하여 각도 측정 → 누적오차 발생

➢ 두 센서를 융합하여 사용할 경우, 더 정확한 측정 가능

2.4 필기서명 인증

❖ 본인인증 기술

- 생체인식 인증 기술 중 하나
- 특성벡터(속도, 가속도, 시간, 획순서 등) 추출하여 판별 → 정교한 본인인증 가능

❖ 다양한 특성 비교

- 모방 불가능
- 기존 본인 인증 수단이 가지는 분실, 도난, 유출 등의 문제점 보완

❖ 서버에서 검증이 가능

➢ 서명 통한 본인 인증 필요한 분야 적용에 적합

03. 제안기법

03. 제안 기법

❖ 스마트폰에 등록된 카드 대상

1. 평균적으로 고액결제 하는 카드 (ex. 용도에 따라) 및 보안 위협의 risk가 큰 카드를 등록

2. 비대면거래, 대면거래 모두 활용 가능

➢ 사용자가 원하는 카드를 등록하여 선택적으로 제공하고자 함

03. 제안 기법

❖ 신용카드 명의자와 결제된 카드가 등록된 스마트폰의 소유자가 일치하는지 확인

- 카드 소유자의 스마트폰으로 지문 인증 요청

➢ **카드 사용자가 본인 명의 카드로 결제했음을 인증**

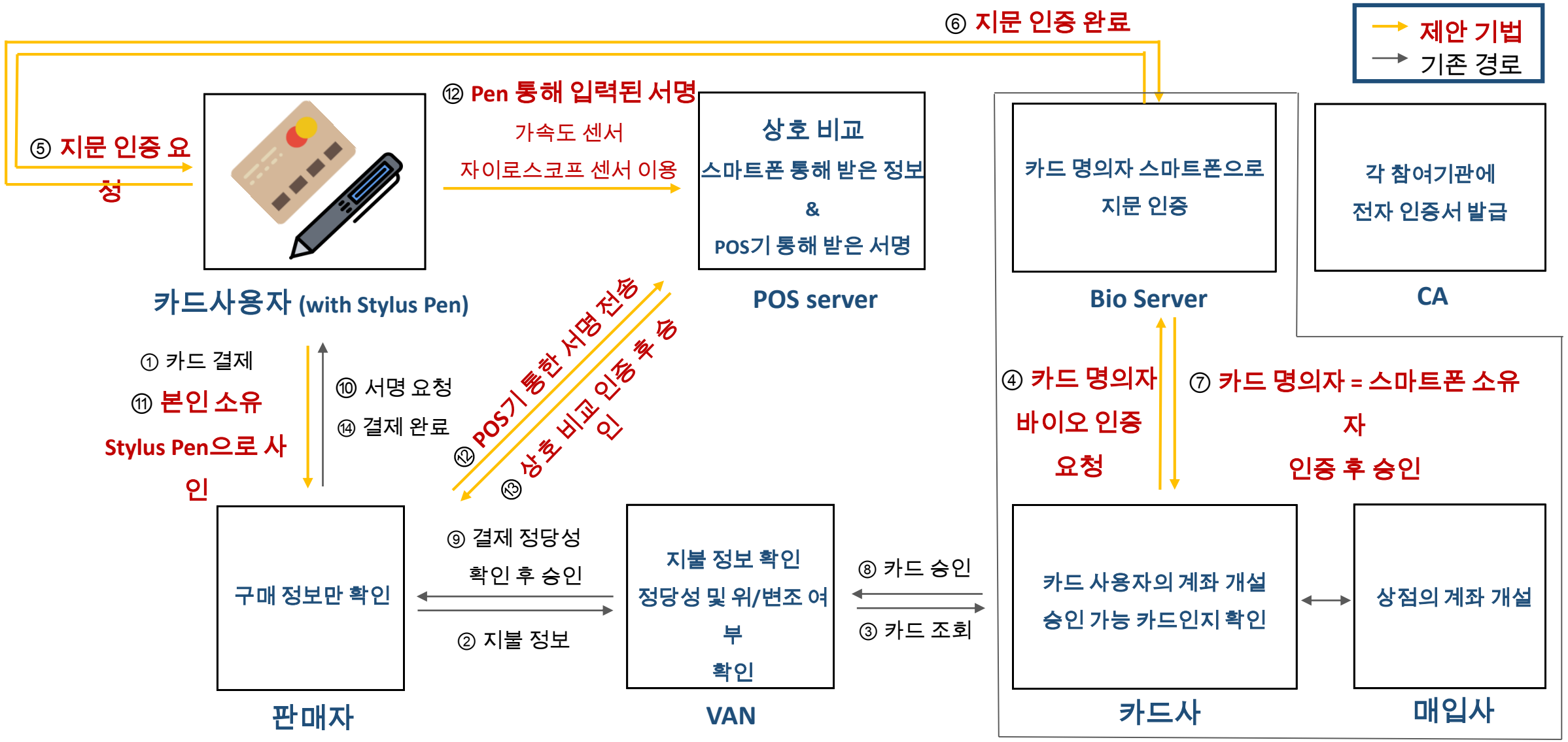
❖ 서명하는 값이 실제로 본인의 Stylus Pen으로 입력한 값인지 확인

- Stylus Pen에 내장된 센서 측정값
  → 스마트폰 통해 POS serve로 전송
- 카드결제기에 입력된 서명
  → POS serve로 전송

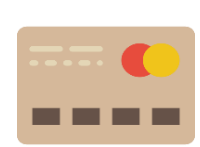
➢ **두 서명의 유사도, 시간 등을 고려한 상호 비교를 통한 인증**

*Stylus pen

03. 제안 기법 : 구성도


⑥ 지문 인증 완료
제안 기법
기존 경로
⑤ 지문 인증 요청
⑫ Pen 통해 입력된 서명
가속도 센서
자이로스코프 센서 이용
상호 비교
스마트폰 통해 받은 정보
&
POS기 통해 받은 서명
카드 명의자 스마트폰으로
지문 인증
각 참여기관에
전자 인증서 발급
카드사용자 (with Stylus Pen)
POS server
Bio Server
CA
① 카드 결제
⑪ 본인 소유
Stylus Pen으로 사인
⑩ 서명 요청
⑭ 결제 완료
⑬ POS기 통한 서명 전송
⑮ 상호 비교 인증 후 승인
④ 카드 명의자
바이오 인증
요청
⑦ 카드 명의자 = 스마트폰 소유자
인증 후 승인
구매 정보만 확인
⑨ 결제 정당성
확인 후 승인
② 지불 정보
지불 정보 확인
정당성 및 위/변조 여부
확인
⑧ 카드 승인
③ 카드 조회
카드 사용자의 계좌 개설
승인 가능 카드인지 확인
상점의 계좌 개설
판매자
VAN
카드사
매입사

03. 제안 기법 : 구성도



카드사용자

판매자

VAN / 카드사 / 매입사

결제

기존 SET protocol의 전달 정보

1. 구매정보 및 지불정보

2. 카드 소유자 비밀키

3. (M1 + M2), M

구매 정보만 확인 후 지불 정보 등 그대로 전달

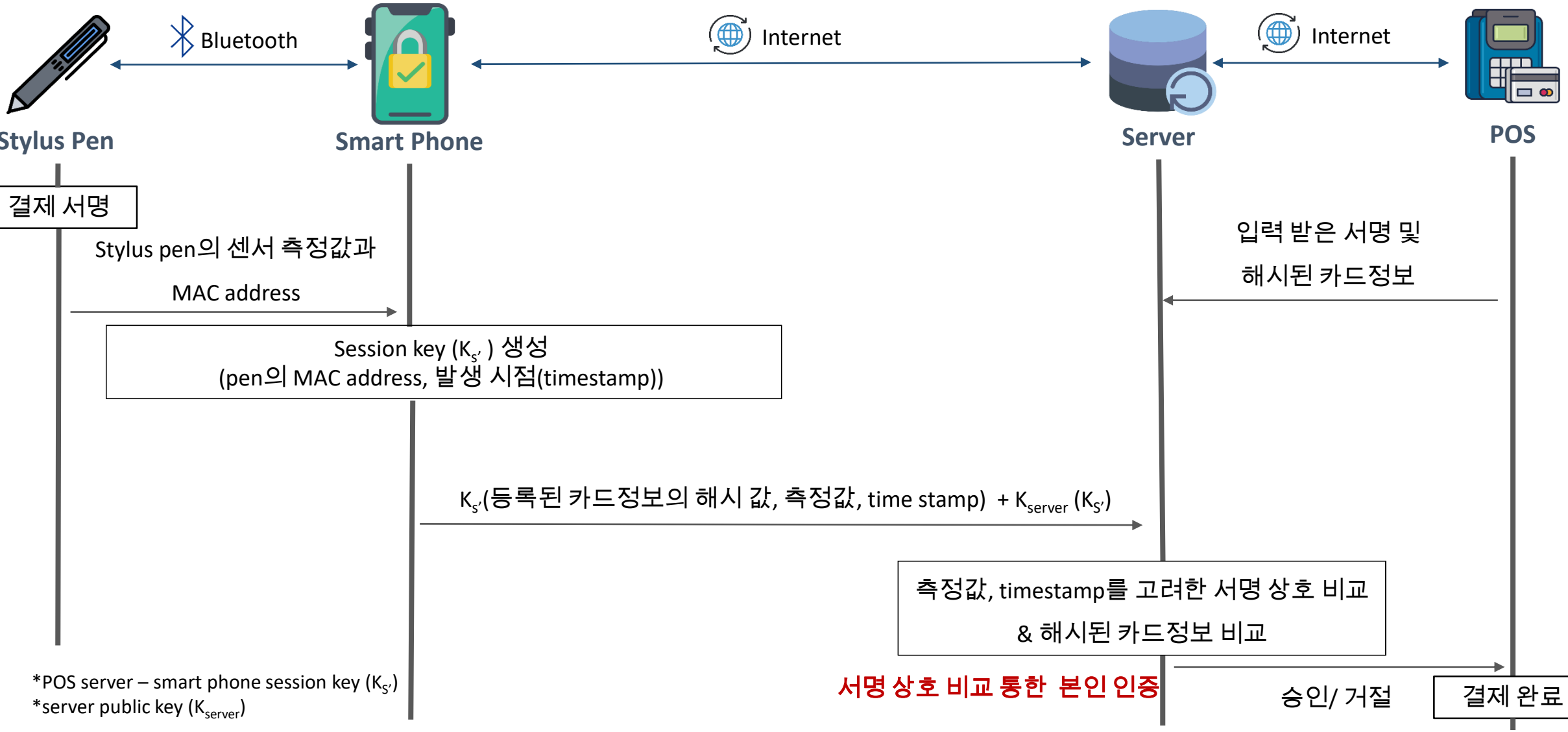
기존 지불정보에 인증 위한 data 추가하여 전송

스마트 폰의 MAC address의 hash 값 + 카드 정보 해시 값

신용카드 명의자 = 스마트폰 소유자

카드가 등록된 스마트폰의 MAC 주소
및 카드 정보의 해시값 비교
스마트폰 소유자 = 카드명의자 확인 후
해당 기기로 바이오 인증 (선택)

03. 제안 기법 : 구성도


Bluetooth
Internet
Internet
Stylus Pen
Smart Phone
Server
POS
결제 서명
Stylus pen의 센서 측정값과
MAC address
Session key ($K_{s'}$) 생성
(pen의 MAC address, 발생 시점(timestamp))
입력 받은 서명 및
해시된 카드정보
$K_{s'}$(등록된 카드정보의 해시 값, 측정값, time stamp) + K_{server} ($K_{s'}$)
측정값, timestamp를 고려한 서명 상호 비교
& 해시된 카드정보 비교
서명 상호 비교 통한 본인 인증
승인/ 거절
결제 완료
*POS server – smart phone session key ($K_{s'}$)
*server public key (K_{server})

04. 결론

04. 결론

❖ Multi Factor Authentication

- **카드 명의자 = 스마트 폰 소유자**

  → 카드 명의자와 동일한 명의의 스마트폰을 소유함으로써 인증 (소유기반)

- **Stylus Pen 통한 서명과 POS기 통한 서명 상호 비교**

  → 두 서명이 같으며, 카드 사용자 명의의 Stylus Pen이 결제서명에 실제로 사용되었음을 확인 (소유 및 속성)

- **지문 인증 (optional)**

  → 카드 명의자 소유의 스마트폰 통해 인증 (속성기반)

➢ **소유 및 속성 기반 본인 인증을 통해, 카드 명의자가 해당 결제 및 카드사용에 직접 동의했음을 증명**

04. 결론

❖ 기존 방식과의 본인인증 신뢰도 비교

	기존 방식	제안 기법
명의 확인 (소유 기반)	낮음	높음
지문 인증 (속성 기반)	없음	높음
결제 서명 (소유 + 행위)	사실상 매우 낮음	높음
신뢰도	낮음	높음

04. 결론

❖ 기존 방식과의 본인인증 보안 강도 비교

	기존 방식	제안 기법
복합 인증 적용	없음	있음
부정사용 위협	높음	낮음
인증 정보 유출 및 해킹 위험성	높음	매우 낮음
보안 강도	낮음	매우 높음

04. 결론

❖ 사실상 보안적 기능이 없는 형식적 절차

- 결제 서명 과정을 본인 인증 과정으로 변경

➢ 금융거래에서의 보안성 증진

❖ 서명 통한 본인인증 과정 필요한 분야에 활용 기대

- 카드 발급 시 명의 도용 방지 위한 본인 인증 절차
- 멤버십 적립

➢ 이외에도 다양한 분야에 적용 가능할 것으로 예상

Q & A