Smart Card Alliance

Host Card Emulation (HCE)

Mobile & NFC Council
Smart Card Alliance
June 18, 2015

Smart Card Alliance Mobile & NFC Council

- Raise awareness and accelerate the adoption of all applications using NFC
- Access control, identity, loyalty, marketing, payments, peer-to-peer, promotion/coupons/ offers, transit, …
- Accelerate the practical application of NFC, providing a bridge between technology development/specifications and the applications that can deliver business benefits to industry stakeholders.

Today’s Webinar Topics and Speakers

- **Introduction & HCE Overview**
  - Sadiq Mohammed, Vice President, MasterCard
  - Chairman - Mobile and NFC Council

- **Security Considerations for HCE**
  - Peter Helderman, Principal Consultant
  - UL

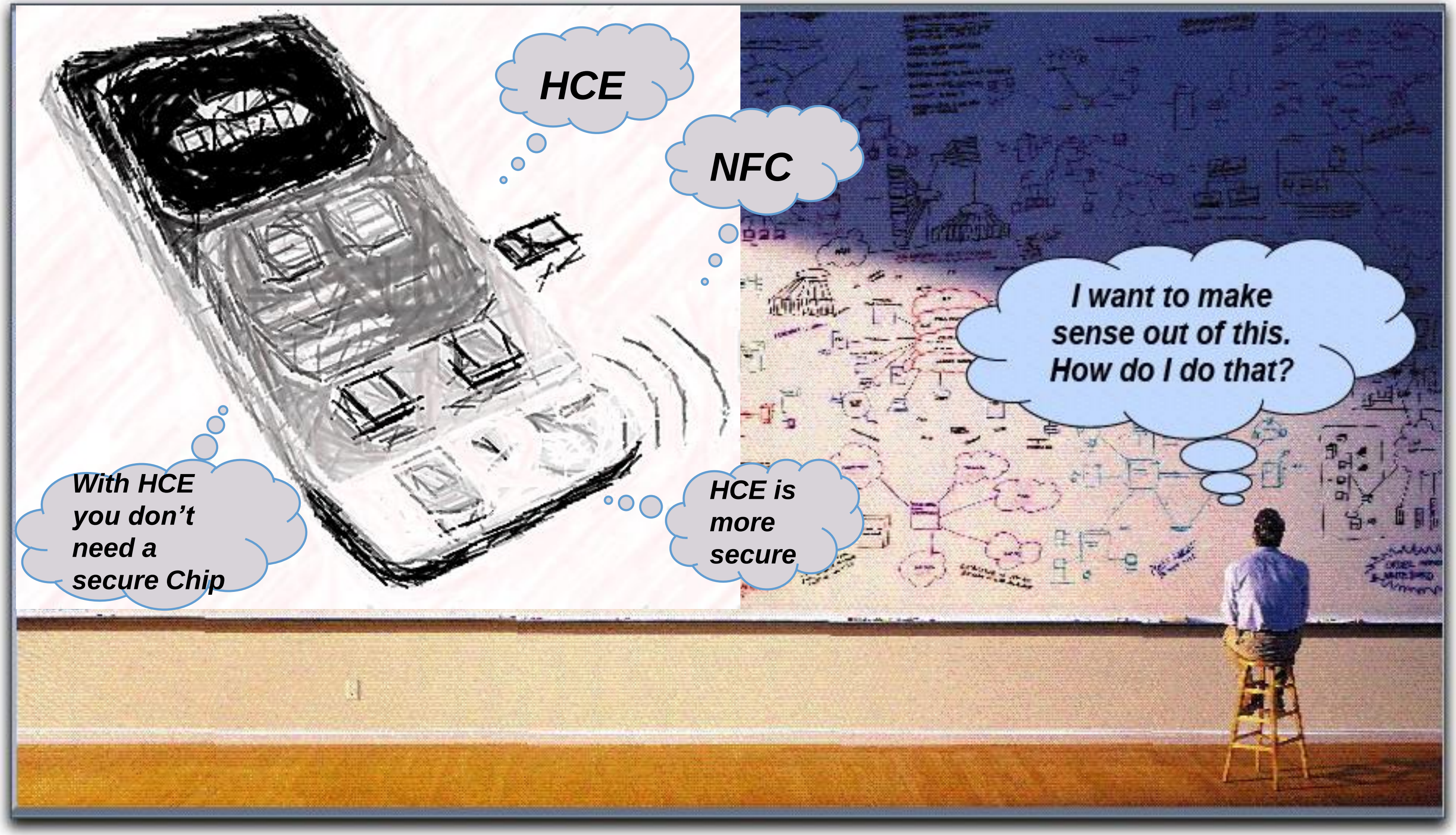
- **HCE Uses Cases and Challenges**
  - Sree Swaminathan, First Data Corp
  - Vice Chairman - Mobile and NFC Council

- **Summary /Conclusions & Q&A**
  - Randy Vanderhoof
  - Executive Director, Smart Card Alliance

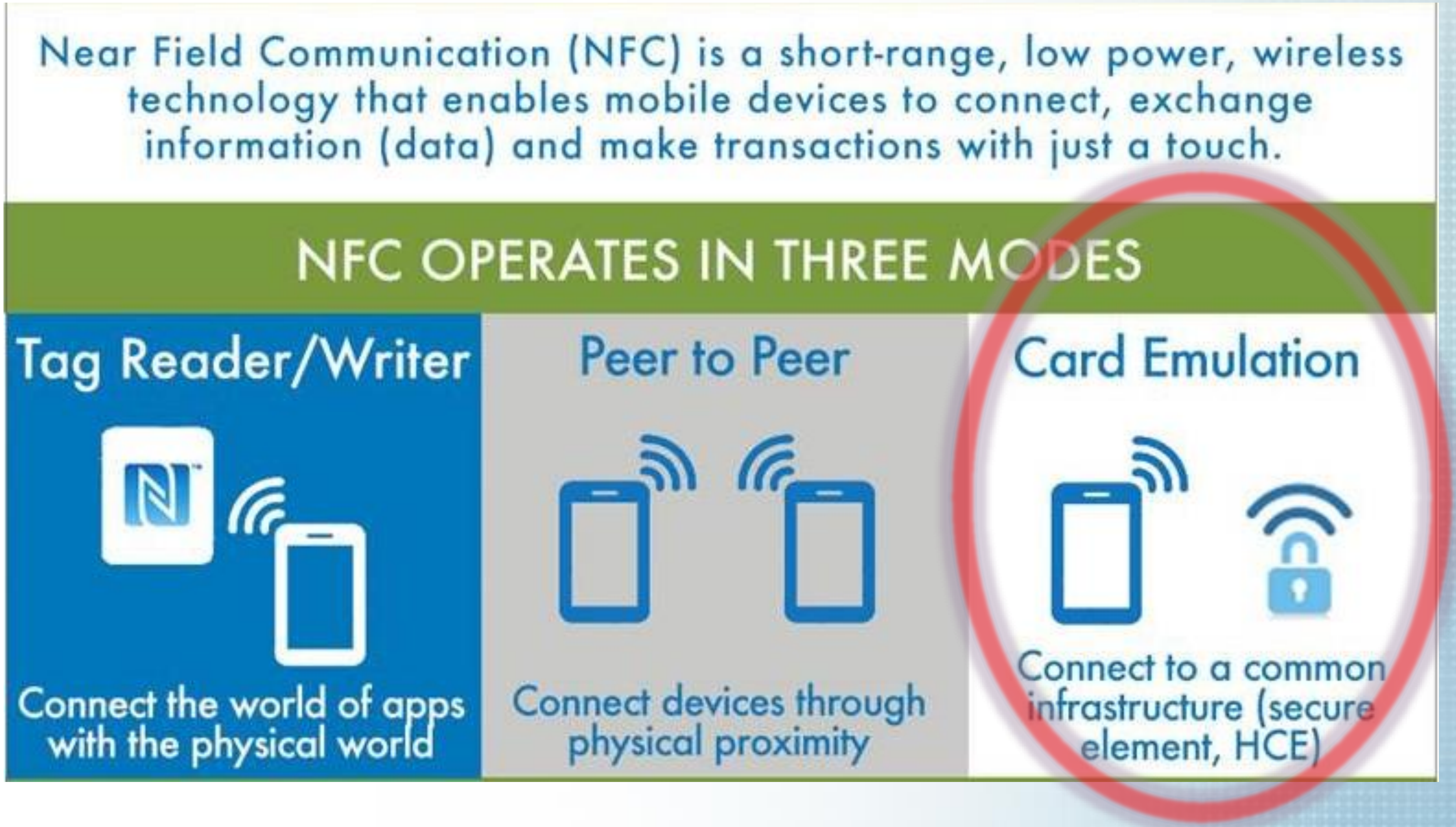
Smart Card Alliance

Introduction & HCE Overview

Introduction to Today's Webinar


HCE
NFC
I want to make sense out of this. How do I do that?
With HCE you don't need a secure Chip
HCE is more secure

Let’s Start with NFC!



Near Field Communication (NFC) is a short-range, low power, wireless technology that enables mobile devices to connect, exchange information (data) and make transactions with just a touch.

NFC OPERATES IN THREE MODES

Tag Reader/Writer

Connect the world of apps with the physical world

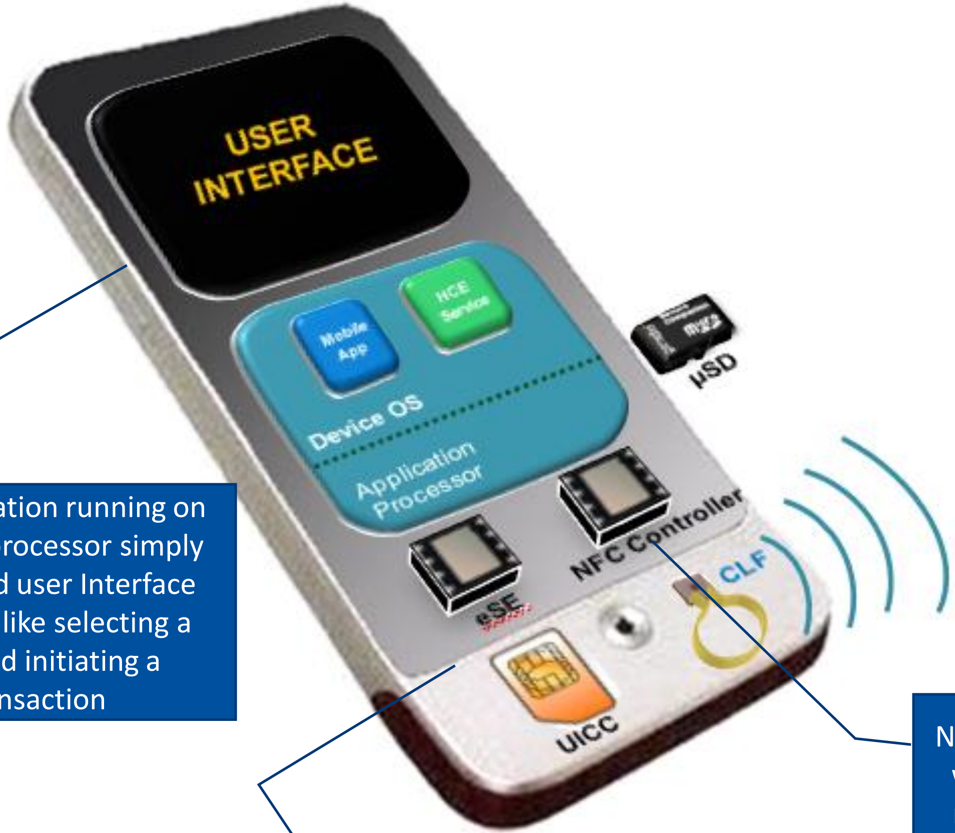
Peer to Peer

Connect devices through physical proximity

Card Emulation

Connect to a common infrastructure (secure element, HCE)

Initial Implementations with NFC



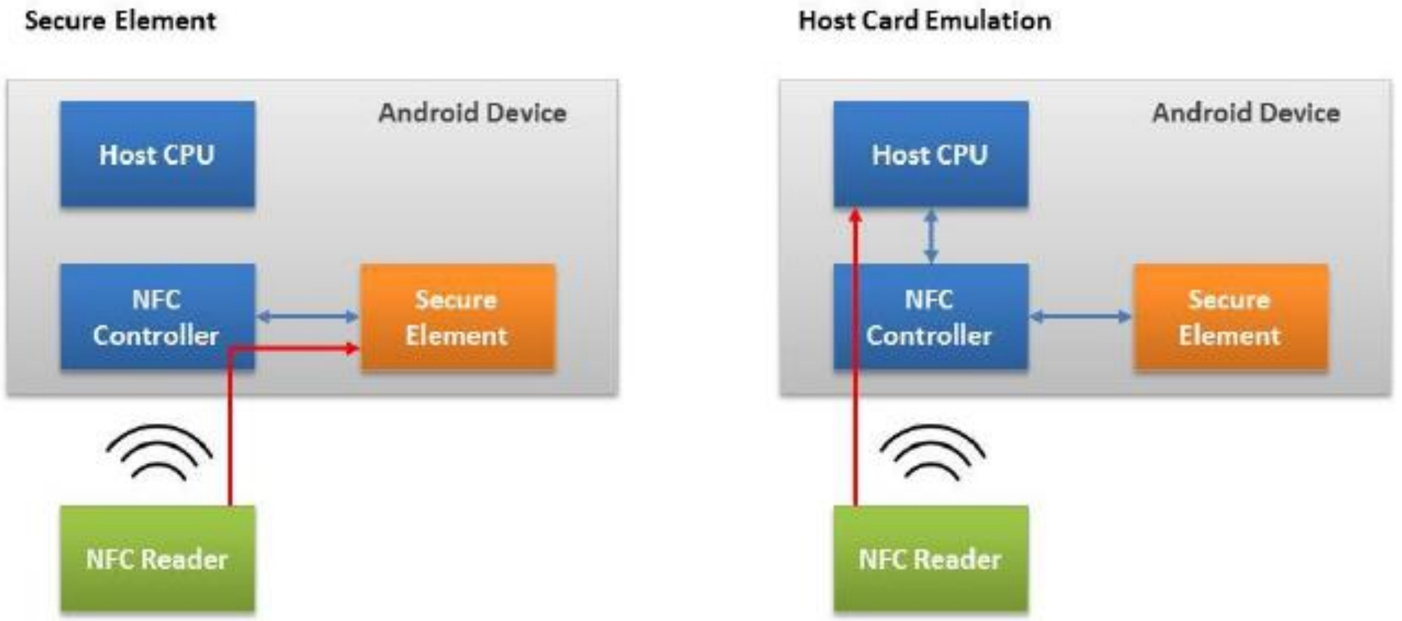
The application running on the main processor simply performed user Interface functions like selecting a card and initiating a transaction

NFC controller interacts with an external card reader and transmits data to and from the application

A Secure Element or SE in the form of an eSE or UICC or µSD – a single chip microcontroller hosted the application and stored the credential data

What Is Host Card Emulation (HCE)?

HCE is mechanism for an application running on the "Host" processor (the mobile device's main processor – where most consumer applications run) to perform Card Emulation transactions with an external reader.



Current support for HCE:

- ✓ Google Android Kitkat 4.4 and higher
- ✓ Blackberry OS 7 and higher
- ✓ Microsoft Windows 10

Smart Card Alliance

Implications of HCE

Benefits

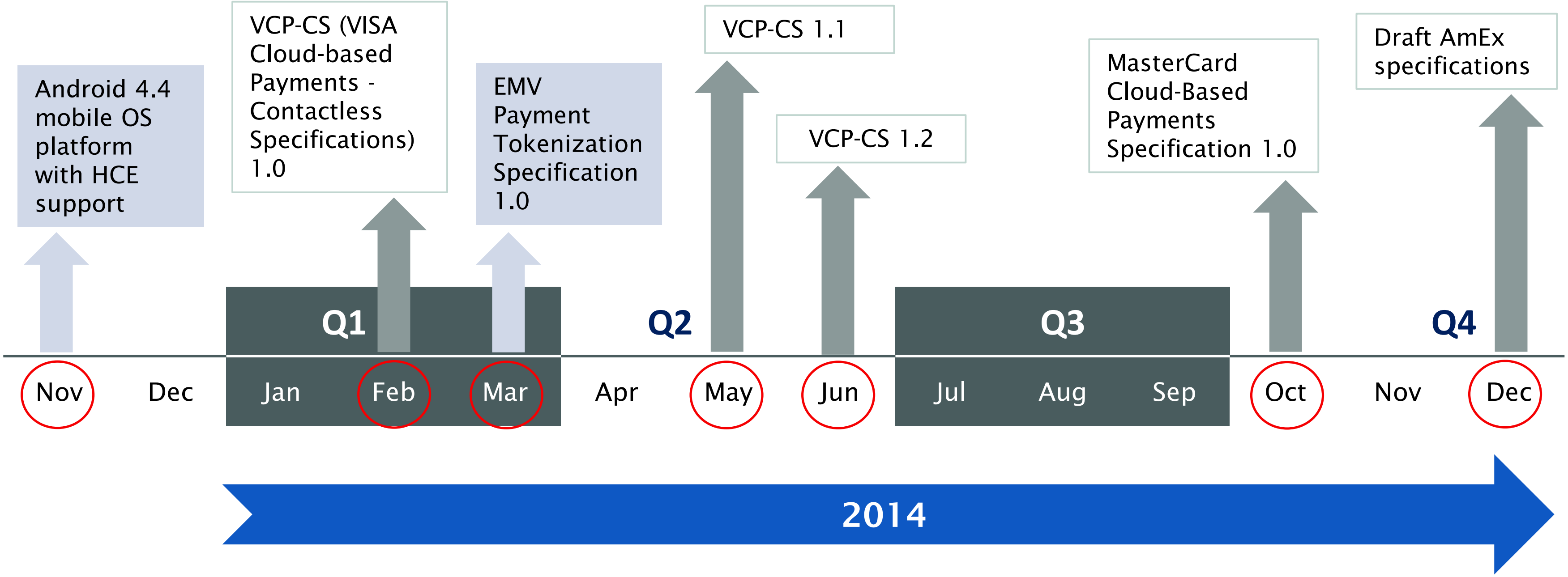
- Reduced complexity for application developers and opens up NFC capability for new applications.
- Easy and flexible card provisioning to mobile device.
- No dependency on MNO or SE owner.

Limitations

- No hardware secured storage of data and credentials on device.
- Dependent on OS capability.
- Alternate security considerations for HCE can increase backend complexity.

Major Standards, Specifications and Evolution History

Host Card Emulation is a relatively (in payment industry terms) recent idea. However the major brands have rapidly endorsed and developed specifications to help vendors.



Android 4.4 mobile OS platform with HCE support

VCP-CS (VISA Cloud-based Payments - Contactless Specifications) 1.0

EMV Payment Tokenization Specification 1.0

VCP-CS 1.1

VCP-CS 1.2

MasterCard Cloud-Based Payments Specification 1.0

Draft AmEx specifications

Q1 Q2 Q3 Q4

Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

2014

EMV Tokenization Specifications

- PAN, expiry date, cardholder name, cryptographic keys to be tokenized
- Tokens have similar format to original data
- Token ranges different from original PAN ranges etc.
- Different business models—digitized card in mobile, card-on-file online etc.

VCP-CS

- Compatible with EMV tokenization spec
- Defined components of HCE eco-system: for provisioning, tokenization, verification, lifecycle management etc.—with general responsibilities
- Behavior guidance for application in mobile. Compatible with VCPS

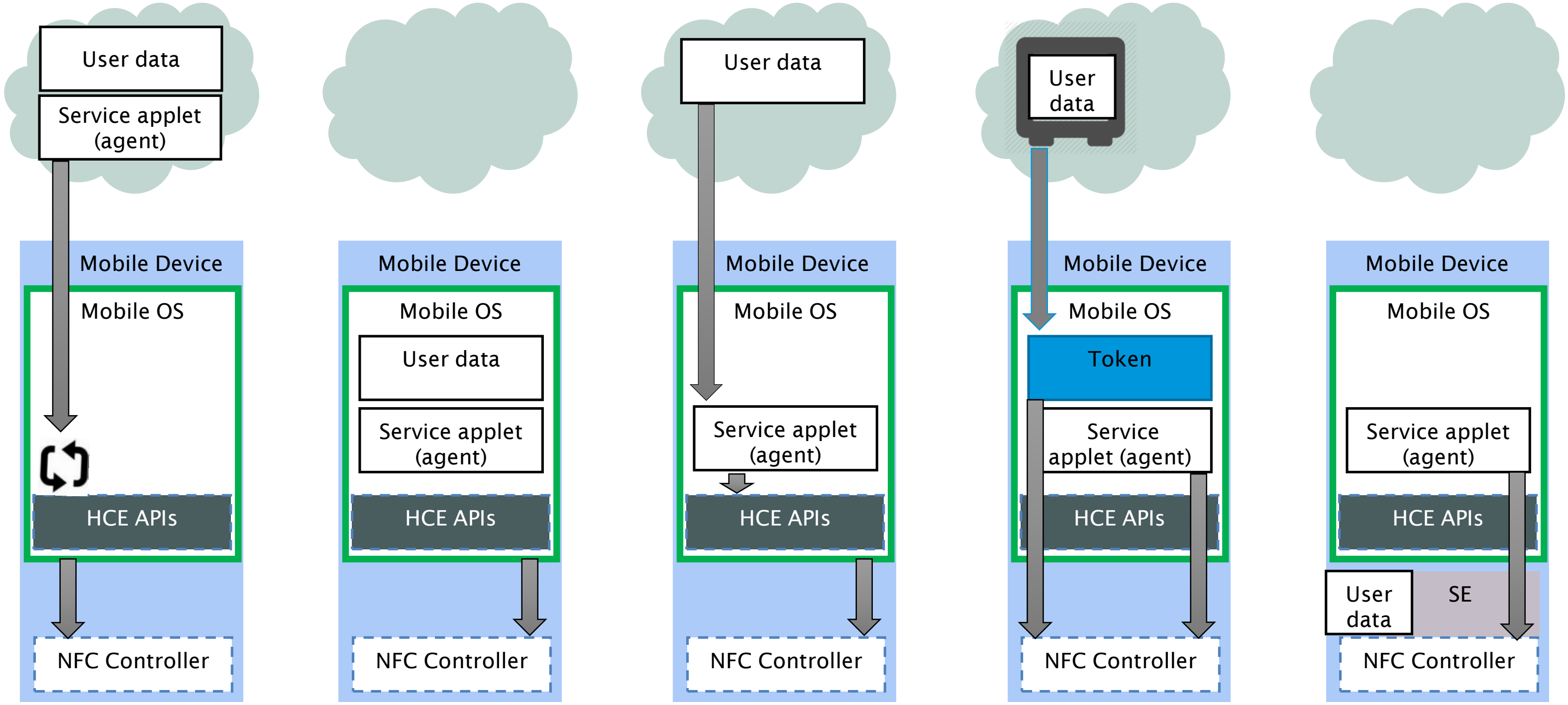
MasterCard CBP

- Compatible with EMV tokenization spec
- Defined components of HCE eco-system—with specific responsibilities and actions
- Defined specific behavior for application in mobile in detail.

Different Models of HCE

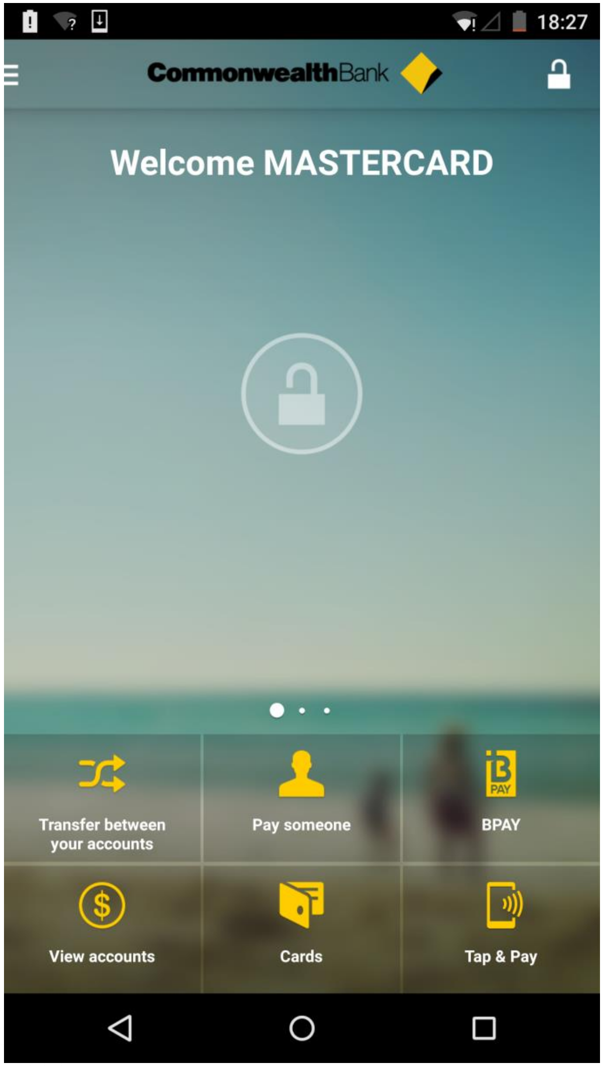
Since HCE capable OS can route card data from anywhere, card emulation can be done from several places, leading to several deployment models

Model—1	Model—2	Model—3	**Model—4 (Payment)**	Model—5 (SE-based)
· Applet in cloud · User data and keys in cloud · **Internet connection needed for every transaction**	· Applet in OS · User data and keys in OS · **Not secure**	· Applet in OS · User data in cloud · **Internet connection needed for every transaction**	· Applet in OS · User data in cloud · Token downloaded to OS · **Internet only during token replenishment**	· Applet in OS · User data in SE · **Dependency on SE issuer (MNO)**

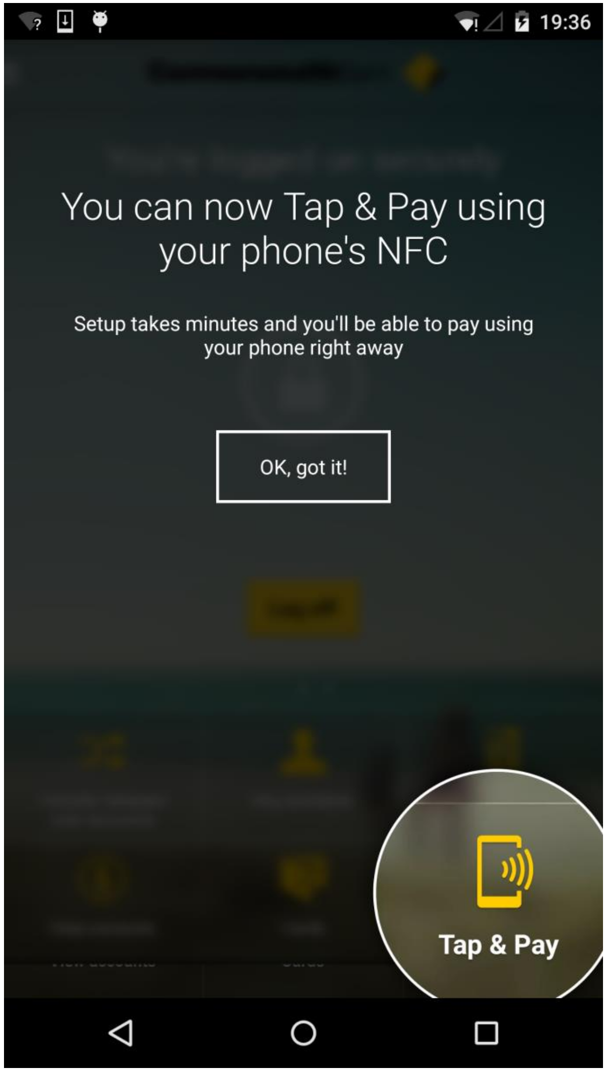


Smart Card Alliance

An Example Commercial Deployment of HCE

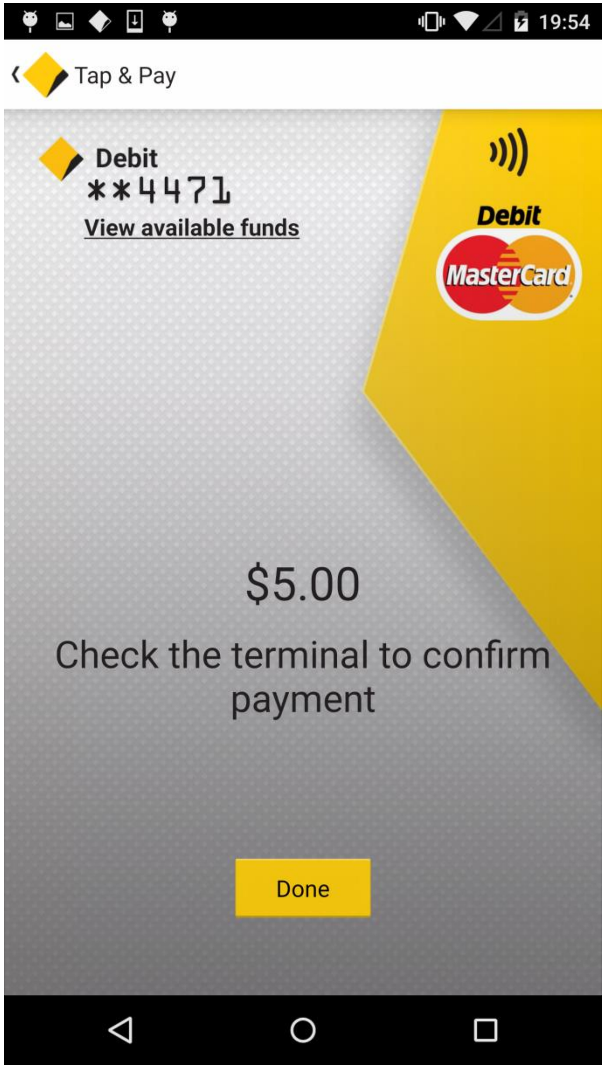


Welcome MASTERCARD



You can now Tap & Pay using your phone's NFC

Setup takes minutes and you'll be able to pay using your phone right away



$5.00

Check the terminal to confirm payment

Security Considerations for HCE Solutions

Perceived HCE Security Concerns

Cloud Based Secure Element ?

Scalability over Security ?

Tamper resistance

Applet Based solution ?

Less Privacy

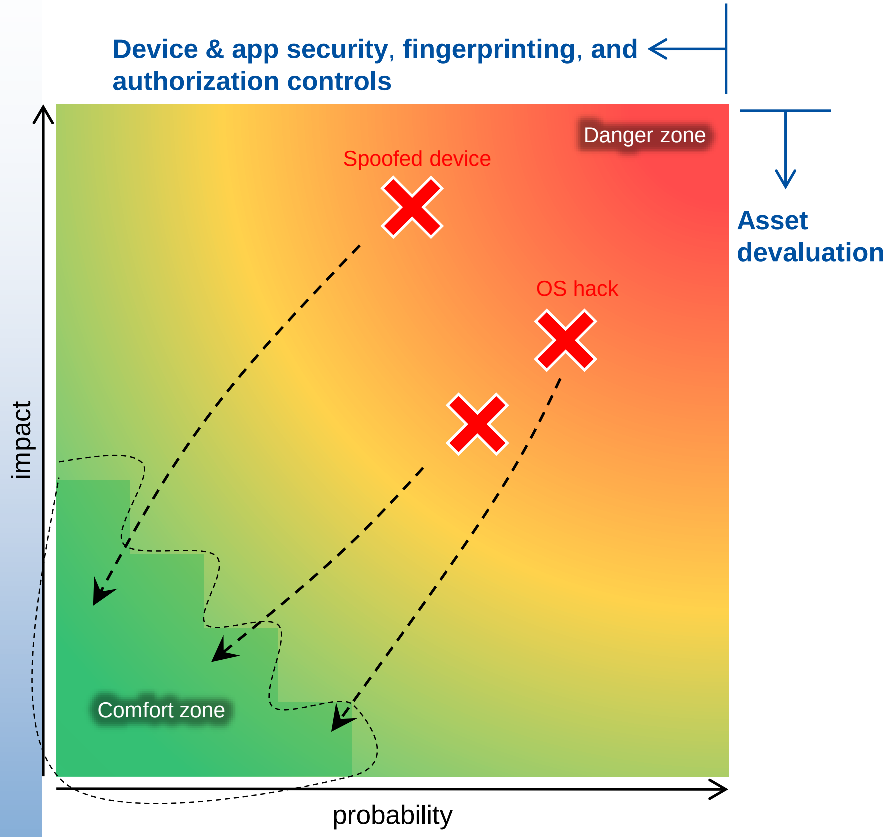
EASY ATTACK ON APPLET?

Hardware vs Software

vulnerable to malicious attack ?

Integrity of HCE Apps ?

Mitigating HCE-related Risks



Managing risks by reducing impact and probability:

1 Device & app security

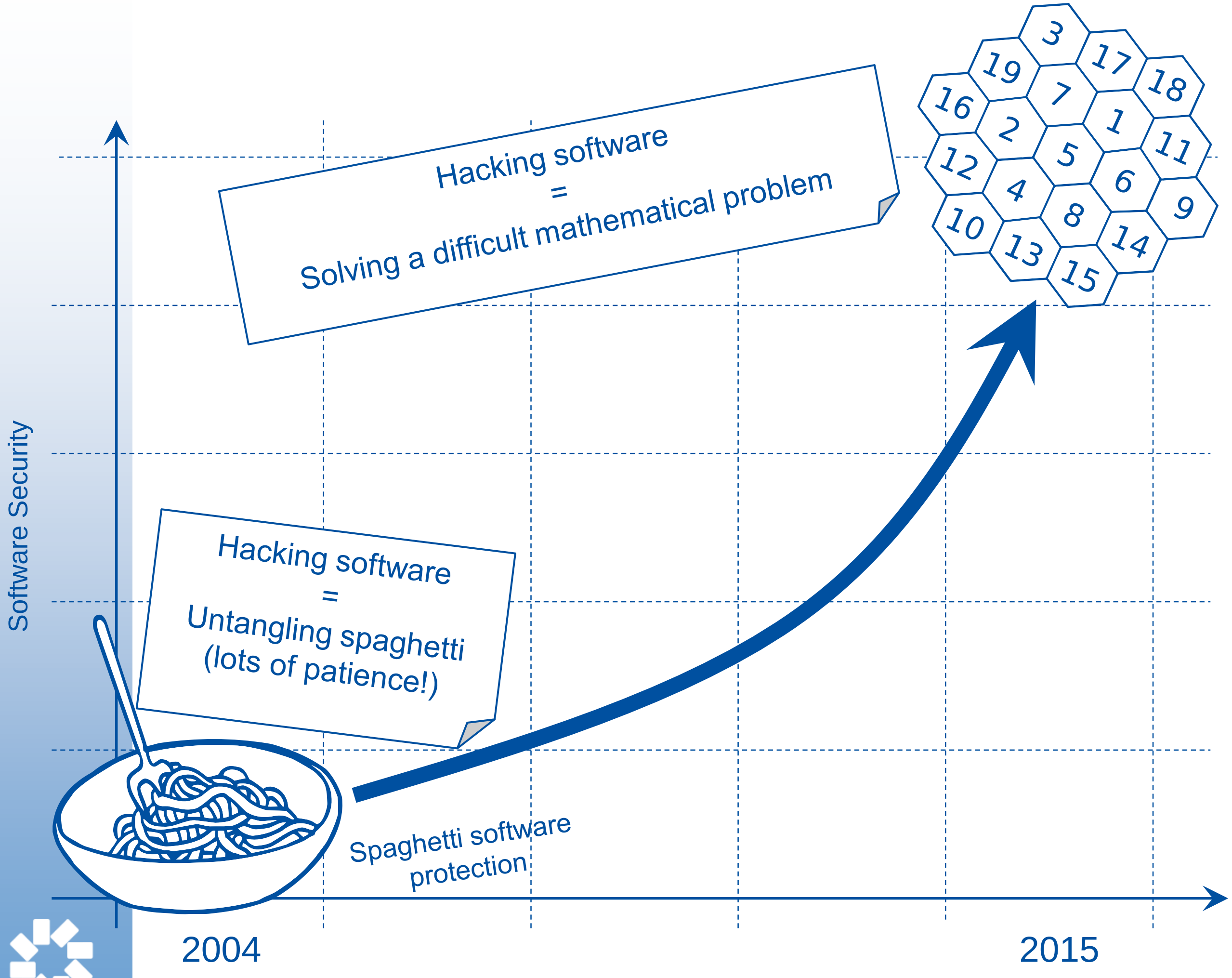
2 Authorization controls

4 Asset devaluation

3 Fingerprinting

1

Device & App Security

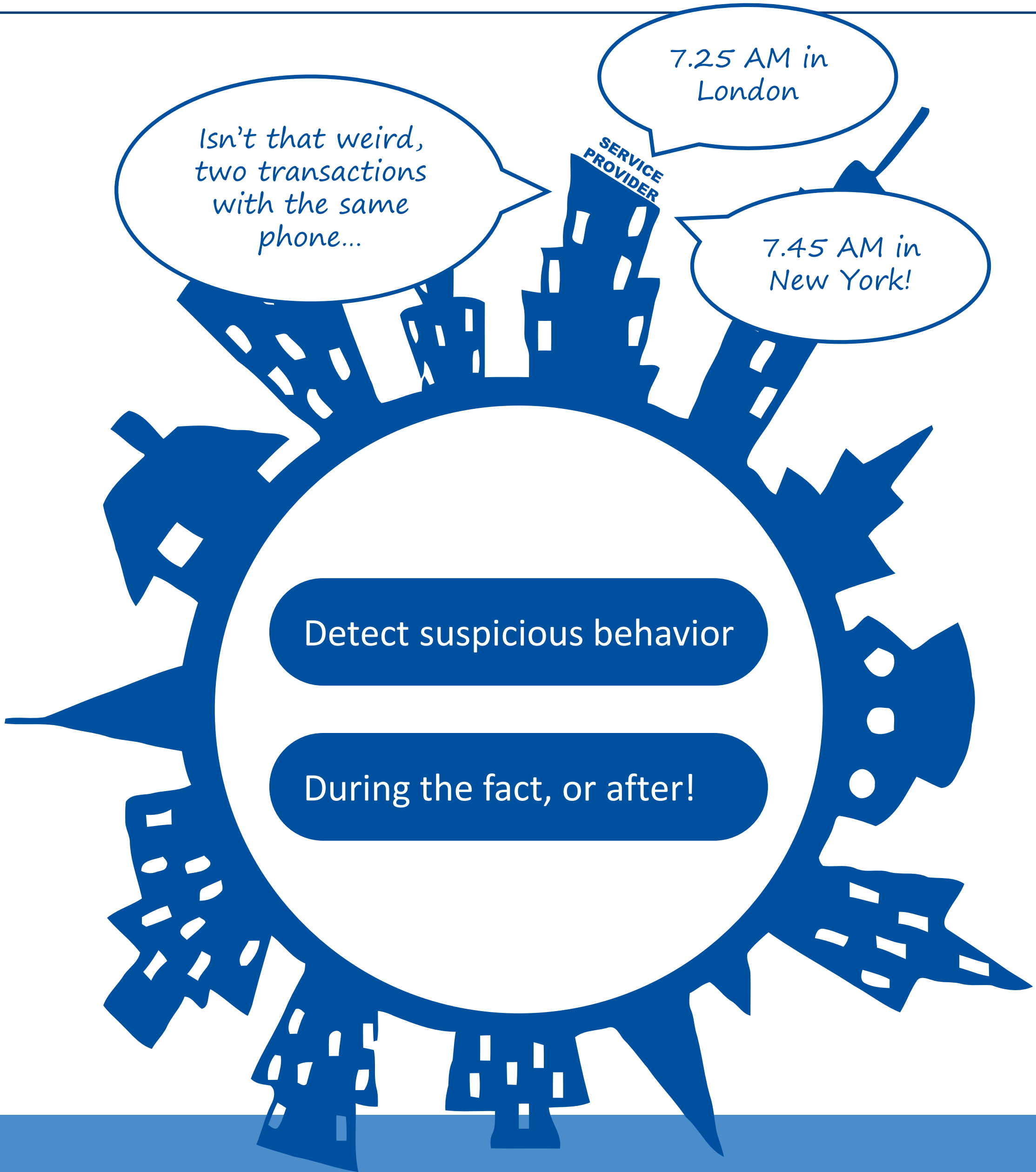

Software Security
Hacking software = Solving a difficult mathematical problem
3
19
17
16
7
18
2
1
11
12
5
6
4
9
8
10
14
13
15
Hacking software = Untangling spaghetti (lots of patience!)
Spaghetti software protection
2004
2015

- Code obfuscation
- Protection code injection
- Whitebox cryptography
- Secure virtualization
- TEE (device security)

Smart Card Alliance

2

Authorization Controls



Detect suspicious behavior

During the fact, or after!

3

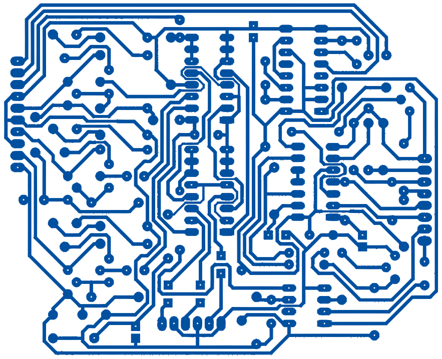
Fingerprinting

Human fingerprint

fido alliance

Apple Touch ID

Device fingerprint



GSMA

Mobile Connect

INTRINSIC ID

PUF

TrustZone

Secure OS

Smart Card Alliance

4

Asset Devaluation

Payments

- Tokenization uses surrogate values in the place of actual credentials
- Domain restriction controls will deter usage in other domains (e.g., CNP)
- Assurance levels can employ additional fraud controls
- Token compromise does not require reissuance of primary plastic cards

Transit

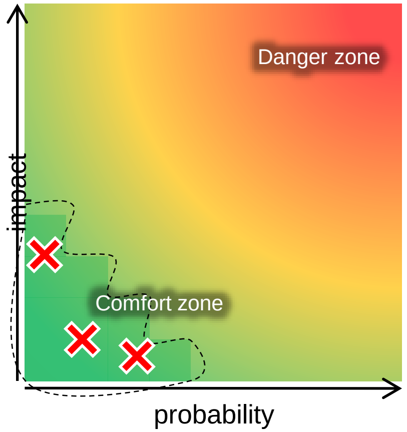
- Tokenization uses surrogate values in the place of actual credentials
- Transit passes can be imported for a particular trip

Access control

- Derived credentials applicable to the mobile form factors while PIV / CAC cards maintain their credence
- Assurance level can increase/decrease the value of the credentials based on the access type

HCE Security - Summary

- HCE in itself contains no security architecture – it is up to the issuer of the HCE app to implement security controls.
- HCE implementations can be made secure through appropriate security measures on the device and back-end systems and by using the standard risk mitigation controls of ‘impact’ and ‘probability’
- Impact of a successful mobile app exploit is reduced through <u>tokenization</u>
- Probability of a successful mobile app exploit is managed through:
  - <u>Authorization controls</u>
  - <u>(Device) fingerprinting</u>
  - <u>Software hardening</u>
- The ‘security of HCE’ is to a large degree determined by the implementation of these risk mitigation measures



Smart Card Alliance

HCE Use Cases and Challenges

HCE Use Cases

Payments

- Open Loop
- Closed Loop

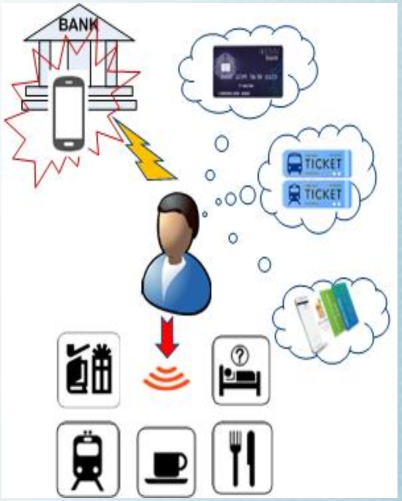
Access & ID

- Transit
- Access

Value Added Services (VAS)

- Offers
- Loyalty

Host Card Emulation (HCE)

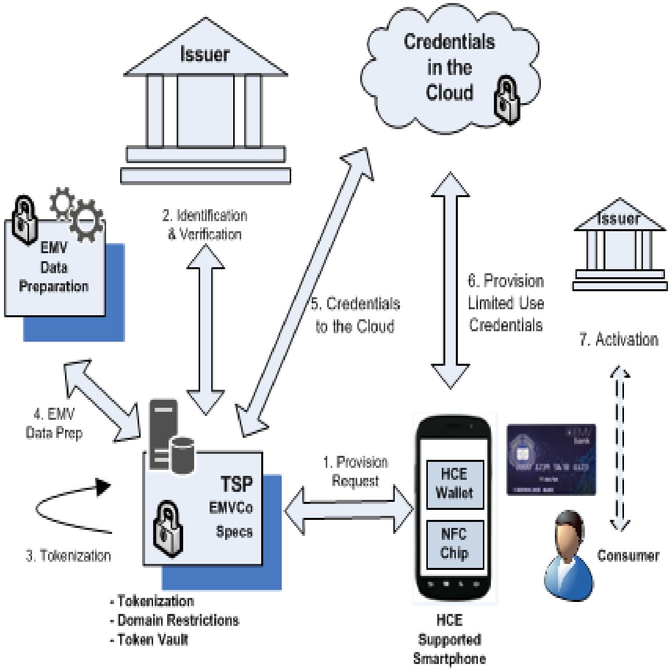


HCE Payment Use Cases - Examples

- Consumer’s bank/merchant/device manufacturer offers HCE-based payment app
- Consumer downloads the app on their HCE-enabled device and enters the details of their card credentials
- Bank authenticates the consumer and approves the request
- Bank’s HCE platform digitizes[1] the credentials and provisions[2] to the device
- Now the consumer can tap the mobile device to make payments at stores, restaurants and combining their loyalty, coupons, tap at transit POI, hotel access, buy tickets from movie posters, etc…

[1] Digitization = Tokenization and delivery of credentials to the device

[2] Provision = Adding credentials to the device in such a way that enable NFC transactions



- Behind the scenes the HCE app can employ the Trusted Execution Environment to ensure sensitive data is stored, processed and protected against malware or attacks on trusted applications.
- Cardholder can be authenticated using their biometric or PIN for every transaction.
- Transactions with tokens are passed from the merchant terminal to the issuer which gets validated by the issuer before authorizing.

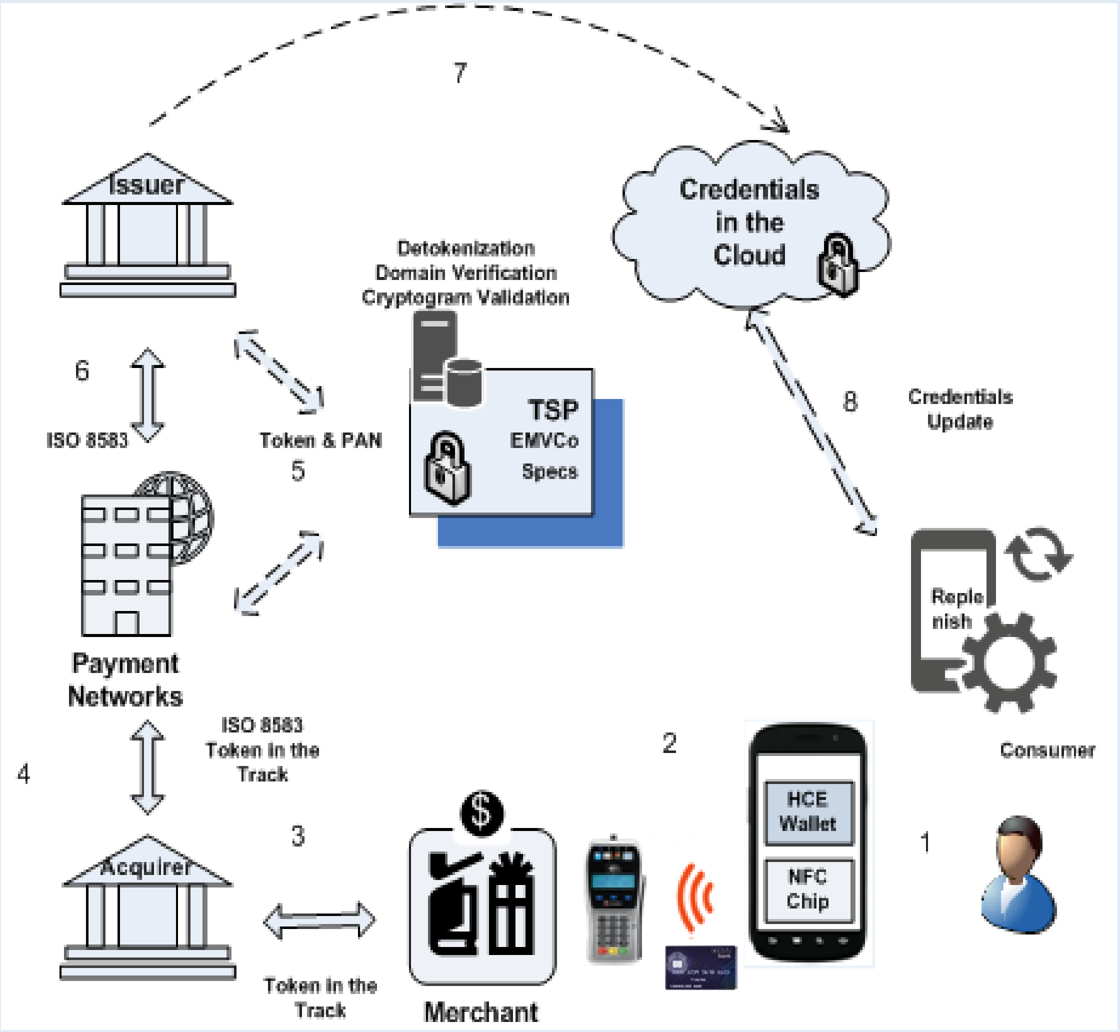
HCE Pilots, Examples, Deployments

Significant increase in activity from the middle of 2014 onwards. Expected to accelerate through 2015 and early 2016.

Date	Type	Market	Issuer	Status
December 2013	Commercial launch	Canada	Tim Hortons	HCE mobile payment app in Blackberry
December 2014	Pilot	Canada	Royal Bank of Canada	RBC Interac Debit card
2014	Pilot	Spain	Banco Sabadell	EMV-based contactless payments
May 2014	Commercial launch	Spain	Bankinter	Mobile Virtual Card – HCE application to enable one-time-use credit/debit card
May 2014	Commercial launch	Ukraine	PrivatBank	Liqpay – HCE payment application
2014	Pilot	Russia	Sherbank	Mobile wallet
2014	Pilot	USA	Capital One	Closed User trial
June 2014	Commercial launch	Spain	BBVA	VISA HCE compatible payments
Mar 2015	Commercial launch	Australia	Commonwealth Bank of Australia	MasterCard compatible HCE payments.
Apr 2015	Commercial launch	Netherlands	ING	MasterCard compatible HCE payments
1Q 2014, May 2015	Commercial launch	USA	Google	Google Wallet 2.0 based on HCE Android Pay based on HCE

Smart Card Alliance

Payment Use Cases – HCE Transaction and Credentials Update

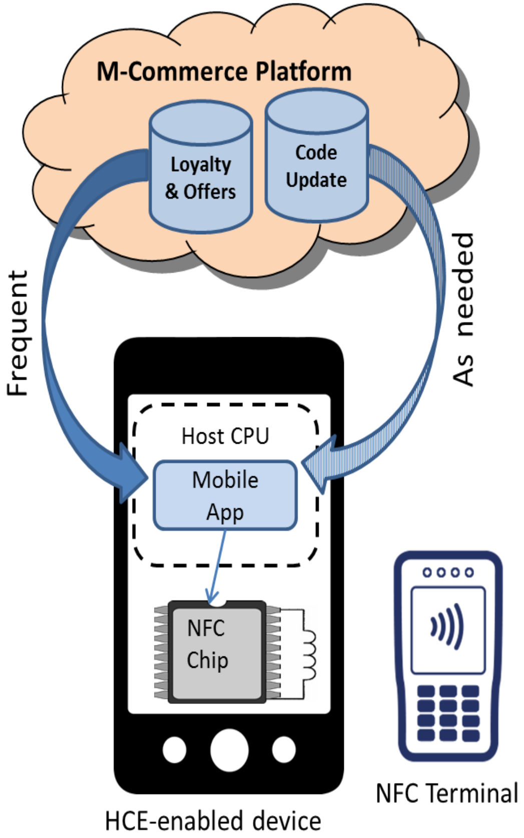


1. Initiate HCE Payment
2. NFC/ In-app Transaction
3. ISO Auth Message
4. Authorization Request/Response
5. Routing / Detokenization
6. Detokenization/Auth Response

7-8. Host Synchronization, Life Cycle Management, Credentials Update

Loyalty and Offers – Value Add Services

- Many mobile apps for smartphones host and manage loyalty and offers, but are limited to QR / barcode scanning
- Loyalty cards and offers can be presented to the POS via NFC
- Combining payments, loyalty and offers into a single NFC tap greatly increases the value of a mobile commerce application
- HCE is a highly effective method for managing and presenting loyalty and offers via NFC
- With high level of interest in mobile commerce, we should expect several changes and new entrants providing offers

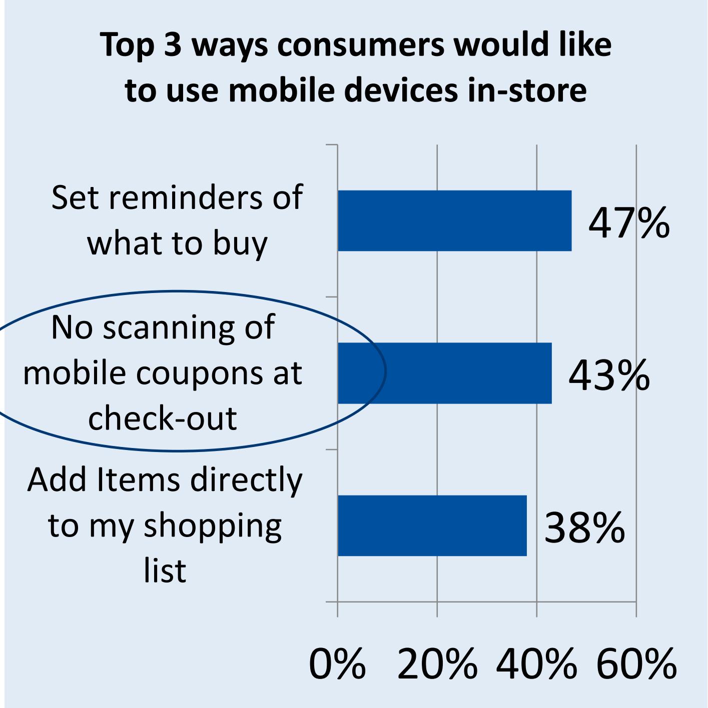


Payment + Offers + Loyalty Examples:

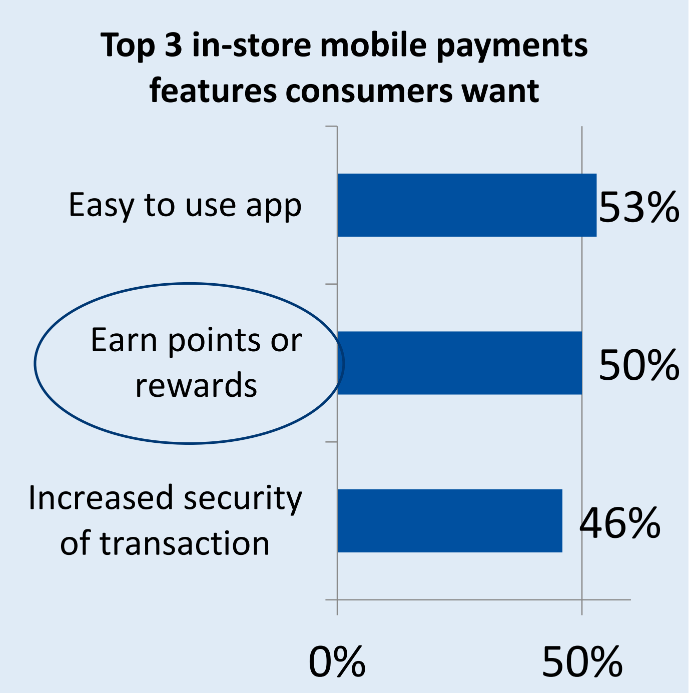
- **SoftCard's Smart Tap**
- **Google Wallet Single Tap**

Why Use NFC for Offers and Loyalty?

- Consumers want “more than payments” from their mobile applications.
- Starbuck’s and Dunkin Donuts apps prove the value of loyalty + payments.
- NFC provides convenience of payments, offers and loyalty in a single tap



Source: JiWire Mobile Audience Insights Report Q3 2013



Source: Euromonitor International’s Hyperconnectivity Survey 2014

Transit Use Cases with HCE

- HCE offers speed and convenience to transit industry for both the consumer and transit worker

For the passenger:

- Consumers can purchase their transit passes through their mobile device
- As agencies move to account based systems (ABS), HCE facilitates the authentication of the tokens linked to their account

For the transit worker:

- Agencies can issue their employee credentials via the cloud, which are downloaded by the respective transit employee
- Agencies, via HCE, can verify presented credentials to allow or deny access to areas or infrastructure within their systems; e.g., first responders

- London, UK's TfL, Chicago's CTA and Salt Lake City's UTA have implemented ABS
- Philadelphia's SEPTA, Washington DC's WMATA and Portland, OR's TriMet are in the planning/development stages for ABS

Access: Hotels, Parks & Recreation

Hospitality, event and theme park operators are using mobile apps in innovative ways to engage consumers during their stay. HCE allows users to perform transactions while in that branded app.

Hotel and Office Access:

- Hotels can push limited use room keys to mobile apps
- Temporary access to office and facilities can be granted on need basis

Theme Parks and Events:

- Contactless access and payments are popular with outdoor venues; provides robust solution for:
  - Access to guest rooms
  - Expedited access to rides, attractions and events
  - Token for purchasing with prepaid account

Hotel, Office,
Parks, Events
Access

- Vendors have implemented transport independent technology for HCE and BLE for residential, hospitality and enterprise

Smart Card Alliance

Advantages and Challenges in HCE Use Cases

Payments

Advantages

- Contactless EMV Capable
- Large memory to add multiple cards
- More autonomy and control for the issuer for provisioning
- No Trusted Service Managers
- HCE apps can coexist with other HCE and SE-based apps

Challenges

- Implementation is issuer-specific and can be complex for the issuer
- Device needs to be online for frequent credentials update

Offers and Loyalty

Advantages

- Single Tap can combine Payments + Offers + Loyalty
- HCE-based implementations enable protocols to be updated as easily as updating any mobile app
- Simple on the device side
- Real-time updates

Challenges

- No de facto industry standard available yet
- Requires POS changes
- Reconciliation of the offer / no digital clearinghouse

Transit & Access

Advantages

- Transit - HCE can work with account-based AND card-based systems; similar benefits to payments and offers/loyalty
- Access – HCE allows operators to control the credentials for the duration of validity

Challenges

- Transit - MIFARE implementations may require reader firmware upgrades; reader firmware for MIFARE MIFARE Classic is not compatible with HCE protocols
- Access – Diversity of protocols used can complicate use cases

Smart Card Alliance

Summary & Conclusions

Conclusions and Resources

- HCE is a promising development to increase NFC adoption as it opens up NFC capabilities to a wider range of applications
- With standards and specifications development, it is clear there is broad support for HCE from networks, to device platform providers to application owners
- Security concerns can be overcome with the right compensating controls and risk management
- Mobile & NFC Council will continue to monitor the developments and new uses cases with HCE and continue to provide educational resources on this topic.

Resources

- **“Host Card Emulation 101,”** Smart Card Alliance Mobile & NFC Council white paper
- Other mobile payments and NFC resources available at http://www.smartcardalliance.org/publications-payments-mobile-payments-nfc/

Webinar Project Contributors

- Maarten Bron, UL
- David deKozan, Cubic
- Peter Helderman, UL
- Philip Hoyer, HID
- Bob Dulude, HID
- Simon Laker, Consult Hyperion
- Shahriar Mamun, Kona I
- Sadiq Mohammed, MasterCard
- Akif Qazi, Discover
- Tony Sabetti, CPI Card Group
- Brian Stein, CH2M
- Sree Swaminathan, First Data
- Sanjay Varghese, Capgemini

Q&A

Smart Card Alliance

Randy Vanderhoof
rvanderhoof@smartcardalliance.org

Sadiq Mohammed
sadiq_mohammed@mastercard.com

Peter Helderman
peter.helderman@ul.com

Sree Swaminathan
sridher.swaminathan@firstdata.com

191 Clarksville Road
Princeton Junction, New Jersey 08550
WWW.SMARTCARDALLIANCE.ORG