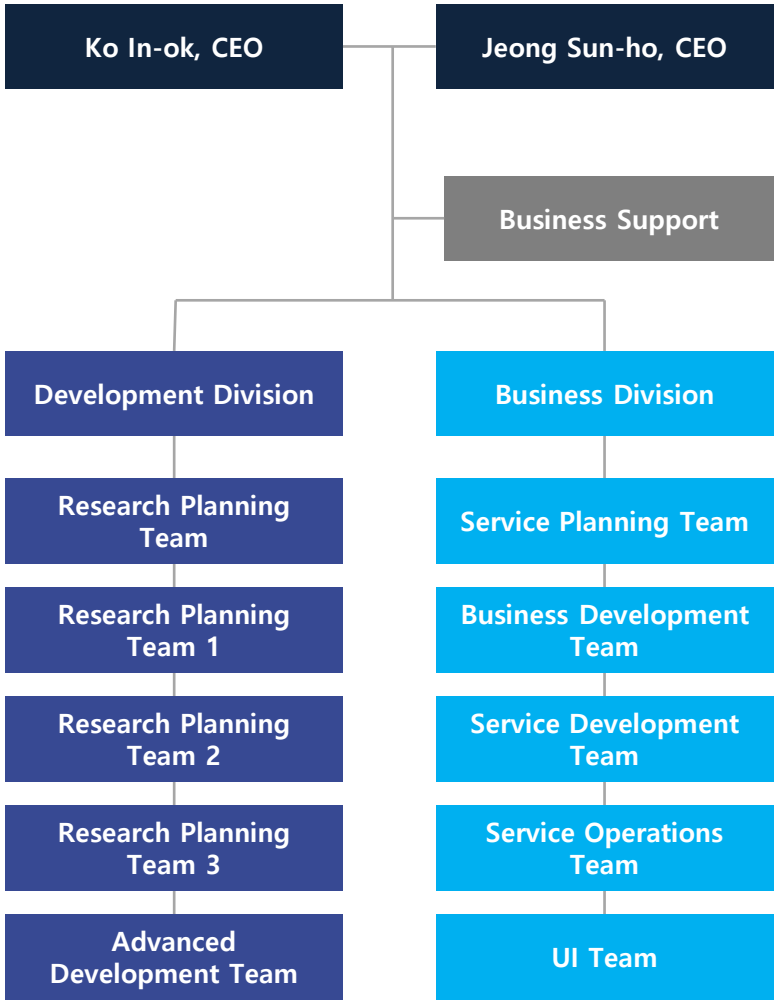
COMPANY INTRODUCTION

1. General Information

General Information

The Best Partner. Always the No.1
Ksmarteck is your trusted partner for a bright IT future

Company Name	Ksmarteck Co., Ltd.
Date of Establishment	May 24, 2010
CEO	Ko In-ok / Jeong Sun-ho
Location	A-1207, Lions Valley, Gasan-dong, Geumcheon-gu, Seoul
No. of Employees	51
Capital	KRW 500 million
Credit Rating	Corporate Credit Rating (NICE): B0 Technology Credit Rating, Technology Rating (e-Credible): B+, T3
Contact	TEL : 070-7510-1000 / FAX : 02-2026-3448
Company Registration Number	113-86-39275
Type of Business	Software Development / Service
Main Businesses	• USIM/NFC related financial IT service and operation (SM) • S/W development and operation, quality assurance • QR code / NFC solution • Mobile security solutions



2. Business Areas

Business Areas

Our main businesses are based on T-base Security, NFC, QR code, video conversion solutions, operation of services/systems, and SI for various financial companies.

Solution

NFC, QR Code, Video Conversion Solutions

- **T-base solutions**
  - T-sign certification solution
  - T-otp, T-bio (biometric) solution
  - T-cert (certification) solution
- **My QR (corporate QR code solution)**
  - Automatic generation of mobile websites
  - Provision of mobile web screen templates
- **W-TRSP (video conversion solution)**
  - Automatic generation of mobile websites
  - NFC service platforms (service, management)
  - NFC Tag Read/Write App
  - Credit Card Read/Write App
- **Partners**

Operation

Service and System Operation Business

- **Operation of QA/QC service and system for LG Electronics**
- **Hana Card service and system operation**
- **Partners**

Service/SI

Project Implementation for Various Financial Companies

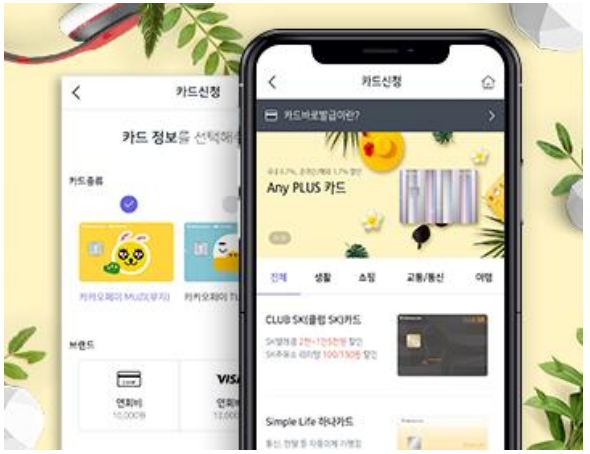
- **Development of financial services using USIM/NFC**
- **S/W quality activities**
  (Web, mobile, server application, app, etc)
- **SI**
- **Partners**

3. Key Achievements

Key Achievements

We are expanding our business domain based on the best technologies in terms of security technology, mobile environment optimization, user sensitivity, and service stabilization.

Hyundai Motors | Development of Hyundai Digital Key app
Developed smart phone app for the implementation of Hyundai Digital Key 1.0



Hana Card | Implementation of Hana Card's instant review process
Customer convenience service that shortens the card application and review time

Hana Card | Implementation of Hana card's corporate mobile app
Optimized mobile service for corporate card users

Hyundai Motor Group | Hyundai Digital Key Service Platform
Developed digital key service platform to support the controller, mobile web, and smart card of Hyundai Motors' digital key service

BC Card | Implementation of BC Card MPM QR payment service
Provided various features enabling the store owner to create a QR code to enable customers to use QR technology to pay, to view the payment result and history, and to manage users.

Hana Card | Hana Card T-sign Easy Authentication
Provided a service enabling app login through PIN number/fingerprint, based on TEE and WBC

4. Solutions

Service Area

T-base Security is a comprehensive security authentication solution that can be used for verification in various areas.

T-sign

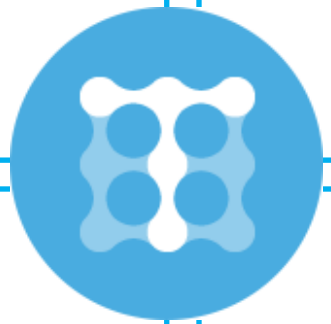
2-Channel/2-Factor authentication service solution based on a strong security model

- An alternative to the existing ARS and SMS certification
- Secure storage functions such as easy password storage

T-OTP

Next-generation OTP creation service solution based on a strong security model

- Supplementation of security vulnerabilities of the existing OTP authentication services and improvement of the inconvenient issuing process
- Prevention of OTP leakage through TUI (Trusted UI) functionality



T-cert

Convenient public/private authentication service security solution not based on Active X

- Feasible implementation without modifying existing infrastructure
- When using TEE, the certificate can be used for up to 3 years (as announced by KISA)

T-IoT

A solution that provides strong IoT security

- Introduction of the first T-IoT solution for car key services in Korea
- Hotel/building entrance/exit management systems currently under development
- Plans to be combine the technology with car-sharing solutions

4. Solutions

Strong Points

A secure authentication solution that has acquired international security standard certifications and can be used on any OS, any device, and any browser regardless of the network.

01 Strong Security

- WBC-based Software Protection: acquired FIPS140-2
- Acquired CC certification for IT security international standards

02 Convenient User Experience

- Authentication made possible without installing ActiveX or executables in the device.
- Provided combined authentication method using the iris/fingerprint
- Support various user environments on any OS, any device, and any browser

03 Reduced Cost

- On the user side, there was a cost reduction effect brought about by the shortened use time
- On the provider side, there was a management cost reduction effect.

※ FIPS (Federal Information Processing Standard): Under US information security standards, the highest level of software is Level 2.
※ Common Criteria (CC) certification: International standard for IT security

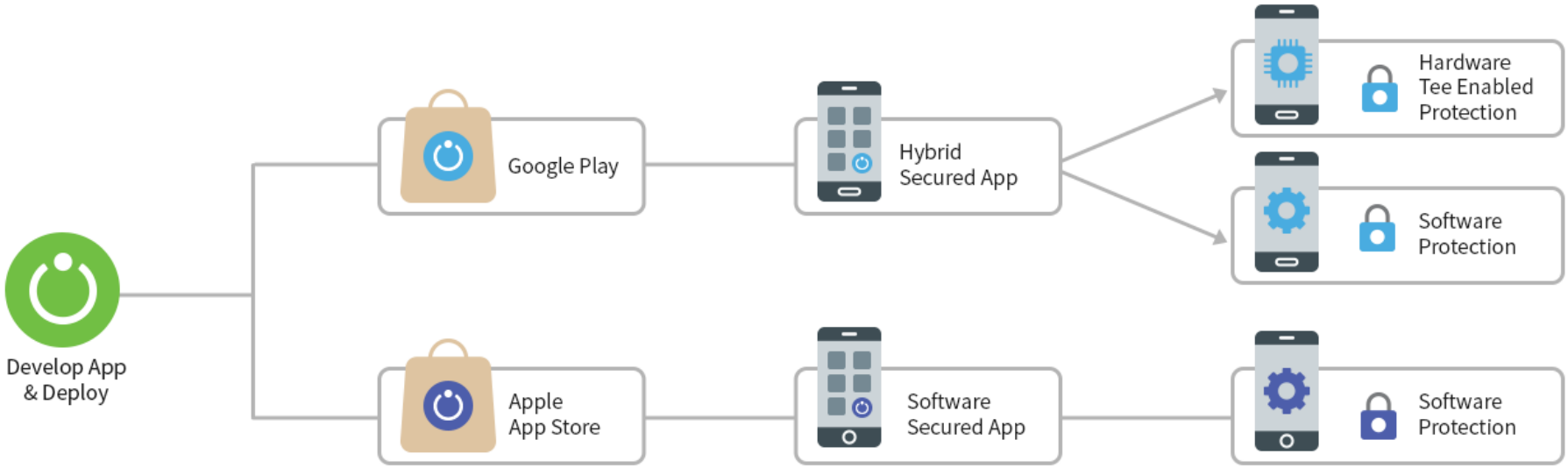
Related Patents

User authentication method on a mobile device (10-2014-0087334)	Cloud certification method for internet services using a mobile device (10-2014-0108111)	Secure text input method on an information terminal (10-2015-0046706)	Two-channel user certification method using a mobile device (10-2015-0099616)
Security method and system for application programs based on trusted execution environment (10-2015-0173339)	On-line signature certification device and method based on trusted execution environment (10-2016-0025088)	Security keypad provision method and system based on trusted execution environment (10-2016-0057914)	Authenticated login service system and method using a mobile device (10-2017-0133945)

4. Solutions

Service Areas

Possible to select among ①TEE, ②WBC, and ③TEE+WBC for implementation depending on the use environment and application range of the device.



	TEE	WBC	TEE+WBC
Supported OS Version	▪ AOS: 4.3 or higher with TEE (about 80%) ▪ iOS: not supported	▪ AOS: 4.1 or higher (about 98.8%) ▪ iOS: 8 or higher (about 98% or above)	▪ AOS: 4.1 or higher (about 98.8%) ▪ iOS: 8 or higher (about 98% or above)
Security method	▪ Hardware security	▪ Software security	▪ Hardware + Software Security
Certification Grade	▪ CC	▪ FIPS140-2	▪ CC ▪ FIPS140-2
Cost	▪ Middle	▪ Middle	▪ High

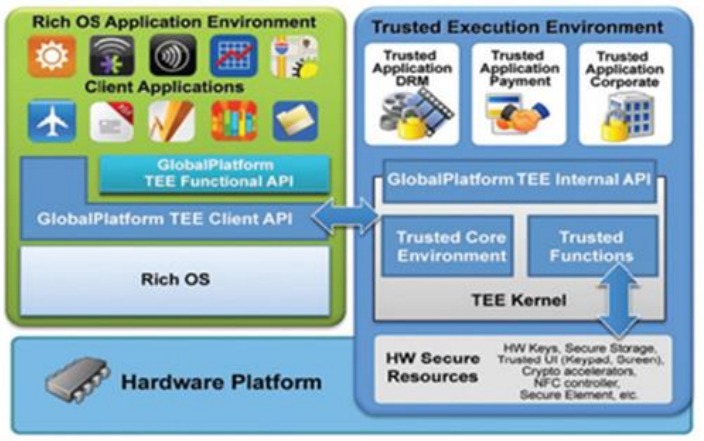
※ Security strength: TEE> WBC> Existing software security
※ Common Criteria (CC) certification: International standards for IT security
※ FIPS (Federal Information Processing Standard): Under US information security standards, the highest level of software is Level 2.

TEE Overview

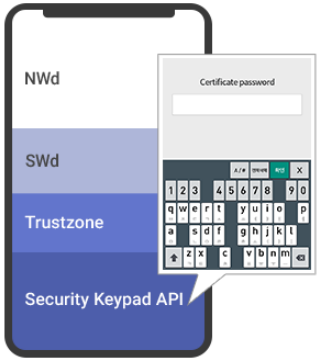
TEE is a physically separated security area in a CPU which is only accessible by authorized apps through a dedicated API, and major data storage can be managed in the secure operating environment of the Trustzone.

Overview

- The TEE is a physically separated security area in a CPU, and access to it from the Android OS area is only possible through pre-approved apps.
- The TEE is able to carry out various encryption and decryption calculations requiring heavy computation through strong CPU power

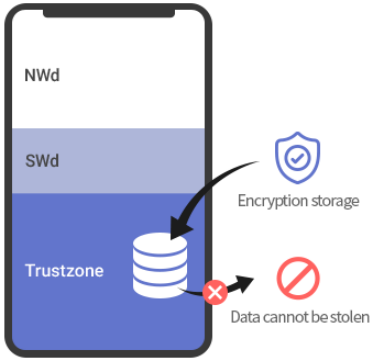


※ TEE architecture as defined by Global Platform (GP)



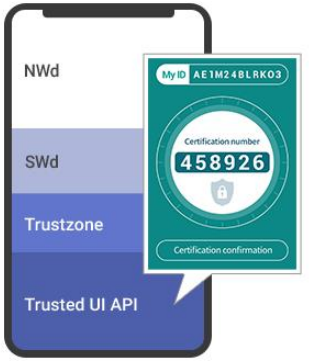
Virtual Keypad executed in SWd

Execute the safe environment
by using API call that can not be accessed
from outside during Data Input



Trustzone that can not be exposed to the outside

Operation of major data storage and
management in the Trustzone's secure environment



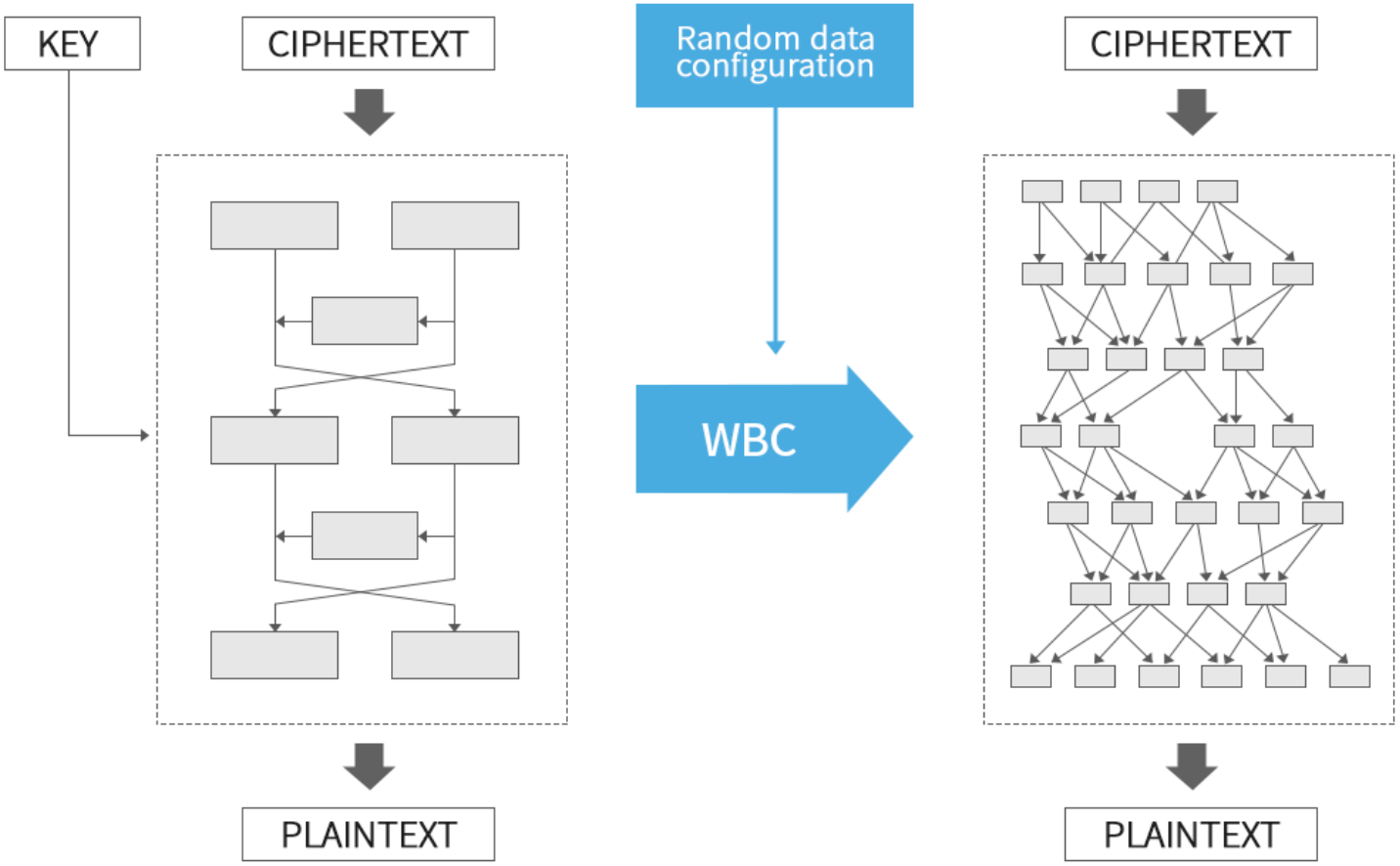
Execution of Output UI in the Trustzone

Enhance security of user I/O
using UI API provided by Trustzone

2. Software Protection Overview

Software Protection Overview

WBC (White Box Cryptography): to prevent reverse engineering, encryption KEY information is encrypted.
A technology that prevents hackers from easily stealing a KEY by mixing it with an algorithm



※ **Periodic KEY Table (S-BOX) exchange** is required → **Since frequent security update is necessary given the characteristics of financial apps,** there are few limitations in use

Thank You

Jeong Sun-ho, CEO
shjung@ksmartech.com
010-2922-5369

ksmartech