Secure Device Forum 2019

Asia IC Card Forum
One Card, One Asia on the Silk Road

Secure Infrastructure Trends in Korea

2019. 7. 17.

Prof. Ho Hyeorn Han (Kyung Hee University)

Presented by

Prof. Ki Han LEE (Seoul Women's University)

Status of Digital Signature in Korea

- 20 years Experience from Digital Signature Act(1999. 7. 1.)
- Banking Service, Electronic Government Service
- Internet Shopping & Trading, Mobile Banking
- Active Users : +30m
- 6 Certified Service Providers
- Less than 1% financial Transaction fee (the lowest level)

Trends

PKI + FIDO

PUF (Physical Unclonable Functions)

DID (Decentralized Digital Identity)

OCF (Open Connectivity Foundation; PKI + IoT)

Cloud Based Digital Signature

PKI & FIDO

- **User Terminal**

RP Client : Apps that allows communication with RP servers

FIDO Authentication Device : Electronic signature and key management function for FIDO authentication and generation of public key pair for FIDO registration

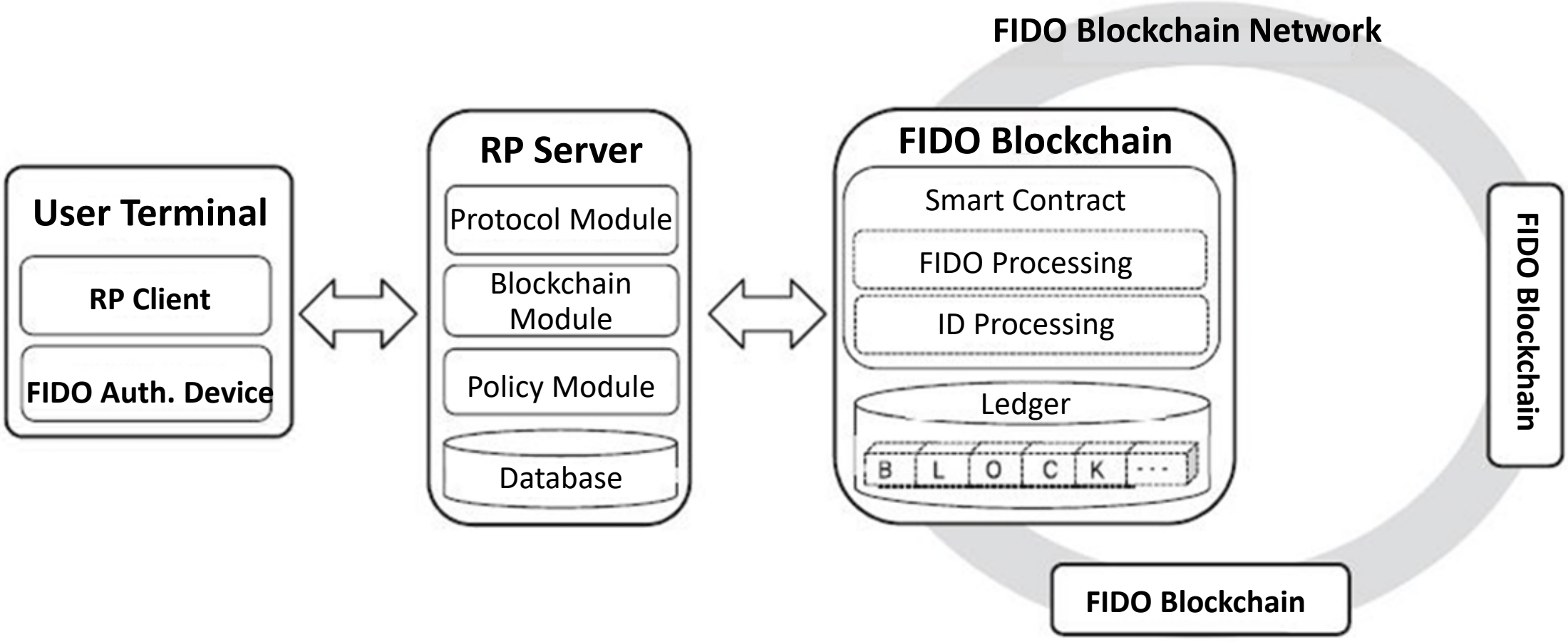
- **RP Server : Offer application services**

Generate FIDO request message

FIDO Blockchain Module: Verify FIDO response message with smart contract

FIDO Policy Management Module: Generate Independent FIDO Request Messages, Manage DB of User's Account Information

The Structure of FIDO Blockchain



Physical Unclonable Functions

PUF in Samsung Smartphone

PUF

Single Spending imbedded in Chip
Prevent KEY Exposure
Discriminate Fake

Intel SGX, ARM Tee

Single Spending imbedded in Chip
Discriminate Fake

DID Alliance

- DID Alliance in Korea (2019. 6.)
- Blockchain Based Decentralized Digital Identity
  - Lead By Korea PKI Forum & Korea FIDO Forum

OCF

Open Connectivity Foundation

OCF are currently focusing on IoT deployments across verticals including

automotive, healthcare, industrial and smart home.

OCF Diamond Members

CableLabs, Cisco, Electrolux, Haier, intel, LG, Qualcomm, SAMSUNG

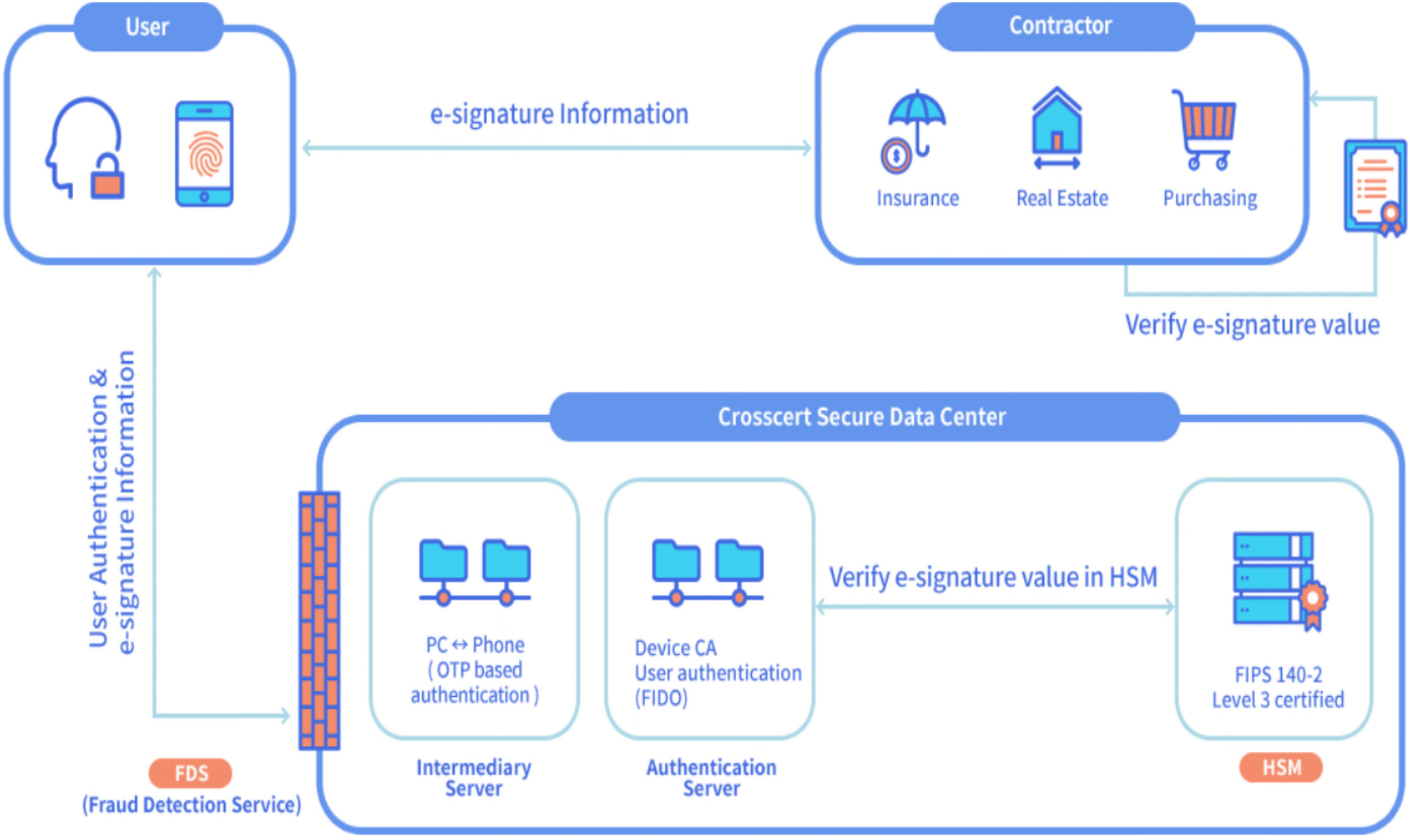
Samsung, LG are game changers in Smart Home and Automotive

Key Technology : PKI, FIDO

Cloud Based Digital Signature

- Any Where, Any Time Digital Signature
- Simple Certificate Ownership
- Issuing Certificates in the Cloud
- No Certificate Download
- No Knowledge of Cryptography and Digital Signature
- Easy Development
- No Program or No Plugin in the Client

Cloud-Based Digital Signature Architecture



By Crosscert

Q&A