NFC payments, state of the art, from an special security point of view

SIM Based?
Host Card Emulation?
…
Apple Pay?

Mario Maawad Marcos
mmaawad@lacaixa.es

2 basic models of NFC for banks(apart from Apple Pay)

SIM - *Card Emulation*

So far, It is the only certified technology

- ✓ *It needs a hardware "Secure Element". To be feasible in a banking environment the most convenient is the SIM based model, which uses the SIM of the Mobile Operator*
- ✓ *"la Caixa" has signed an agreement with the three major MNO in Spain: Telefonica Movistar, Vodafone i Orange*
- ✓ *It is currently available*

The MNO has an special role

HCE - *Host Card Emulation*

Visa and MasterCard have announced that they will allow a new technical way to deploy NFC payments, what we call HCE..

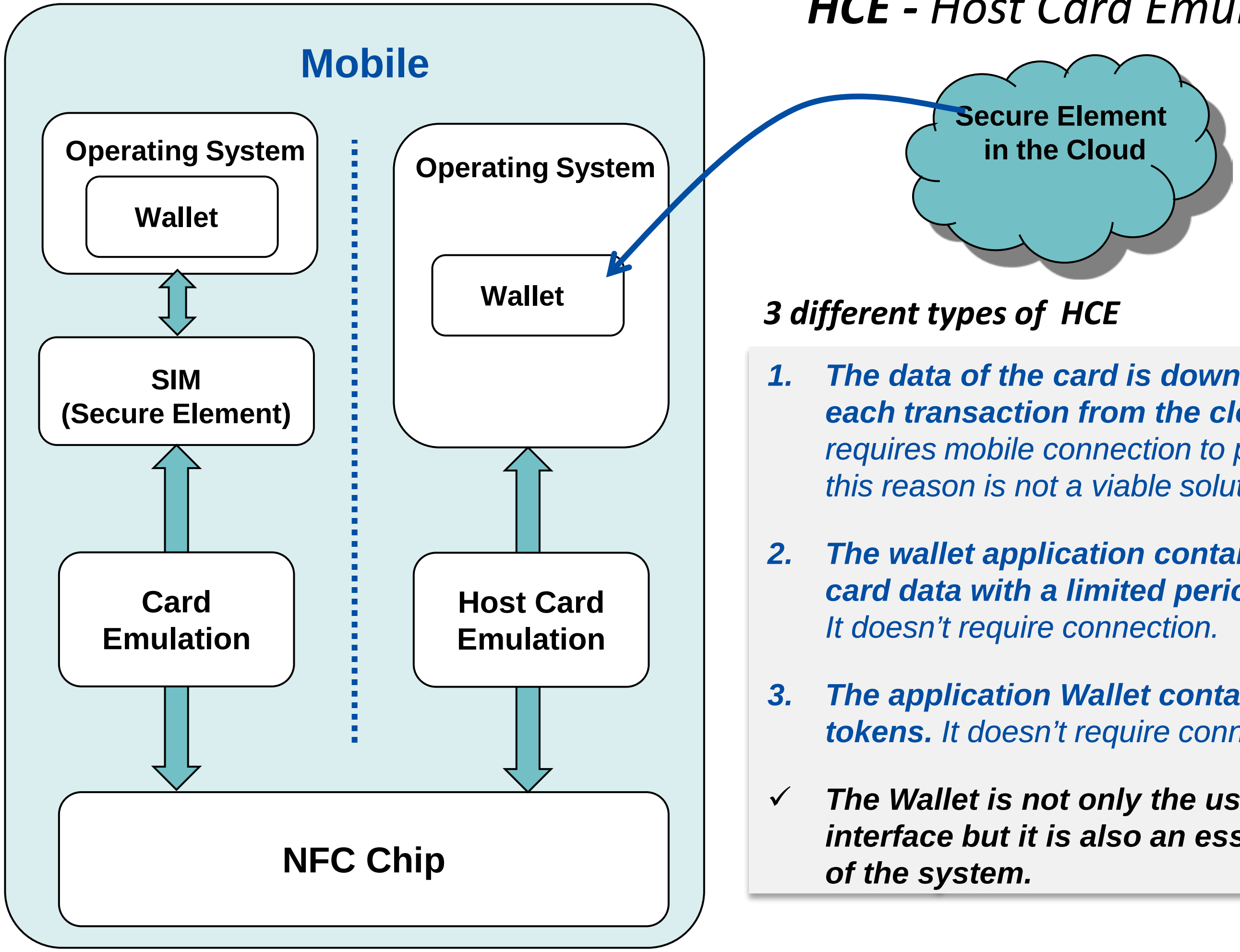
- ✓ *No need of "Secure Element"(Software based)*
- ✓ *It is independent from the Secure Element's owner simplifying the ecosystem*
- ✓ *Visa specifications have been published in April 2014. There is no certification process available. So far, only projects of less than 10.000 cards are allowed.*

MNO plays no role.

Description of the NFC models

SIM - Card Emulation

- ✓ The card data is downloaded over the air and stored in the "Secure Element" within the chipset of the SIM.
- ✓ Since the card data is in the secure element, the data stored is the full data of a phisical card.
- ✓ **The Wallet application is used only as an interface with the user, but it doesn't contain relevant data.**



HCE - Host Card Emulation

3 different types of HCE

1. **The data of the card is downloaded in each transaction from the cloud**. It requires mobile connection to pay, and for this reason is not a viable solution.
2. **The wallet application contains the card data with a limited period of time**. It doesn't require connection.
3. **The application Wallet contains tokens.** It doesn't require connection.

- ✓ **The Wallet is not only the user interface but it is also an essential part of the system.**

Ecosystem's impact

SIM - Card Emulation

It needs a new ecosystem due to the fact that includes a new hardware.

New actors:

- ✓ ***MNO:** SIM's owner*
- ✓ ***SP TSM Provider: Is the trusted third party who downloads the card over the air (OTA).***

HCE - Host Card Emulation

The ecosystem doesn't change. It need new infrastructure in the bank. There is no need for new actors.

- ✓ *Provider of the infrastructure needed in the cloud and in the downloaded application, for the authorization of the transactions and to provide additional security validations.*

Principal changes

- ✓ *With HCE there is no need to reach an agreement with the MNOs and there is no need to have a SP TSM*
- ✓ *HCE requires a "black box" in the banks infrastructure.*

SIM based complexity and advantatges

Agreement with the 3 major MNOs in Spain

movistar

vodafone

orange™

Over 80% of market share

Acceptance infrastructure ready

Over 350K POS terminals

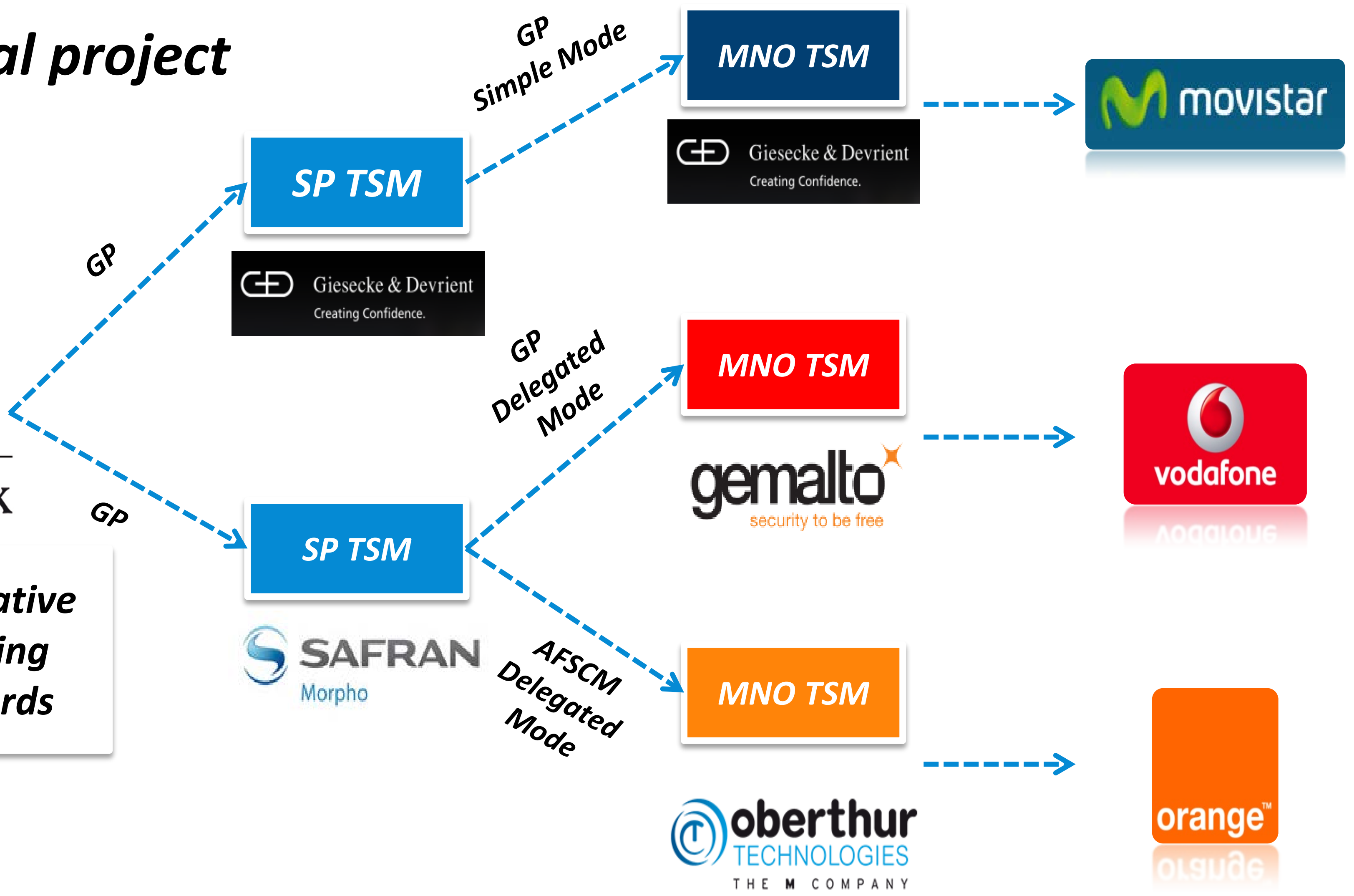
Over 1200 Contactless ATMs

Large portfolio of NFC handsets

- ***A number of different handsets - over 10 Android devices available for CaixaBank's project***
- ***Several versions of Android OS***

A global project

CaixaBank

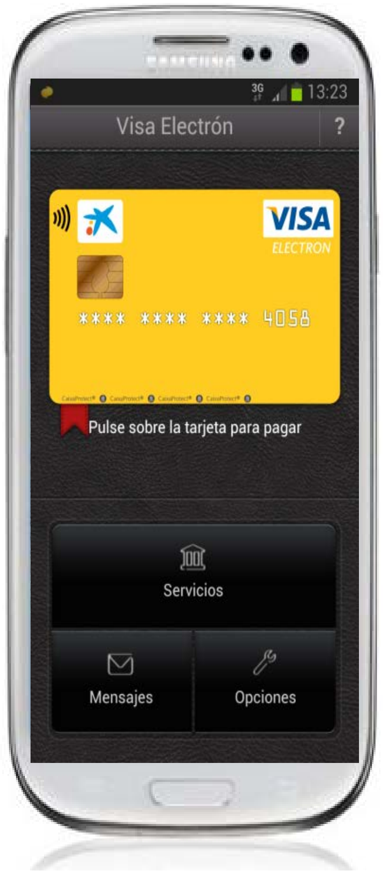


A new innovative way of issuing payment cards

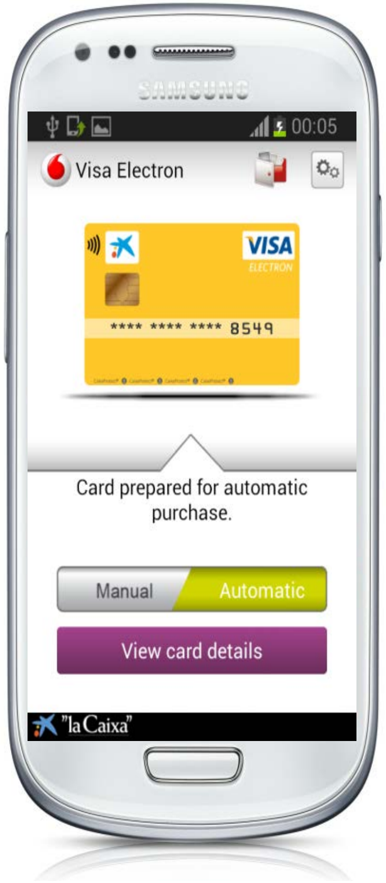
Your mobile is your Wallet
3 different wallet approaches

- ***Movistar: NFC Wallet***
  - ***Horizontal Integrated Wallet***
  - ***Moving to SP Wallet***
- ***Vodafone: Vodafone Wallet***
  - ***Horizontal umbrella with Vertical Apps***
  - ***Apps with Vodafone Look&Feel***
- ***Orange: Orange NFC + CaixaWallet NFC***
  - ***Horizontal umbrella with Vertical Wallets***
  - ***Vertical Wallet with SP Look&Feel***

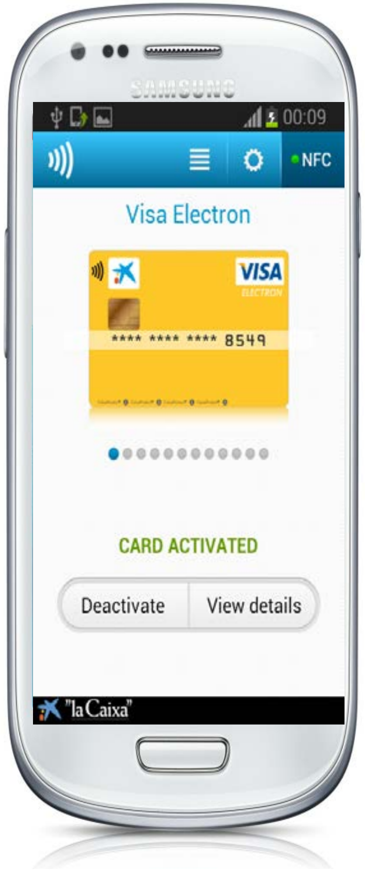
movistar


3G 13:23
Visa Electrón ?
VISA ELECTRON
**** **** **** 4058
Pulse sobre la tarjeta para pagar
Servicios
Mensajes
Opciones

vodafone


00:05
Visa Electron
VISA ELECTRON
**** **** **** 8549
Card prepared for automatic purchase.
Manual | Automatic
View card details
"laCaixa"

orange


00:09
NFC
Visa Electron
VISA ELECTRON
**** **** **** 8549
CARD ACTIVATED
Deactivate | View details
"laCaixa"

HCE requirements

Required Infrastructure

✓ ***Mobile NFC compliant**: It requires an NFC mobile which supports HCE and the adapted Operating Systems*

  ✓ *BlackBerry 10*

  ✓ *Android 4.4 (Kit Kat) – from November 2013*

Google's role

✓ *Android is the O.S most important, Google controles the access to the HCE solution.*

✓ *Google has introduced HCE without informing previously to any actor (MNOs, cards schemes, banks, etc…)*

✓ *The 4.4 version has introduced some changes which are impacting directly in the SIM solution too.*

✓ *Google can introduce other changes in the future which could modify the current behaviour. Google controls this solution.*

Introducció – Comparativa HCE versus SIM (CE)

	HCE	SIM	Comentaris
Provisioning	↑	↓	Since there are less actors the provisioning is technically simpler in the HCE solution. A key point is that there is no need to change the SIIM.
User experience	↓	↑	It depends on the security level wanted to be defined with HCE, the user experience could be affected. With the SIM is always Tap&Go.
Security	↓	↑	Since HCE is not using a hardware secure element where the card data are stored, the solution will be less secure. In the SIM model it is better to provide security to the wallet too.
Business model	←	→	The business model depends on the agreements. In the HCE case with less actors should be easier to define, but the final cost depends on the agreements.
Madurity	↓	↑	The SIM model is standardized. The HCE solution is newer and the certification process is not so defined.

Both solutions have their advantages and the correct solution depends on the situation of the entity and the market where is based.

HCE alternatives

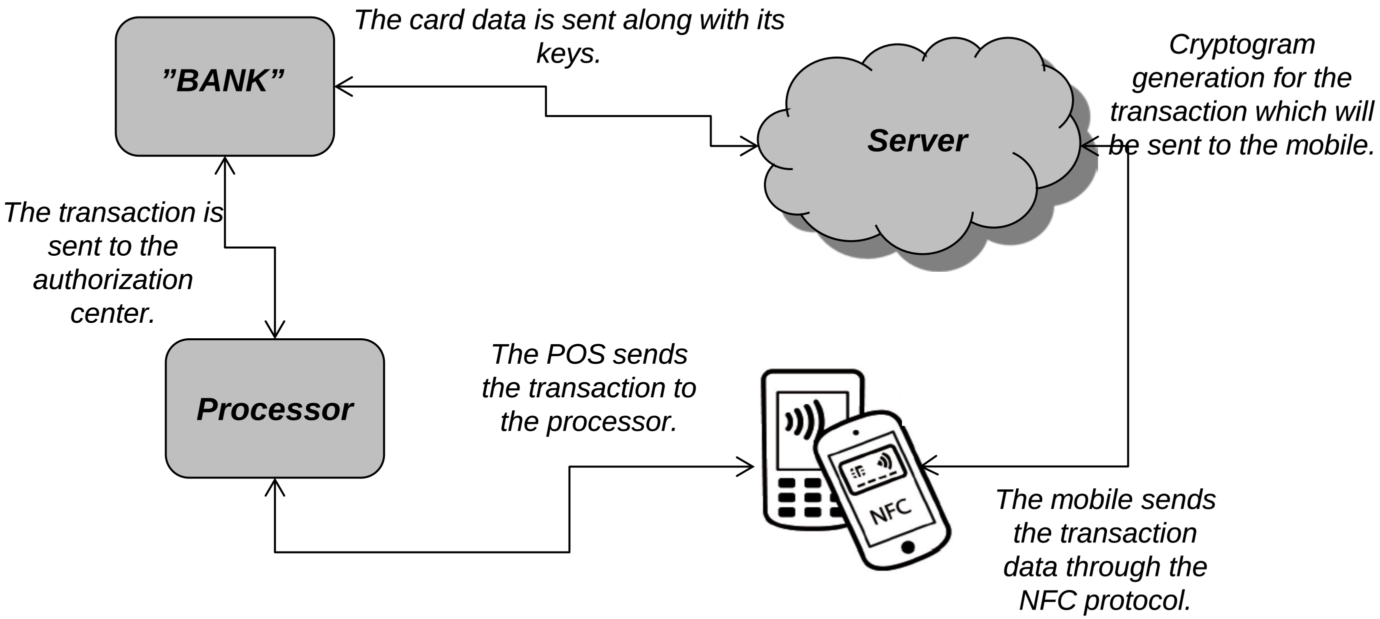
- HCE is in an initial state and the rules are not completely defined. The possibilities to implement it are still opened.
- The certification process defined by the card schemes are not completely closed yet.

3 basic alternatives

1. SE in the Cloud
2. Limited credentials
3. Tokens

1. SE in the Cloud

- On each transaction the client connects to a server to download the payment credentials.
- The payment is done in the same way as in the HW SE solution.


"BANK"
Server
Processor
NFC
The card data is sent along with its keys.
Cryptogram generation for the transaction which will be sent to the mobile.
The transaction is sent to the authorization center.
The POS sends the transaction to the processor.
The mobile sends the transaction data through the NFC protocol.

PROs

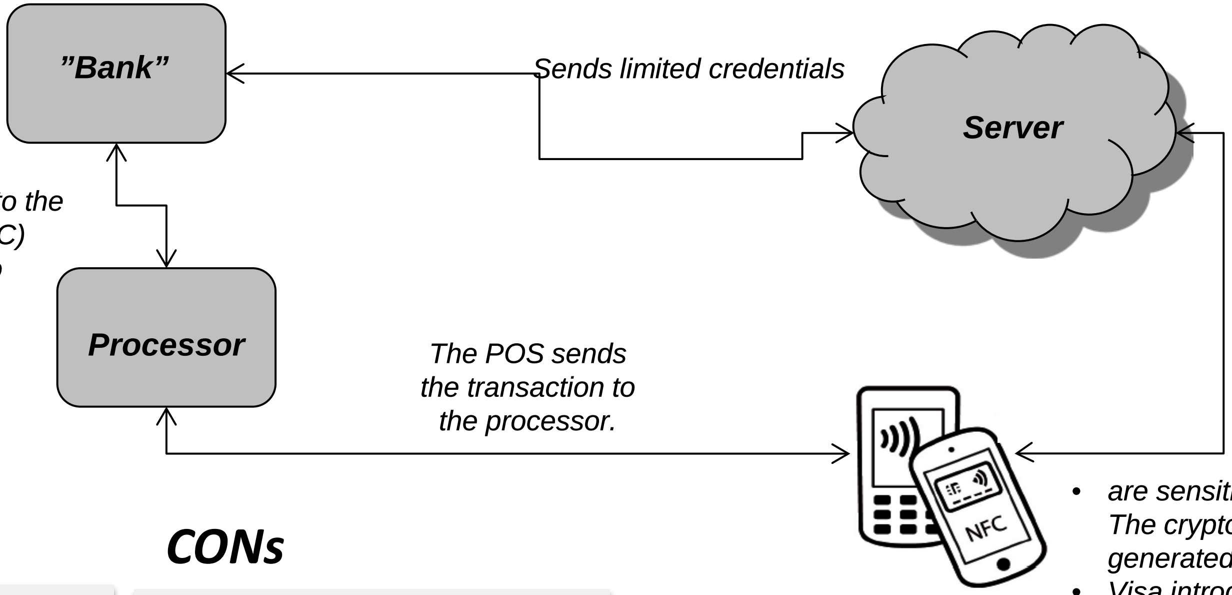
1. There is no need to modify anything in the acceptance infrastructure.
2. Can process offline payments.

CONs

1. It requires connection to the Cloud server during the payment and the time to do it could be slow, moreover it requires WIFI or 3G connection of the mobile.

2. Limited credentials

- *Doesn't require client online connection, since the cryptogram is generated on the mobile for each payment.*
- *There is impact in the authorization center since has to support CVN for a "limited Use Key".*



- *The transaction is sent to the Authorization Center (AC)*
- *Impact in the AC: has to support CVN*

The Authentication Server sends the limited credentials with a session key to be stored on the mobile and be used in the future.

The POS sends the transaction to the processor.

- *are sensitive data stored on the mobile. The cryptogram for the transaction is generated on the mobile app.*
- *Visa introduces the use of a new key: new CVN for a Limited Use Key. A LUK (Limited User Key) is generated from the UDK together with other data (time, random counter, etc…)*

PROs

1. *No need to modify the issuer profile*
2. *No needs connection.*

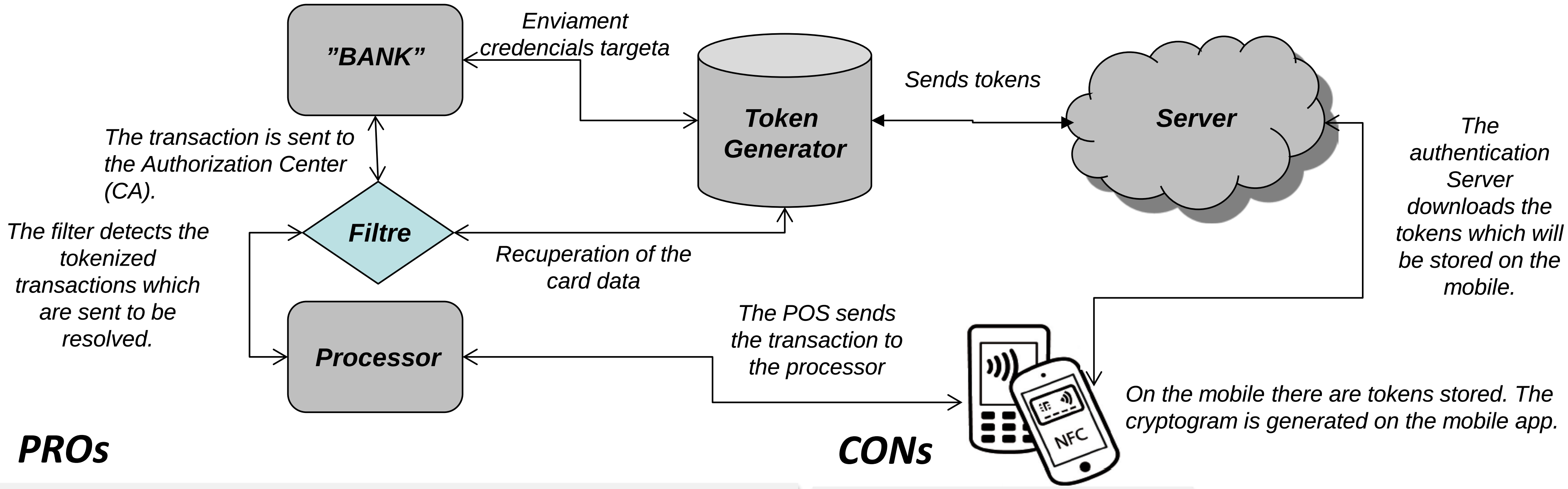
CONs

1. *Only online transactions*
2. *Stores sensitive data on the mobile.*

→ ***The Wallet applies measures to limit the risk***

3. Tokens

- *No needs client connection due to the fact that the cryptogram is generated on the mobile for each payment.*
- *There is impact in the issuer and in the acceptance.*



"BANK"

Enviament credencials targeta

Token Generator

Sends tokens

Server

The transaction is sent to the Authorization Center (CA).

The authentication Server downloads the tokens which will be stored on the mobile.

The filter detects the tokenized transactions which are sent to be resolved.

Filtre

Recuperation of the card data

Processor

The POS sends the transaction to the processor

On the mobile there are tokens stored. The cryptogram is generated on the mobile app.

PROs

1. *Recommended by EMVCo*
2. *No need connection to pay.*
3. *Possibility to define a risk policy at a token level (ex: Token is valid for transactions of less tha X Euros)*

CONs

1. *Only online transactions*
2. *Mobile stores sensitive data.*

→ ***The measures to limit the risk have to be applied in the app (Wallet)***

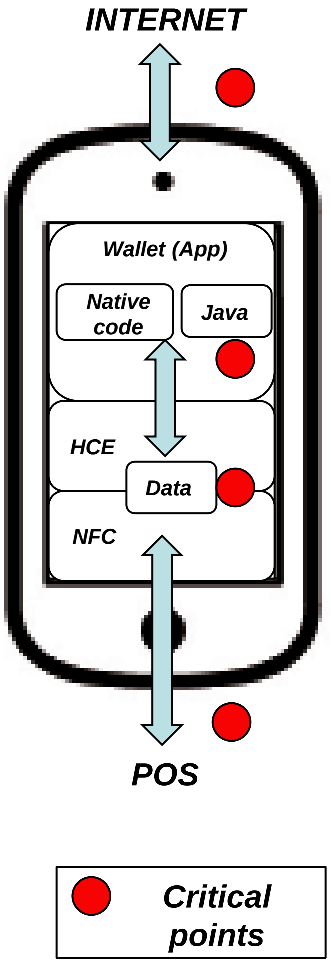
Comparison

	1. SE in the Cloud	2. Limited credentials	3. Tokens
Security	⬆⬆	➡	⬆
Connection	⬇⬇	⬆	⬆
Certification	⬆	➡	⬈
Existing infrastructure	⬆	⬇	⬇⬇
Performance	⬇⬇	⬆	⬆

The1 solution needs connection, so is discarded. Between the 2 and 3 for security reasons the 3 should be chosen although it introduces more complexity.

Security analysis

- ***The preferred solution is the token based.***
- ***You should authenticate the mobile which is connecting.***
  - *To be sure that the mobile owner is the owner of the credit card.*
  - *The communications with the server have to be secure (SSL, TLS, https)*
- ***The App (Wallet) where the sensitive data is stored is the critical point of the solution:***
  - ***The mobile is vulnerable:** The software could be modified, the communications could be eavesdropped and the encrypted data could be read.*
  - ***Mobiles and applications** used for payments are not uniques and hackers could clone them, the client will not be able to know it.*



Measures to be adopted on the App (Wallet)

- ***Identity based on entropy***
- *Creation of a "**Software Secure Element"***
  - ***Cryptography "White Box"***
  - *"**Tamper proofing**" (It requires codification in native code, no java)*
  - ***Obfuscation***

Conclusions SIM Vs HCE

HCE Security

- ✓ In terms of security, the best one is the token based.
- ✓ The security of the App (Wallet) is a must

SIM Security

- ✓ Security based in Hardware (Secure Element).
- ✓ The security of the App is not so important

And now..

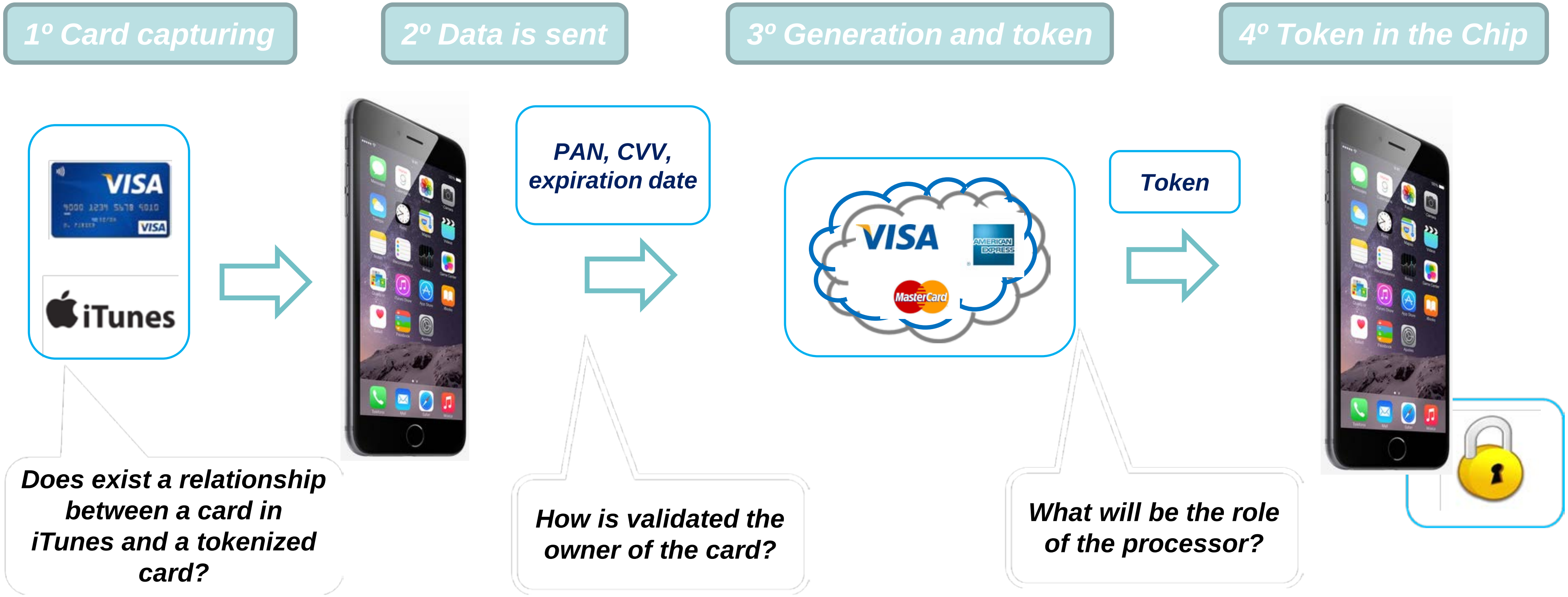
Apart from SIM based, HCE..

A newcomer ..

Apple Pay...

	SIM CARD EMULATION	HCE (HOST CARD EMULATION)	APPLEPAY (In analisys)
What is stored?	Card Data (the same as in the physical card)	Temporary token for card.	Temporary token for card.
Where is stored?	Secure Element(SIM)	In the Wallet software security	Secure Element (Dedicated chipset)
Enrollment	Request at Homebanking and downloading on the SIM	Request at HomeBanking and downloads the Tokens in the wallet	• Links the card with an Apple account or snapshot •Downloads the tokens in the chipset.
The payment?	PIN in the wallet and the card is sent to the POS.	PIN in the wallet and the token is sent to the POS.	PIN or TouchId in the wallet and the token is sent to the POS.
Mobile requirements	NFC mobile and SIM NFC compliant	NFC mobile, Android > Kit Kat (4.4)	Iphone 6
Impact	• One Wallet for MNO. • Contract the service.	• Only one Wallet • Contract the service • Tokens and authorization management	No impact to banks: VISA, AMEX MCARD provide tokens.
Highlights	✓SECURITY ✓No impact in the authorization ✗ MNO dependency. ✗ Enrollment complexity(change the SIM)	✓Activation & Enrollment easy ✗ Wallet security. ✗ Impact in authorization and tokens	✓Activation & Enrollment easy ✓SECURITY. ✓No impact: authorization or banks ✗ Apple proprietary

Enrolment ApplePay



1º Card capturing

2º Data is sent

3º Generation and token

4º Token in the Chip

PAN, CVV, expiration date

Token

Does exist a relationship between a card in iTunes and a tokenized card?

How is validated the owner of the card?

What will be the role of the processor?

ApplePay payment

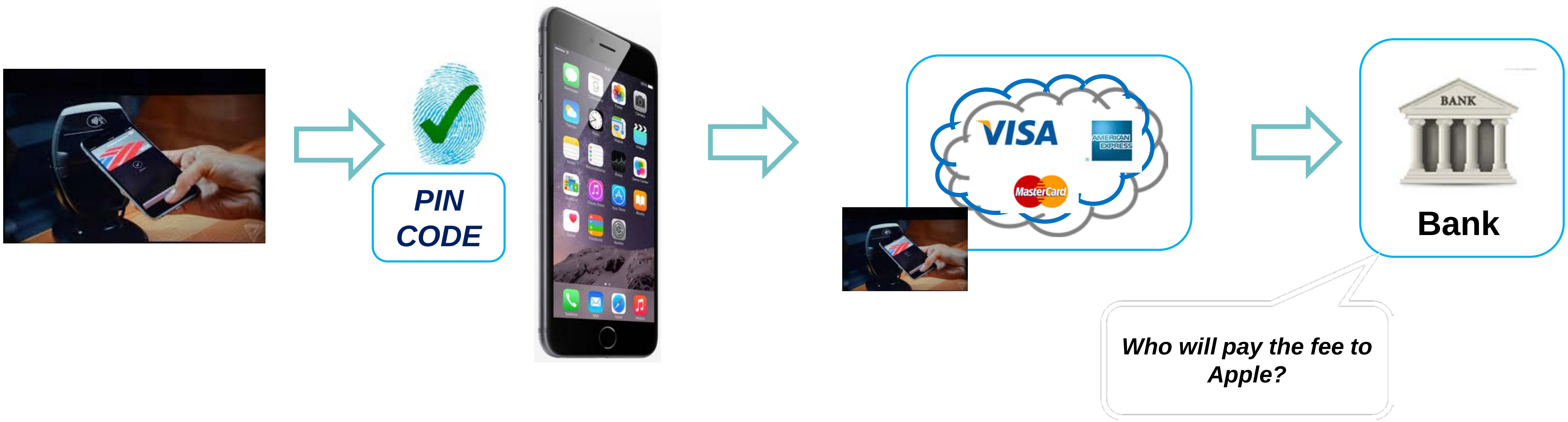
1º TAP TPV

2º Authorization

3º Token

4º Token to EMV

5º Authorization



PIN CODE

Bank

Who will pay the fee to Apple?

"la Caixa"

THANK YOU!