TEE 기술 소개 및 활용 방안

SOLACIA ensures trust and confidence in user experience
by making digital interactions
secure and convenient.

SOLACIA

We're always here to help you

SOLACIA ensures trust and confidence in user experience by making digital interactions secure and convenient.

SOLACIA Hansol

Contents

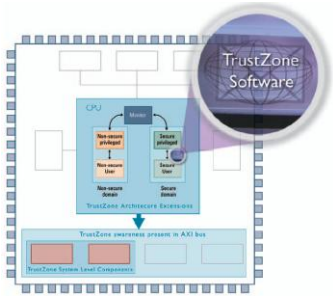
- **TEE 기술 소개**
  - TEE Overview
  - Use Case
  - Secure Elements 비교
- **TEE 활용 방안**
  - FIDO와의 결합
  - HCE + TEE & Cloud SE

1. TEE 기술 소개

1) TEE Overview (1/2)

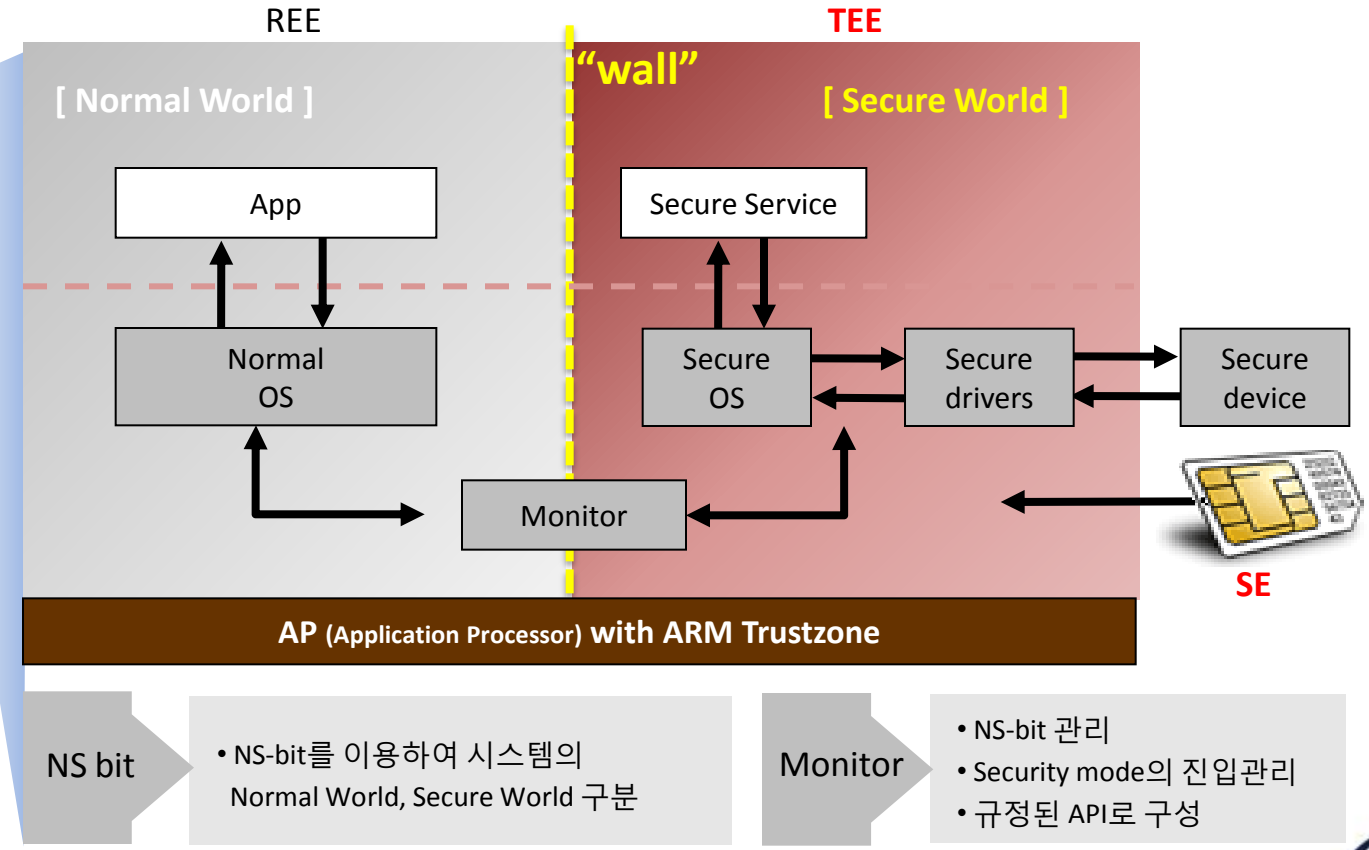
❑ 안정성 보장을 위하여 'TrustZone' IP 기반의 AP 칩을 통해 프로세서와 주변장치, 저장장치를 대상으로 보안 서비스를 제공하는 소프트웨어 플랫폼

– Normal World와 Secure World의 엄격한 분리를 지원하는 하드웨어 기능(TrustZone)과 이를 이용하여 보안 서비스를 제공하는 소프트웨어(SP)로 구성



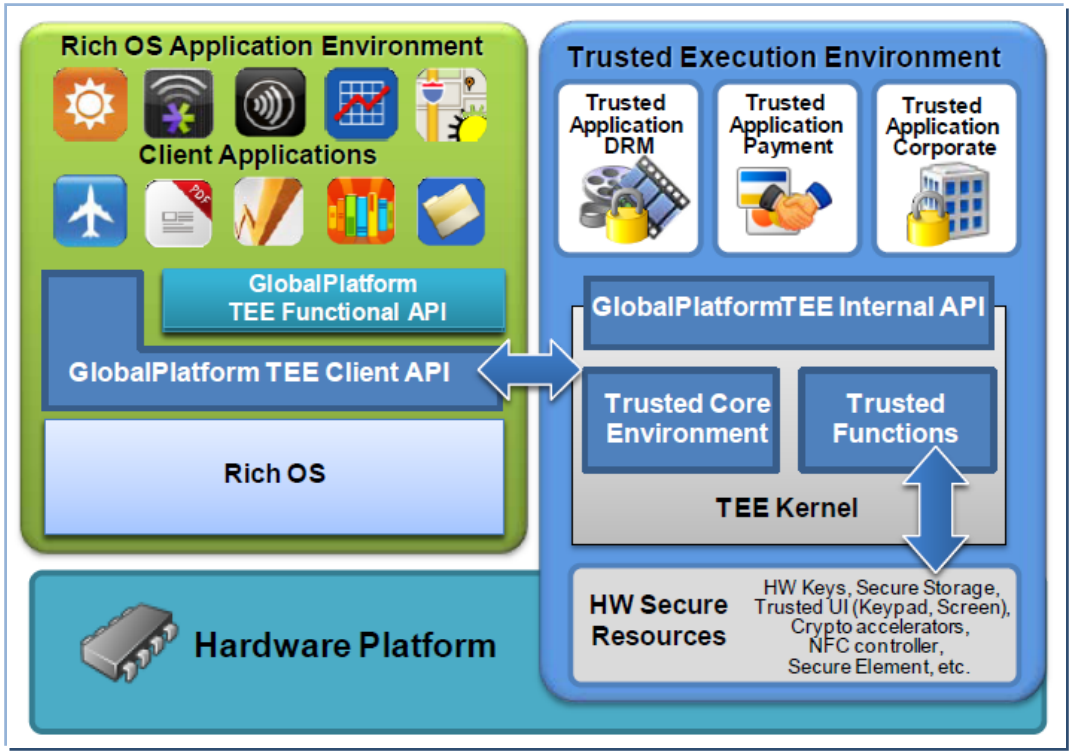
[특 장 점]

- **Hardware-based Isolation**
- H/W, S/W **보안 결합으로 보안 수준 향상**



1) TEE Overview (2/2)

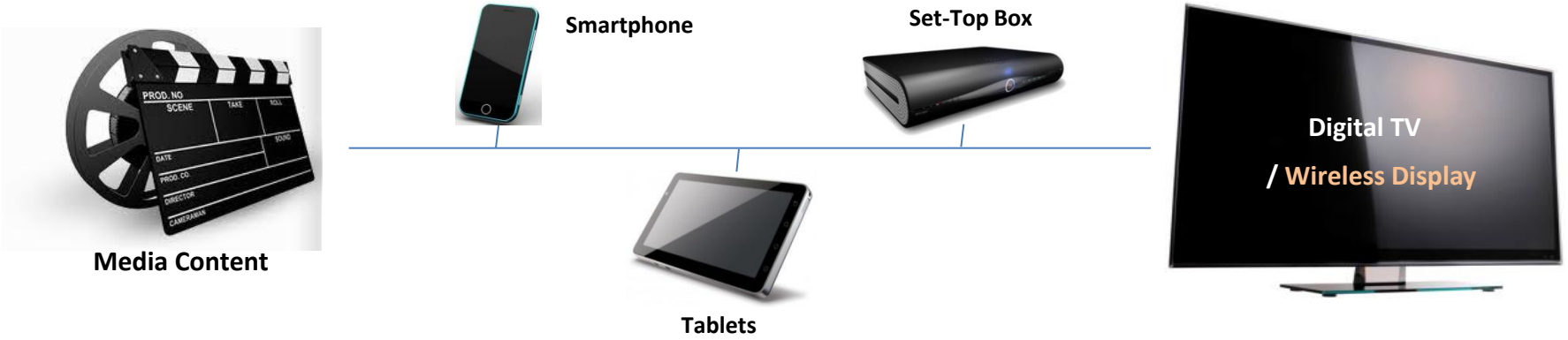
- TEE = Trusted Execution Environment
  - Trustzone H/W 를 이용하여 개방형 Operating System에 독립적으로 격리된 실행 환경을 제공



- H/W기반의 독립된 실행 환경 제공
- 안드로이드(REE)와 TEE에 별도의 API 제공
- TEE는 user interface, memory, video / audio h/w, crypto accelerator등에 접근
- Secure Boot, Secure Storage 등의 기능
- Global Platform에서 활발하게 표준화 中
- 스마트카드와 유사한 보안 체계를 가짐

Premium Content Protection

- DRM (Digital Rights Management)이나 다른 Content Protection 솔루션들이 TEE 기술을 통해 보안 강화
- Content Protection을 위한 TEE 기술들
  - Secure Playback, Secure Data path에 대해 TEE 기술 적용
  - Software CAS (Conditional Access System)
  - encryption / decryption key를 위한 Secure Storage

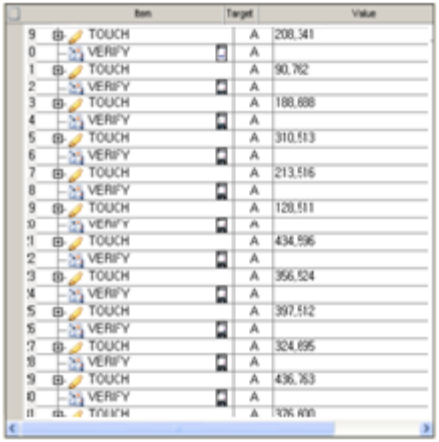


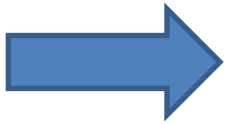
Payment

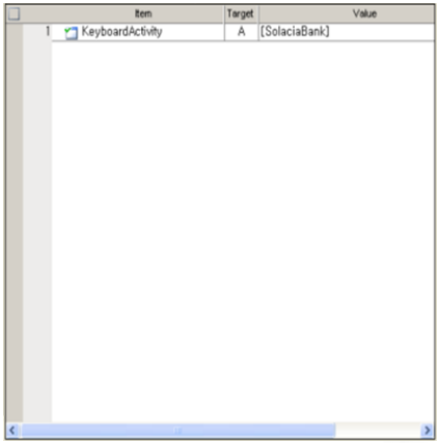
- TEE를 통해 Secure Element와 보다 안전하게 연동
- 공인인증서, Key 등의 중요한 데이터 저장 공간으로 활용
- Trusted User Interface 사용하여 결제 message를 안전하게 display 가능

Secure Input

- Device hooking 이나 Malware 등을 통해 유출 될 수 있는 개인 정보 보호
- TEE가 직접 touch screen input정보를 처리하여 Rich OS 는 접근이 불가 함







BYOD(Bring Your Own Device)

- 스마트 기기의 확산과 모바일 오피스에 대한 Needs 증가로 인한 개인 휴대기기의 업무 사용 빈도 증가에 따라 '개인 자율성 vs 회사 정보 보안'이라는 문제에 대한 해결책으로 TrustZone 기술을 활용

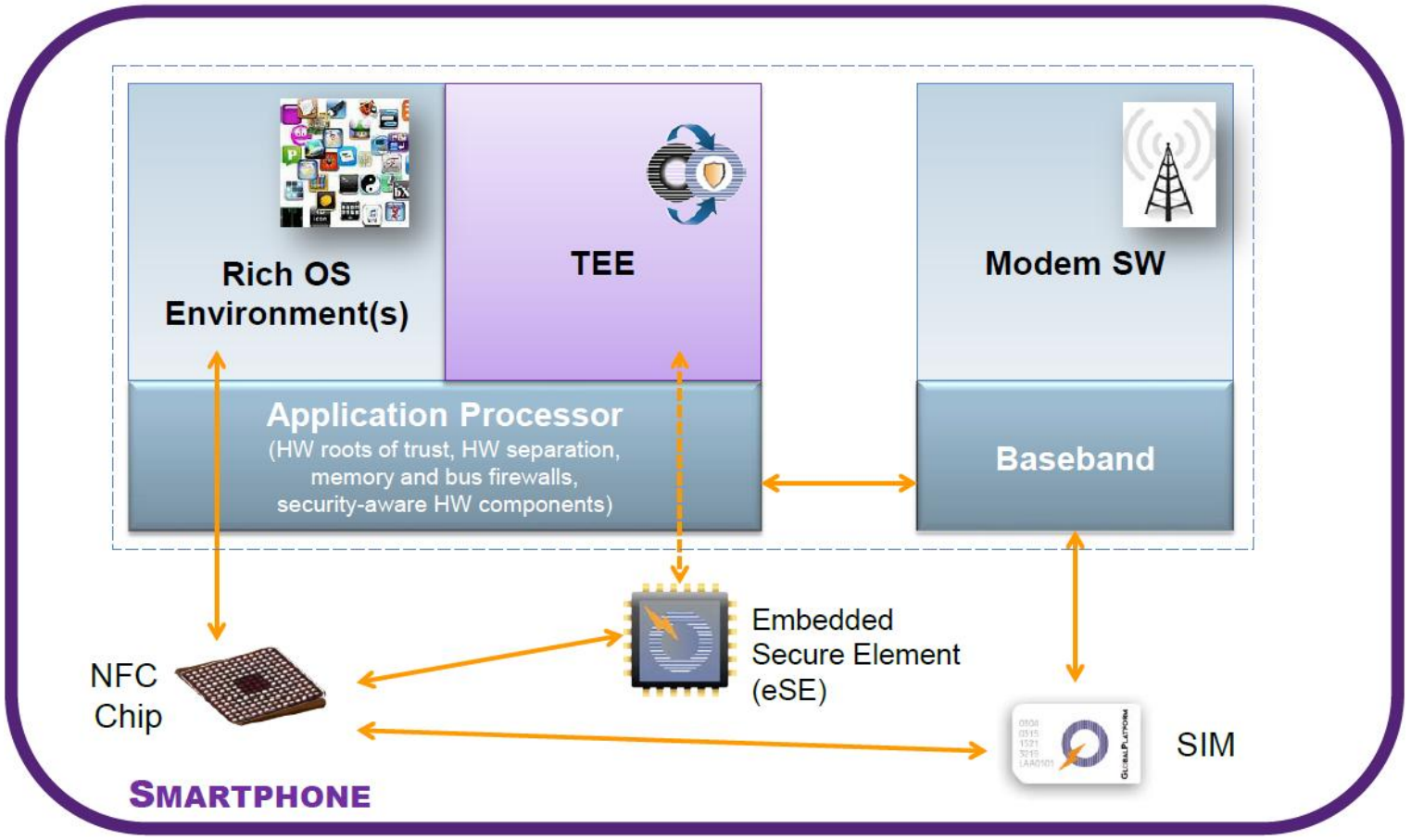
3) Secure Elements (1)

❑ USIM, Mobile TPM, TEE는 상호 보완적인 기술임

구 분	USIM 기반	Mobile TPM (Trusted Platform Module)	TEE
개요	• USIM을 활용하여 보안 기능 제공 (공인인증서 등)	• 물리적으로 독립된 보안 Chip을 활용하여 보안 기능 제공	• TrustZone 지원 AP Chip 기반 Secure OS를 통해 서비스 제공
보안성	• USIM 내부의 다양한 Application에 보안 서비스 제공 • Tamper-resistant	• Secure Boot등 단말과 연관된 추가 보안 서비스 가능 • Tamper-resistant	• S/W Attack에 대한 방어 가능 • H/W, S/W 보안 결합으로 인한 보안 수준 향상
경제성	• 별도의 USIM 비용 필요 • 이미 하나의 보안 플랫폼化 (massively deployed)	• 보안적용을 위한 별도의 Chip 개발 필요 • 단말 제조라인 변경 및 원가 상승	• AP Chip 기반 위에 보안 플랫폼 제공으로 단말제조라인의 변경이 없고, 원가 상승 부담이 없음

4) Secure Elements (2)

❑ “Simplified” Mobile Security 구조

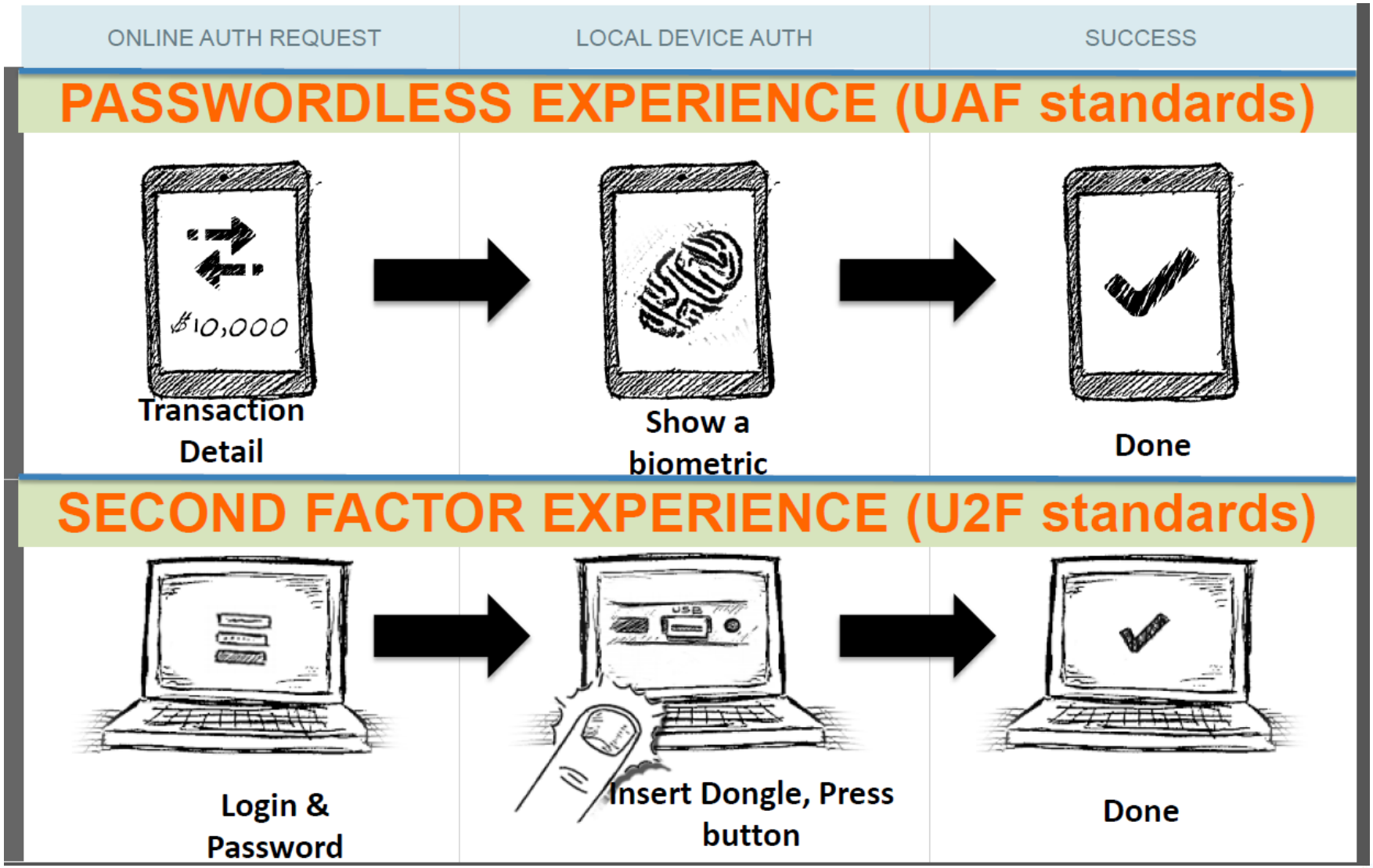


출처: Global Platform

2. TEE 활용 방안

1) FIDO와의 결합 (1/2)

- FIDO (Fast IDentity Online) Alliance



출처: FIDO white paper

1) FIDO와의 결합 (2/2)

❑ Client(device) 정보 보호에 TEE 기술 사용

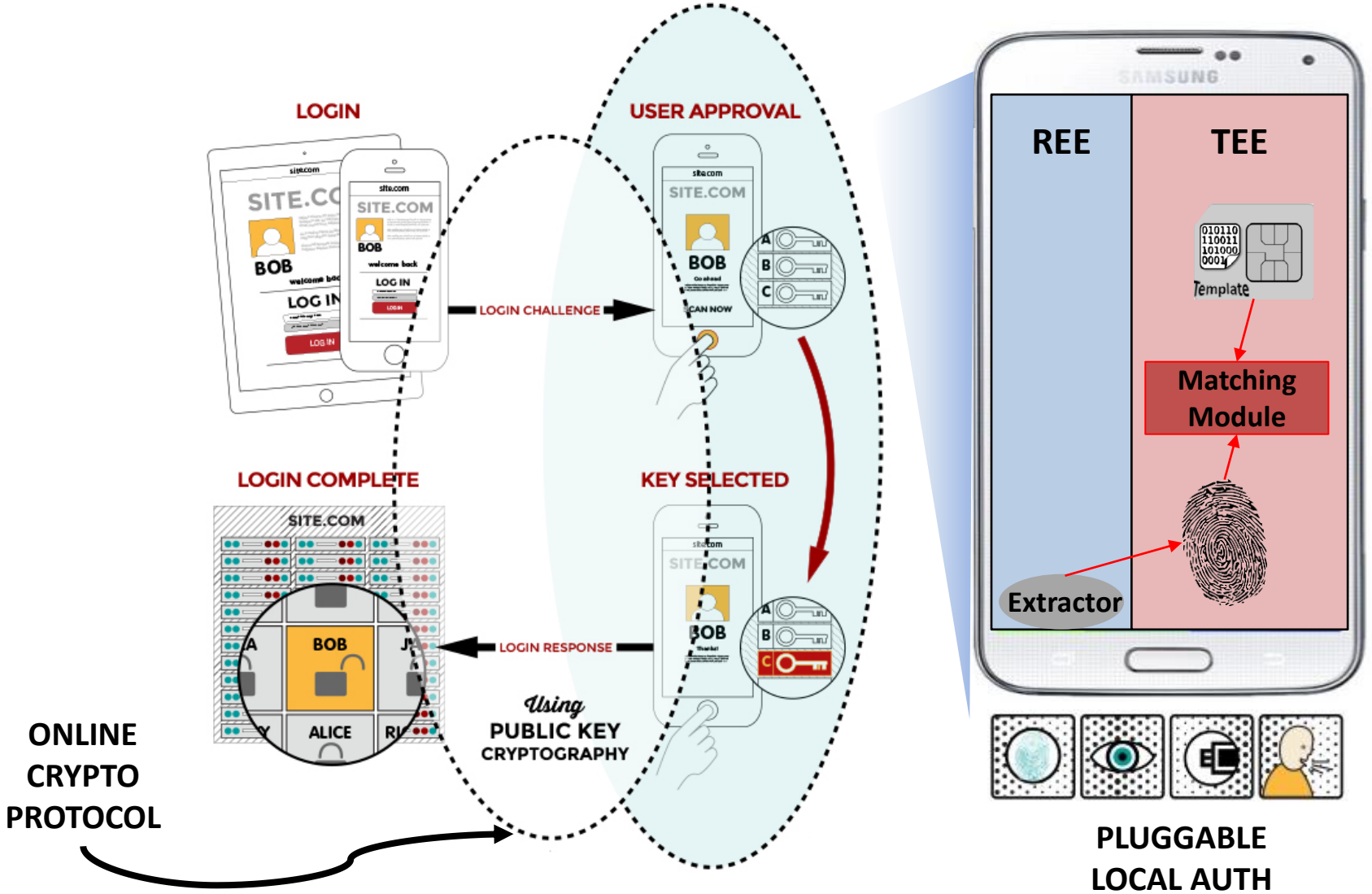
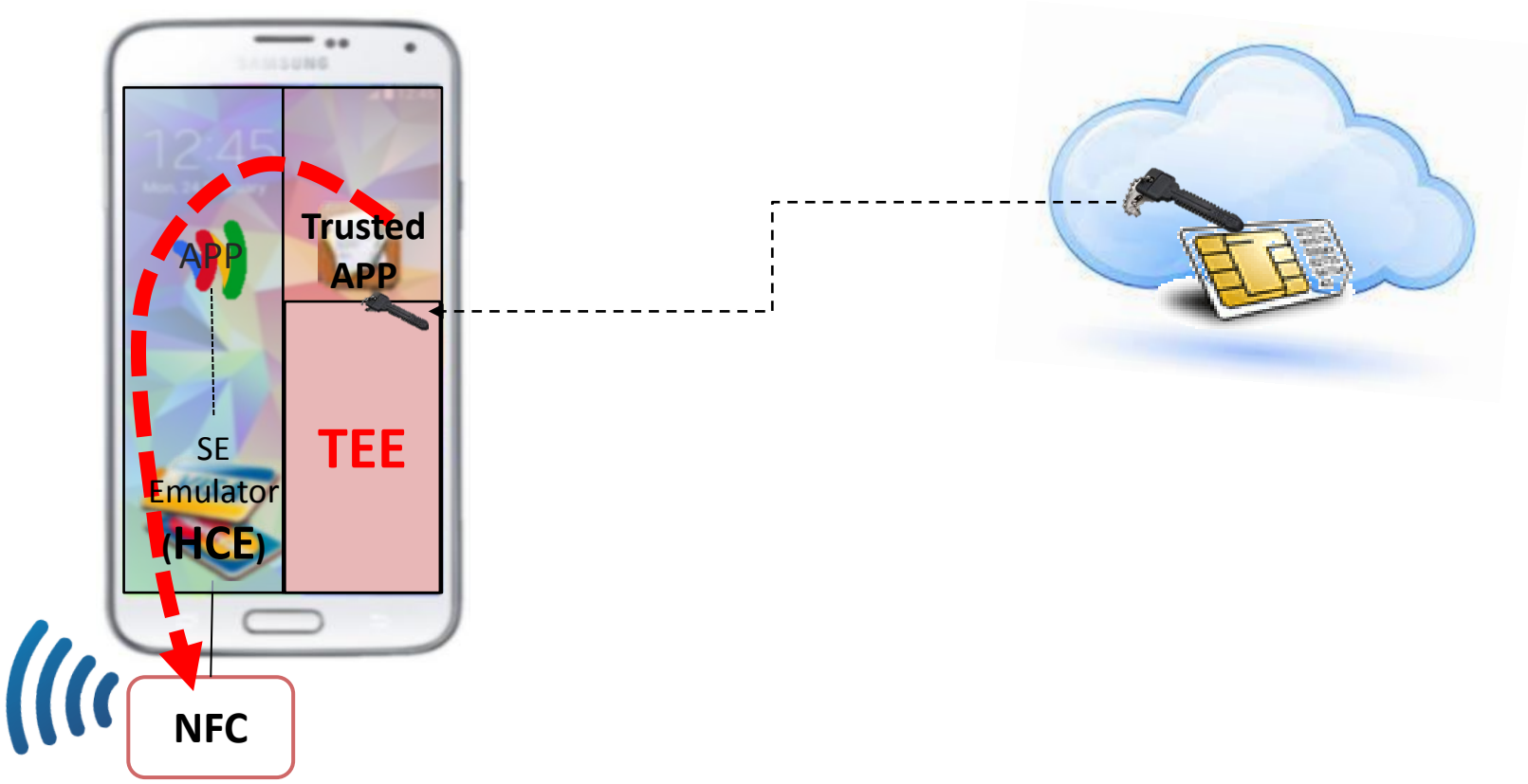


그림 출처: FIDO white paper

2) HCE, TEE and Cloud SE

- HCE (Host Card Emulation) + TEE : Trusted Application이 마치 Java card Applet처럼 동작
- Cloud SE에서 제공하는 Token을 좀더 안전하게 보호하기 위하여 TEE 기술을 적용



Rule the trusted world

Presented by
Mobile Security Division: baek@sola-cia.com