# Tokenization:
## *What, Why and How*

## ICMC 2015
**11/5/2015**

**Peter Helderman**
**UL Transaction Security**

TRANSACTION SECURITY

300 EXPERTS

LOCAL EMPLOYEES IN 34 COUNTRIES

- ✓ MOBILE
- ✓ PAYMENTS
- ✓ TRANSIT
- ✓ DATA SECURITY

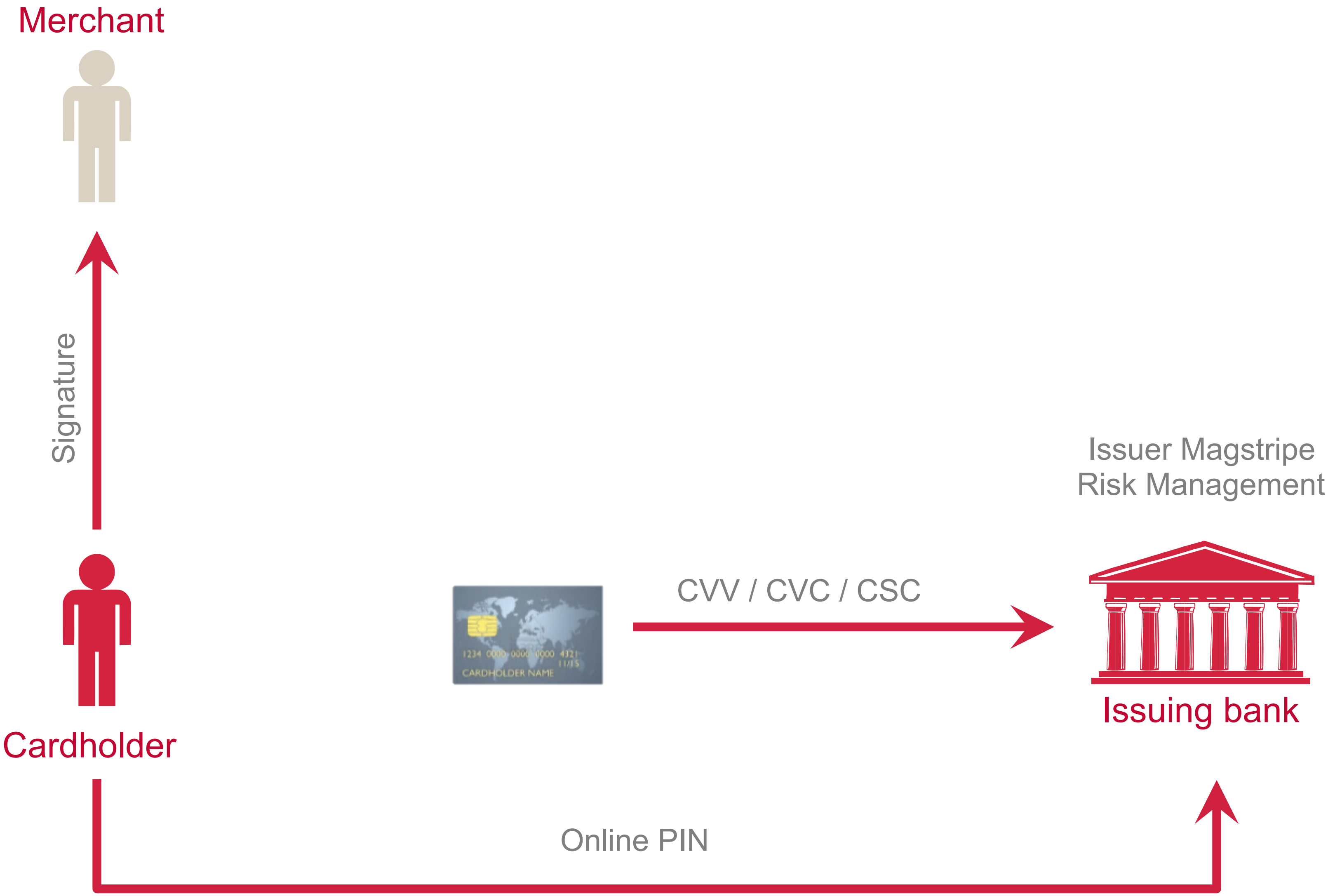
- ✓ INDEPENDENT
- ✓ MARKET LEADER
- ✓ GLOBAL REACH

PARTICIPATING IN >30 INDUSTRY ORGANIZATIONS

*“We have EMV…*

*… why do we need tokenization ?”*

# From Magstripe…



Merchant

Signature

Cardholder

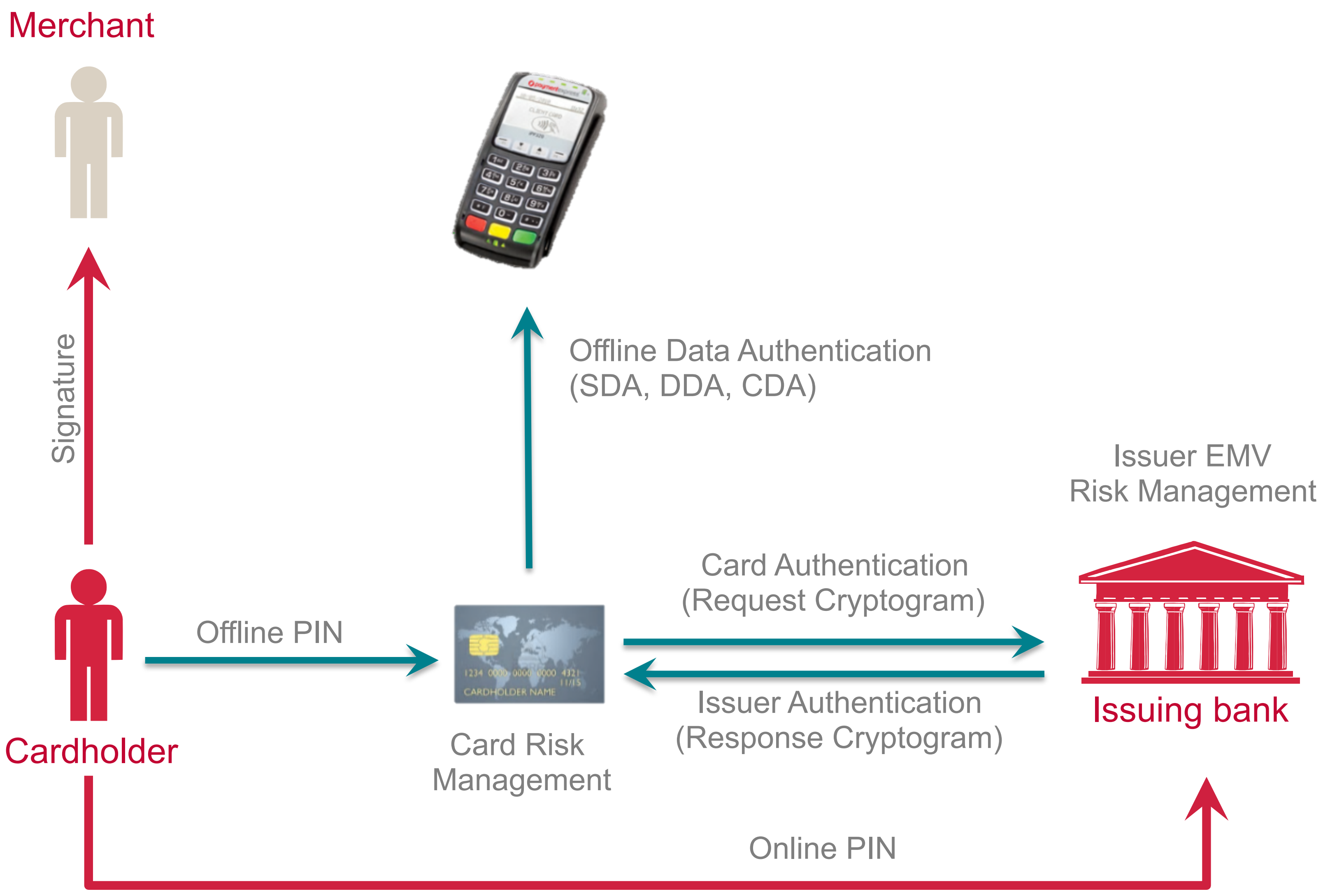
CVV / CVC / CSC

Issuer Magstripe
Risk Management

Issuing bank

Online PIN

# … to EMV



Merchant

Signature

Offline Data Authentication (SDA, DDA, CDA)

Issuer EMV Risk Management

Card Authentication (Request Cryptogram)

Offline PIN

Issuer Authentication (Response Cryptogram)

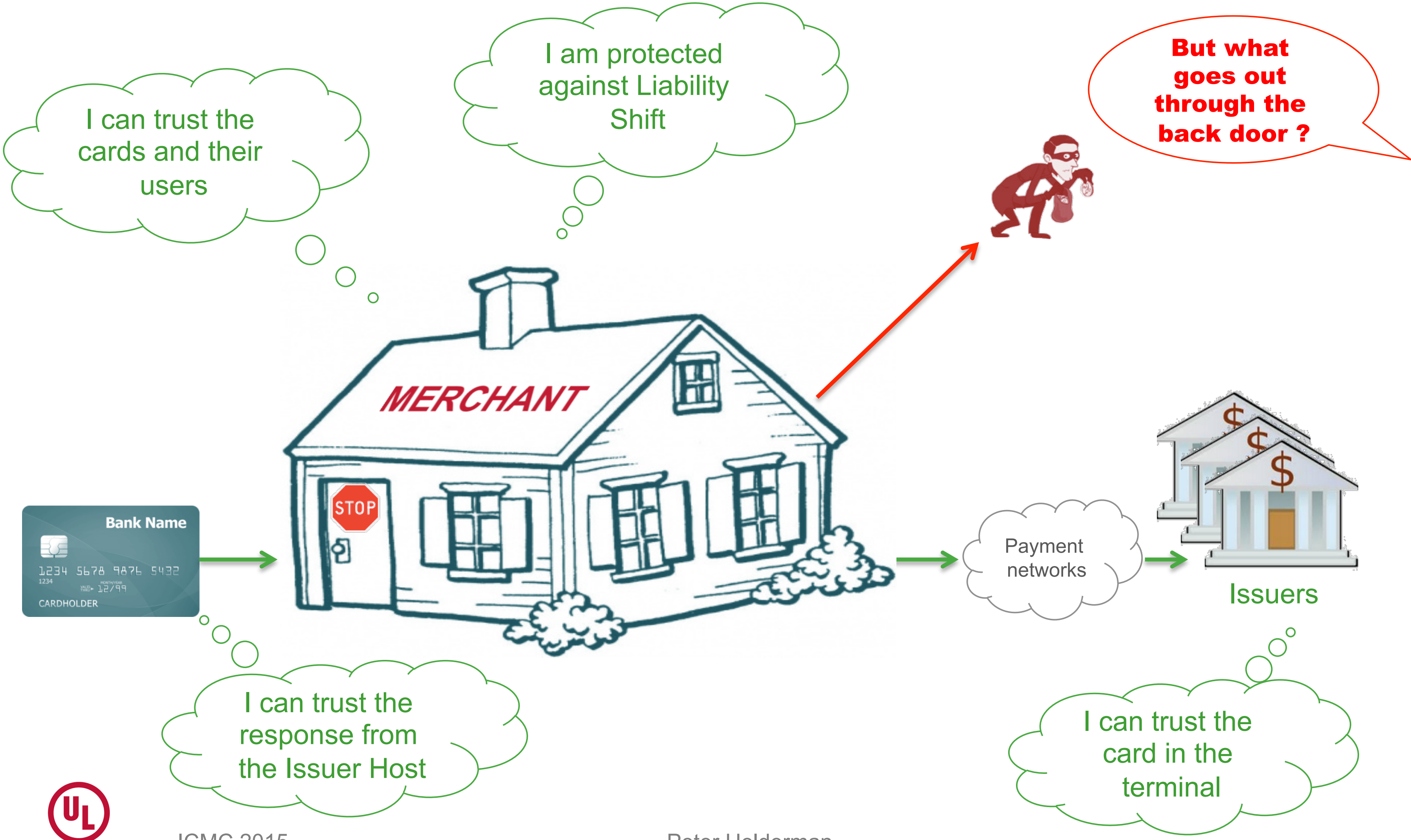
Issuing bank

Cardholder

Card Risk Management

Online PIN

# But EMV solves only part of the problem !



I can trust the cards and their users

I am protected against Liability Shift

But what goes out through the back door ?

I can trust the response from the Issuer Host

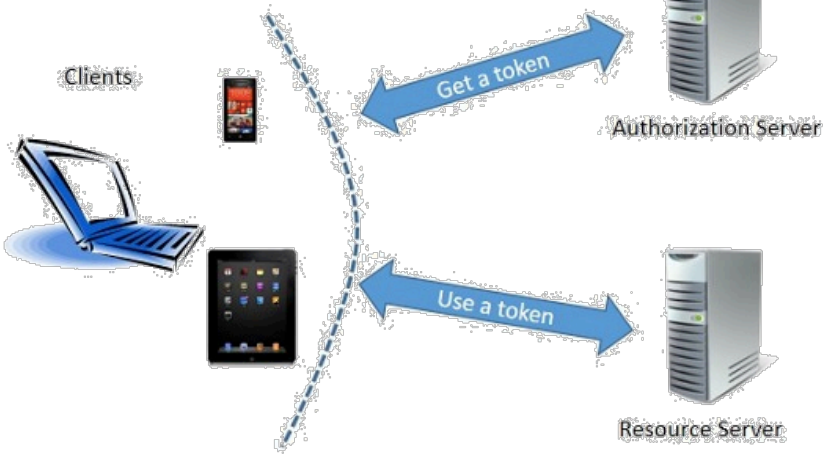
I can trust the card in the terminal

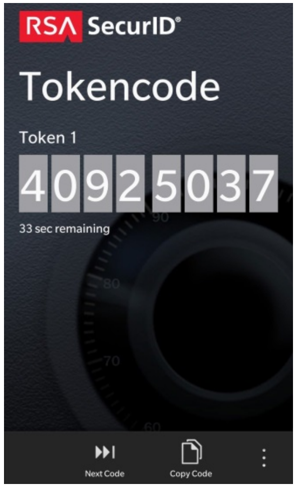
# *Tokenization explained*

# Beware the terminology!

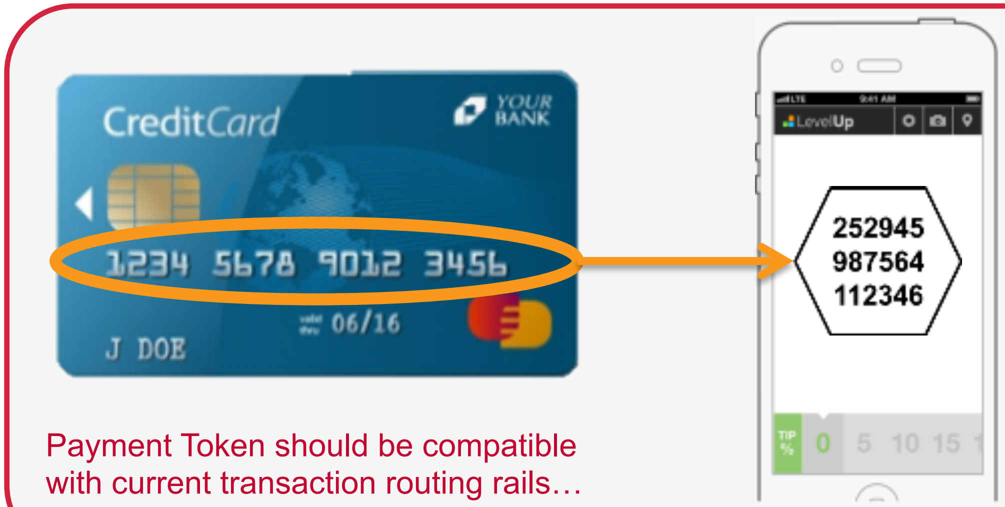
"Tokenization" and "Tokens" have many different **meanings** in this industry!
We will use the **EMVCo** terminology.

In-Page Tokenization
"SEAMLESS INTEGRATION"
AJAX DRIVEN FOR A TRANSPARENT EXPERIENCE
MERCHANT WEBSITE
PAYMENT INFORMATION
TokenEx
MERCHANT PROCESSOR
PROCESSOR INDEPENDENT





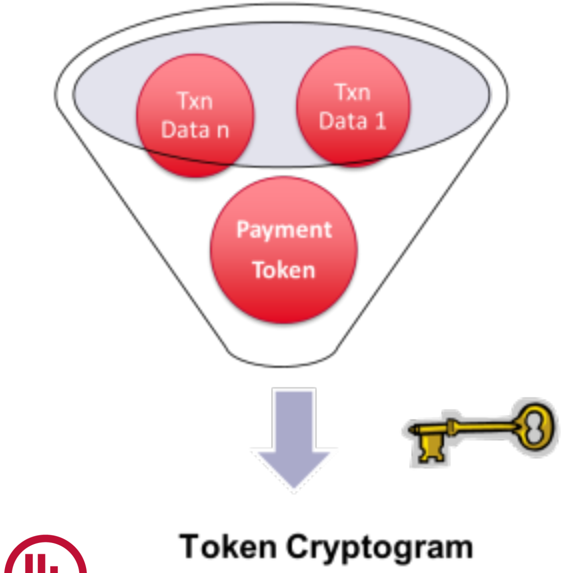
# What is a Token?



Payment Token should be compatible with current transaction routing rails…

**Payment Token:**
A surrogate value for a PAN that is that must pass basic validation rules of an account number.

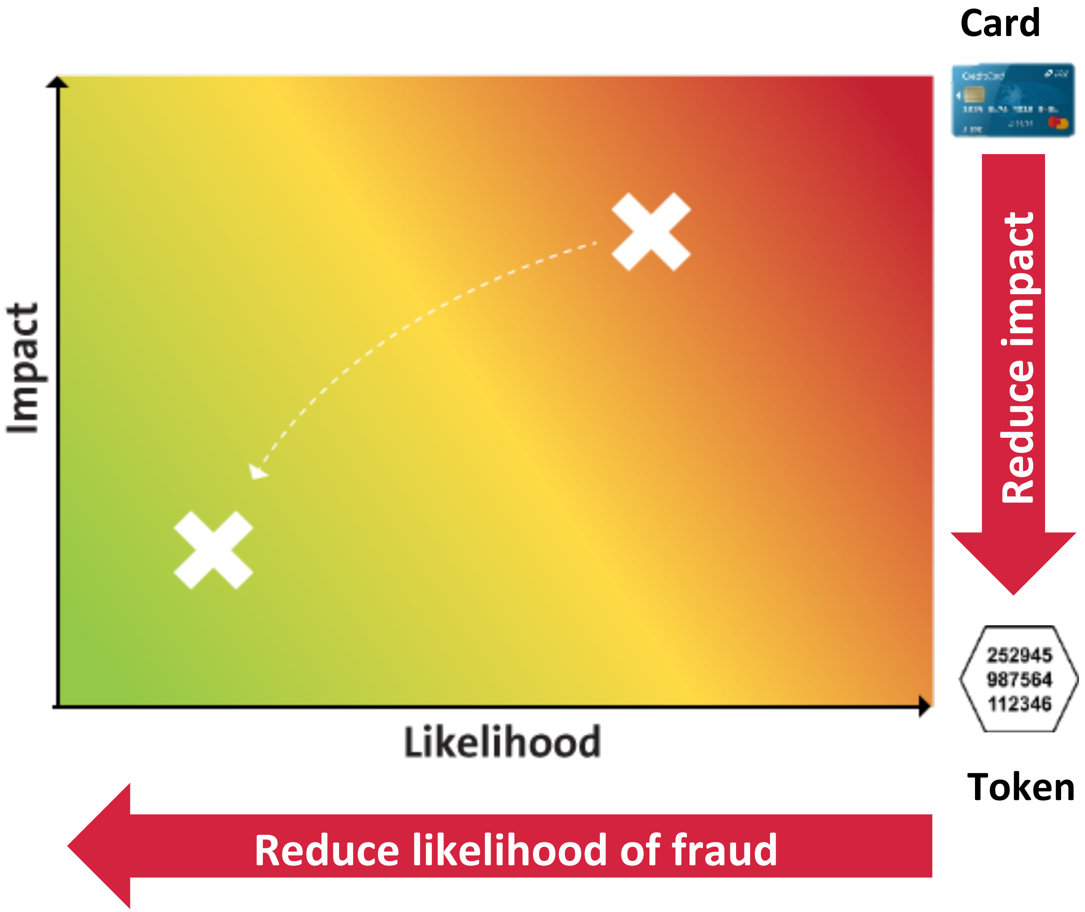
**Tokenization is the process of replacing the PAN by a payment token.**



**Token Cryptogram:**

- A cryptogram generated using the Payment Token and additional transaction data to create a transaction-unique value.
- Similar to the Application Cryptogram in EMV
- Can be a dynamic CVC value

# Tokenization reduces impact of fraud



## Tokenization

Improves security by removing payment credentials from transaction…

… with minimum changes to the processing infrastructure…

… in a technology neutral way.

# Token domain

In order to prevent cross-channel and cross-merchant fraud, it is possible to restrict the usage of tokens only to specific domains.

Domains can be:

- Channel specific
- Merchant specific
- Digital wallet specific

NFC payment

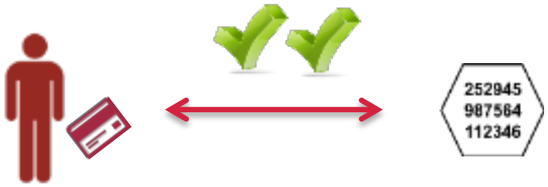
At Starbucks

Token domain restriction controls are performed during transaction processing.

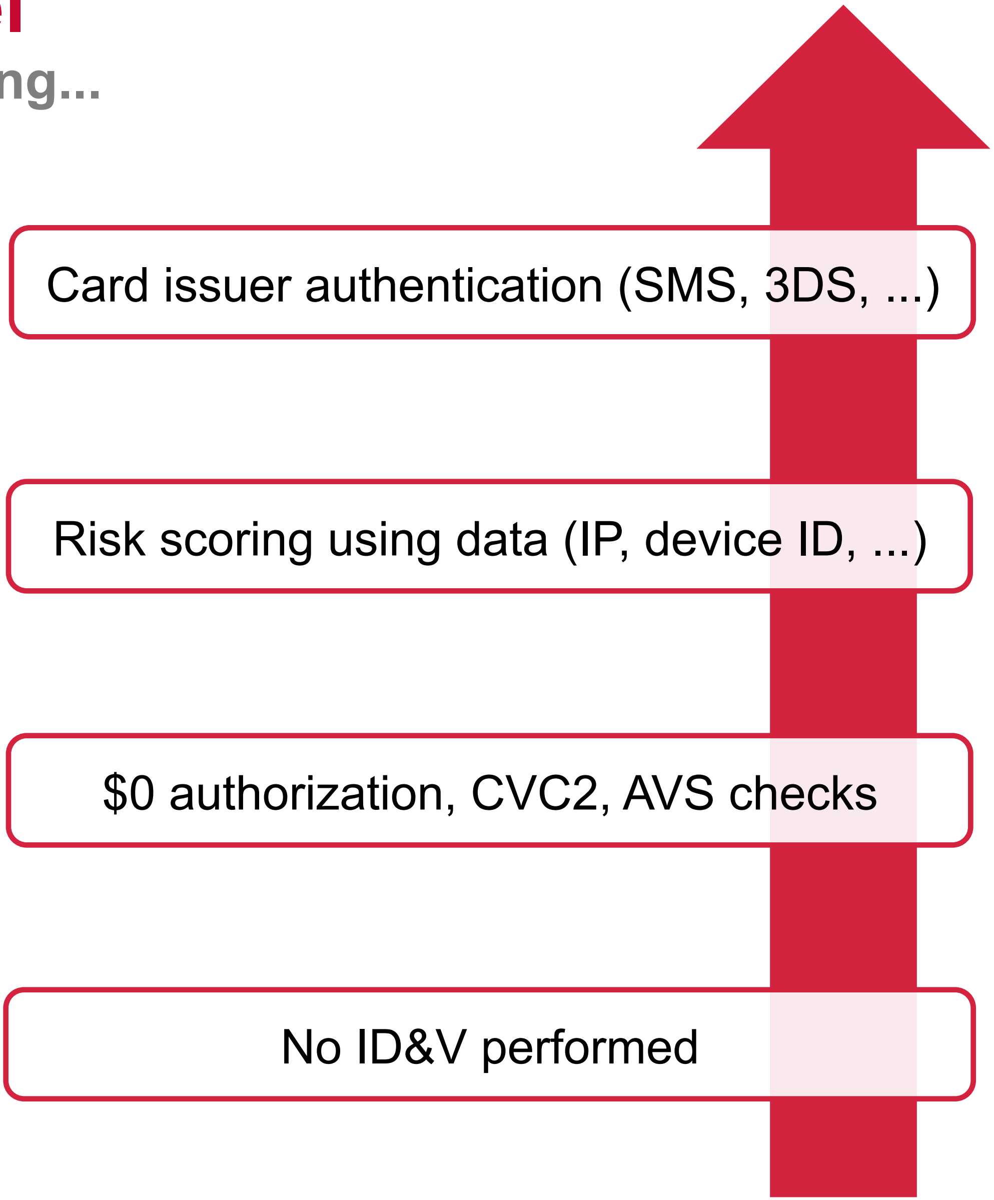
# Token assurance level

## Not all tokens are equally strong...

- Before token issuance, **identification and validation (ID &V)** methods can be used.
- Depending on the level of authentication, the token may have a higher **assurance**.



How strong is the binding between cardholder and token?



Card issuer authentication (SMS, 3DS, ...)

Risk scoring using data (IP, device ID, ...)

$0 authorization, CVC2, AVS checks

No ID&V performed

# Tokenization roles

### Cardholder

Do not (always) need to know that token replaces account

### Acquirer

Process transactions. New fields to support tokenization.

### Issuer

Maintain current role. Authenticate cardholder.

### Token Requestor

Entity requesting the PAN to be replaced by a Token. Can be:

- Issuers
- Merchants
- Wallet providers

### Token Service Provider

Provide Tokens to registered Token Requestors.

- Token provisioning
- Maintain Token vault
- Provide APIs
- Risk management

### Payment Network

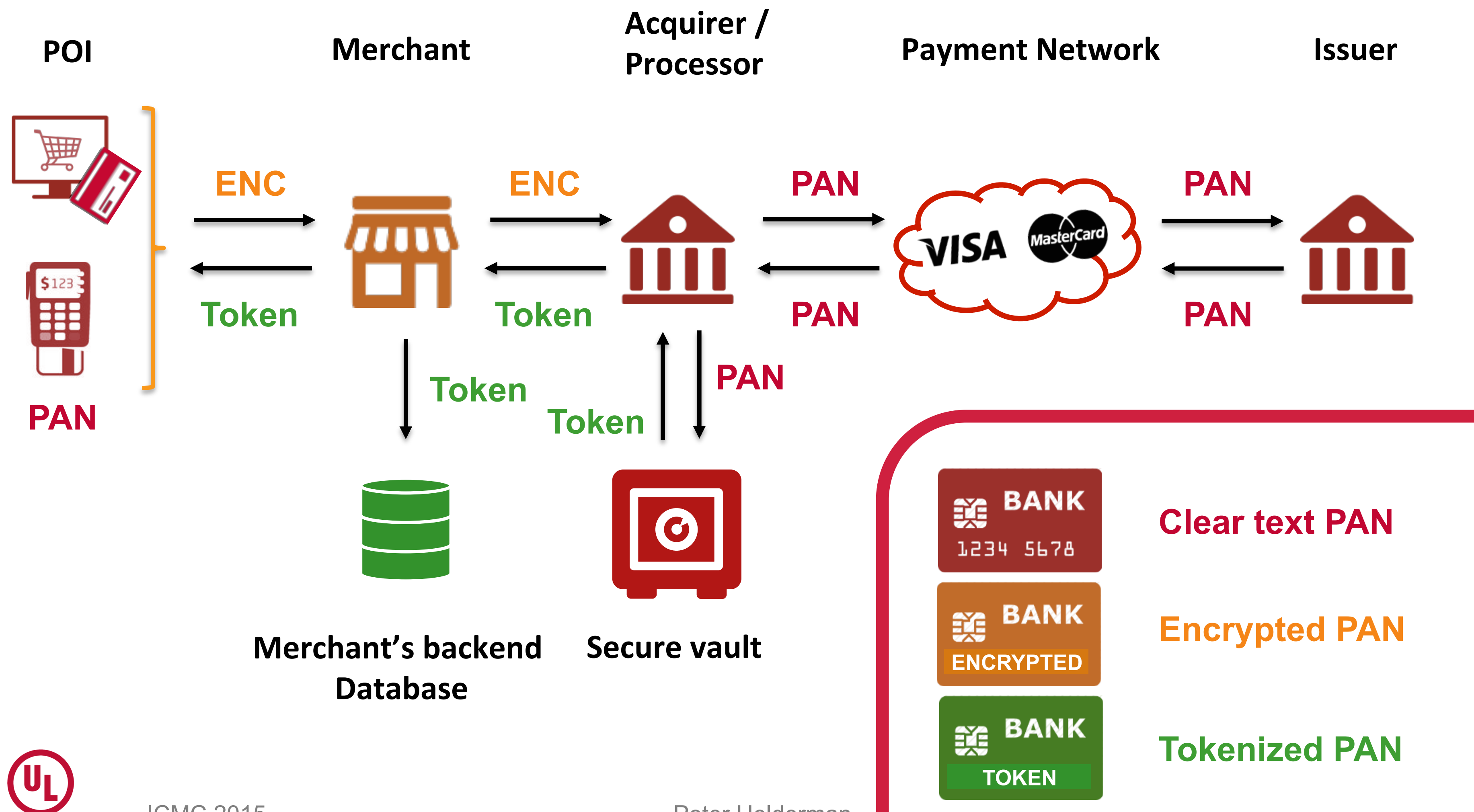
Should provide messaging support to process tokens. EMVCo suggests that the Payment Network is the natural player to be the Token Service Provider.

# *Tokenization examples*

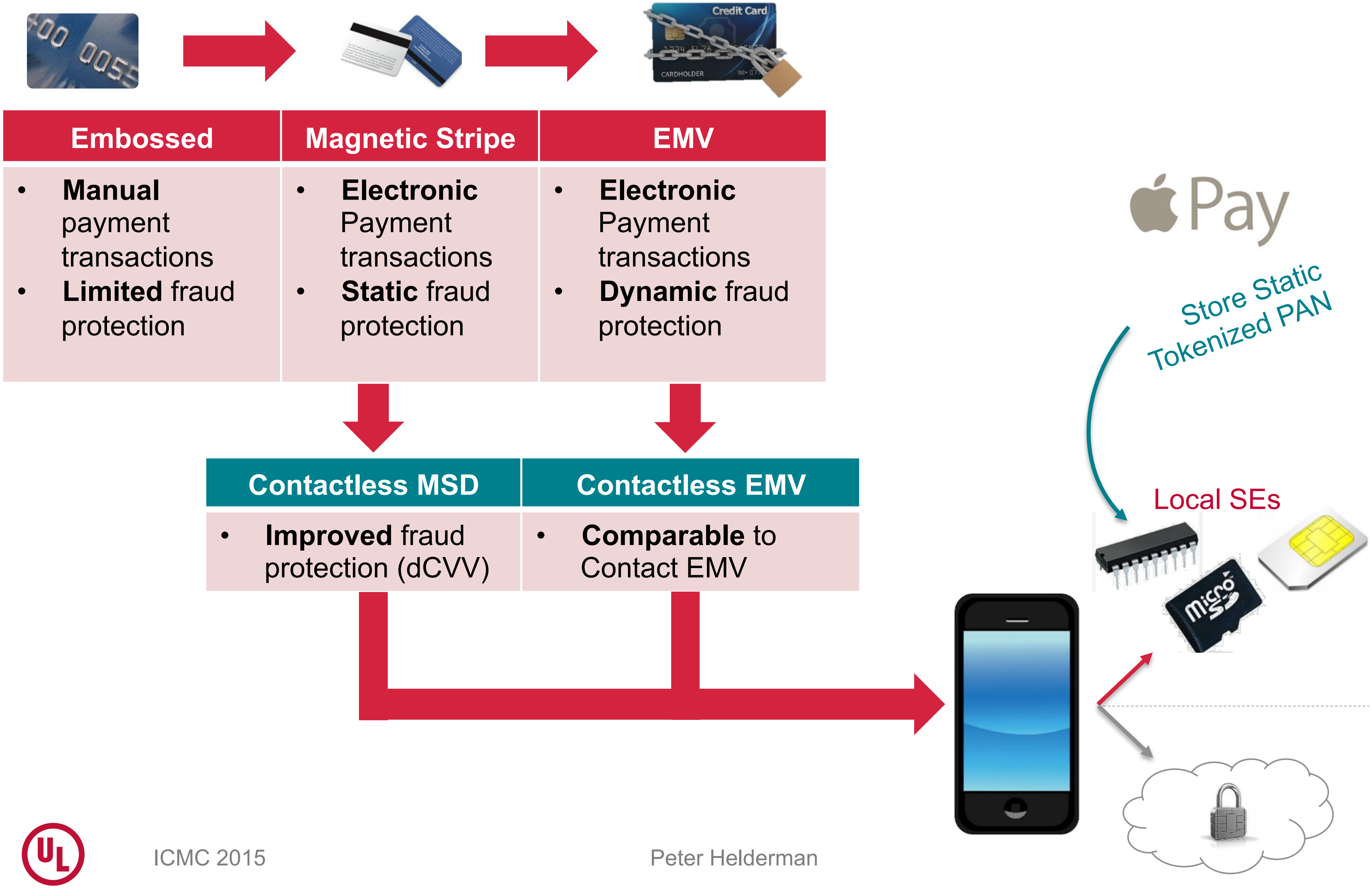
- *Acquirer Level*
- *Payment Network Level*
- *Cloud Based Mobile Payments*

# Acquirer Level Tokenization

## Encryption and Tokenization combined



# *Side Step: Payment Card Evolution*



**Embossed**

- **Manual** payment transactions
- **Limited** fraud protection

**Magnetic Stripe**

- **Electronic** Payment transactions
- **Static** fraud protection

**EMV**

- **Electronic** Payment transactions
- **Dynamic** fraud protection

**Contactless MSD**

- **Improved** fraud protection (dCVV)

**Contactless EMV**

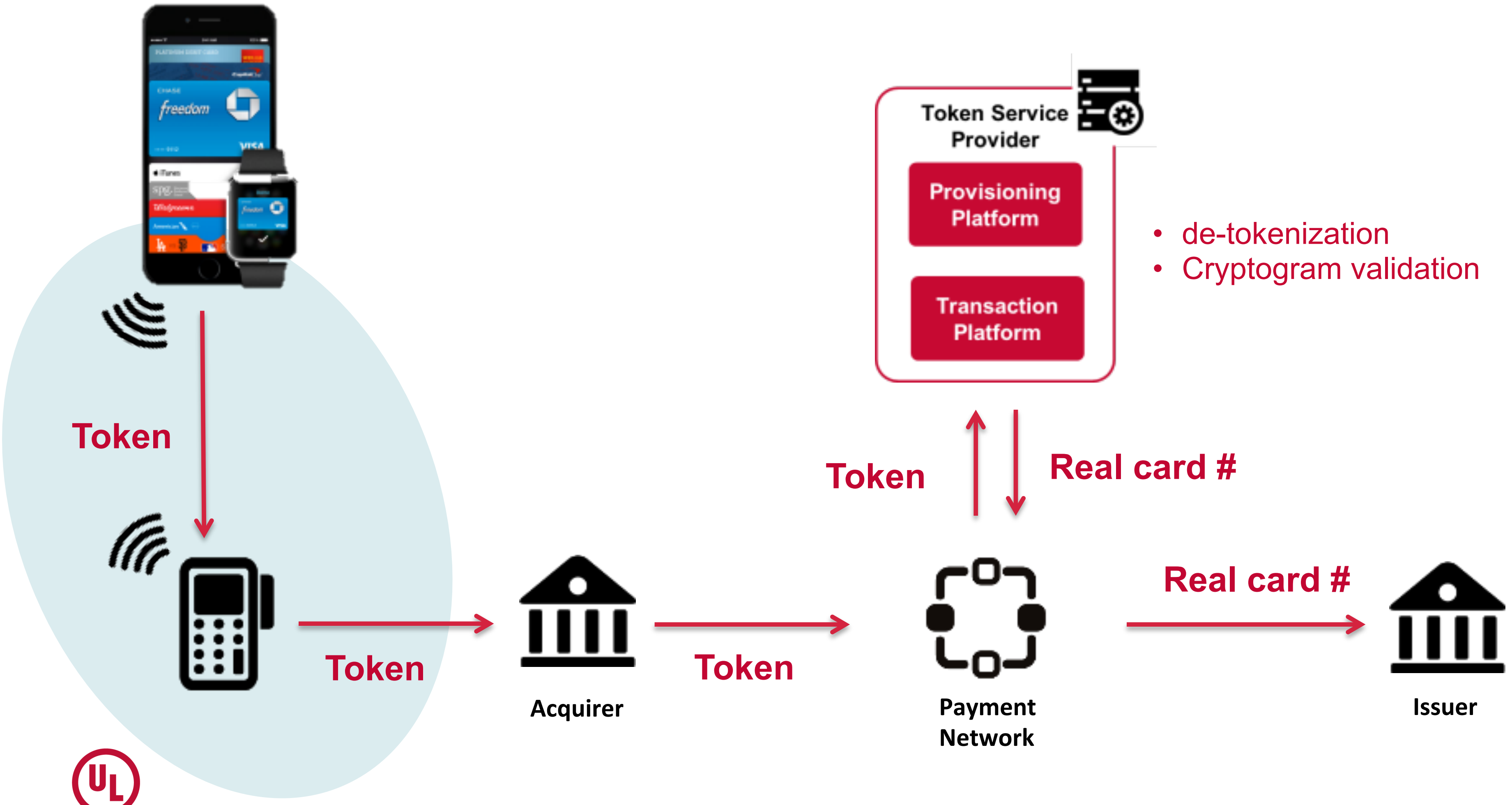
- **Comparable** to Contact EMV

# Network Level Tokenization

Pay

The terminology

| | |
|---|---|
| Device Account Number ⟷ | Payment Token |
| Dynamic security code ⟷ | Token Cryptogram |



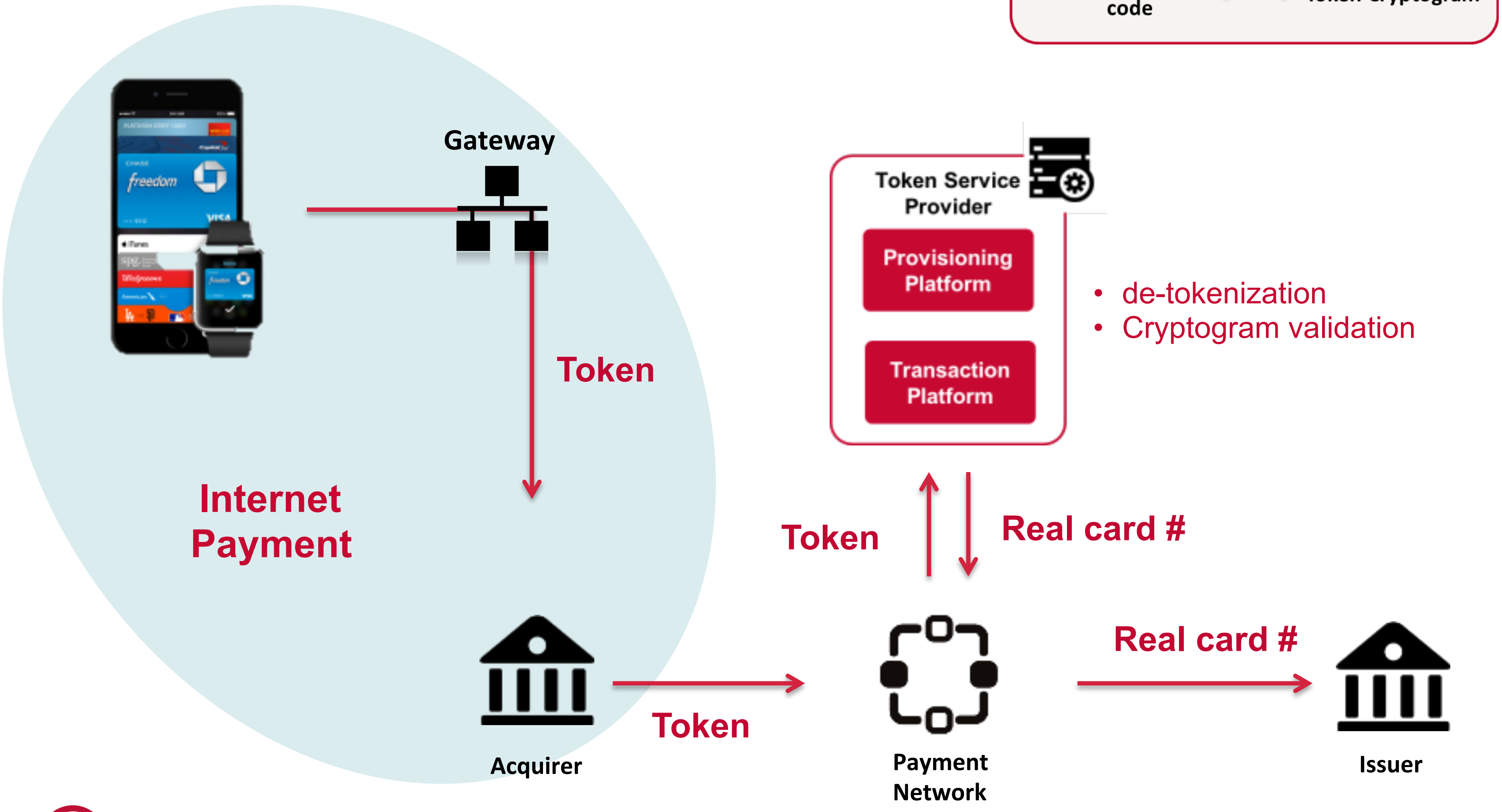
- de-tokenization
- Cryptogram validation

# Network Level Tokenization

Pay

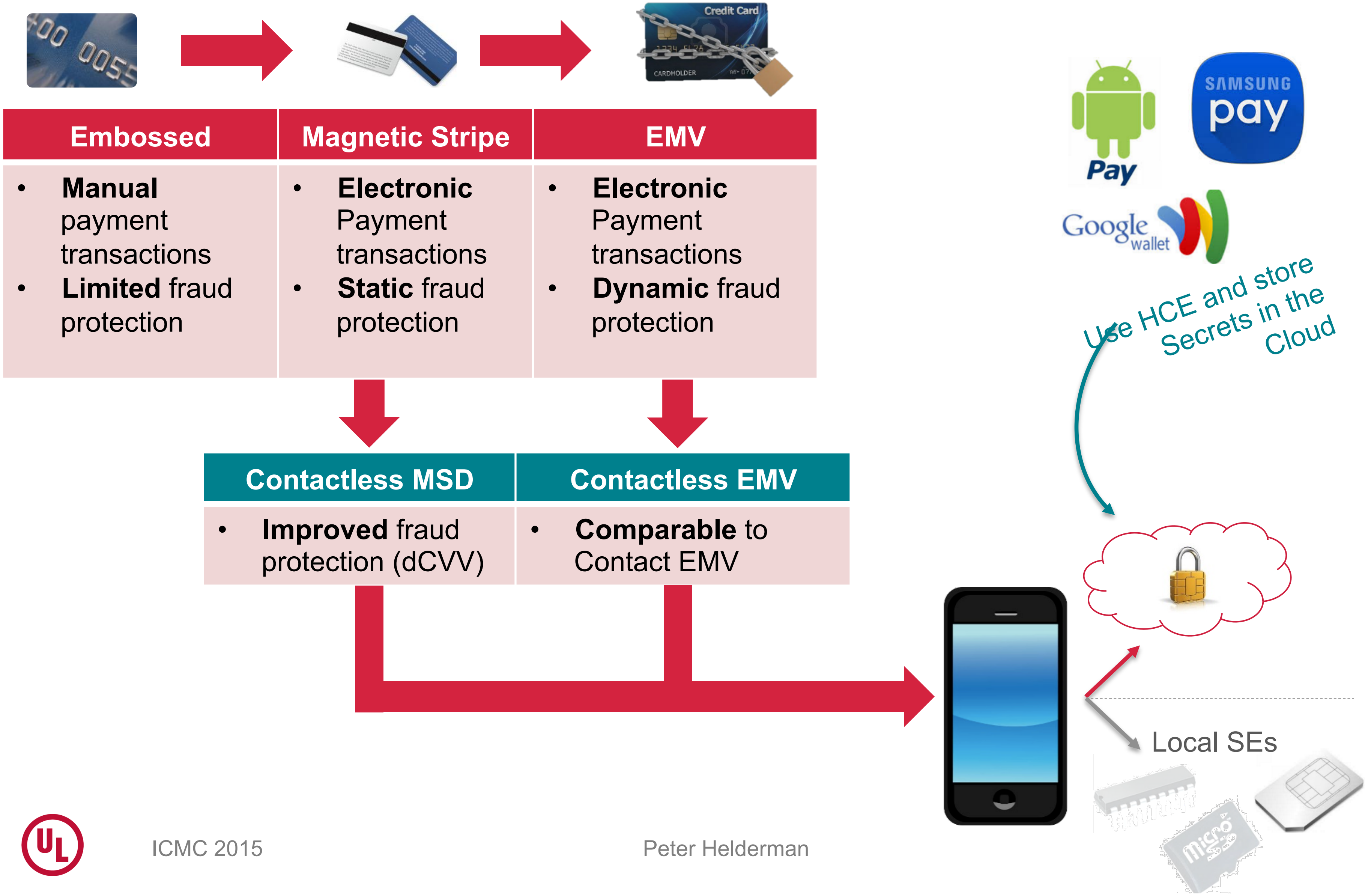
**The terminology**

| Apple | EMVCo |
|---|---|
| Device Account Number ↔ | Payment Token |
| Dynamic security code ↔ | Token Cryptogram |



- de-tokenization
- Cryptogram validation

# Side Step: Payment Card Evolution



| Embossed | Magnetic Stripe | EMV |
|---|---|---|
| - **Manual** payment transactions<br>- **Limited** fraud protection | - **Electronic** Payment transactions<br>- **Static** fraud protection | - **Electronic** Payment transactions<br>- **Dynamic** fraud protection |

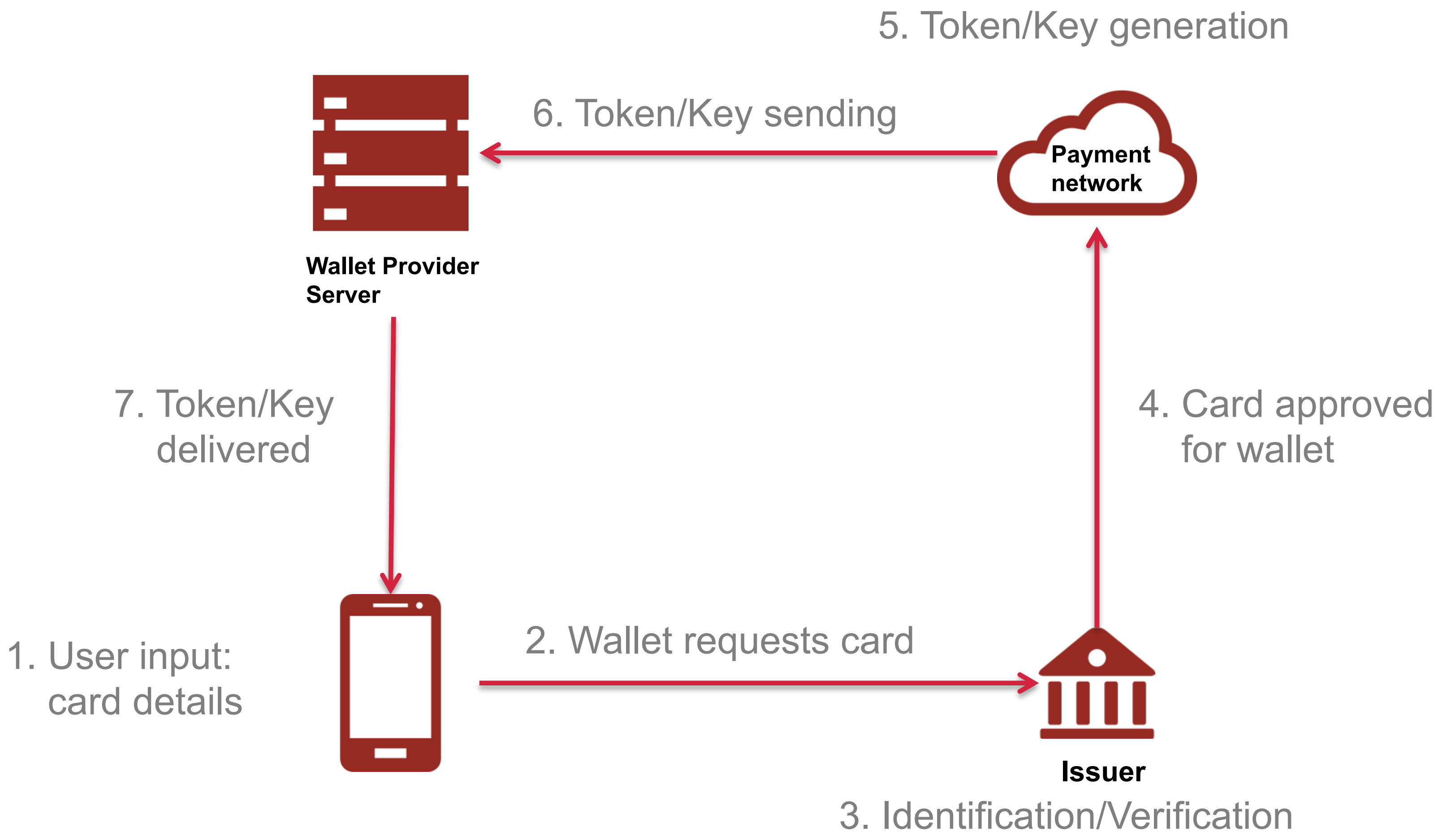
| Contactless MSD | Contactless EMV |
|---|---|
| - **Improved** fraud protection (dCVV) | - **Comparable** to Contact EMV |

Use HCE and store Secrets in the Cloud

Local SEs

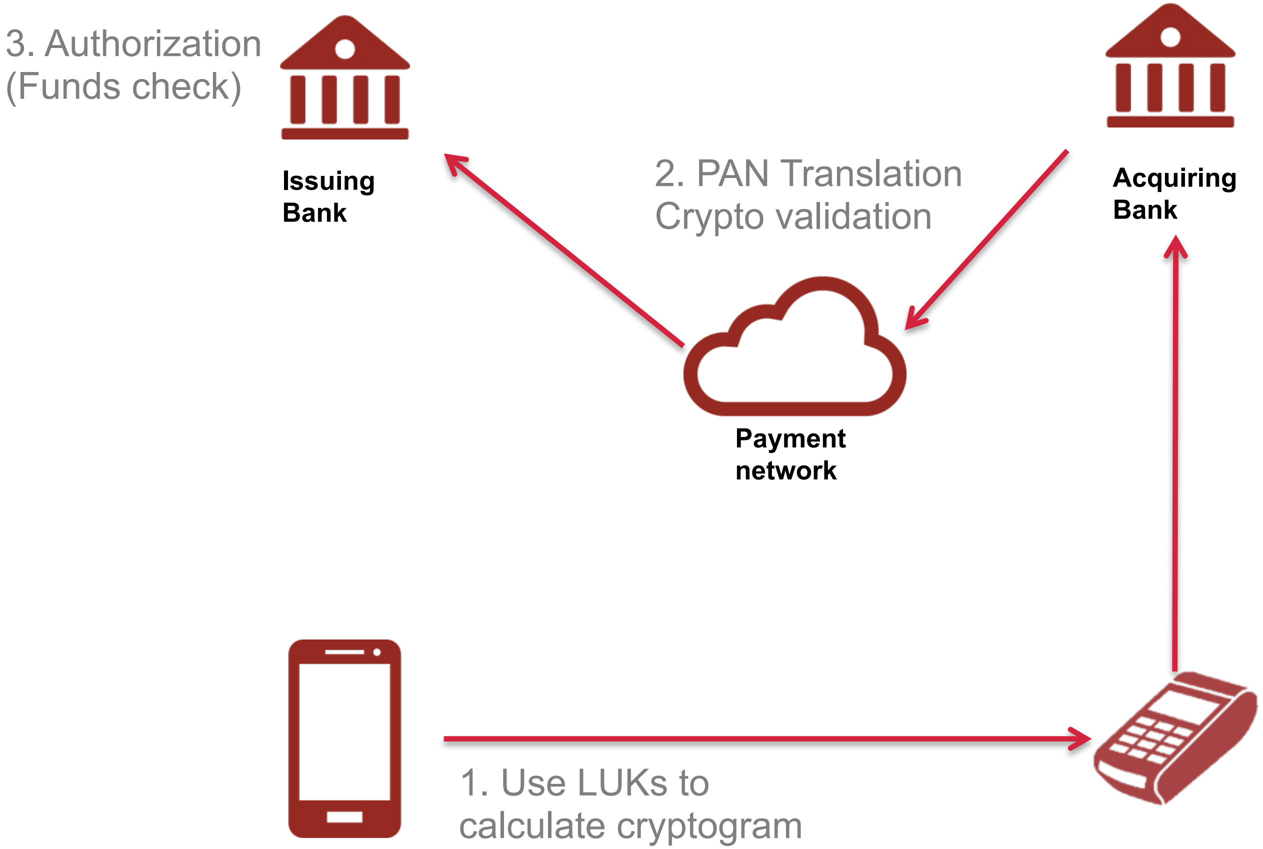
# Cloud Based Mobile Payments

## Provisioning a Card



# Cloud Based Mobile Payments

## Payment

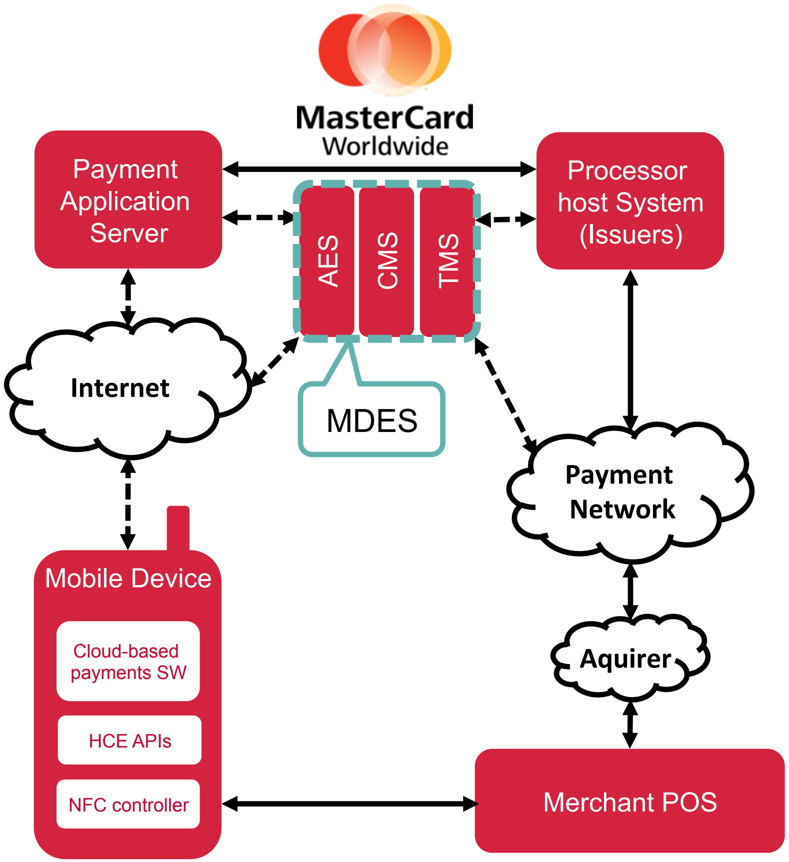

3. Authorization
(Funds check)

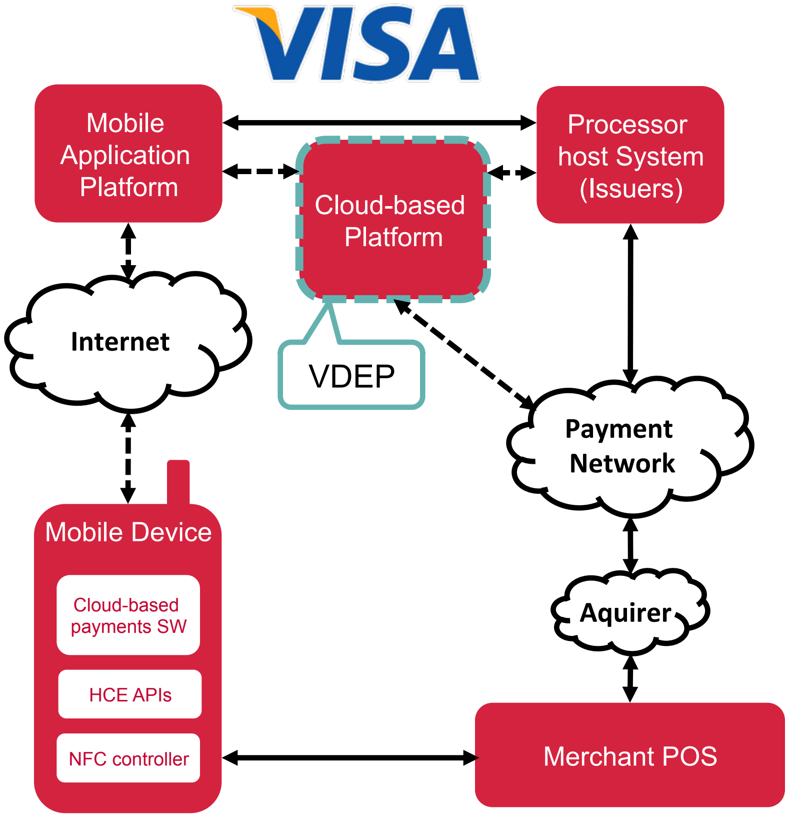
2. PAN Translation
Crypto validation

1. Use LUKs to
calculate cryptogram

# Cloud Based Mobile Payments

## MDES and VDEP





Google wallet

Pay

SAMSUNG pay

# Conclusions

EMV is not enough

Tokens allow for Asset Devaluation

PAN (EMVco) Token vs. Token Cryptogram

Protecting data at rest, eCommerce

CBMP use Token Cryptograms

ApplePay uses PAN tokenizantion

# Thank You

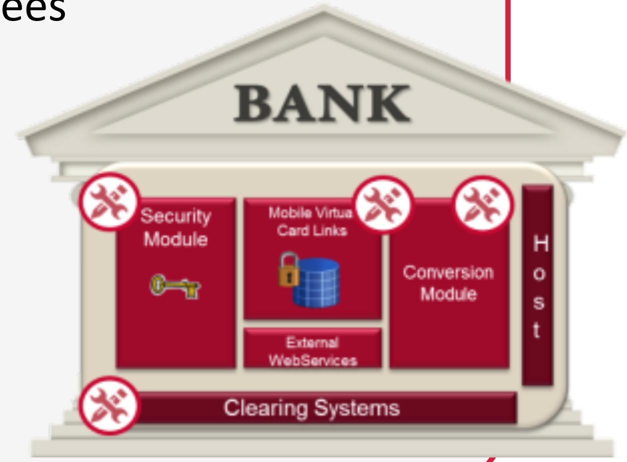
Peter Helderman
Principal Consultant
UL Transaction Security
peter.helderman@ul.com

# Challenges

The idea of tokenization is to allow transactions to be performed using the **current processing rails**, without changes to all existing routing mechanisms.

However, there are important **impacts** that need to be considered:

- Handling of clearing files with tokenized data
- Pre-authorization followed by payment with physical card [e.g. hotel]
- Card product differentiators and related interchange fees [e.g. MasterCard Black, Visa Platinum]
- Card-linked benefits [e.g. points, mileage, insurance]
- Recurring payments and partial shipment
- Refunds and cancellation flows
- Handling chargebacks and disputes


BANK
Security Module
Mobile Virtua Card Links
Conversion Module
External WebServices
Host
Clearing Systems