




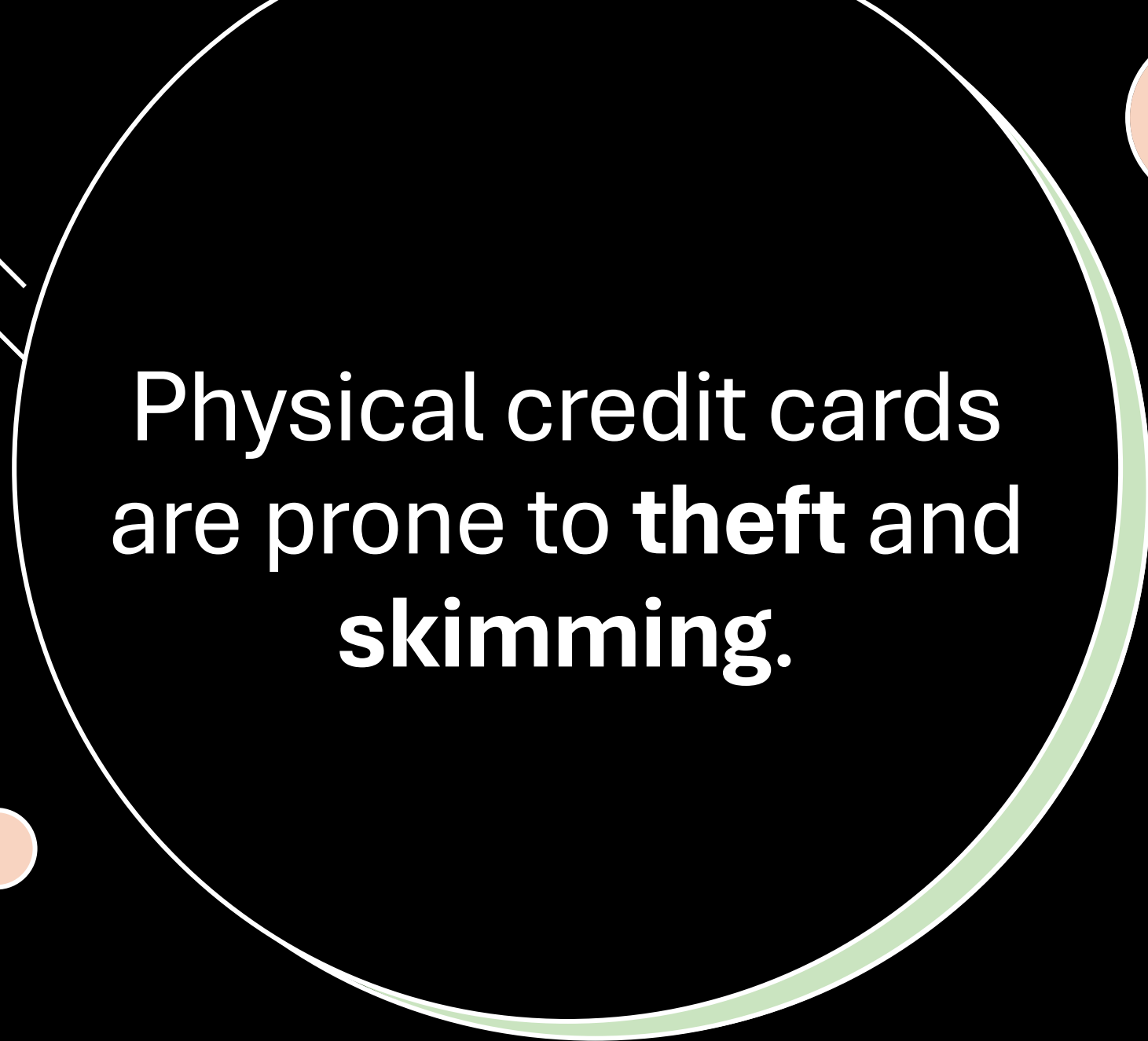

# In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping

**Raja Hasnain Anwar**<sup>\*</sup>, Syed Rafiul Hussain<sup>‡</sup>, and Muhammad Taqi Raza<sup>\*</sup>

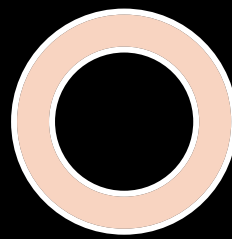
<sup>\*</sup>University of Massachusetts Amherst, <sup>‡</sup>The Pennsylvania State University

August 14, 2024

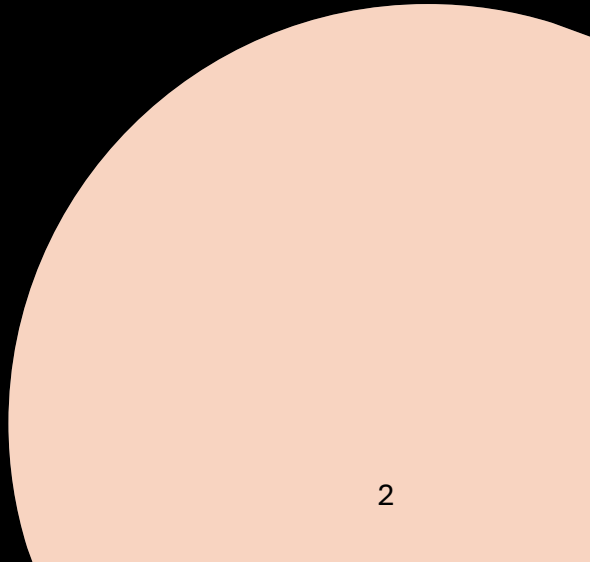






Physical credit cards  
are prone to **theft** and  
**skimming**.



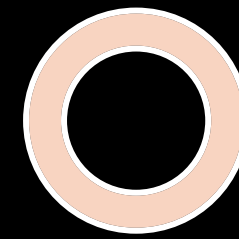
**Our view of the  
digital payments  
security**





Physical credit cards are prone to **theft** and **skimming**.

Digital wallets are a **secure** alternative to physical cards.




**Our view of the digital payments security**



# Why?

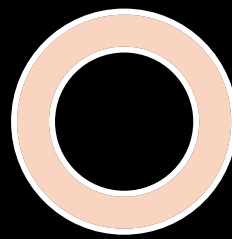

Digital wallets are a **secure** alternative to physical cards.

**Our view of the digital payments security**



Because of the **FaceID, Fingerprint, and on-device encryption** mechanism...

Digital wallets are a **secure** alternative to physical cards.



**Our view of the digital payments security**



What if I told you...

An attack can add  
your **stolen card** to  
their wallet



What if I told you...

An attack can add  
your **stolen card** to  
their wallet

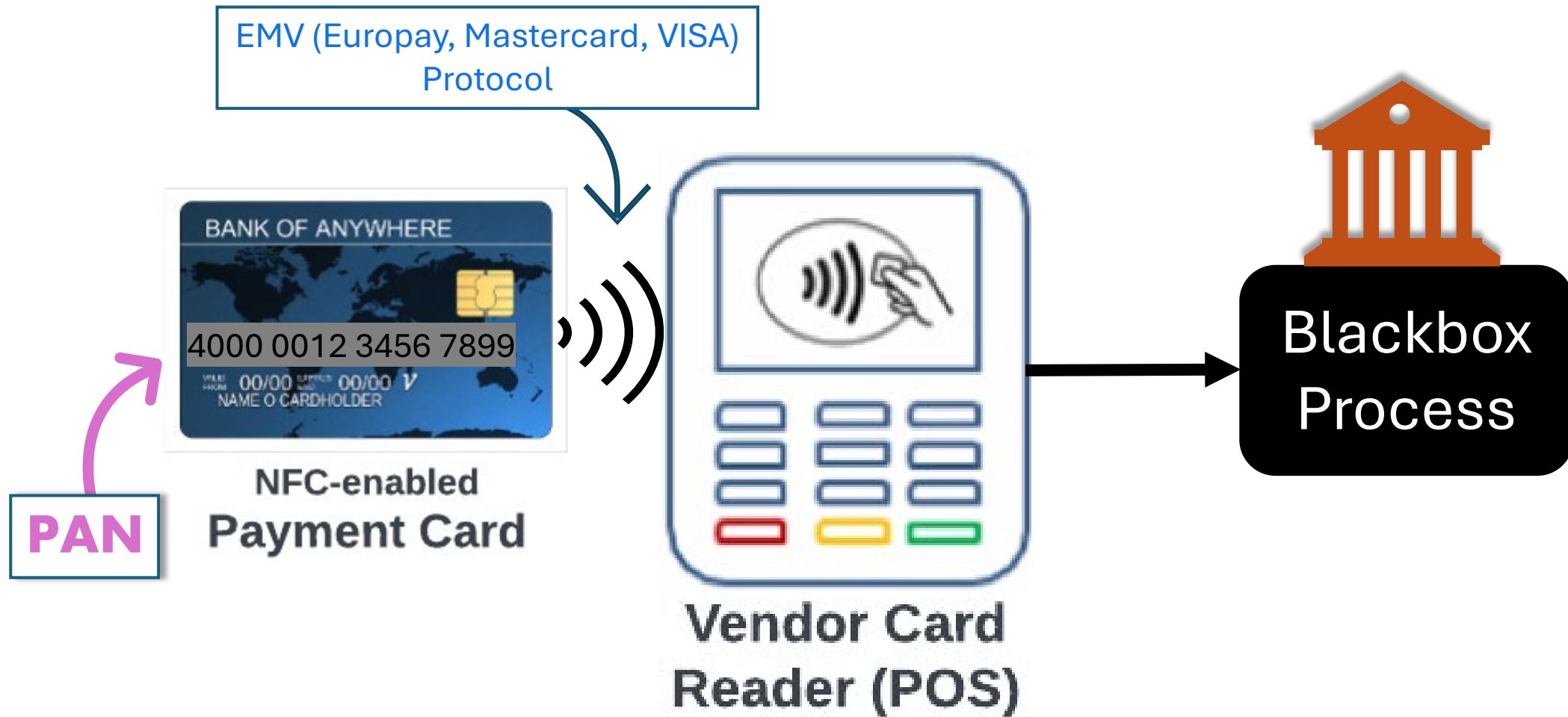


& use it even  
*after* you **lock**  
or **replace** it.

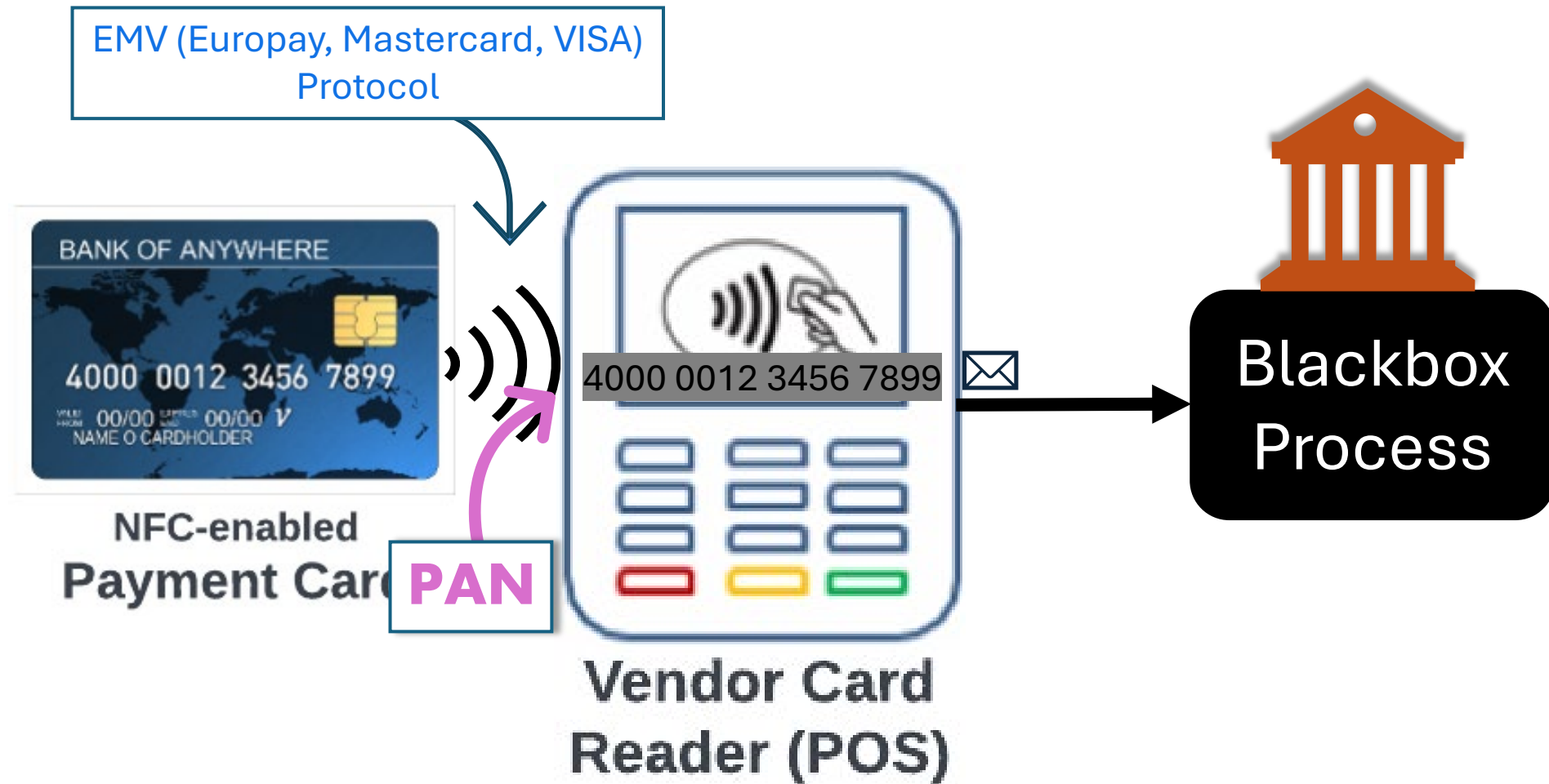
What if I told you...



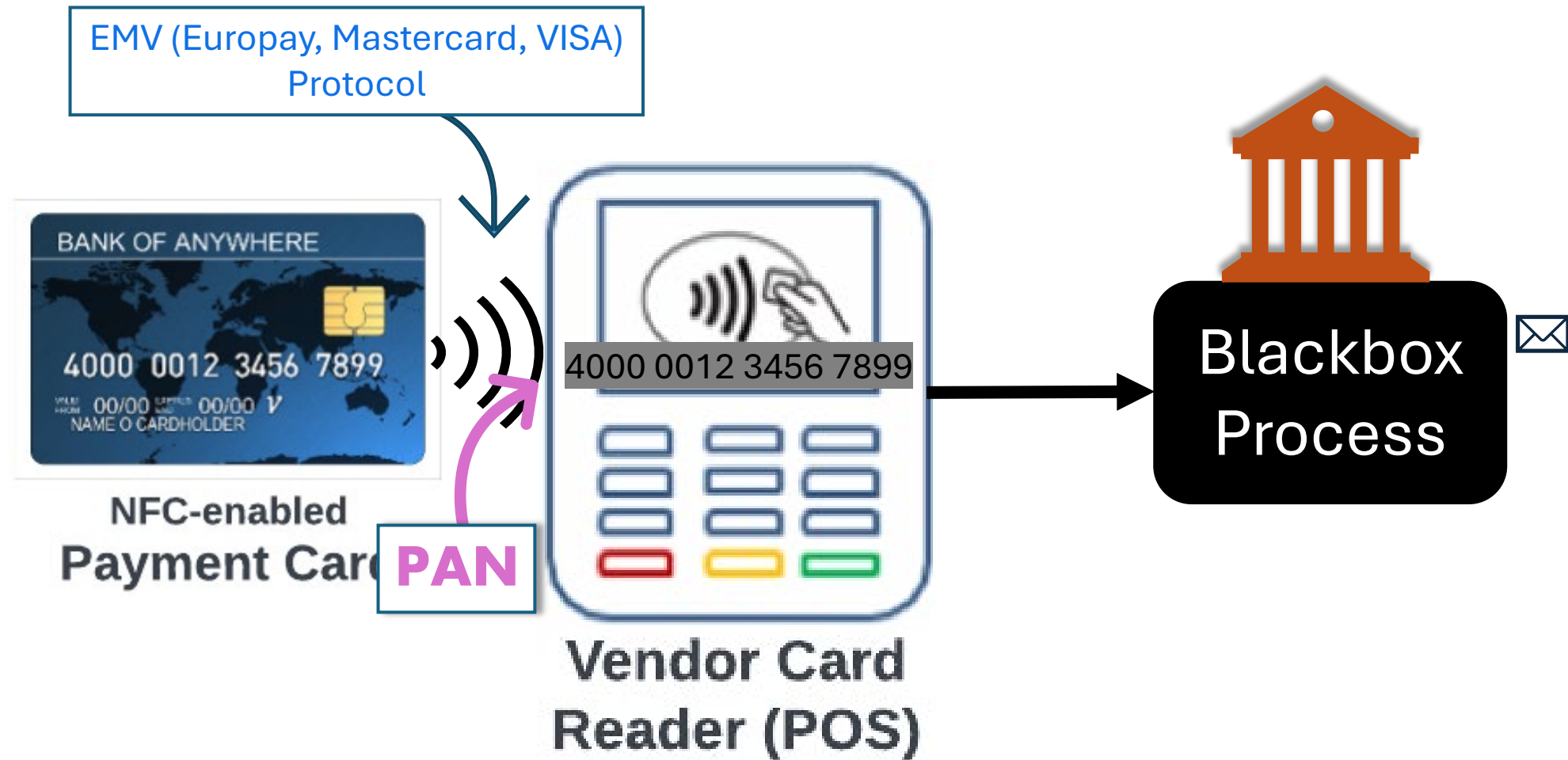
# Digital Payments – Classical Way



# Digital Payments – Classical Way



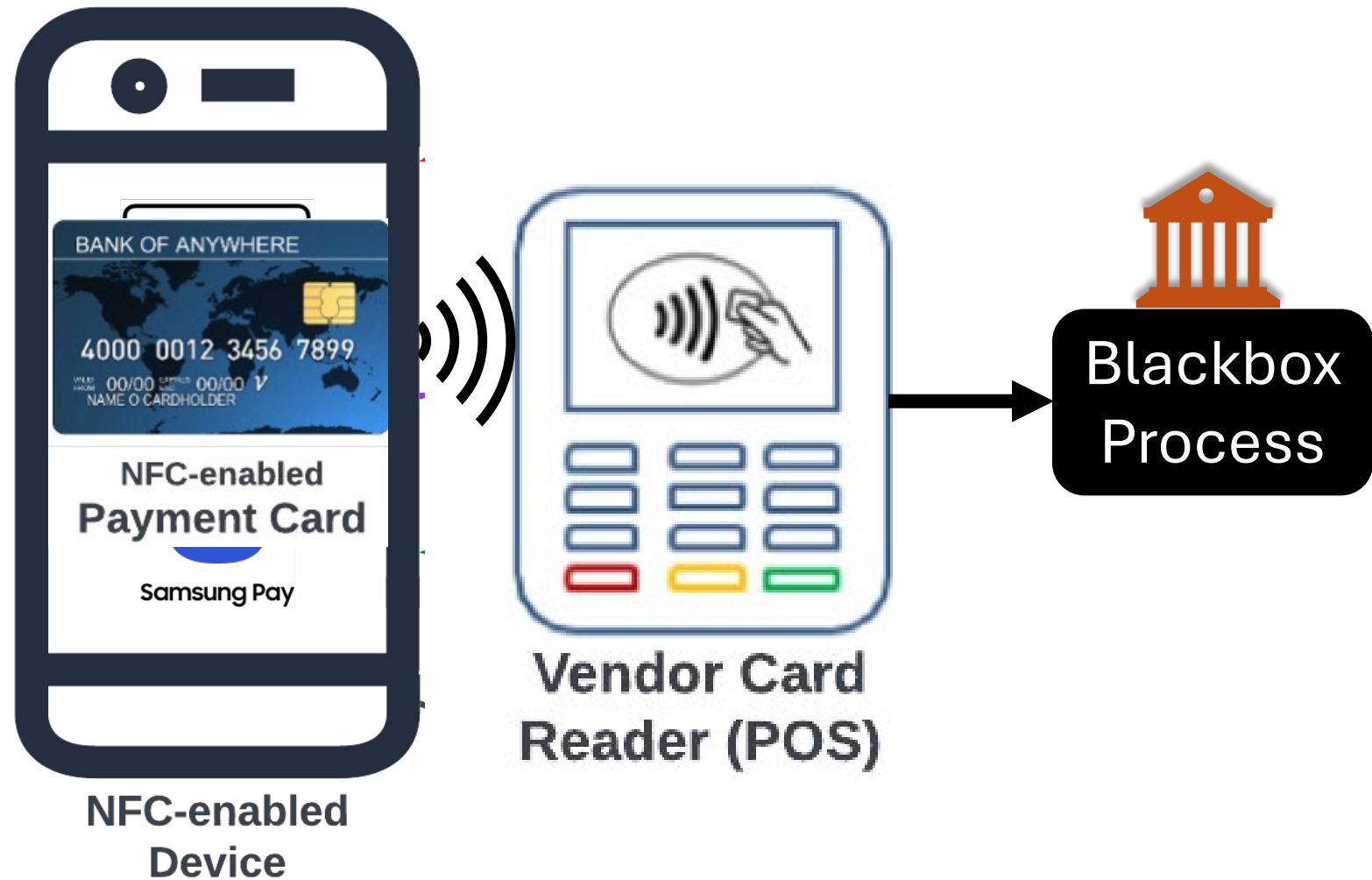
# Digital Payments – Classical Way



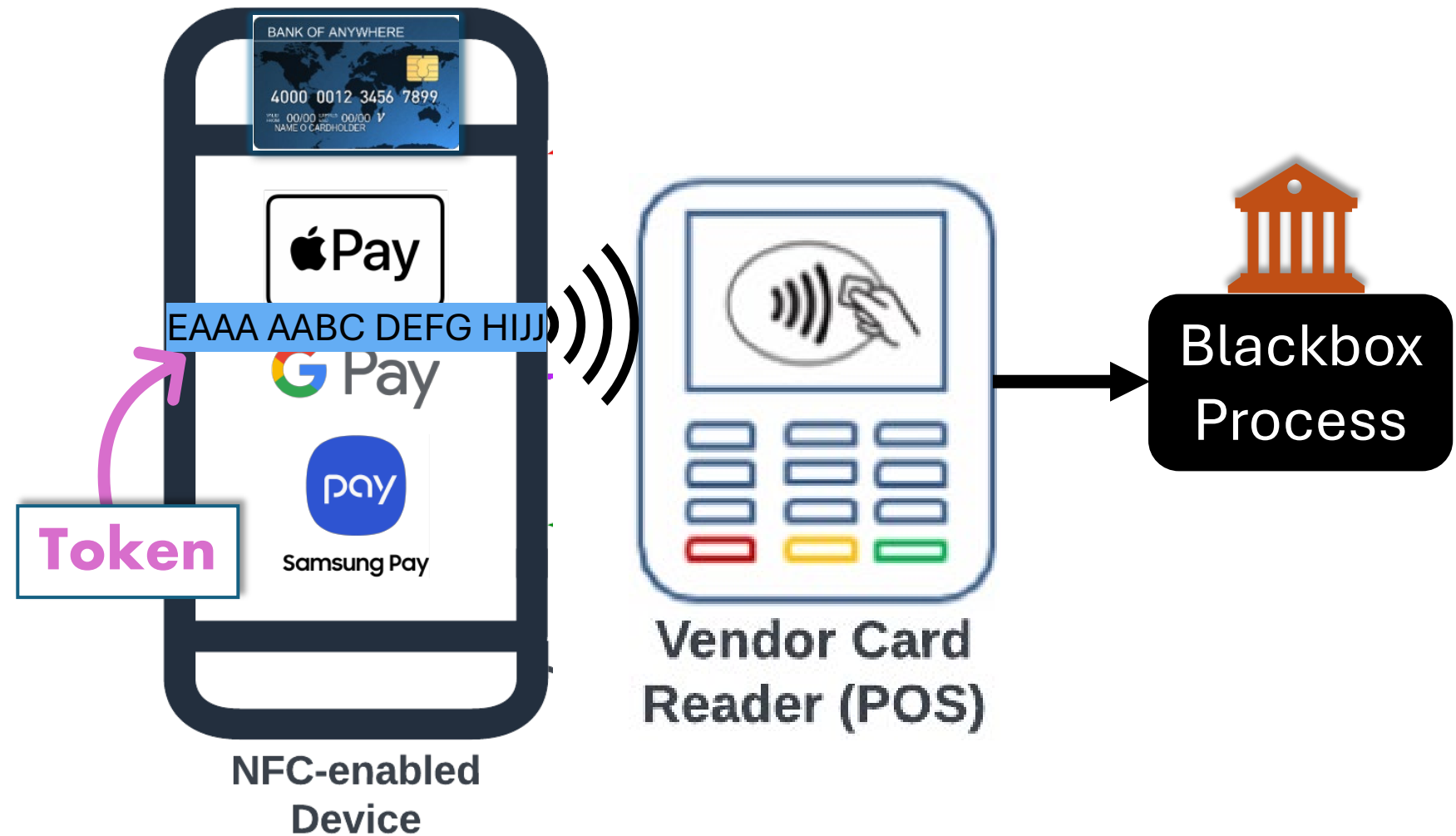
# Digital Payments – Digital Wallets



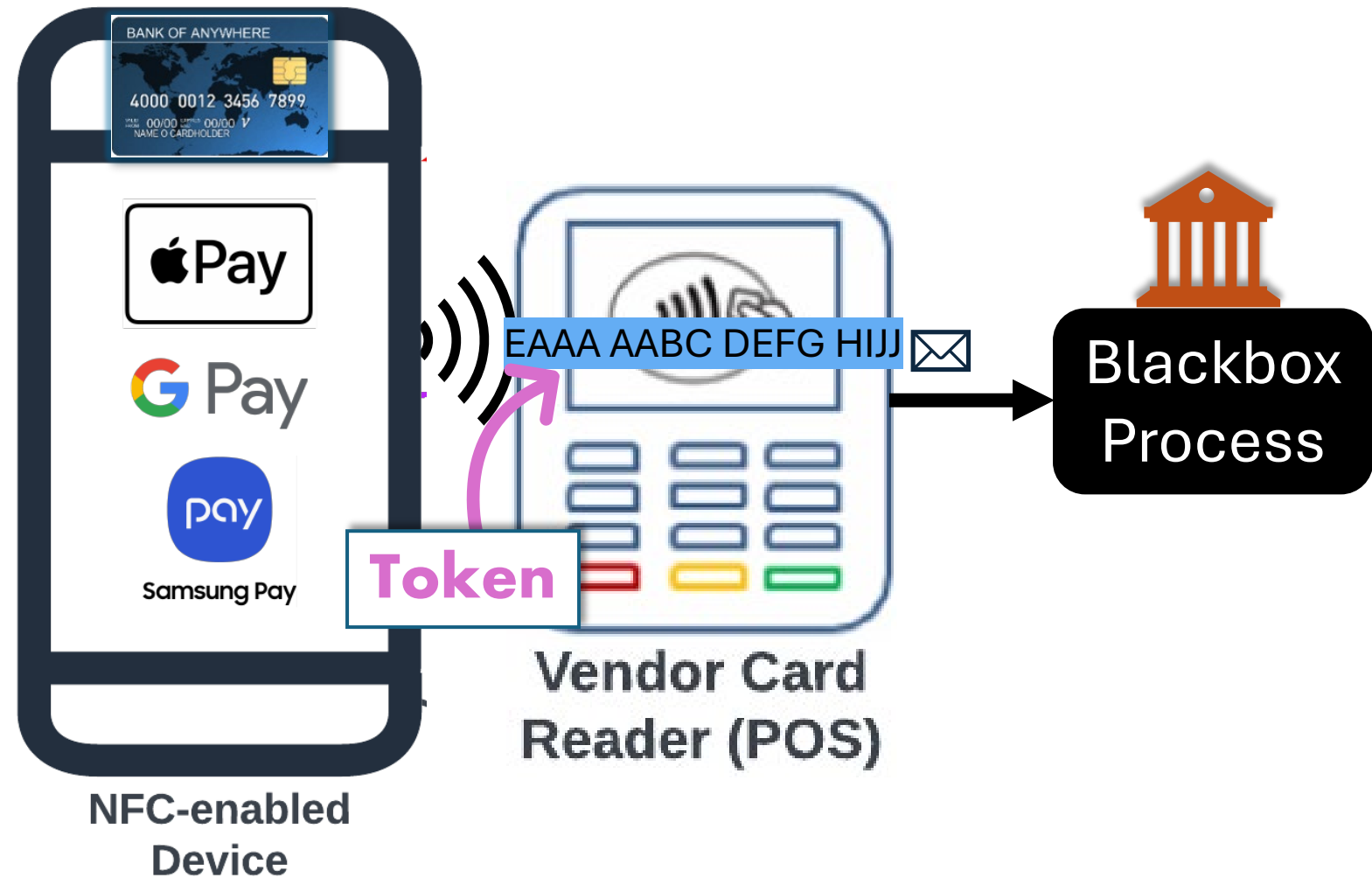
# Digital Payments – Digital Wallets



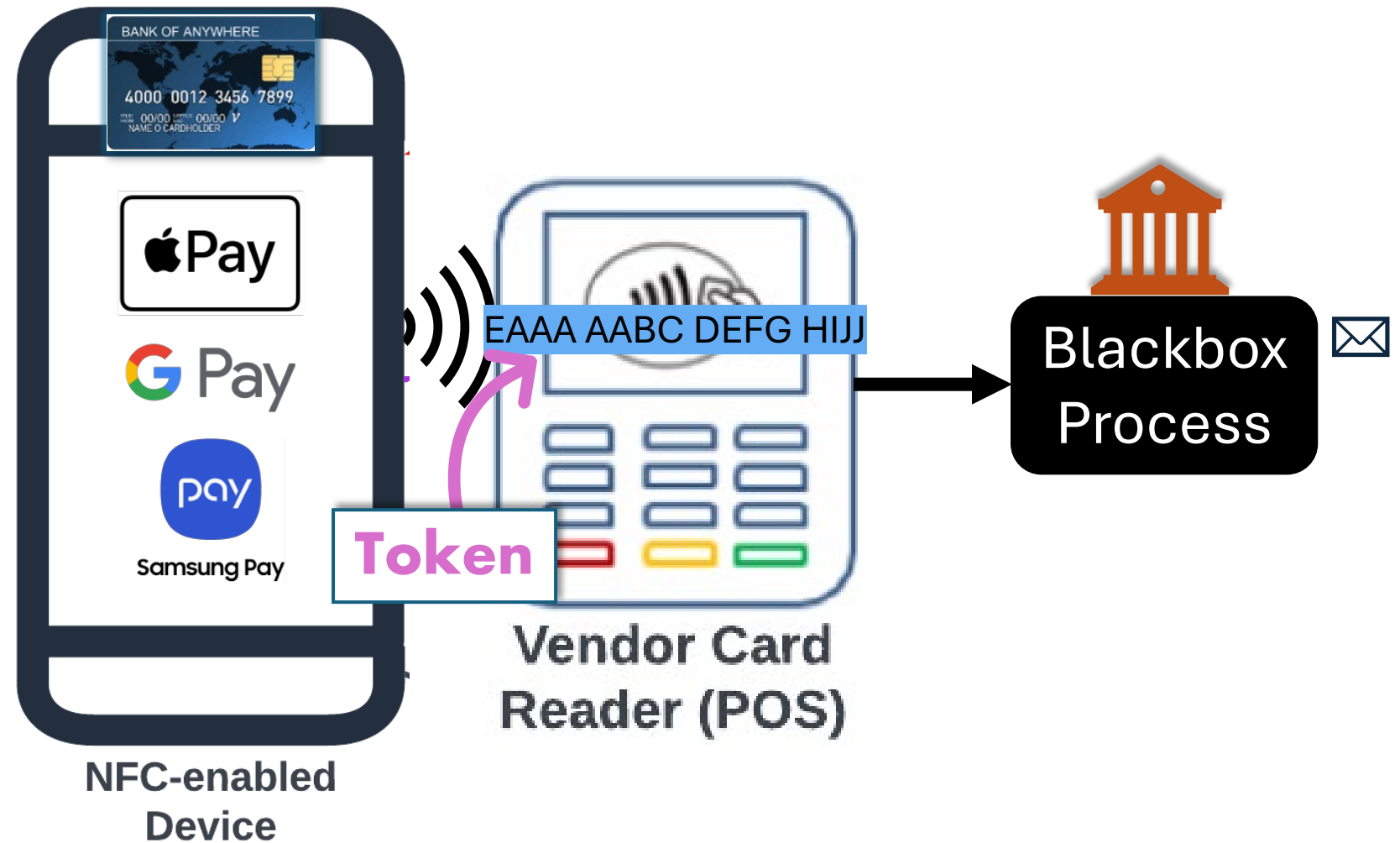
# Digital Payments – Digital Wallets



# Digital Payments – Digital Wallets



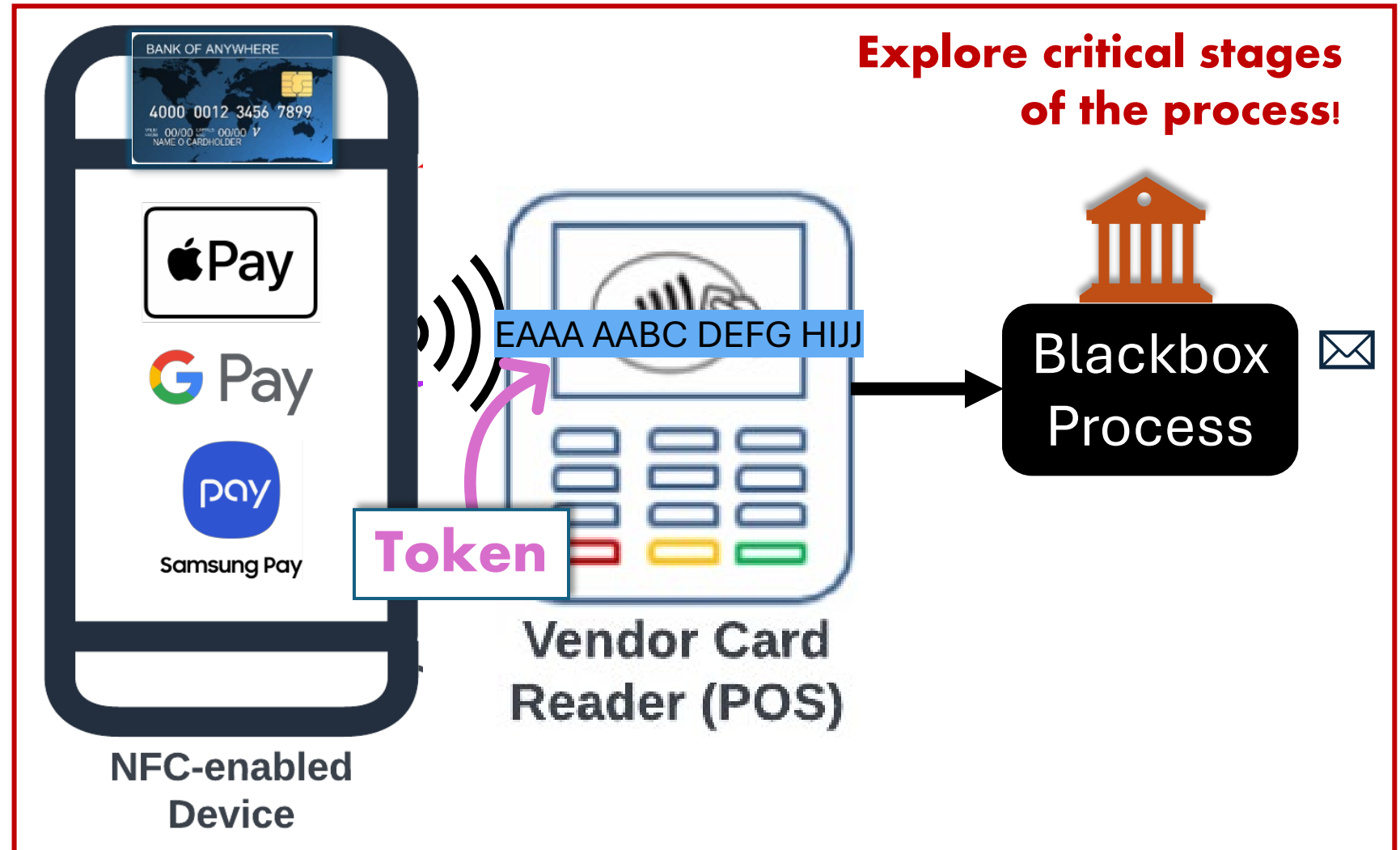
# Digital Payments – Digital Wallets





# Digital Payments – Digital Wallets

- Securely store the card number
- Virtual number (**token**) for payments
- Multiple devices
  - Multiple users



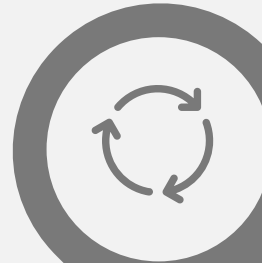


# Critical Procedures

Cardholder Verification



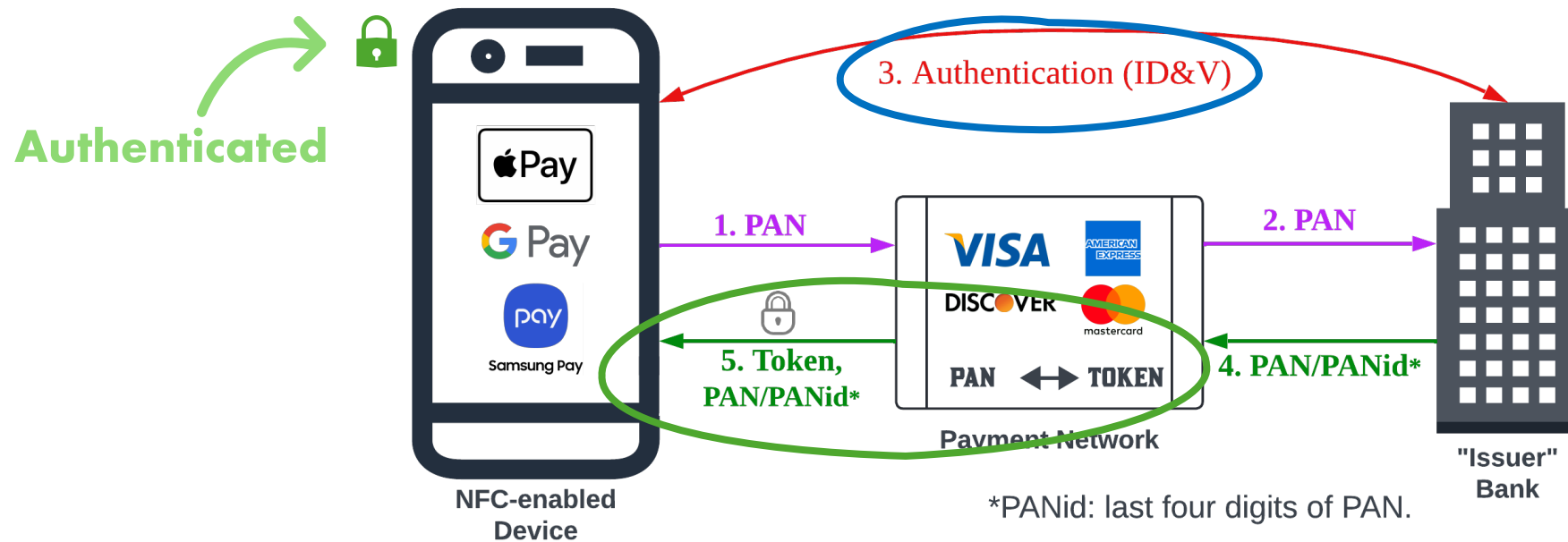
Card Replacement



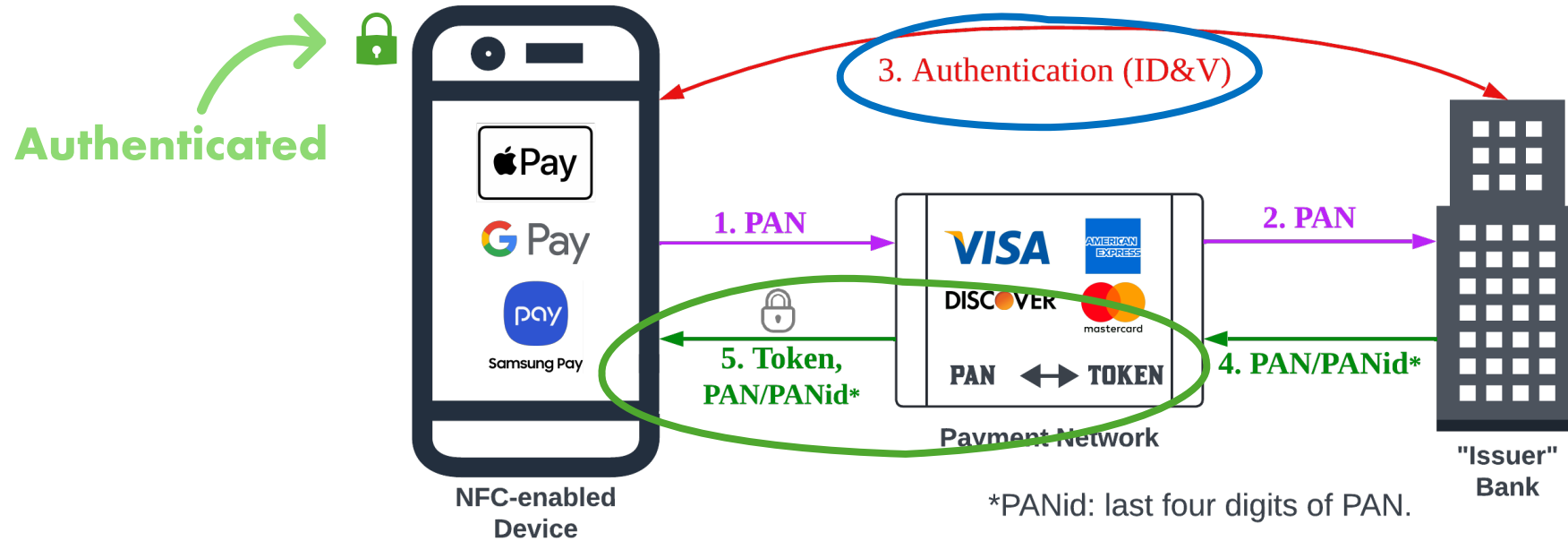
User Authentication



## User Authentication







## User Authentication

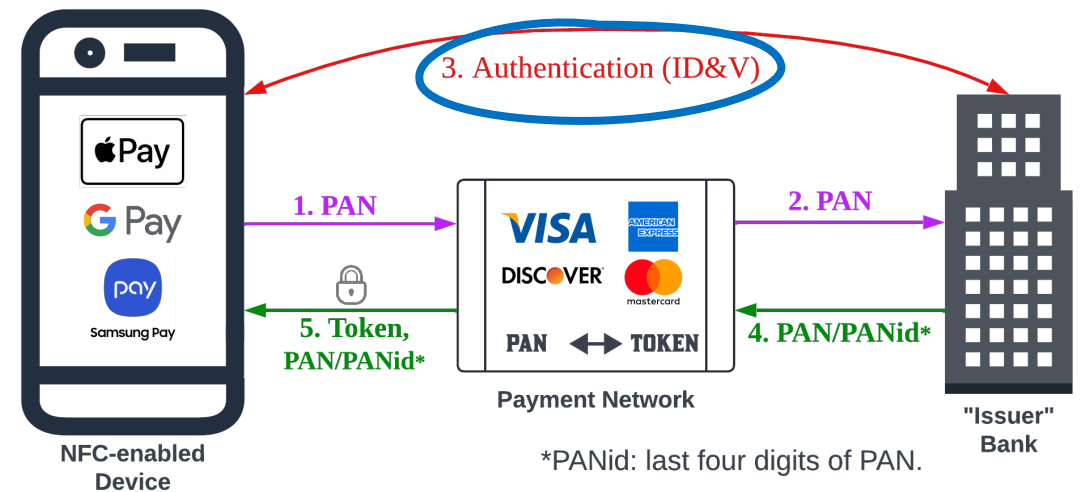


How does the cardholder's identity link to the digital wallet?

# User Authentication

Cardholder adopts multiple **identities** across the ecosystem:

- Cardholder ID 
- Banking ID 
- Device ID 
- Wallet ID 



**Missing strong mapping across identities because of the distributed ecosystem.**

# User Authentication

Missing strong mapping across identities because of the distributed ecosystem.



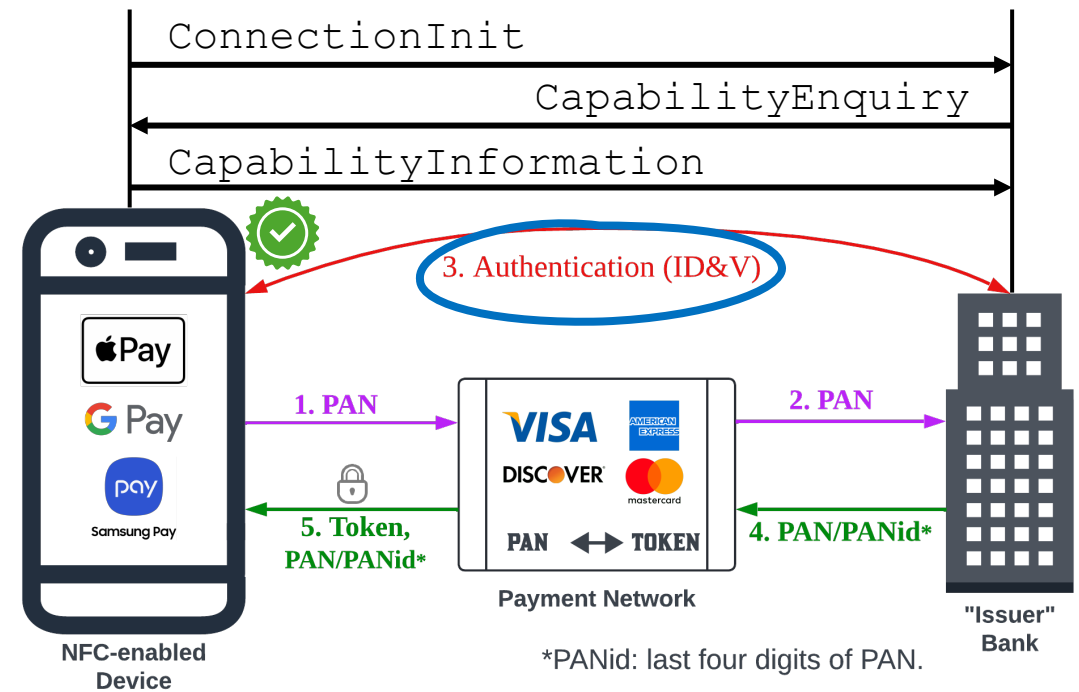
**Banks delegate the choice of authentication method to the wallet.**

- **Knowledge-based Authentication (KBA)**

- Billing Address
- ZIP Code
- Date of Birth
- Last four digits of ID (e.g., SSN)

- **Multi-factor Authentication (MFA)**

- SMS
- Call
- Email



# User Authentication



Banks delegate the choice of authentication method to the wallet.

## PayPal

Debit or credit card

BANK OF ANYWHERE

4000 0012 3456 7899

Card type  
Visa

Expiration date  
01/23

Security code  
...

Billing address  
XYZ Street, 123, Cambridge, MA

Link Card

**KBA**

## Apple Pay

### Card Verification

Choose how to verify your card for Apple Pay.



Email  
r\*\*\*\*0@gmail.com ✓

Text Message  
\*\*\*-\*\*\*-3626

Call Bank of America  
1-888-383-7800

**MFA**

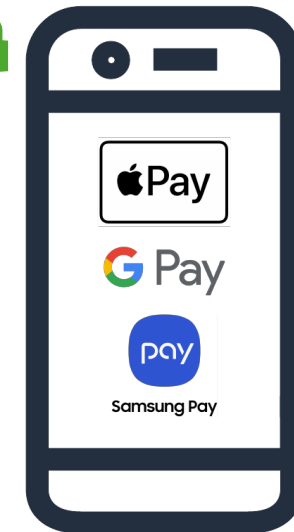
**KBA**

**Delegation of authentication allows an attacker to add a stolen card to their wallet using weaker authentication.**

# Card Lock – Physical Card vs. Digital Wallet

## How to secure a lost card?

Card Issuer Banks	Physical Card	Wallet (one-time)	Wallet (Recurring)
AMEX	x	✓	✓
Chase	x	✓	✓
Discover	x	✓	✓
US Bank	x	x	✓
Citibank	x	x	✓
BoAmerica	x	x	✓



NFC-enabled  
Device



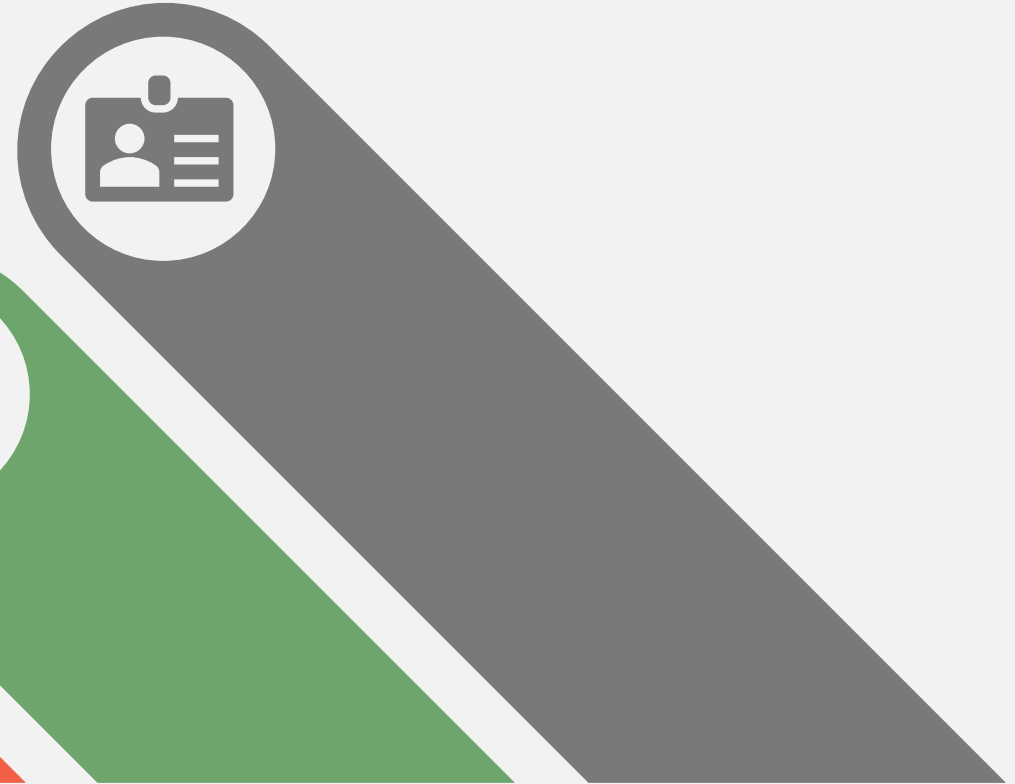
**Banks have established an unconditional trust with digital wallets.**





# Critical Procedures

Cardholder Verification



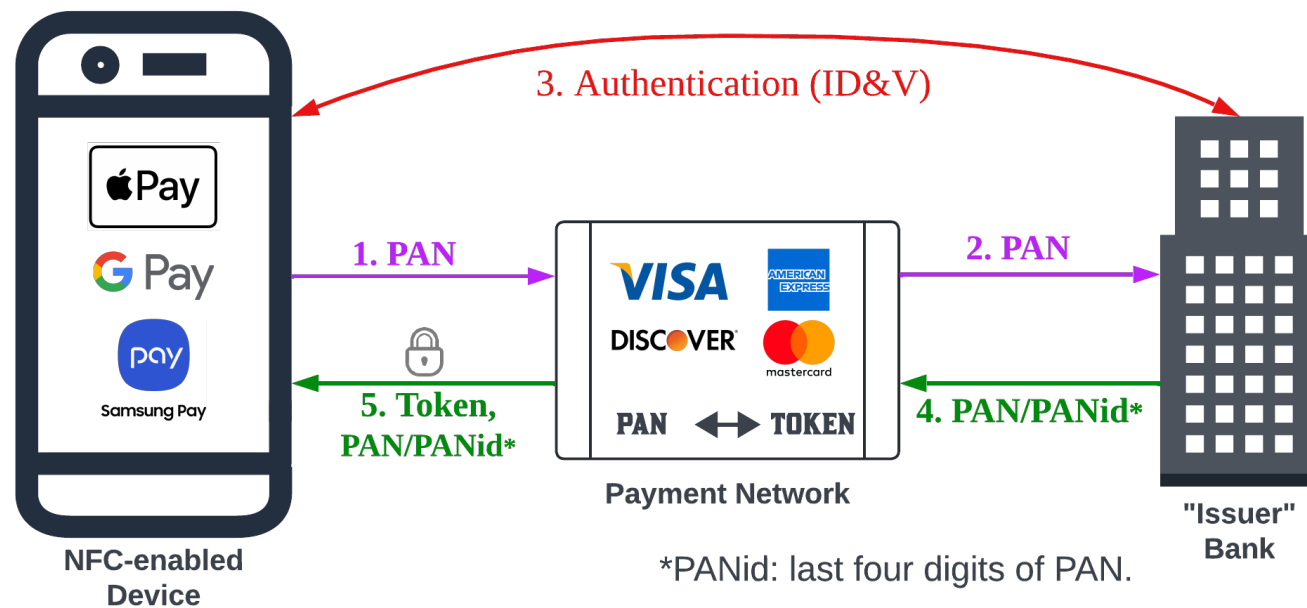
Card Replacement



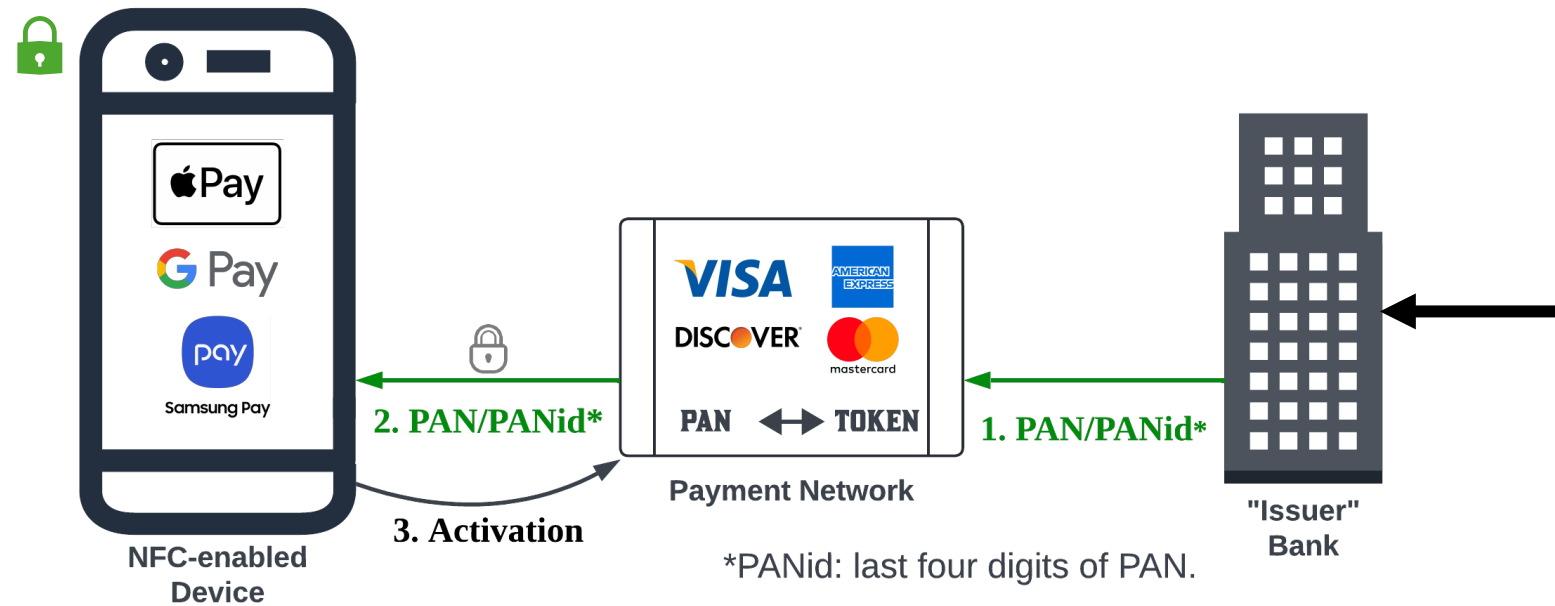
User Authentication



# Recap



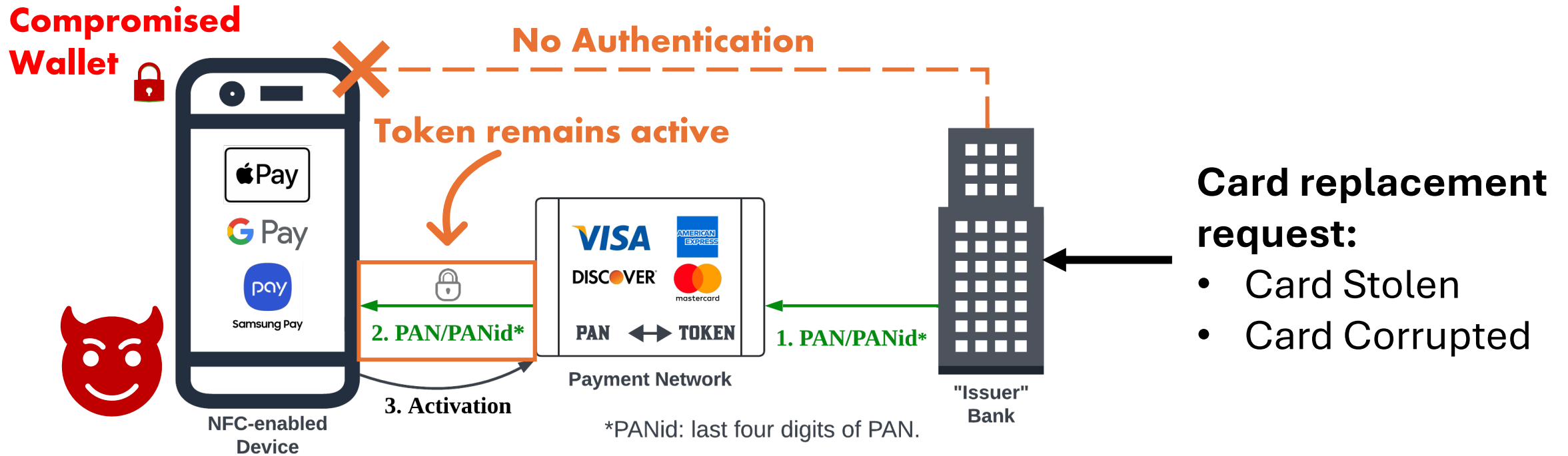
# Card Replacement



## Card replacement request:

- Card Stolen
- Card Corrupted

# Card Replacement



## Card replacement request:

- Card Stolen
- Card Corrupted

An additional benefit to the Merchant is that the replacement of the underlying PAN has no impact on any affiliated Payment Token(s), so the Payment Token can continue to transact uninterrupted.

**EMV® Payment Tokenisation: A Guide to Use Cases v2.1 (\$10.7)**



# Critical Procedures

Cardholder Verification



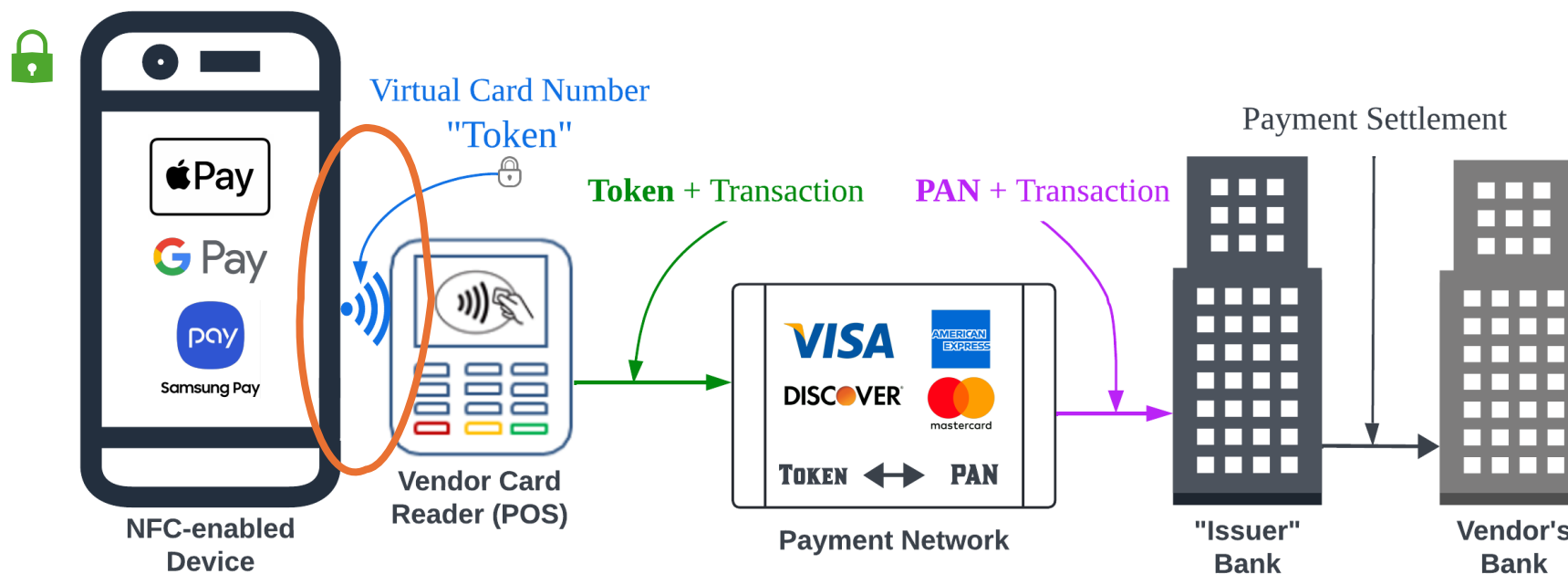
Card Replacement



User Authentication



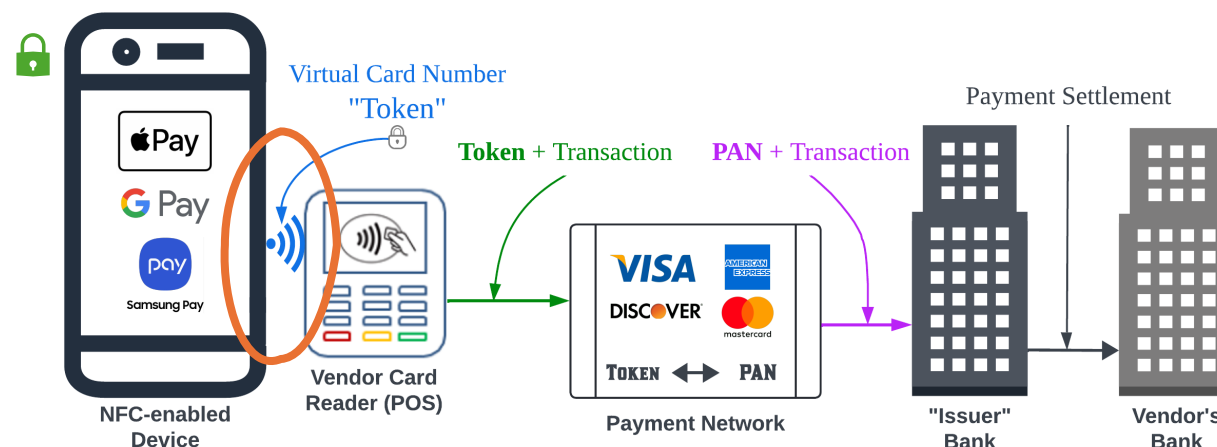
# Cardholder Verification



# Cardholder Verification

## Cardholder Verification Methods (CVMs)

- Offline PIN
- Online PIN
- Signature
- ZIP Code
- **Consumer device CVM (CDCVM)**



**CDCVM:** unlock *wallet app* using fingerprint or face recognition to make transactions.



Terminal performs no CVM.

When the applicable CVM is 'No CVM required', if the terminal supports 'No CVM required' it shall set byte 3 of the CVM Results to 'successful'. W

**EMV® Integrated Circuit Card Specifications for Payment Systems: Book 4 (§6.3.4)**

# In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping

Raja Hasnain Anwar

*University of Massachusetts Amherst*  
ranwar@umass.edu

Syed Rafiul Hussain

*Pennsylvania State University*  
hussain1@psu.edu

Muhammad Taqi Raza

*University of Massachusetts Amherst*  
taqi@umass.edu

## Abstract

Digital wallets are a new form of payment technology that provides a secure and convenient way of making contactless payments through smart devices. In this paper, we study the security of financial transactions made through digital wallets, focusing on the authentication, authorization, and access control security functions. We find that the digital payment ecosystem supports the decentralized authority delegation which is susceptible to a number of attacks. First, an attacker adds the victim's bank card into their (attacker's) wallet by exploiting the authentication method agreement procedure between the wallet and the bank. Second, they exploit the unconditional trust between the wallet and the bank, and by-

Table 1: Summary of card lock policies for major US banks. Some banks allow (✓) certain types of transactions on locked cards while blocking (✗) others.

Card Issuer Banks	Physical Card	Wallet (one-time)	Wallet (Recurring)
AMEX	✗	✓	✓
Chase	✗	✓	✓
Discover	✗	✓	✓
US Bank	✗	✗	✓
Citibank	✗	✗	✓
BoAmerica	✗	✗	✓



# Ethical Considerations

All the tests were conducted on the **authors' devices** using **own credit cards**.

**No financial liability** on the banks, wallets, or merchants.

**No attempt to defraud** another digital wallet user.

All the findings have been responsibly **disclosed** to all the concerned **banks and wallets**.

# Summary

- Banks have unconditional trust on the digital wallets
- Missing binding of cardholder *identities* leads to **weak authentication**.
- Card replacement in wallet does not require **user authentication**.
- In-device **cardholder verification** does not verify the *cardholder*.

# Seeking internship opportunities!

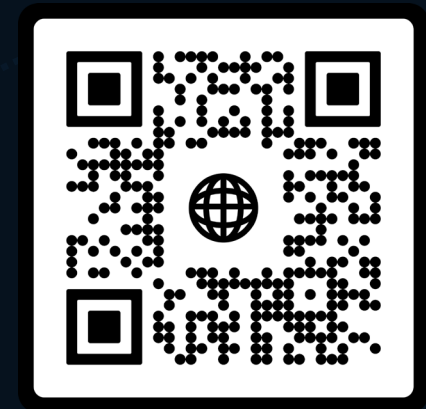
**Raja Hasnain Anwar**

Email: [ranwar@umass.edu](mailto:ranwar@umass.edu)

Web: [rhasnainanwar.me](http://rhasnainanwar.me)

**Khwarizmi Lab @ UMass**

[www.ecs.umass.edu/khwarizmi](http://www.ecs.umass.edu/khwarizmi)



Follow our research