ISSA Portland

New Board Intros

President – James Trumper
Vice President – Eric Dwyer
Treasurer – Harlan Hoult
Secretary – Dawn Hughes

Membership Director – Debra White
Sponsorship Director – Jess Odom
Education Director – Brian Ventura
Past President – Bowe Hoy

ISSA Portland

Thank You Sponsors

Upcoming Events

DATE	MEETING TYPE	CPEs	TOPIC	LOCATION
Oct 12/13	Conference	16	ISSA International Conference	Chicago
Oct 22	Symposium	4	SIEM (3 speakers plus panel)	Downtown or NW Portland
Nov 19	Luncheon	1	Vulnerability Management (Tenable)	Nike
Dec 17	Late Afternoon	1	Privileged Account Management Holiday social will follow the meeting	Con-way/ McMenamins

ISSA Portland

The Rise of Mobile (NFC) Payments and TEE Security

Karl J. Weaver **魏卡爾**
Greater China Biz Dev/Sales Manager
NFC & TEE Rainmaker for the
Chinese Mobile Payment World

Rivetz Corp.
Developer Toolkit for the TEE mobile security ecosystem

Mobile Ecosystem Complexity –

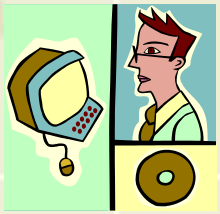
Compromises in Security occur everywhere!

Silicon Chip Manufacturers

Mobile Device Manufacturers

Mobile Operating System Vendors

Value Added Service Providers



Apps Developers

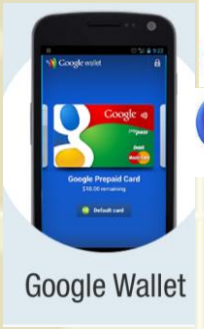
Apps Marketplace (online stores)

MNOs- Wireless Network Operators

Markets

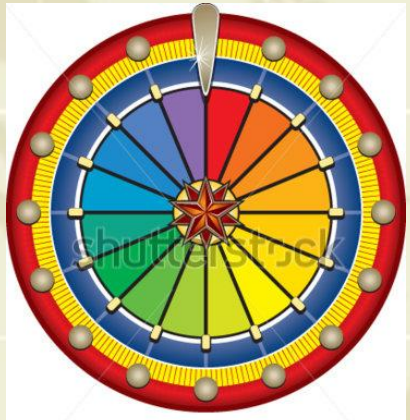
- **Consumers**
- **Individuals**
- **Government**
- **Machines (M2M)**

Multiple routes to the Holy Grail of Mobile Payments

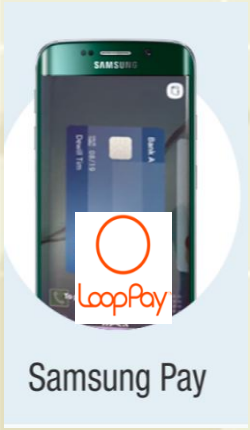


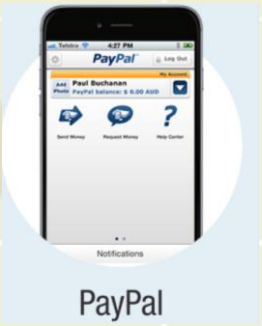
SimplyTapp

Google



Spin the wheel of mobile payment fortune





NFC Mobile Payments:

A Current Industry Snapshot

NFC Mobile Payments: An Industry Snapshot	Sim-Based Solution (SWP NFC USIM	Apple "Pay" (USA-Only- for the moment)	Samsung "Pay" In Europe (Specs. Only)	Samsung "Pay" in the USA	Android "Pay" TBA – Sept. 2015	Host Card Emulation	Google Wallet (USA-Only for the moment)
TYPE:	Physical SE - UICC	Physical eSE (Emebdded)	Physical eSE (Embedded)	Physical eSE + Magnetic Secure Transaction	TBA	Software Emulation	HCE NFC or Sim-based
OWNERSHIP:	Mobile Network operators	Apple	Samsung	Samsung	TBA	Banks	Google
CONTROL:	By Mobile network Operators	Schemes/Apple	TSMs/Samsung	LoopPay/Samsung	TBA	Bank, delegated control on solution provider	Google
MUTLIPLE APPLETS FROM MUTLIPLE ISSUERS ON THE SAME SE	YES	YES, Visa, MasterCard, AMEX	YES, Visa, MasterCard, AMEX	Yes, LoopPay wallet, Supports IDs, loyalty, and membership cards	TBA	N/C	No
TOKENIZATION	NO	YES	Bank can choose either tokenization or non-tokenization solution	In the Future, Yes most likely	TBA	YES	YES

What is a Smart card & Secure Element (SE)

Smart Cards

- Smart Card types: 1) Contact: ICC Cards with contacts for external communications. Card is inserted into a reader/POS terminal for transactions to occur. Follows ISO-7816 standards. 2) Contactless: ICC Cards with no visible contacts. Communicates using Radio Frequency with 13.56 MHz through antennas. Card is tapped at a distance of up to 4 cm. for read/write. Follows ISO- 14443 standards. Hybrid &Dual Interface cards also exit

Secure Elements = Secure ICC Cards (Smart Cards)

- Secure Element : A tamper resistant Smart Card chip that facilitates the secure storage and transaction of payment and other sensitive credentials. Secure Elements are used in multi-application environment and can be available in multiple form factors like Plastic SmartCard, UICC(SIM), eSE, micro SD etc.

Secure Element & NFC phone Architecture

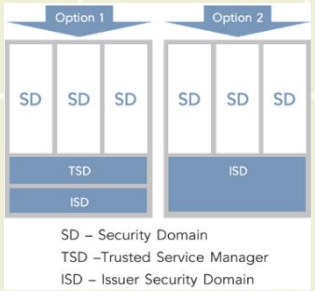
☯ Components of a typical Mobile NFC phone

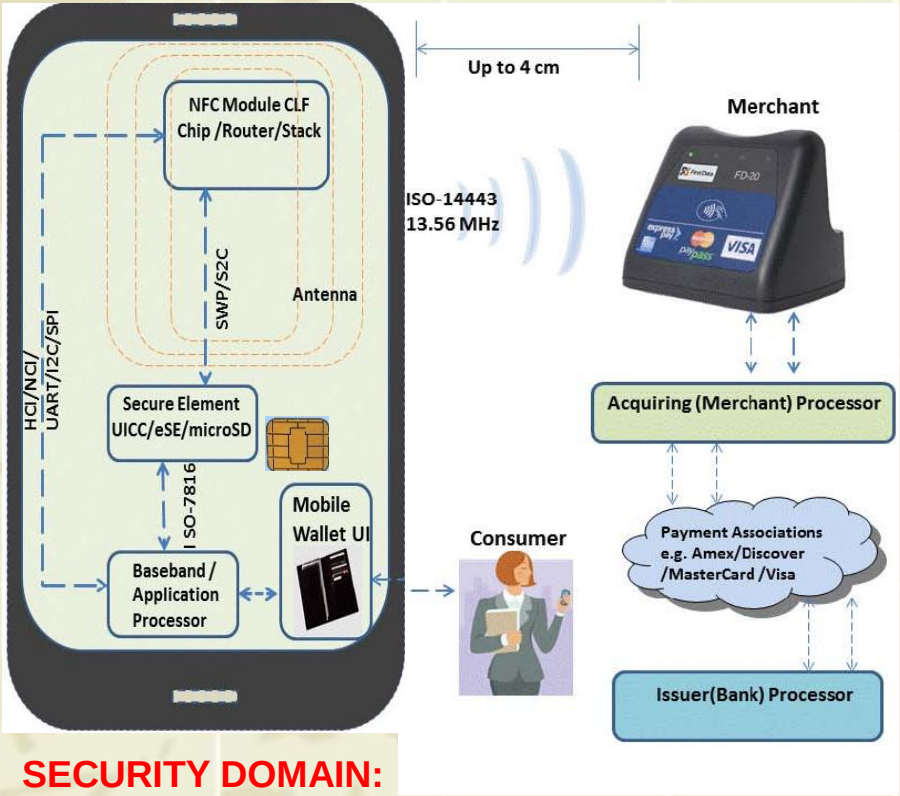
- Secure Element(SE) UICC,
- Embedded SE, micro SD

- **NFC Controller**
- NFC Chip, Stack, CLF
- **Mobile Wallet**
- UI Application for consumer interaction Communication

Protocols/Interfaces

- ISO-7816, ISO-14443, SWP,UART,I2C, SPI
- **Smart OS**
- Android, iOS, BlackBerry OS, Windows Phone
- **SE OS**
- Java, Multos, Proprietary





SECURITY DOMAIN:

A security context within the secure element that includes a set of cryptographic, communication, and data management operations parameterized by unique key material and controlled by a set of assigned permissions. Applications within the secure element request cryptographic services, encryption or decryption, digital signing, or off-element authentication through Global Platform APIs that reference an associated security domain.

Contactless Mobile NFC

Near Field Communication (NFC) is a wireless protocol in smartphones that enables contactless transactions and other data exchange within a variety of devices.

- RF Wireless Technology
- ISO/IEC 14443, 18092, MIFARE, FeliCa etc.
- Payment, Ticketing, Access, Loyalty & Coupons, etc.
- Secure Element to help store payment credentials
- Used in conjunction with Mobile UI(e.g. Wallets)
- E.g. Google Wallet, ISIS Wallet

NFC Forum Specifications

1.Reader/Writer mode Device can read/write NFC Forum supported tag types.
1.ISO 14443 and FeliCa schemes

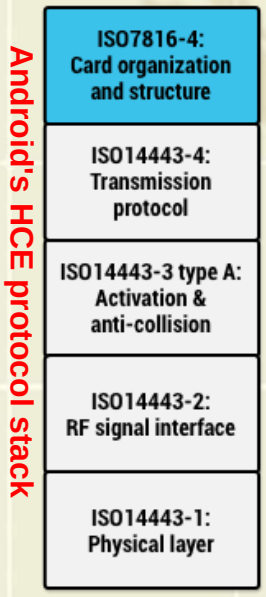
2. Peer-to-Peer Two NFC devices can exchange data between themselves.
ISO/IEC 18092 standard

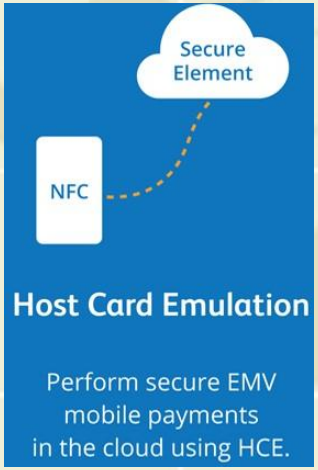
3. Card Emulation NFC device (phone) acts as a contactless card

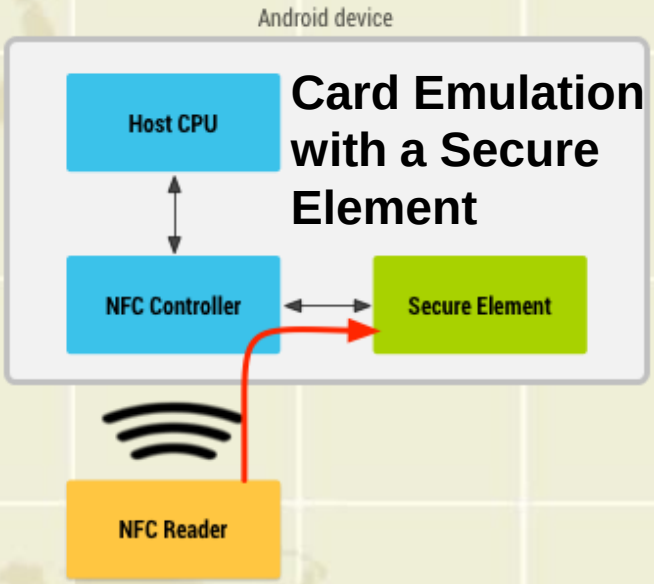
Google HCE- Innovative work-around- to Hardware SE – Where will this lead?

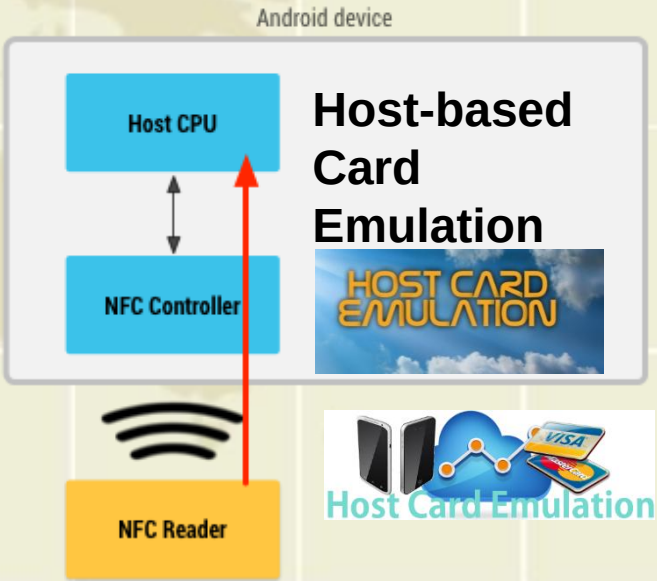
*HCE - **Host**-based **Card Emulation**.*
This allows any Android Kit-Kat 4.4 applications to emulate an NFC card and talk directly to the NFC reader. It's normally emulated by a separate chip(NFC CLF, SIM, MicroSD) in the device, called a *secure element;* with HCE you bypass the need for a hardware SE

Supported NFC Cards and Protocols
NFC-Forum ISO-DEP specification: there are different types of cards that can be emulated.









CONSOLIDATION leading to Smartphone Hybridization

Softcard & Google Partner for Android (Secured) "Pay"

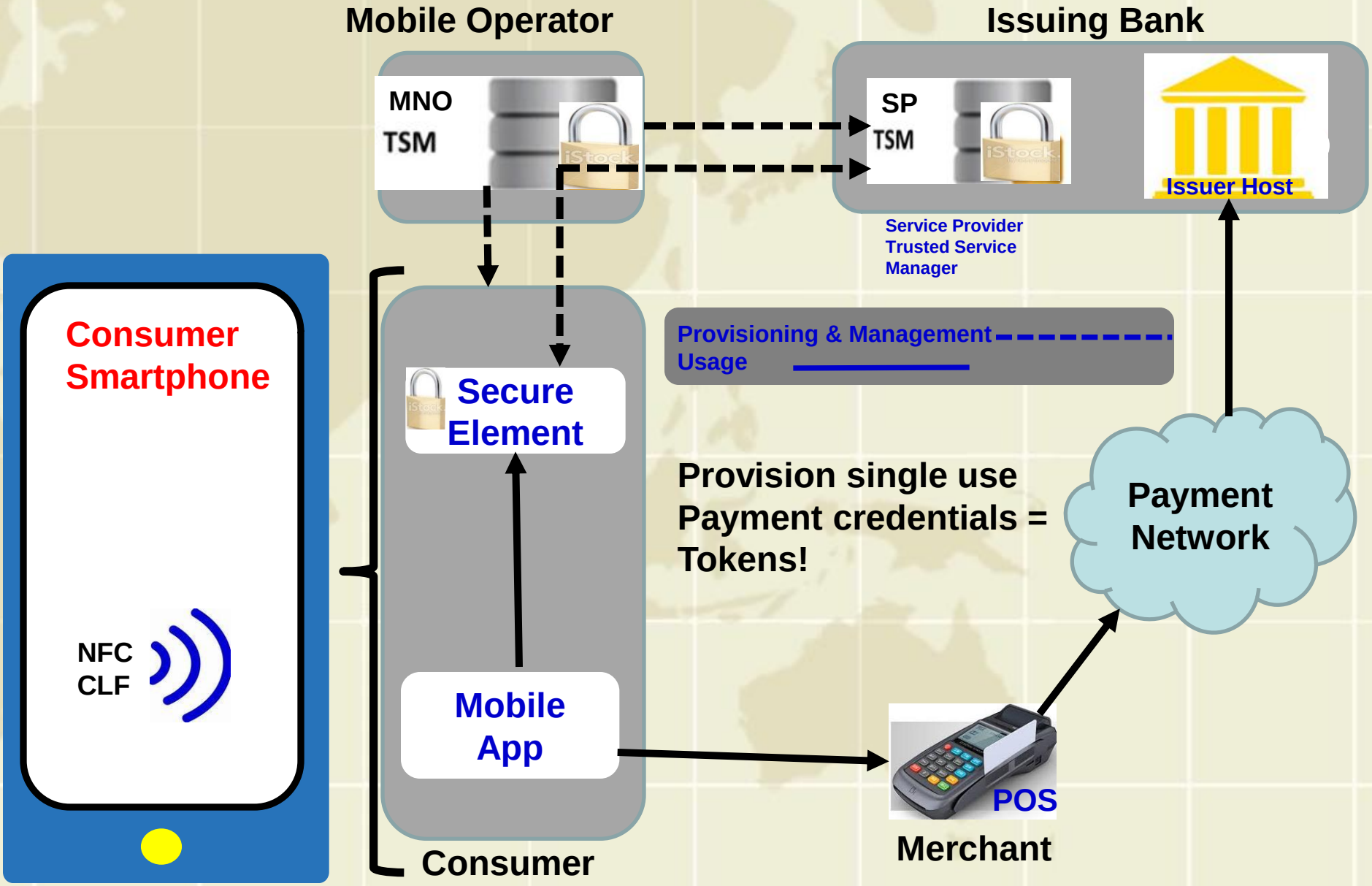
- Win-Win for Both: Softcard gives Google some interesting IP, in addition to a strong channel partner with MNOs in the U.S. to help drive Google Wallet, and result in a secure Android Pay solution.

- Google and Softcard want things to work out with the card networks as both "wallet" solutions worked hard to provide merchants with card-present rates.

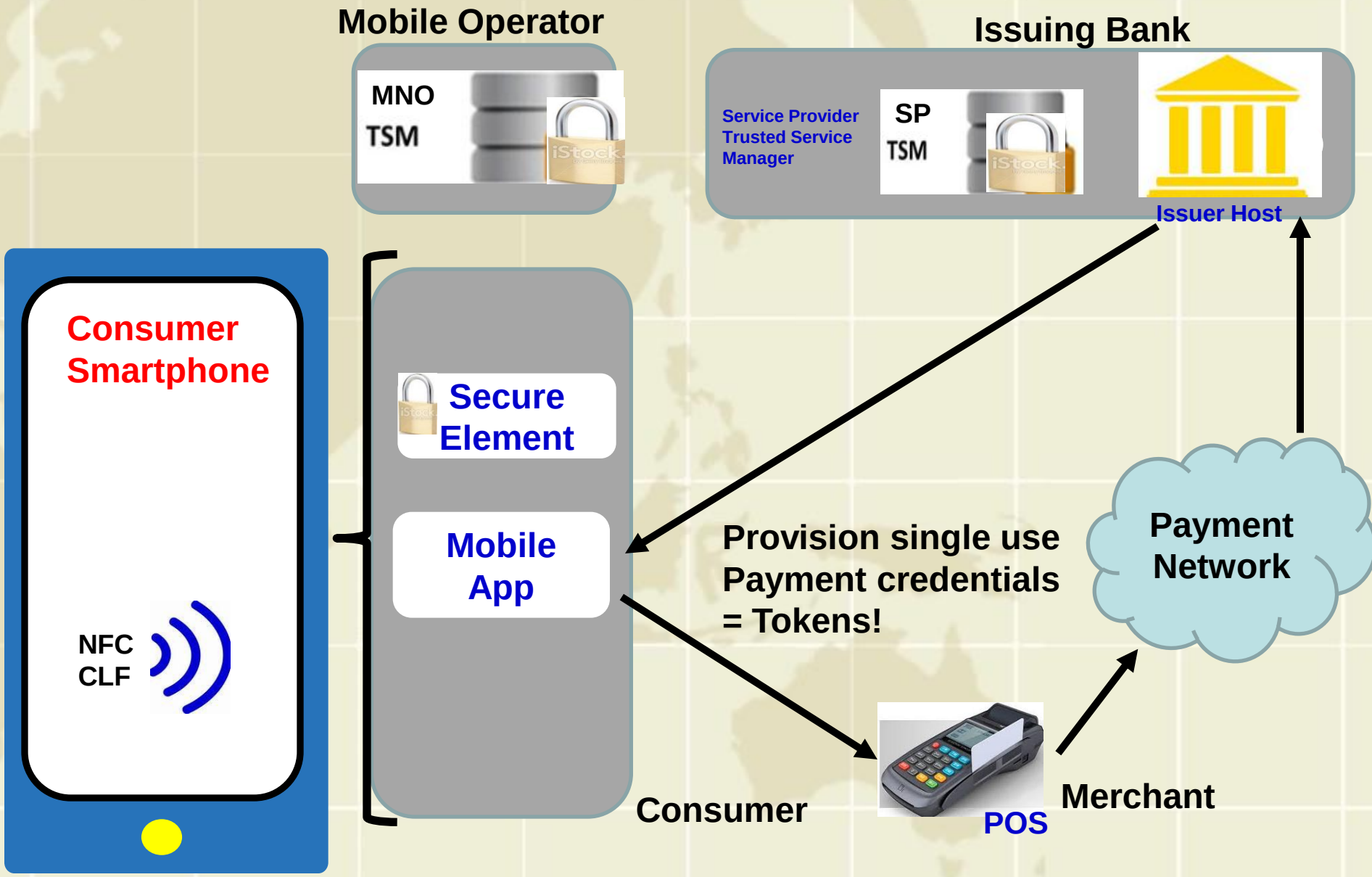
- Softcard technology fits with Android Pay's APIs to utilize Android HCE NFC implementation to pull payment (or authentication) data from either the secure element or some other host (Cloud). Softcard/MNOs and Google seem to be planning to tokenize the payment credentials in the SE for Softcard implementations and they'll have a fully agnostic and flexible payment platform that can run off-line (on select devices with an SE), or as software-only with a cloud connection.

- Expect Android "Pay" with Google's refortified Wallet to run on a Hybrid device using both the Secure Element or HCE NFC and Cloud-based provisioning to process the payment credentials.

SIM SE NFC Payments Ecosystem

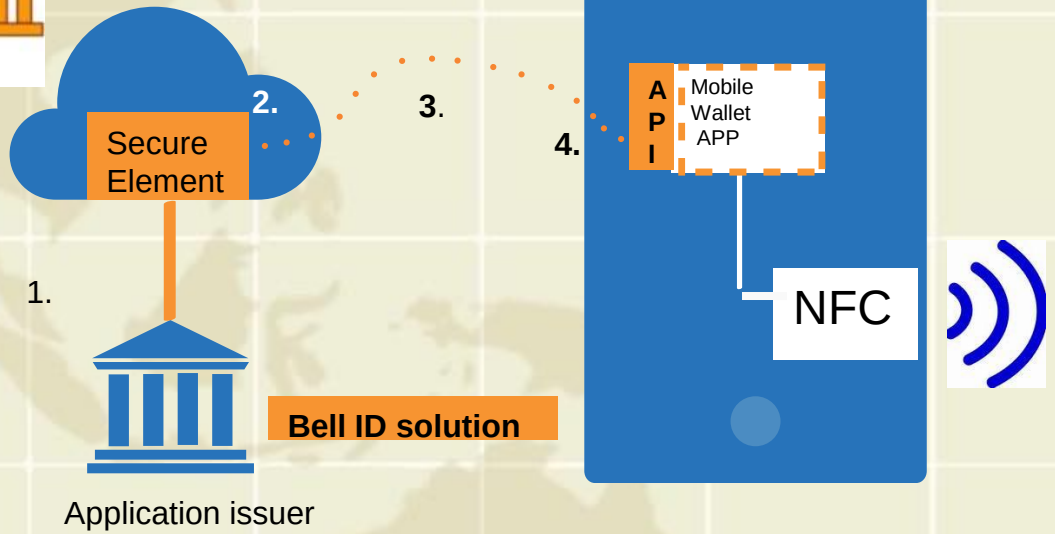


HCE-Based NFC Payments Ecosystem



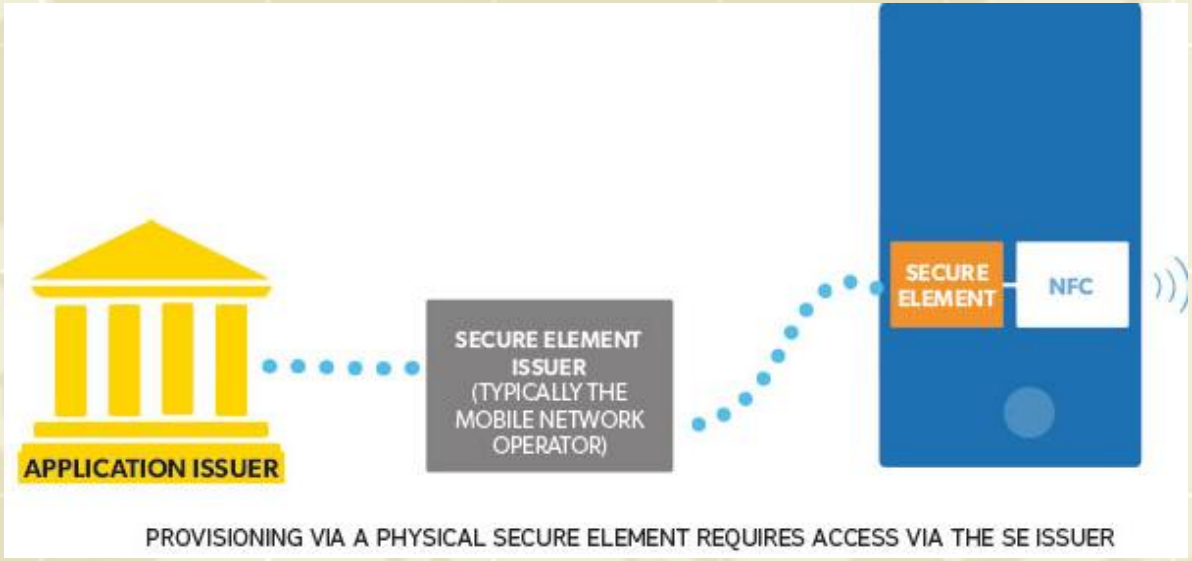
Payment performed from a down-loadable application in the App store of Smartphone Operating System, when it reaches the POS Terminal it behaves like Card Emulation Mode, no MNO or 3rd party required, but there are security issues to consider

How to emulate a SE in the Cloud



1. **Realtime and/or batchfle import of card and personalization data**
2. **EMV command and cryptogram generation (key management / HSM)**
3. **Secure connection**
4. **A Bell ID client API SDK allows for a smooth integration to existing (mobile wallet) applications**

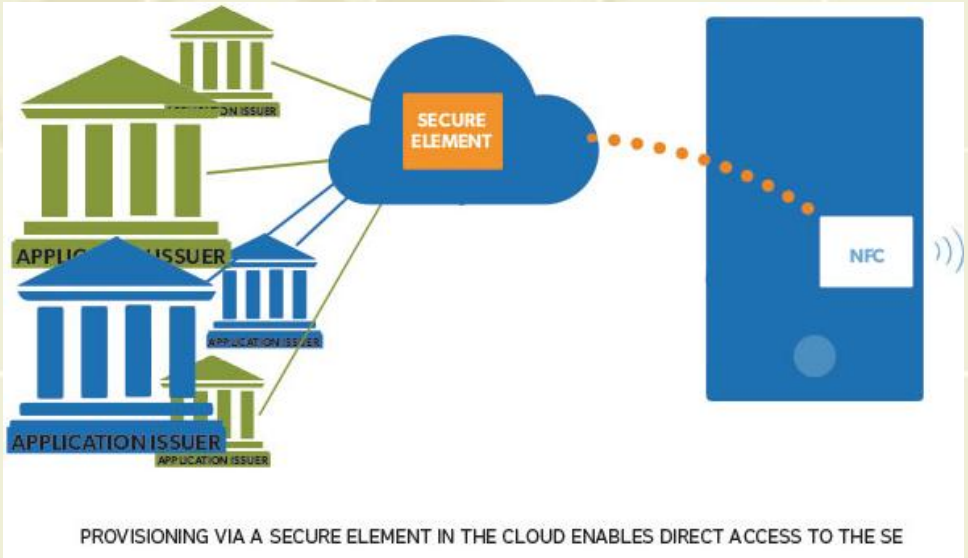
Provisioning in the Cloud



PROVISIONING VIA A PHYSICAL SECURE ELEMENT REQUIRES ACCESS VIA THE SE ISSUER

Originally, credentials and applications would be stored and provisioned in a SE environment in a USIM card by MNOs. By moving the secure element to a remote environment, dependency and costs of SE or Applications are removed

With SE in the Cloud, Application issuers can provision without 3rd party involvement and apps issuers aren't dependent on the device's SE owner for storing credentials and instead can provision directly in the Cloud.



PROVISIONING VIA A SECURE ELEMENT IN THE CLOUD ENABLES DIRECT ACCESS TO THE SE

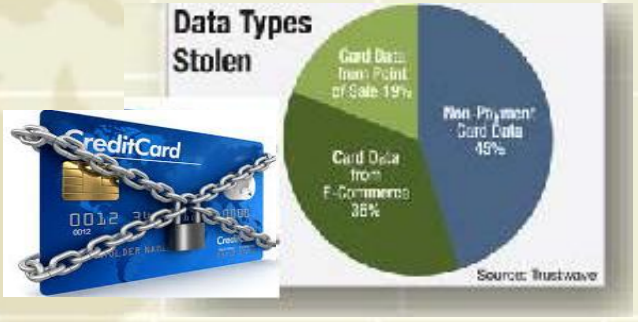
Tokenization of EMV Payments -Beefing Up Security of HCE

Cloud Digital Issuance is the Key

To make secure cloud-based mobile payments possible, there has to be digital issuance systems capable of securely storing credentials in the cloud, issuing them to mobile apps, and providing secure access to those credentials to trusted apps in the phone. Digital issuance systems must manage Tokens downloaded to mobile phones in lieu of real card data for payment transactions.

Tokenization Defined:

the process of replacing a card account number with a unique string of charactersthat is restricted in how it can be used. "Secure" Token PANs can be assigned for use with a specific device(PCI DSS compliant), merchant, transaction type or channel.



Use of a Tokenization Card PAN -, applied on top of HCE, with the Issuer utilizing the Token Service Provider (TSP) to generate Token, delivered to the mobile APP for an HCE transaction. After the transaction is processed in payment network, the TSP converts Token back into a PAN so Issuer can process the transaction.

Emergence of Tokenization for Mobile (NFC) Payment Smartphones

- **Visa**,**MasterCard** and **American Express**-Combined to push greater security in the payment industry through tokenization. .
- Account numbers will be replaced by a digital payment “Token” for online and mobile transactions."
- **EMVCo**--is standardizing tokenization across the payments industry.
- Mobile payments community needs a consistent, secure and interoperable environment to make digital payments," as greater security is pushed for.
- secured, individual payment "token" generated and transferred, that’s the goal

Token comparison Apple & Android

iTunes

Submit iTunes Account in Token Request

Receive Token Card Data

Program token when a card is tokenized

TOKEN CONVERSION TO CARD ON FILE

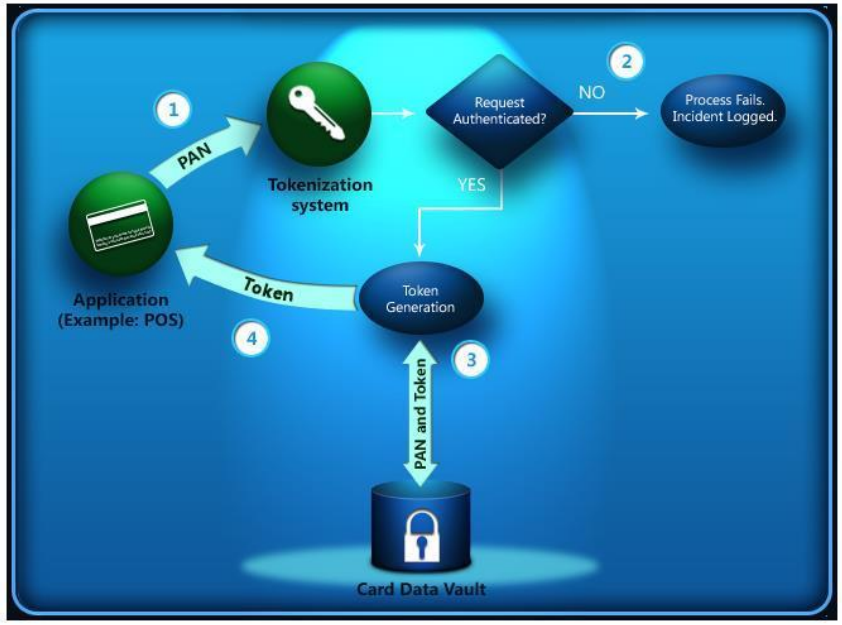
VISA MasterCard AMERICAN EXPRESS

BANK

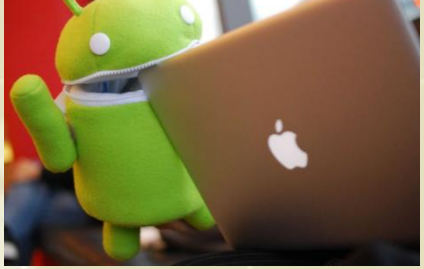
SimplyTapp

Tokenized permanent SE

Tokenized permanent SE



For an EMV transaction iPhone and the point-of-sale terminal generate a cryptogram — the transaction's security key, attached to consumer's personal account number (PAN). The cryptogram & 16-digit # token are then sent back to the Token requester.



Android Pay

Taking a bit out of Apple Pay

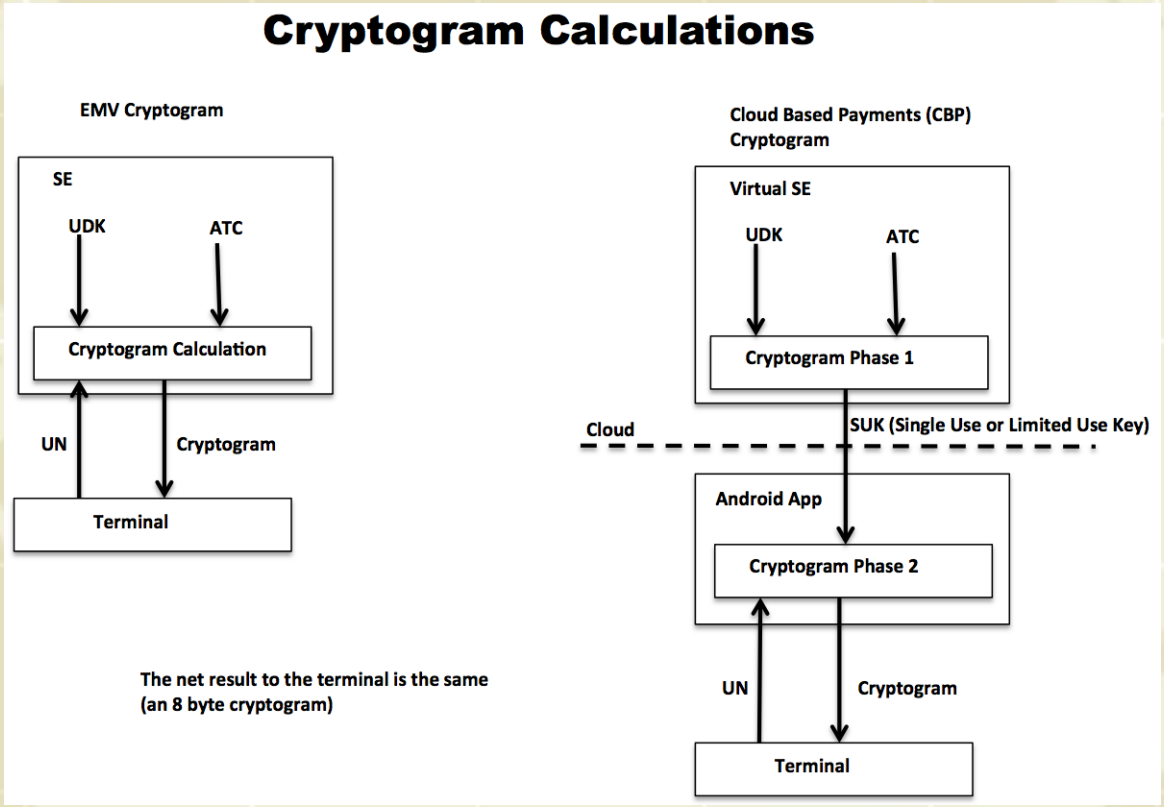
- **Android Pay being developed by China UnionPay in China, creating the new contactless payments product, hoping to significantly increase wireless payments adoption in China. CoolPad, Lenevo, Huawei, ZTE have been introduced to the plan as has Samsung. Google in the Middle!**

- **UnionPay also announced a partnership with Apple for Apple "Pay", to launch just after Chinese New year (Feb 19th)**

- **UnionPay is expected to subsidize the cost of the NFC chip, needed to secure mobile payments, in order to convince smartphone makers to support Android Pay. No determination yet they will use NXP's embedded Secure Element and probably use ARM Trustzone Security feature in all ARM core processors and a mobile device security OS designed to work in cooperation with Trustonic (and many other players) called the TEE – Trusted Execution Environment. They will create a virtual secure element using Host Card Emulation and store payment credentials in the TEE.**

- **UnionPay will try to replicate the Touch ID and biometrics used by Apple Pay for Android Pay, and the key in security.**

EMV vs Cloud-Based Payment Cryptograms



The CBP cryptogram allows all components to be used as before and exposes a "relay threat" only to the android app after the SUK is received, but not to the POS terminal. It also allows the Phase 2 calculation to happen independent of cloud availability at tap time.

The Phase 1 calculation and delivery to the phone from the cloud is expected to be preformed prior to tapping the phone, but not during the tap itself.

A cryptogram in Cloud-Based Payments is created half in the cloud and then the other half when you tap the phone. Otherwise, you could experience latency issues involved with network connectivity This offsets the relay threat with in app security and sensor rich android OS

Merchants who Accept Apple Pay and those that don't!

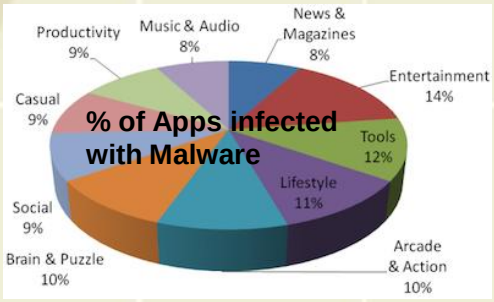
Criminals Make Money from Mobile Malware

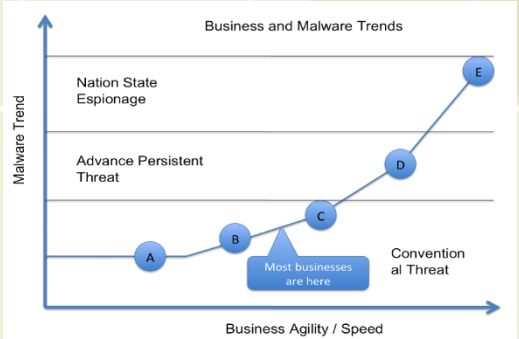
- **Premium SMS Messages**
- ***The malignant app takes control of the infected smartphone and commands it to send a message to a premium SMS number or access premium online content, giving the perpetrators or their partners the chance to request payment from the victim's mobile provider.***
- **Mobile Adware (Madware)**
- ***With so many free apps supported by advertising, Mobile Adware, the worst offenders serve unwanted ads to your smartphone's status bar, add bookmarks to your browser, redirect your browser home page and even read and modify calendar and contact information.***
- **Stealing Information**
- ***Spyware can steal a lot, Log-in details can be passed to hackers, who can use them to access accounts with a monetary value, while personal and business data can be used for future targeted phishing attacks. It all has value.***
- **Bank Fraud**
- ***Mobile malware helps criminals attack your accounts, capturing SMS messages and recording screengrabs or video while you log-in to your account.*** mobile Trojans intercepts pass codes sent to mobile phones as part of a two-factor authentication process,to divert money from your bank account to one owned by the attacker or partners in crime.
- **Ransomware**
- ***screen appears on your phone or tablet threatening to lock the device and encrypt your data unless you pay a ransom***
- **Botnets and Spam**
- ***mobile botnets, with apps that leave malignant code lurking on a smartphone until it's triggered, adding the device to the network of zombie 'bots'.***

Why is Hardware Security required for Mobile Payment Smartphones?

- Software-only solutions at the OS level (OS security, anti-malware, …) cannot protect against any software attacks because
  - OS itself has flaws
  - Handset firmware and OS can be modified

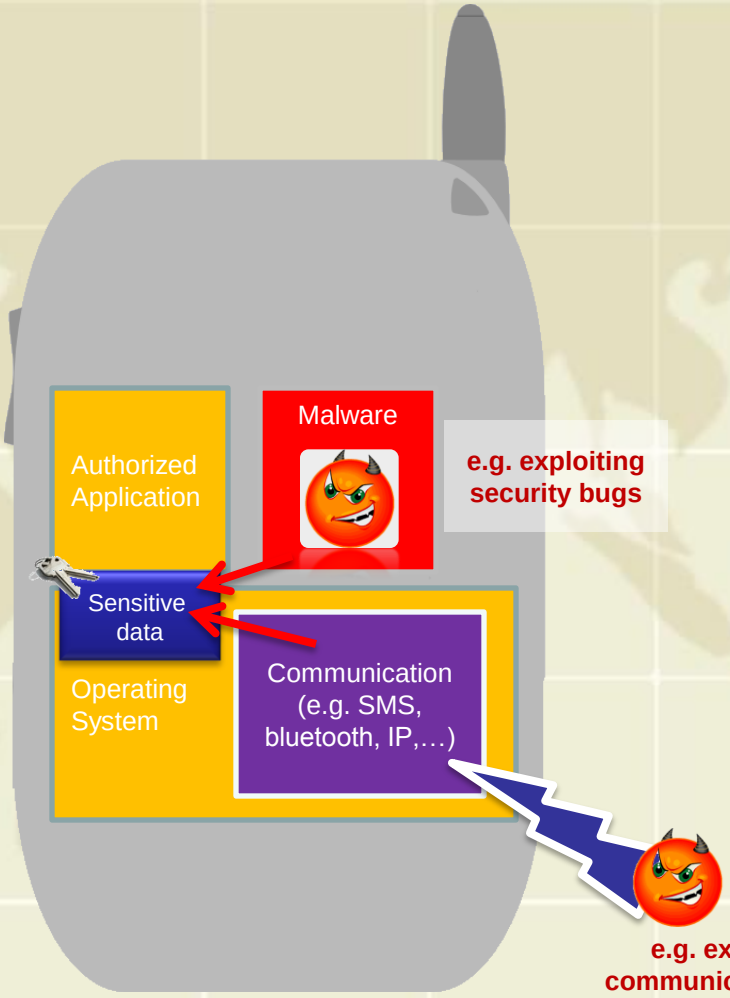
- Hardware attacks require to be countered with hardware protections
- Mobile OS cannot be verified and certified in security and therefore be 100% bullet-proof
- ⇨ Need to minimize this risk and isolate critical code: **Trusted Execution Environment**
- **Online Application Stores are major targets for Malware, Trojans**



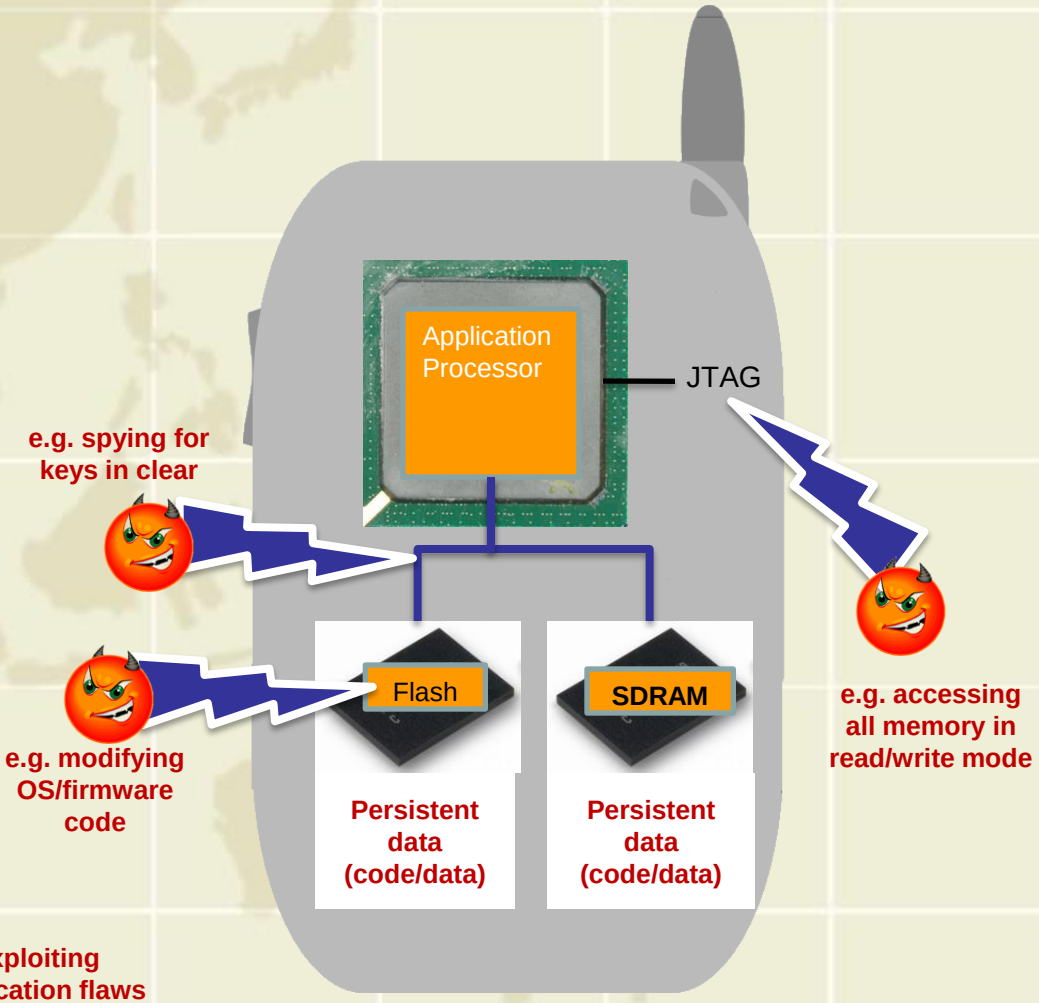


Examples of Attacks

Software / Logical Attacks



Hardware Attacks



SECURITY IS MOVING TO HARDWARE

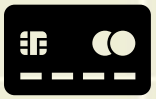
Signature Authentication

Legacy Online Payment

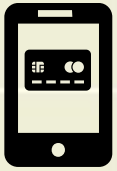
Passwords

Software solutions continue to fail

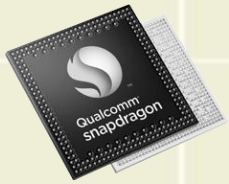
Evolution and disruption are the solution



Embedded Security Chip



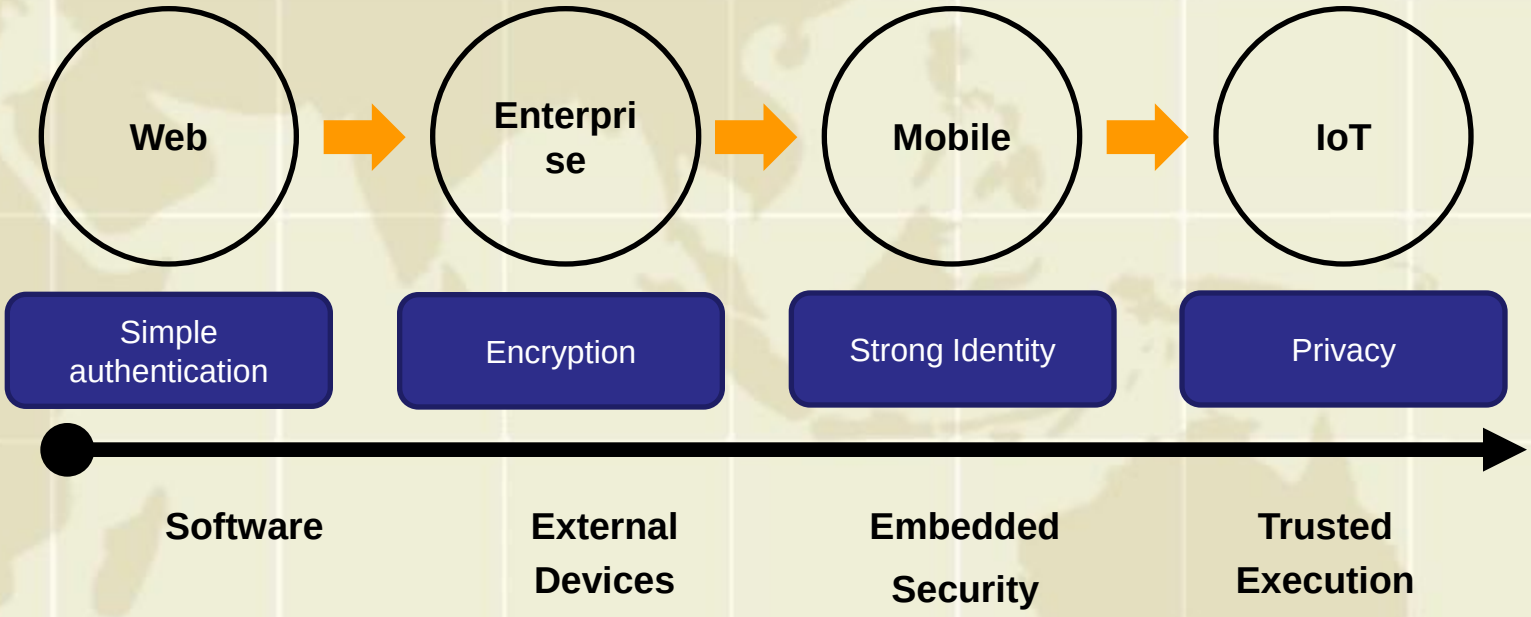
Stored Credit Cards



Hardware Encryption

SECURITY GETS BUILT-IN

rivetz



Layer 8

Known Devices

Secure Instructions

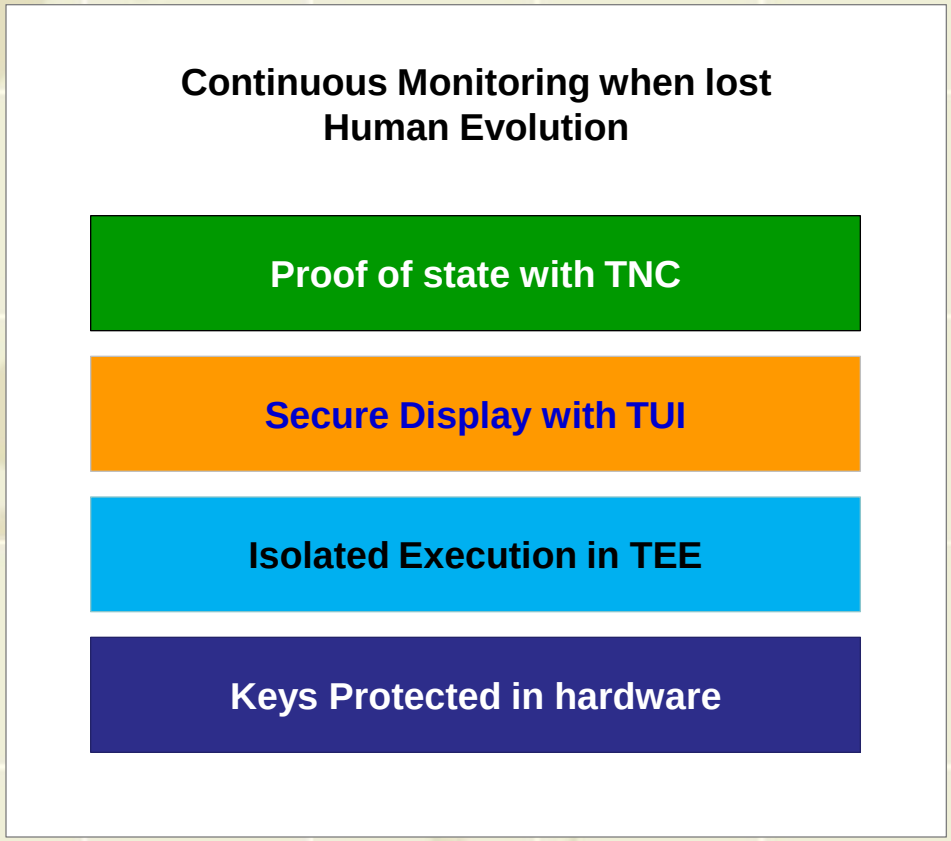
Messages

Money

MODERN TRANSACTIONS: REQUIRE SECURE INSTRUCTIONS

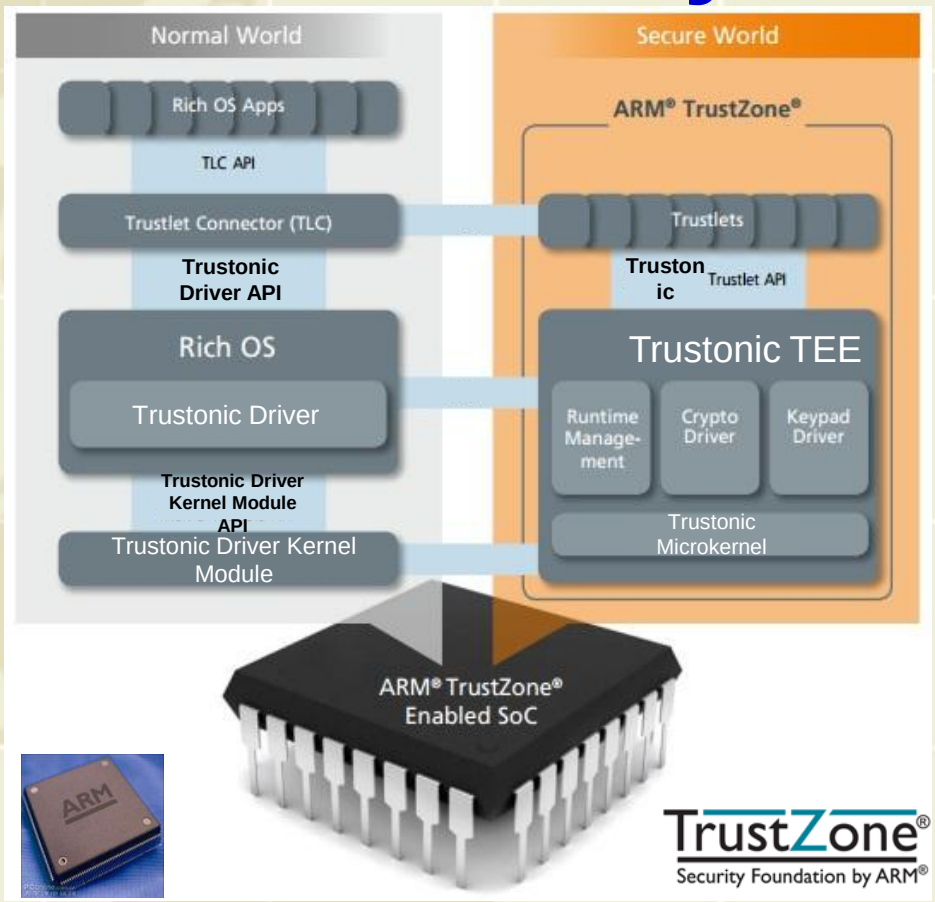
rivetz

- Safe key storage and backup
- Secure Processing
- Secure Display
- Secure Pin/ biometrics
- Proof of state
- Continuous presence



Mobile Payment Smartphones need TEE mobile security

- **There are security challenges in a Smartphone/Tablet PC Mobile Device Environment**
- **Malware and Viruses**
- Privacy, Financial Fraud, Content Protection, Enterprise Data, Secure Space



Solution: (TEE) Trusted Execution Environment

Framework for mobile device security Layer between Rich OS and SE Protection against malware and viruses

TEE Architecture

Environment isolation Rich OS, Trusted Applications, Secure Element
TEE Internal, Client, functional APIs

Key Use Cases for TEE

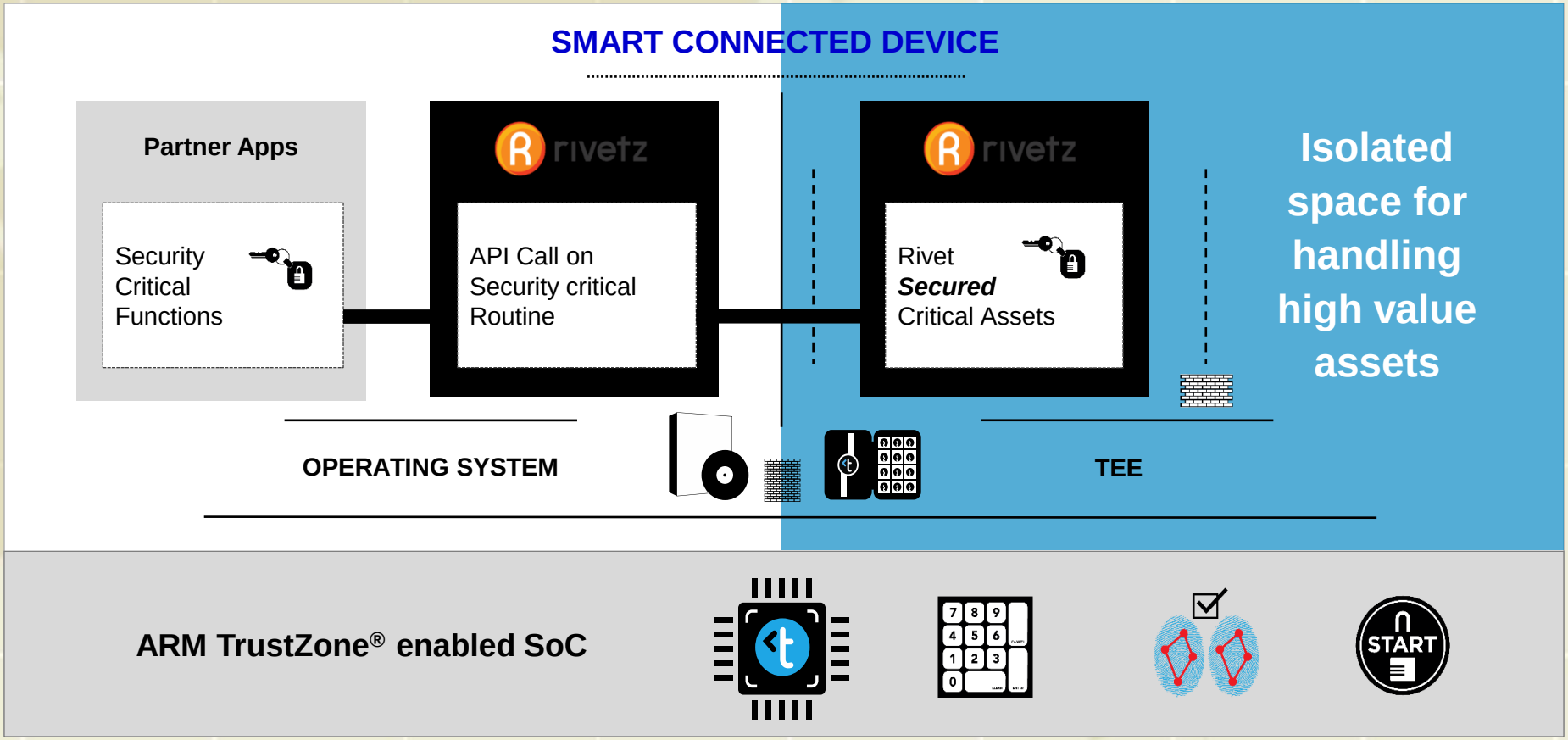
1. **Mobile Payment**
2. **DRM –Content Management**
3. **Corporate Access –Email, Intranet**

rivetz is a Trustonic Partner, provides developer tools to design TEE-enabled Applications!

Rivetz and TEE

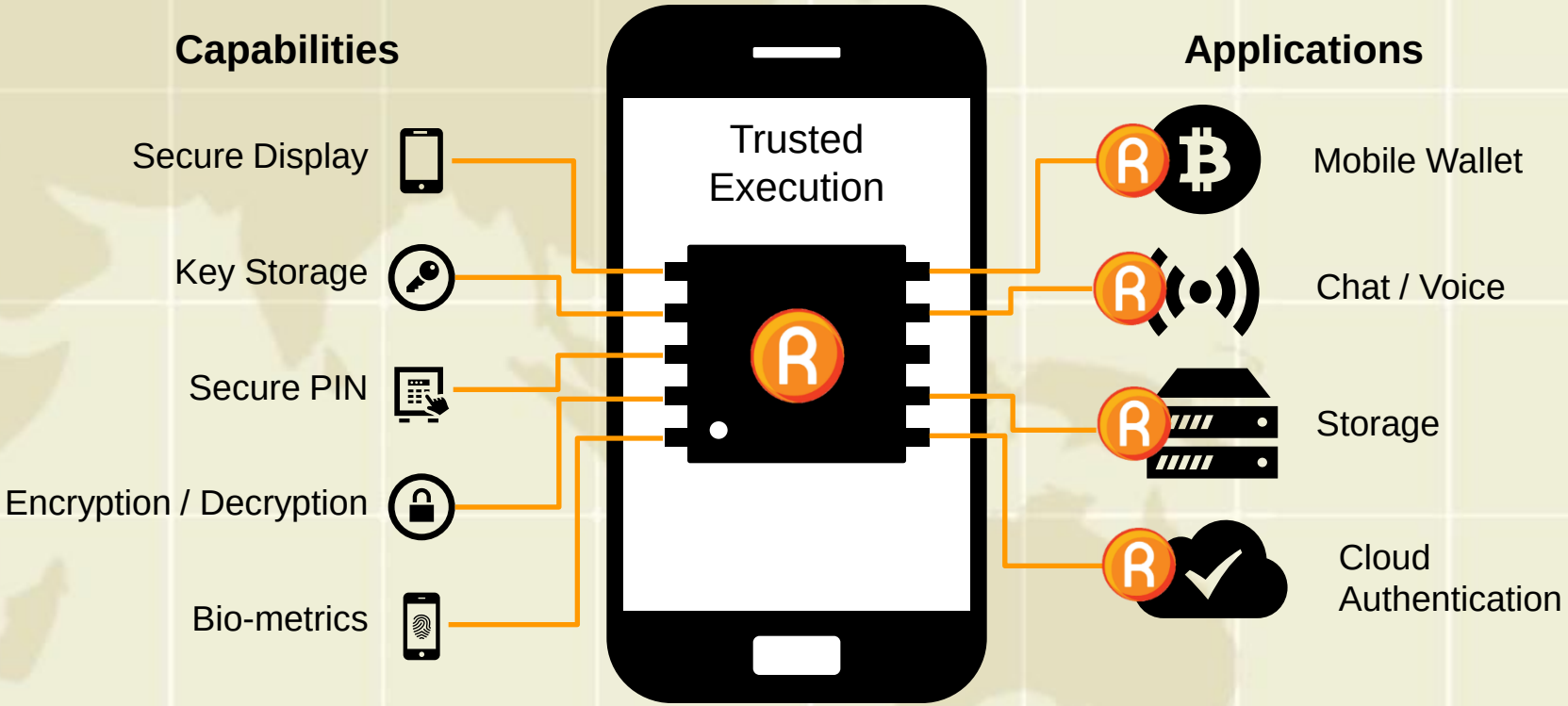
Key assets exposed

Key assets protected



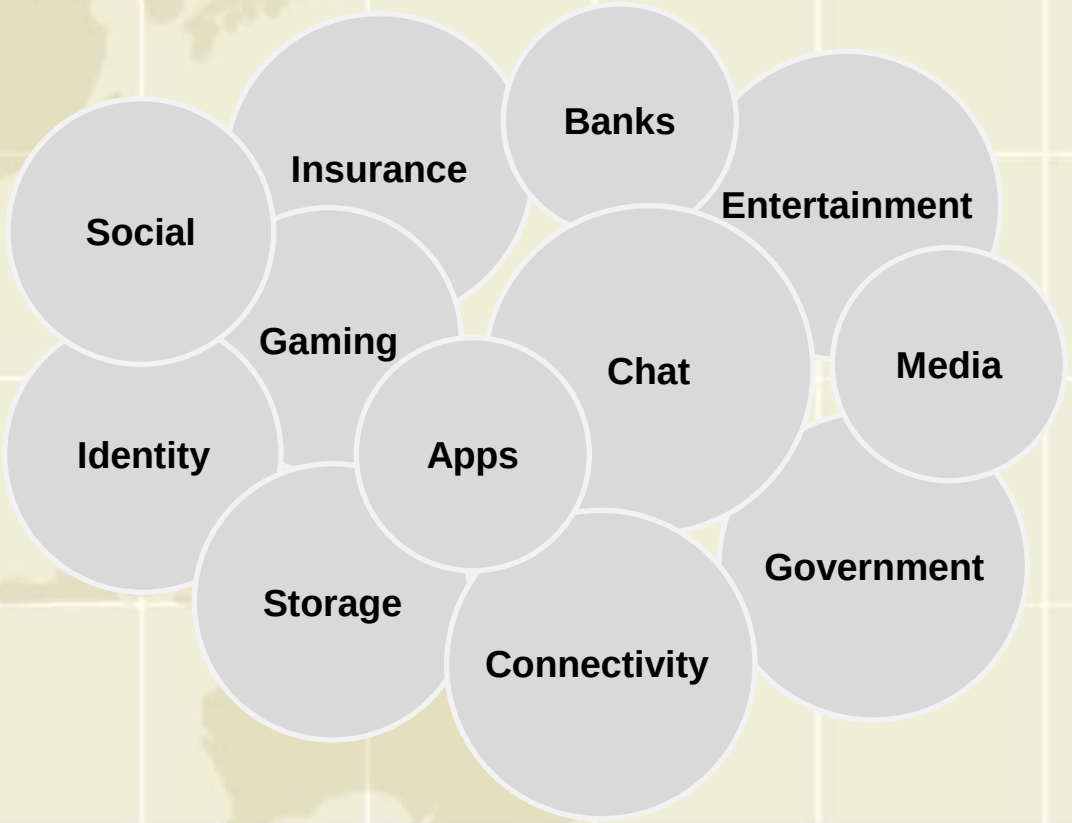
rivetz

Connecting built-in security and APP developers



EVERYONE NEEDS BUILT-IN APPICATIONS SECURITY

- Authentication
- Encryption
- Privacy
- Chat
- Secure Communications
- IoT

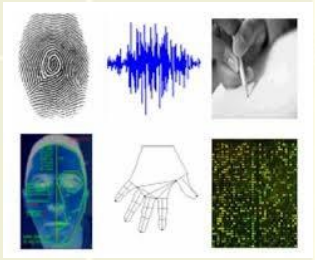


Mobile Commerce with Biometic Identity – distruptive for Commerce

Pay | P | SAMSUNG pay | ?

Direct From Bank
Credit on Demand

Biometric Identity Service Provider



MOBIO concept is to develop new mobile services secured by biometric authentication means. Scientific and technical objectives include robust-to-illumination face authentication, robust-to-noise speaker authentication, joint bi-modal authentication, model adaptation and scalability.

Mobile Biometrics Definitions

Biometrics Smart Mobile Device	Smartphones, Tablets, and Wearables that have one or more Embedded Biometrics integrated into the device.
Embedded Biometric	A biometric that is fully integrated into a smart device including the sensor and related software required to access the sensor and store biometric data on board.
Biometrics App	Downloadable software application that provides biometric capability for a Smart Device. It can be a standalone capability or it can leverage Embedded Biometrics or other Biometric Apps that have been previously downloaded. It can be purchased by the user or provided free of charge by a vendor or service provider.
Mobile Biometric Payment Transaction	Any transaction that includes a payment that is secured via biometric authentication. This DOES NOT include payments currently facilitated by payment systems such as Apple Pay that use a biometric as a Convenient Pin or Password Replacement only.
Mobile Biometric Non-Payment Transaction	Any Non-Payment Transaction – such as accessing a bank or credit card account or logging onto to eGoverment services — that is secured via biometric authentication. This DOES NOT include Non-Payment Transactions currently facilitated by payment systems that use a biometric as a Convenient Pin or Password Replacement.

- ***Biometric authentication has been around for ages, from thumbprint scanners to iris verification and capillary scans (looking at the blood vessels under your skin). Today's devices, both mobile and stationary, are equipped with more sensors than ever before. It's not unreasonable to think that they'll be equipped with more scanners in the coming years and that those sensors will be able to verify our identities.***

Mobility Fuels Biometric "Boom"

- Global biometrics market poised to explode - "ticket to ride".
  - Pace of market development accelerating as previously unrealized biometric opportunities coalesce around rapid expansion of mobile consumer applications.
- Biometrics being "seized" to reduce user friction & simplify user experience.
  - Facilitate more interaction, communication, engagement, comfort, security, and ultimately more information access and digital transactions - the "holy grail of mobility".
- Biometrics have the potential to disrupt global commerce and fundamentally shift power and control of consumer PII (Personal Identifiable Information) away from "monetization" enterprises
- Turf over which major consumer technology companies – hardware and software, device, and services – will fight with established banks, CC companies, payment processors, retailers, etc plus emerging start-ups.
  - ALL seek to PROFIT off changing the way we interact and conduct business.
- Not clear how market development will play out, who wins and loses, and how ecosystems will transform.
  - HOWEVER, NO QUESTION "invisible integration" of biometrics is critical this transformation.
  - Biometrics will facilitate trusted, reliable, free flowing global commerce while offering consumers increased privacy and PII protection.

Conclusion

- **Mobile payments need "Tamper-Resistant" embedded security, the most secure uses a USIM /Secure Element with TSM payment platform on the Smartphone (Former Softcard and soon-to-be Android Pay in the USA).**
- **The addition of Cryptograms and tokenization provides an even higher layer of security for USIM-and Cloud-based mobile payment credential(Apple & Android payment methods) Smartphones.**
- **The TEE – Trusted Execution Environment can add additional layers of security, especially for HCE – Host Card Emulation or other mobile payment applications not normally residing in the USIM card with stored credentials in the Secure Element. Hence the Cloud!**
- **The use of less secure payment technologies will not fly in an age were Hackers have very sophisticated jail breaking software tools.**
- **Trusted computing online web sites are needed and consumer privacy needs to be respected globally. The ethics of software people are in question, time to build a United Nations of Trust in the Global Software developer Landscape.**
- **Microsoft will use Azure for mobile payments on Lumia (Nokia) Smartphones, using HCE, and their wallet application, every company should call it "Pay" to be associated with what Apple has started!**
- **Biometric Authentication will be used by Alibaba's AliPay Wallet to authenticate facial recognition, withint 2 years expect most Smart & Connected devices to incorprate built-in/embedded mobile biometrics functions.**
- **China will allow Apple pay, Samsung Pay and Android Pay to compete on an even playing field which also benefits local Chinese Smartphone OEMs that are utilizing these technologies.**

THANK You 谢谢你!

For More Information call or email me

Karl J. Weaver **魏卡爾**

Greater China Biz Dev/Sales Manager
NFC & TEE Rainmaker for the
Chinese Mobile Payment World

Rivetz Corp.
Developer Toolkit for the TEE
mobile security ecosystem

Mobile 手机：+1-425-260-4378
Email 电子邮件：karljweaver@rivetz.com
Web 网站：www.rivetz.com
微信查询 WeChat: 1-425-647-9315 (search)
微软 Skype: karljweaver,Woodinville,WA,USA