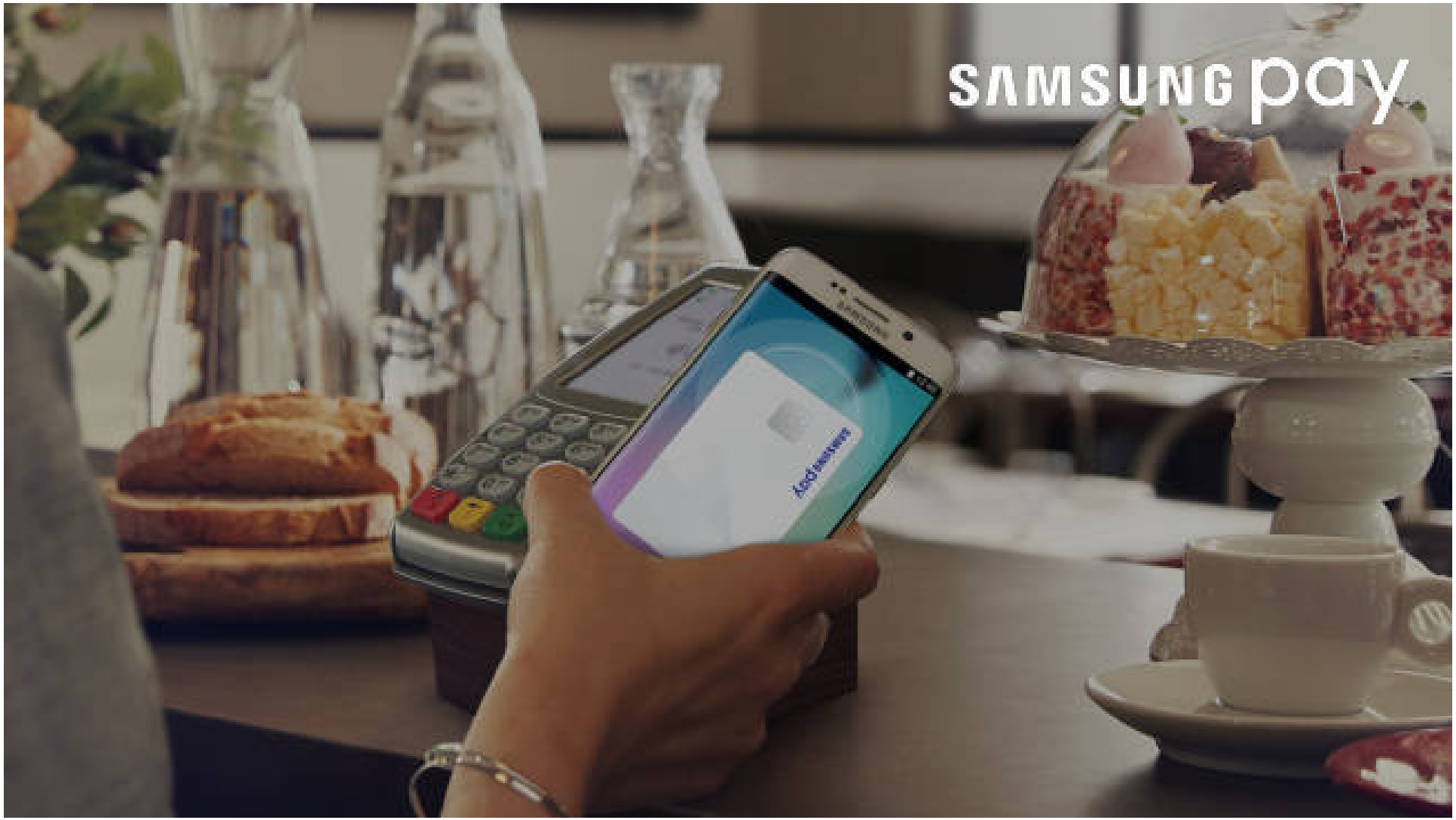
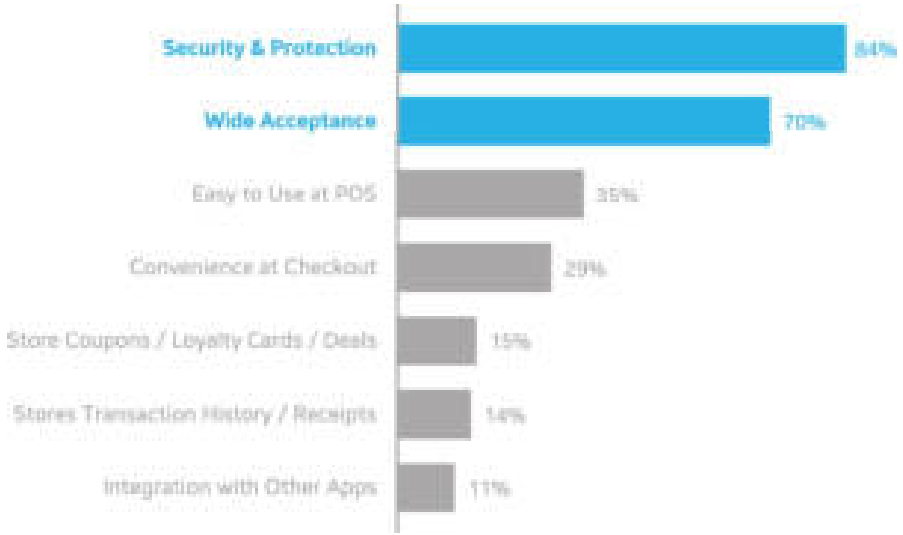

SAMSUNG pay

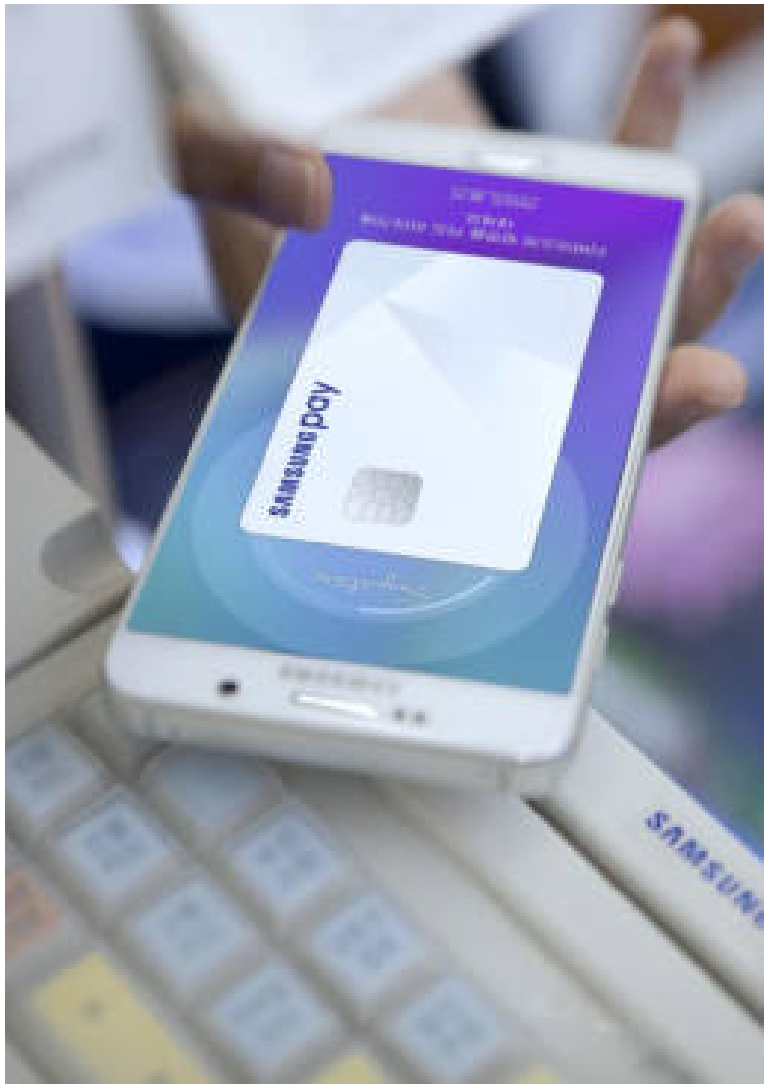
SAMSUNG pay

M-Payment Scenario

Most important factors to the end-user in a mobile payment app



* The data above is based on market research conducted by Samsung



SAMSUNG pay

M-Payment Scenario

Wide acceptance is the biggest barrier of adopting m-payments across solutions

* The data above is based on market research conducted by Samsung.

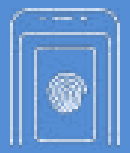
SAMSUNG pay

Safe and secure mobile payments

available virtually anywhere you can use your card.

Everywhere

Secure



Simple

SAMSUNG pay

Everywhere – Widely Accepted

Works almost everywhere cards are accepted

SAMSUNG pay

Secure - Device

Designed with our highest level of security available.

User Authentication

Samsung KNOX

TrustZone

SAMSUNG pay

Secure - Data

Designed with our highest level of security available.

Tokenization

Personal Data Protection

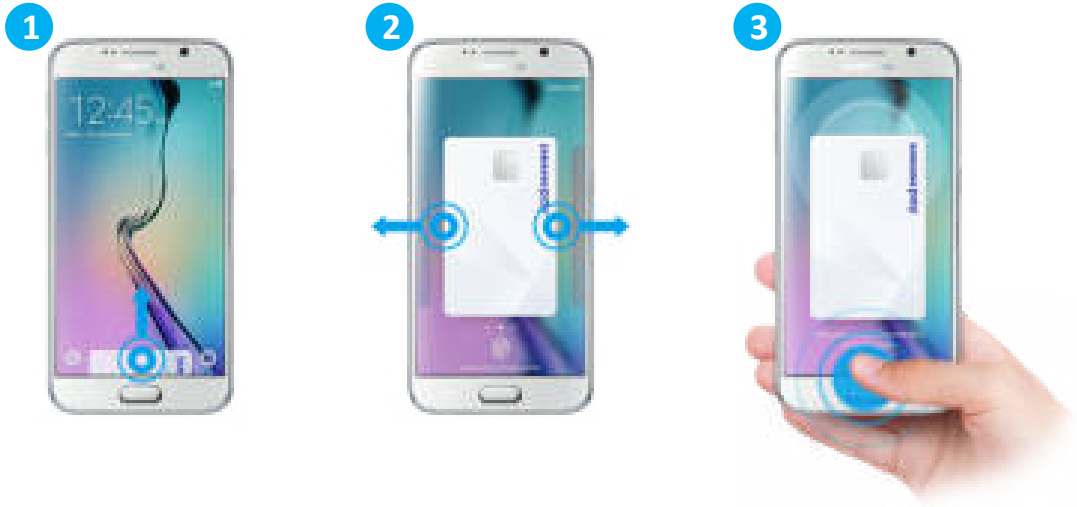
Remote Wipe

PII = Personal Identifiable Information

SAMSUNG pay

Simple

Designed to make paying with your phone fast, easy, and convenient.



SAMSUNG pay

Eligible Devices

A510 & A520

A710 & A720

A910

G920* & G925*

G928

G930 & G935

N920

G950 & G955

* NFC only

SAMSUNG pay

Partners - Launched

SAMSUNG pay

Partners - Coming Soon

Market comparison

Software provider	Monetization	Safety	Offline (in-store) Range	Online (in-app/ e-commerce) Range	Consumer base Potential	Expansion Potential
Samsung Pay	No ISSUER transaction fee	TEE; Attestation; Finger Print; Token; Knox	NFC; MST		Premium → Premium + Mid Q2'17	
Apple Pay	ISSUER Transaction fee	TEE; Finger Print; Token	NFC		Premium	
Android Pay	No ISSUER transaction fee	HCE; Token	NFC		Android Users	
PayPal / Paysafecard	Transaction Fees		None		All	

Value Added Services

Issuer Apps Integration

Allows user to open issuer's bank application from Samsung Pay and also app-to-app ID&V

Membership and PLCC

Allows users to include personal (insurance, health care, etc), membership, PLCC and co-branded *cards*

Digital Promotions

Partner's promotion, push-notifications and geofence campaigns

Smartwatch

Payments thought Samsung Gear smartwatch

Transit

Include transportation cards to be used on subways, trains and buses

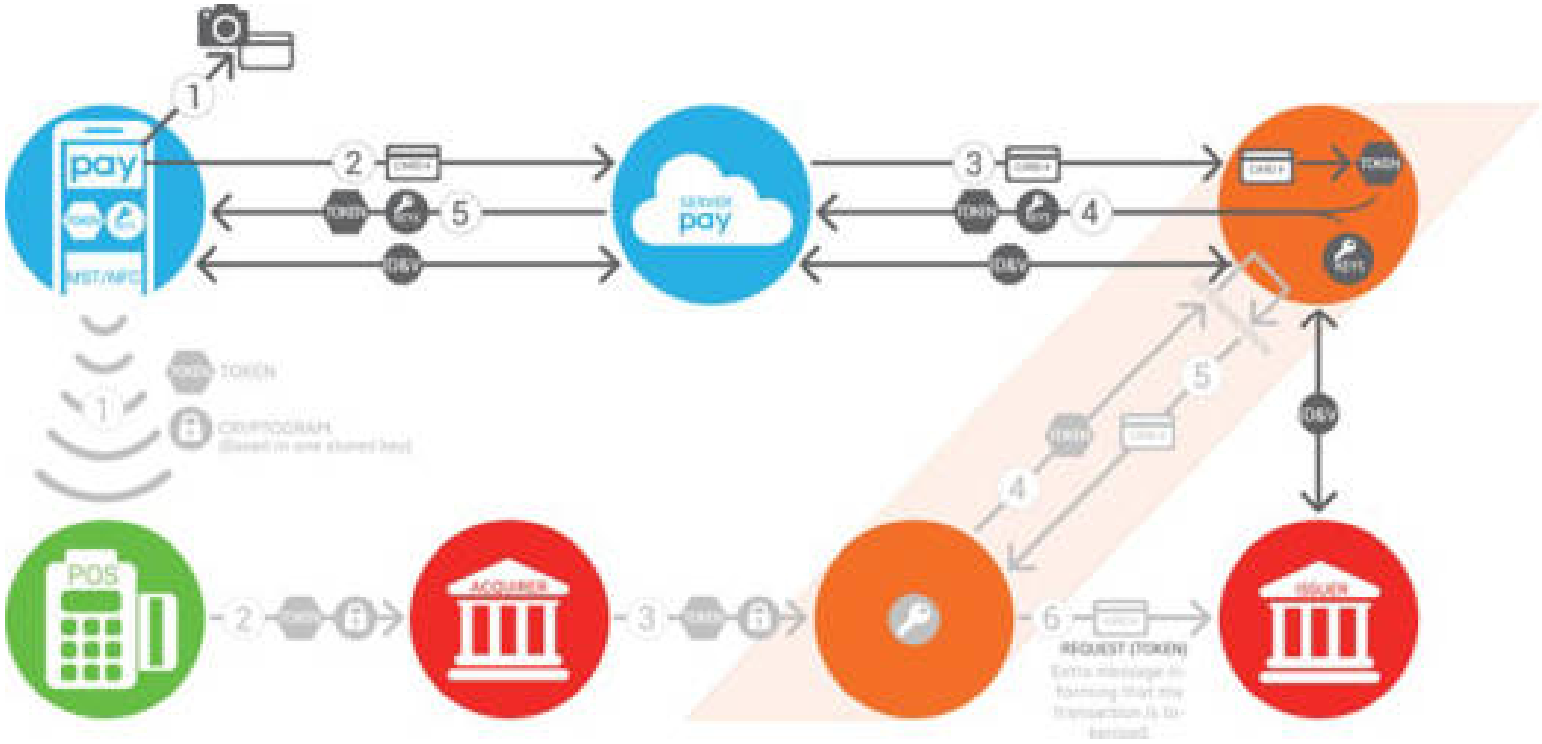
SAMSUNG pay


SAMSUNG pay
Thank you!
Obrigado
감사합니다

Appendix

SAMSUNG pay

Process Overview



System Overview

Card Provisioning Mechanics

Sign-up

- User signs up for Samsung Pay using their Samsung Account.
- Card information is immediately encrypted and securely sent to the appropriate credit card network.

Tokenization

- Upon determining card validity, account info and device integrity, Network & Issuer send a **Token** to device.
- Token is stored in Trusted Execution Environment on the device, leveraging Samsung KNOX's Architecture.
- The Token (known as the Digital Card Number) is used in place of an actual credit card number.

Policy

- No Credit Card Information is stored on our devices or servers.

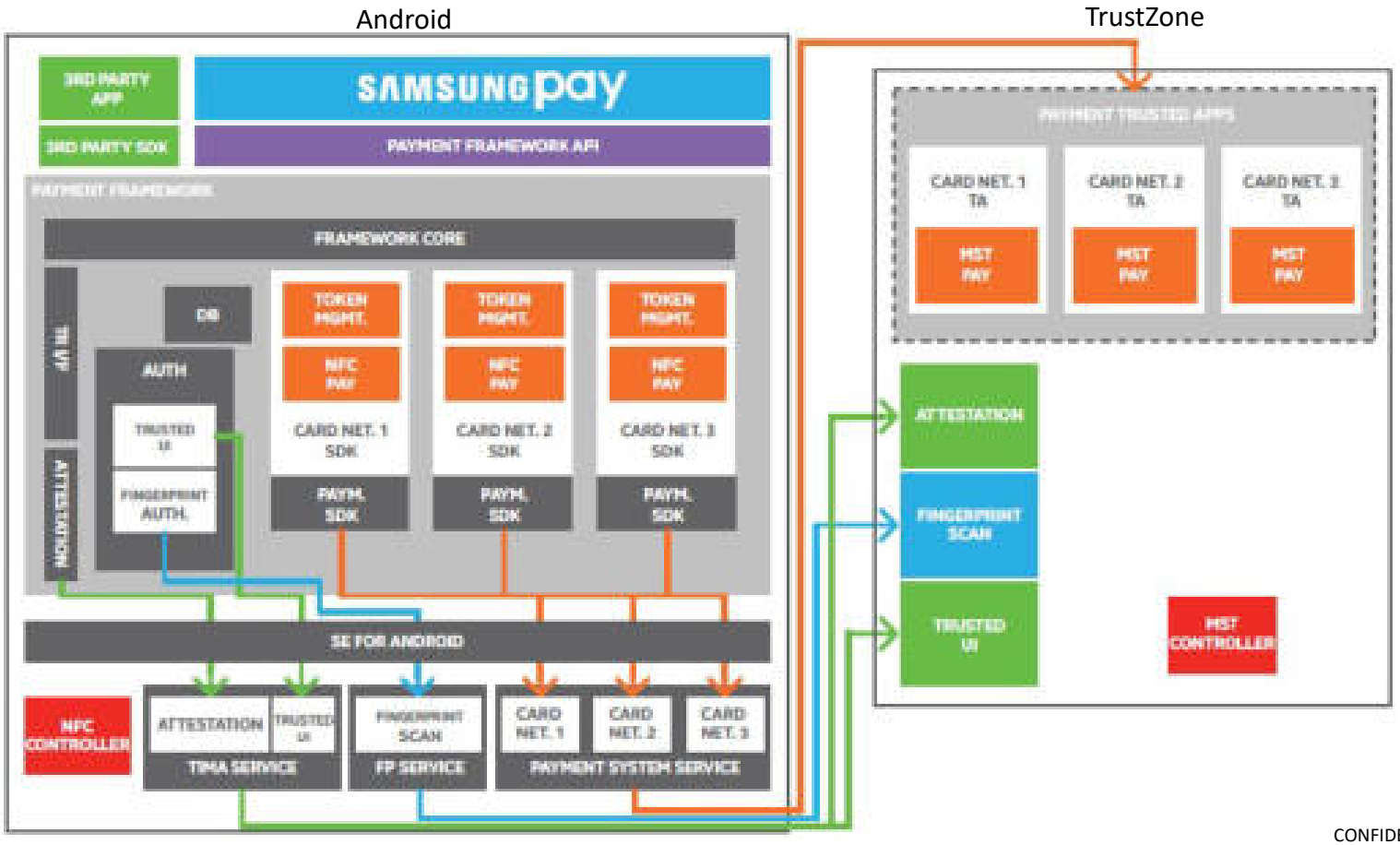
Payment Mechanics

Security Methodology

- At time of transaction, Samsung Pay sends Token and Cryptogram to the merchant POS.
- At the same time, the incremented ATC (in the discretionary field) is sent to prevent replay attacks.
- Cryptogram is effectively a *one-time use* digital signature or Verification Value (Visa) or Checksum (MC) that verifies the cryptogram from device with the one generated by TSP in the cloud.

SAMSUNG pay

Trusted Execution Environment



Multiple Layers of Security

Cardholder protection

- Implemented ID&V process in cooperation with card issuers' best practices to prevent fraud during enrollment

Tokenization

- Token and keys provisioned to device

TEE-based security for device and data at rest

- Card data and keys protected by hardware based keys
- Trusted Application for each card network; handles crypto logic; assists in implementing public-key cryptography and more
- Trusted PIN pad and fingerprint authentication directly against TEE
- System integrity check via Secure Boot, Trusted boot and remote attestation, Verification of Trusted App and Mandatory Access Control

End-to-end encryption for data in transit

- Secure communication channel between card network trusted app in TEE and TSP with mutual authentication and end-to-end encryption
- Card data in transit not visible to Samsung servers

Remote management

- Manage lost of stolen phones using Samsung's Find My Mobile
- Issuers can remotely suspend or delete cards enrolled in Samsung Pay

KNOX and Four Pillars of Security

TrustZone – H/W based cryptographic keys
TUI – Trusted User Interface / Trusted PIN
Trust Zone Application Sand Boxing – Apps are isolated from each other
Trusted Boot – Boot Loaders & Kernel are measured before executed
TIMA Attestation – Device providers remote server software integrity check
Kernel Protection – Real Time Kernel Protection

Security against authorized account access in HCE with KNOX depends on four key concepts:

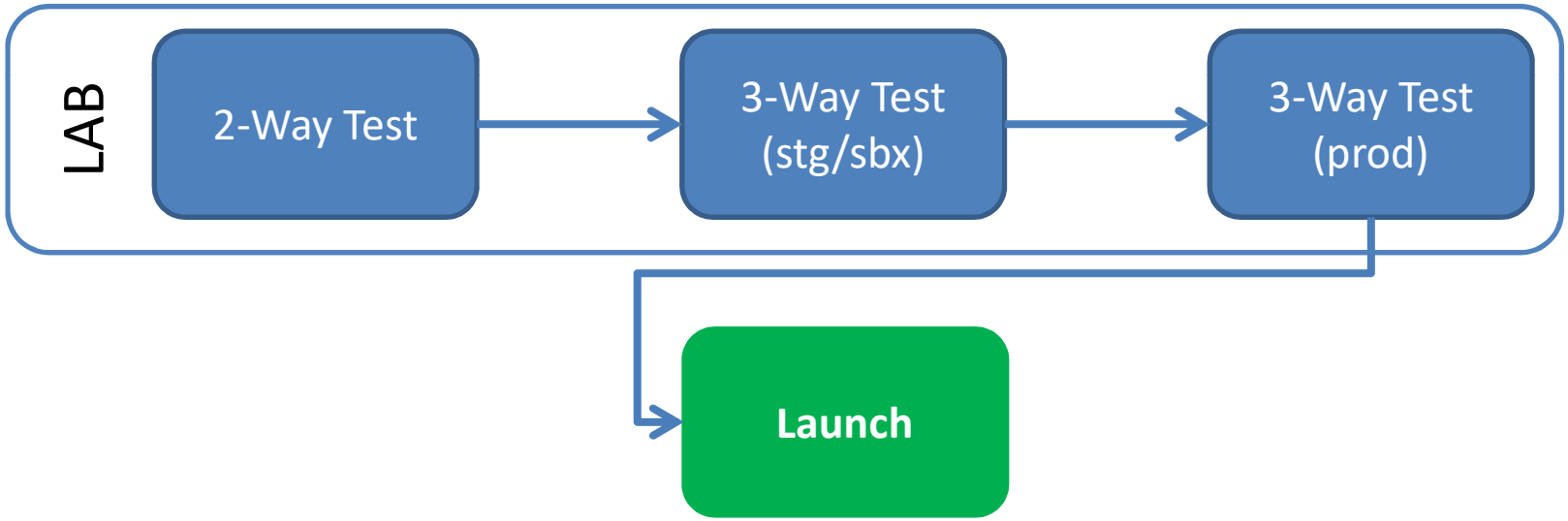
1. Limited use keys – Expire quickly preventing misuse, requires replenish.
2. Tokenization - Tokens reduce risk by replacing the PAN with limited use data.
3. Device Profiles (Fingerprinting/PIN) – validate user at time of transaction.
4. Dynamic risk analysis -user/device/account data is used to perform risk assessment for the transaction in real-time through the client app, MAP, and issuer backend.


SAMSUNG pay
Homologation Process

Homologation Process

SAMSUNG pay

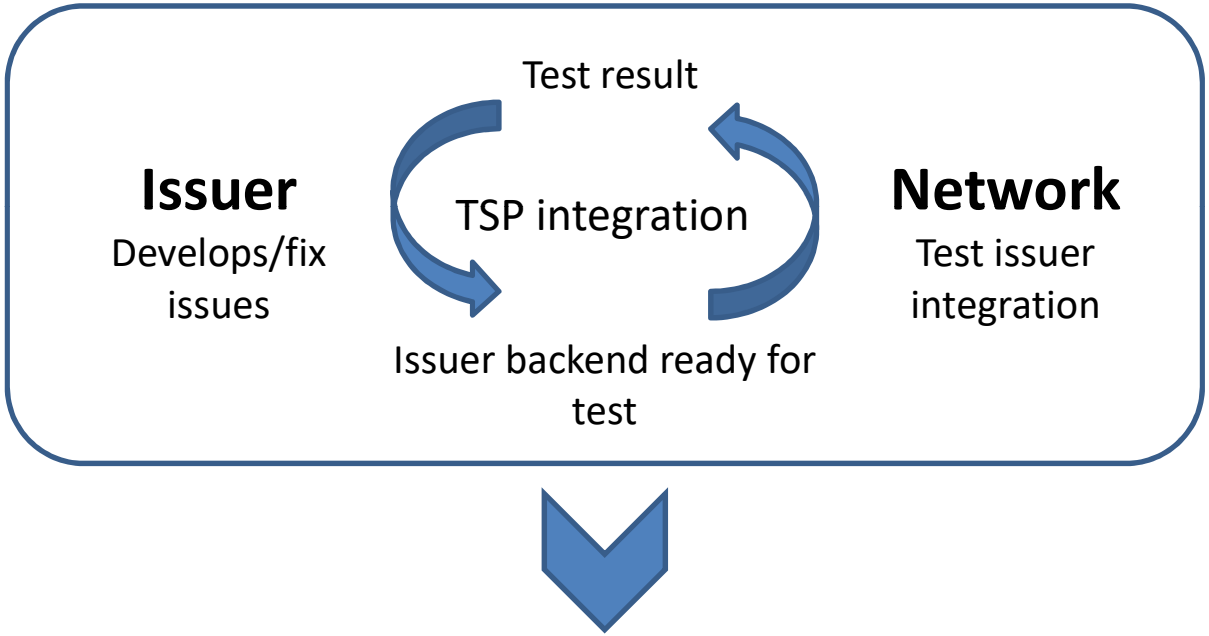
For each card type (debit/credit/combo) this is the process to homologate a new Issuer:



2-Way Tests

SAMSUNG pay

- Issuer integration with Network TSP



Cycle is repeated until NW approves issuer implementation

3-Way Tests (Stg/Sbx)

SAMSUNG pay

- Samsung QA team verifies in stg/sbx environment SSPay integration with issuer and network
  - 3-way agreement to go stage test (Issuer + Network + Samsung)
  - Controlled 3-way E2E
  - All parties pointing to Network stg/sbx server
- Samsung needs eligible test PANs (one per card type)
  - PANs for stg/sbx environment
- Apk for stg/sbx environment
- Tests executed by Samsung
  - Issuer and Network participate during execution

3-Way Tests (Stg/Sbx)

SAMSUNG pay

- Who participates:
  - Issuer: verifies logs, checks result of tests and control LCM portal
  - Network: verifies logs and control LCM portal (if issuer does not have access)
  - Samsung Tester: test execution

3-Way Tests (Stg/Sbx) – Test Cases

SAMSUNG pay

- Provisioning – Enrollment
  - Green/yellow/red paths, card-art, T&C, CS information
- Id&V
  - Call center, SMS, A2A - options available on test environment
- LCM (Life Cycle Management) – Issuer initiated
  - Token states (activate, replenish, suspend, resume, deactivate)

3-Way Tests (Prod)

SAMSUNG pay

- Samsung QA team verifies in prod environment SSPay integration with issuer and network
  - Issuer server goes live
  - Card Network prod
  - Live controlled 3-way
  - Real transaction/real money – prod POS
- Samsung needs eligible PANs (one per card type)
  - PANs for prod environment
  - PANs whitelisted
- Apk for prod environment
- Tests executed by Samsung
  - Issuer and Network participate during execution

3-Way Tests (Prod) – Test Cases

SAMSUNG pay

- Provisioning – Enrollment
  - Green/yellow/red paths, card-art, T&C, CS information
- Id&V
  - Call center, SMS, A2A - all options configured
- LCM (Life Cycle Management) – Issuer initiated
  - Token states (activate, replenish, suspend, resume, deactivate)
- LCM (Life Cycle Management) – User initiated
  - Find my mobile portal
- Transactions
  - MST, NFC, settlement, PIN, notification, cancel, installment, dummy CVV