CONTACTLESS PAYMENTS

Joeri de Ruiter

University of Birmingham

(some slides borrowed from Tom Chothia)

Overview

- EMV
  - Protocol
  - Attacks
- EMV-Contactless
  - Protocols
  - Attacks
- Demo
- Stopping relay attacks

What is EMV?

Standard for communication between chip based payment cards and terminals

What is EMV?

Developed and maintained

EMVCo

Owned by

AMERICAN EXPRESS

MasterCard Worldwide

JCB

VISA

UnionPay 银联 中国银联 China UnionPay

DISCOVER

What is EMV?

- Initiated in 1993
- Worldwide over 1,5 billion cards
- Variants for contactless and internet banking
- Required for Single Euro Payment Area (SEPA)

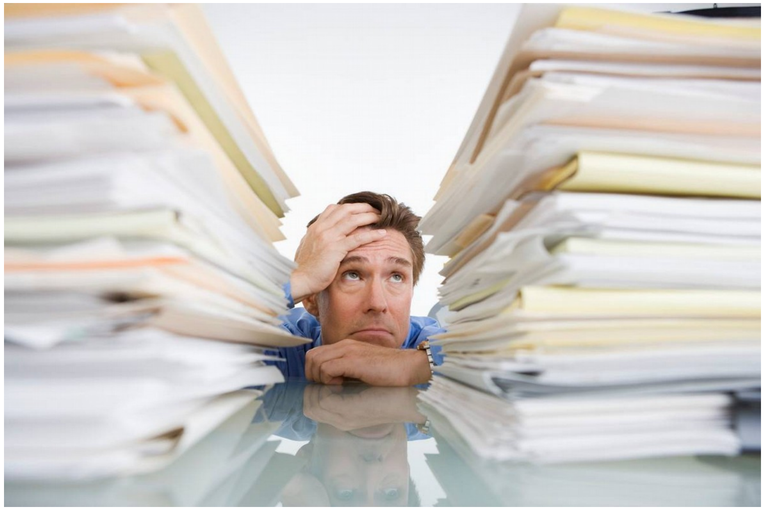
Why EMV?

- Reducing fraud by
  - skimming
  - stolen credit cards used with forged signatures
  - card-not-present fraud (EMV-CAP)

- Liability shift
  - Merchant: if no EMV is used
  - Customer: if PIN is used

Complexity

- Specification over 700 pages (4 books)
  - Book 1 - Application Independent ICC to Terminal Interface Requirements
  - Book 2 - Security and Key Management
  - Book 3 - Application Specification
  - Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements
  - Additional proprietary specifications
- Many options
  - 3 card authentication methods
  - 5 cardholder authentication methods
  - 2 types of transactions
- Everything can be parameterised using Data Object Lists (DOLs)



Key set-up

- Card and issuer/bank: symmetric key (3DES)
  - Authenticate transactions to bank
  - Usually bank has master key and card a derived key
- Payment scheme: asymmetric keypair (RSA)
  - Authenticate issuers
- Issuer: asymmetric keypair (RSA)
  - Authenticate cards
- Cards (optional): asymmetric keypair (RSA)
  - Authenticate cards/transactions to terminal

Key set-up

- Terminal
  - Payment scheme's public keys
- Card
  - Issuer's public key certificate signed by payment scheme
  - Card's public key certificate signed by issuer

Communication

- ISO 7816
- Master-slave
- Application Protocol Data Units (APDUs)
  - Commands

CLA	INS	P1	P2	Lc	Data	Le

  - Responses

Data	SW1	SW2

Communication

- VERIFY

  > 00 20 00 80 08 24 12 34 FF FF FF FF FF

  - 00 20 – VERIFY
  - 00 80 – Plaintext PIN
  - 08 – Length data
  - 24 12 34 FF FF FF FF FF – Data

  < 90 00

  - PIN code correct

EMV session

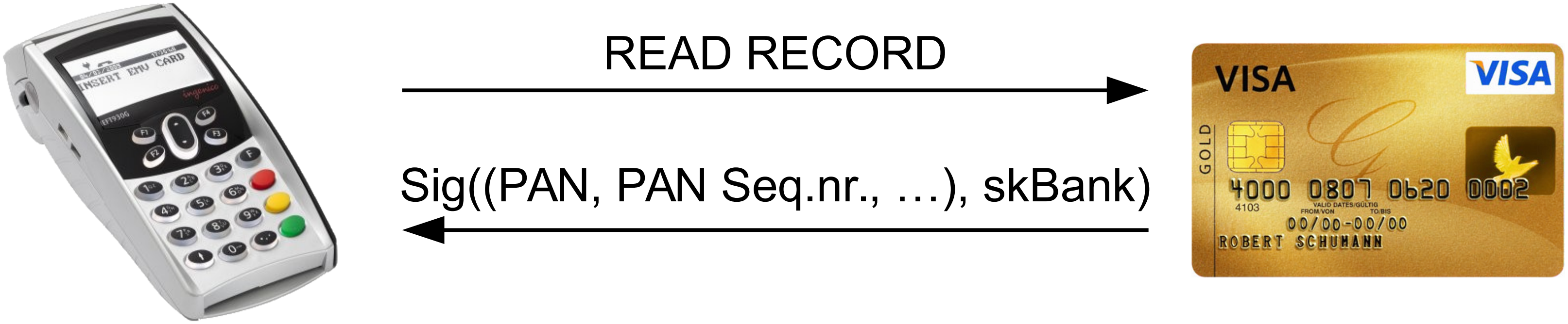
- Initialisation
- Card authentication
- Cardholder verification
- Transaction
- (Scripting)

Initialisation

- Read file 1PAY.SYS.DDF01
  - Contains list of EMV applets on card
- Select EMV applet
  - Processing Options Data Object List (PDOL) returned indicating data the reader must provide to the card
- Send GET PROCESSING OPTIONS command
  - Send data specified in PDOL
  - Application Interchange Profile (AIP) and Application File Locator (AFL) returned
    - AIP indicates support for, e.g., data authentication methods
    - AFL lists available files

Card authentication

- Static Data Authentication (SDA)
  - Static data signed by issuer in Signed Static Authentication Data (SSAD)
  - Data to be included indicated in AFL and optionally the AIP added

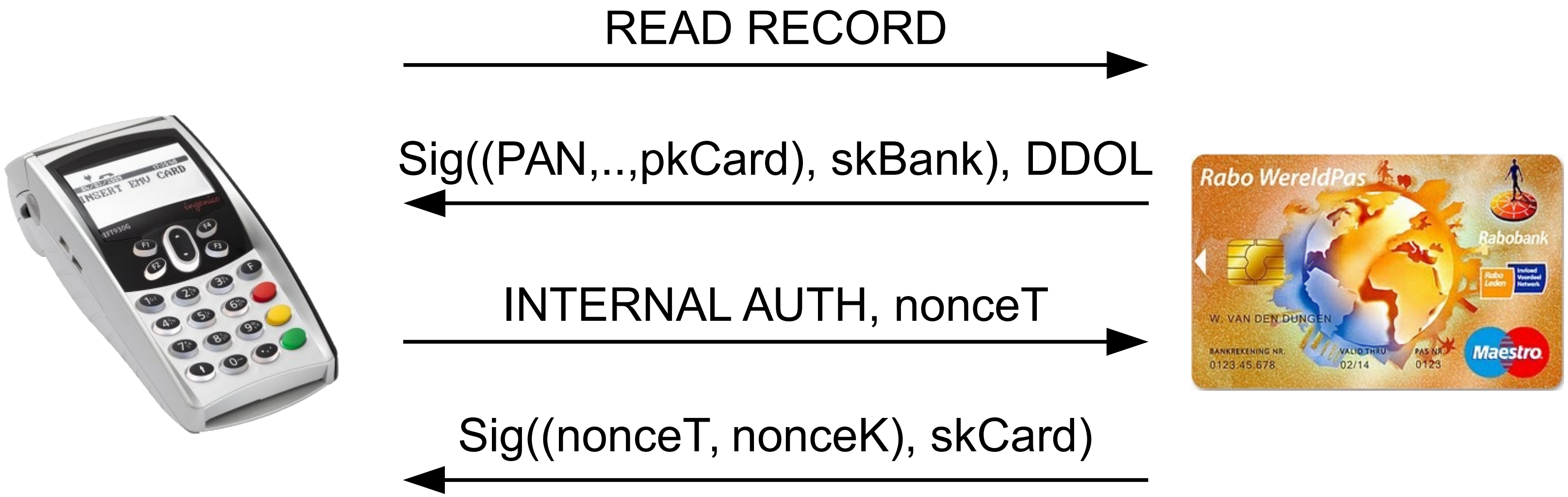


READ RECORD

Sig((PAN, PAN Seq.nr., …), skBank)

Card authentication

- Dynamic Data Authentication (DDA)
  - Public key cryptography used
  - Challenge/response mechanism
  - Challenge data specified by Dynamic Data Authentication Data Object List (DDOL)



READ RECORD

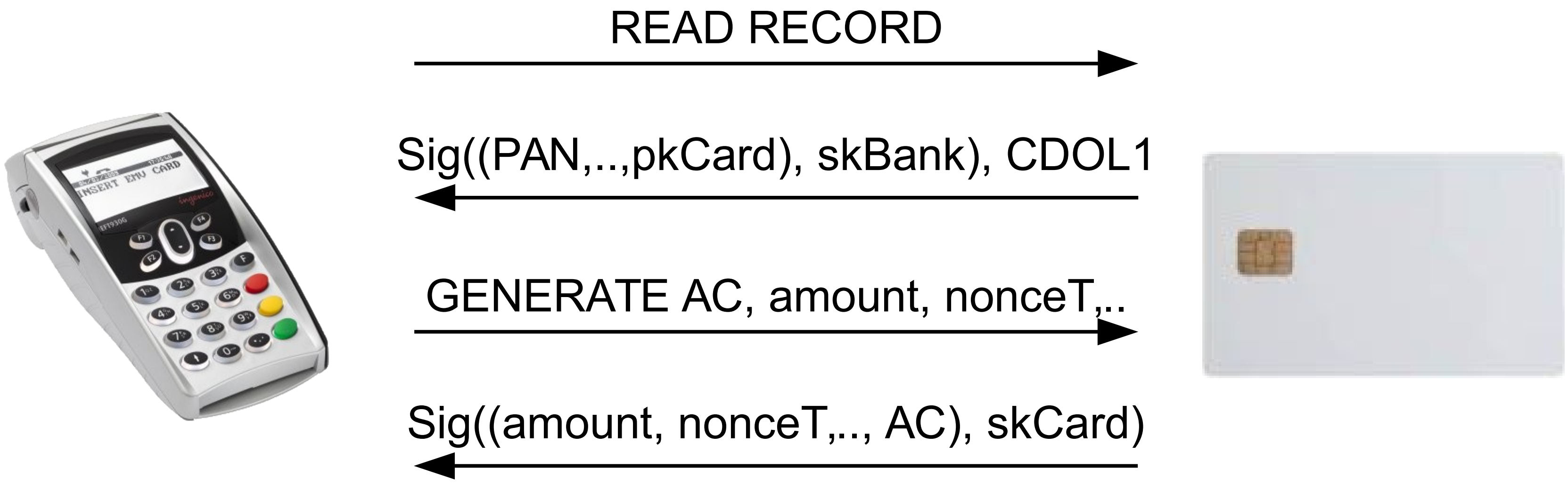
Sig((PAN,..,pkCard), skBank), DDOL

INTERNAL AUTH, nonceT

Sig((nonceT, nonceK), skCard)

Card authentication

- Combined Data Authentication (CDA)
  - Transaction data signed
  - Data from PDOL, CDOL1, (CDOL2) and other data returned in GENERATE AC command



READ RECORD

Sig((PAN,..,pkCard), skBank), CDOL1

GENERATE AC, amount, nonceT,..

Sig((amount, nonceT,.., AC), skCard)

Cardholder verification methods (CVM)

- Based on a list of rules in the CVM List
- None
- Signature
- PIN code
  - Offline
    - With or without encryption
  - Online

CVM List

Rule 0
If unattended cash:
    Enciphered PIN verified online
    Apply succeeding CV rule if this CVM is unsuccessful

Rule 1
If manual cash:
    Enciphered PIN verified online
    Fail cardholder verification if this CVM is unsuccessful

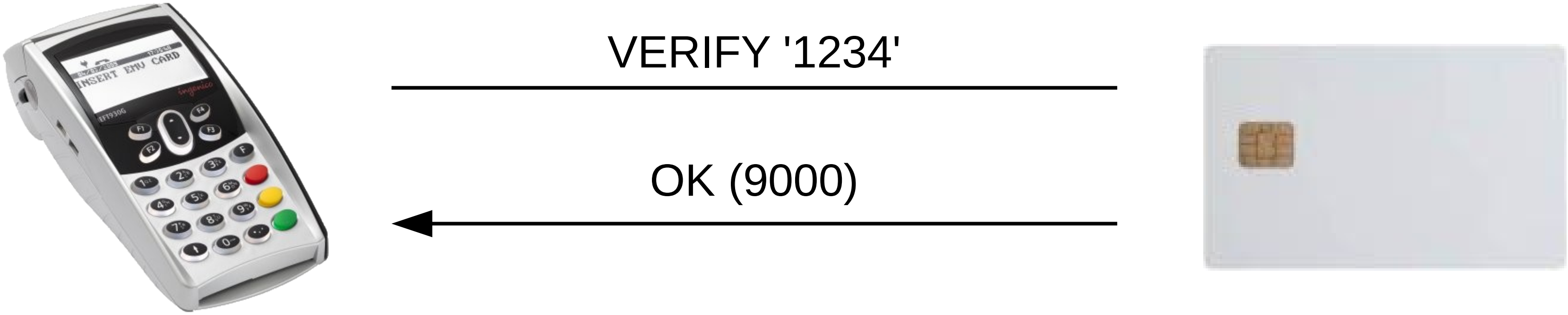
Rule 2
If terminal supports CVM:
    Enciphered PIN verification performed by card
    Fail cardholder verification if this CVM is unsuccessful

Rule 3
If terminal supports CVM:
    Enciphered PIN verified online
    Fail cardholder verification if this CVM is unsuccessful

Rule 4
Always:
    Plaintext PIN verification performed by card
    Fail cardholder verification if this CVM is unsuccessful

Cardholder verification

- Plaintext PIN verification



VERIFY '1234'

OK (9000)

Transaction

- Three different application cryptograms
  - Transaction Certificate (TC)
    - Transaction approved
  - Authorisation Request Cryptogram (ARQC)
    - Online authorisation requested
  - Application Authentication Cryptogram (AAC)
    - Transaction declined
- Data used in GENERATE AC command specified by Card Risk Management Data Object Lists (CDOL1 and CDOL2)
- Issuer specific MAC over transaction data and Application Transaction Counter (ATC) using session key derived from symmetric key and ATC

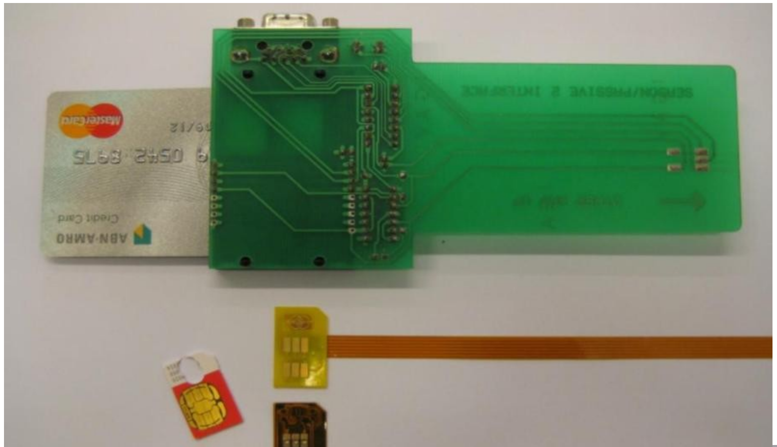
Transaction

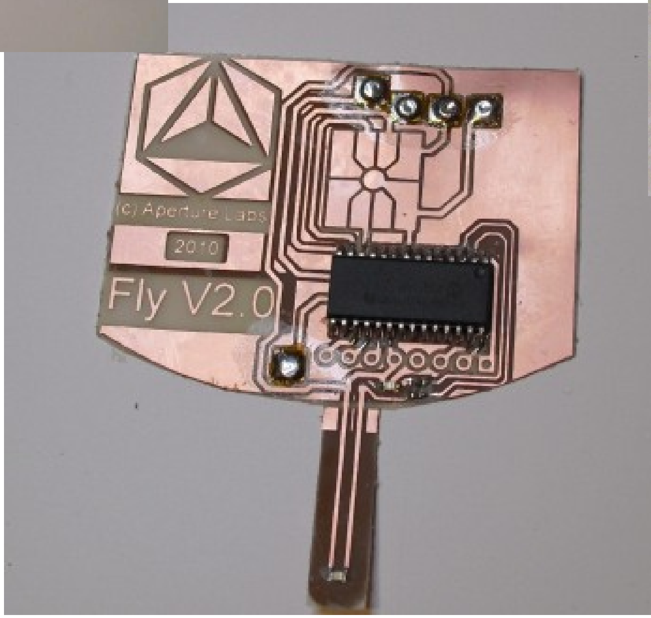
- Offline
  - Terminal request a TC in the GENERATE AC command
  - Card replies with a TC or AAC
- Online
  - Terminal initiated
    - Terminal requests an ARQC and card replies with an ARQC or AAC
  - Card initiated
    - Terminal requests a TC and card replies with an ARQC
  - Terminal forwards ARQC to the issuer and receives an Authorisation Response Code (ARC) in return
  - The ARC is included in in the EXTERNAL AUTHENTICATE or the second GENERATE AC command to authenticate the issuer to the card
  - Card replies with a TC or AAC

Attacking smartcards

- No direct copying possible
- Eavesdropping on communication
  - Existing hardware used for pay TV and SIM cards
- Active / wedge attacks
  - Modifying traffic between card and terminal

Attacking smartcards





Known weaknesses

Skimming

- Data on magnetic stripe also on chip
- Fake e.dentifiers ABN AMRO replaced in branches
  - 2008, 2009
  - 1,5 milion euro damages
  - Download-card

Known weaknesses

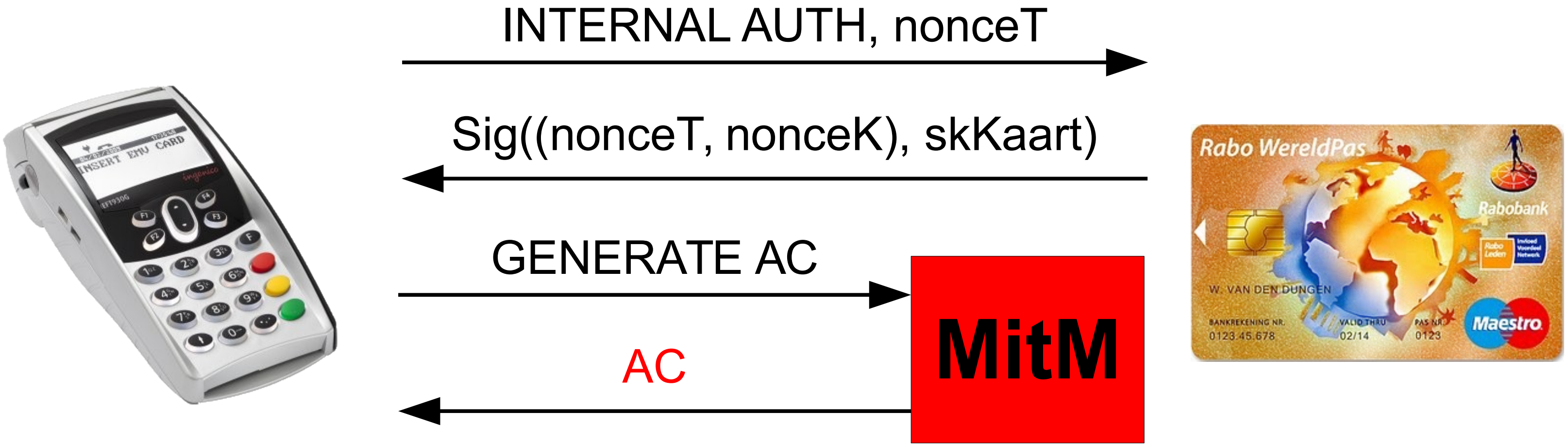
Cloning SDA cards

- Possible for offline transactions
- Only static data authenticated
- Yes-card
  - All PIN codes accepted
- SDA no longer allowed for offline capable cards

Known weaknesses

DDA man-in-the-middle attack

- Possible for offline transactions
- Terminal cannot determine authenticity of a transaction
- Transaction not connected to card authentication



INTERNAL AUTH, nonceT

Sig((nonceT, nonceK), skKaart)

GENERATE AC

AC

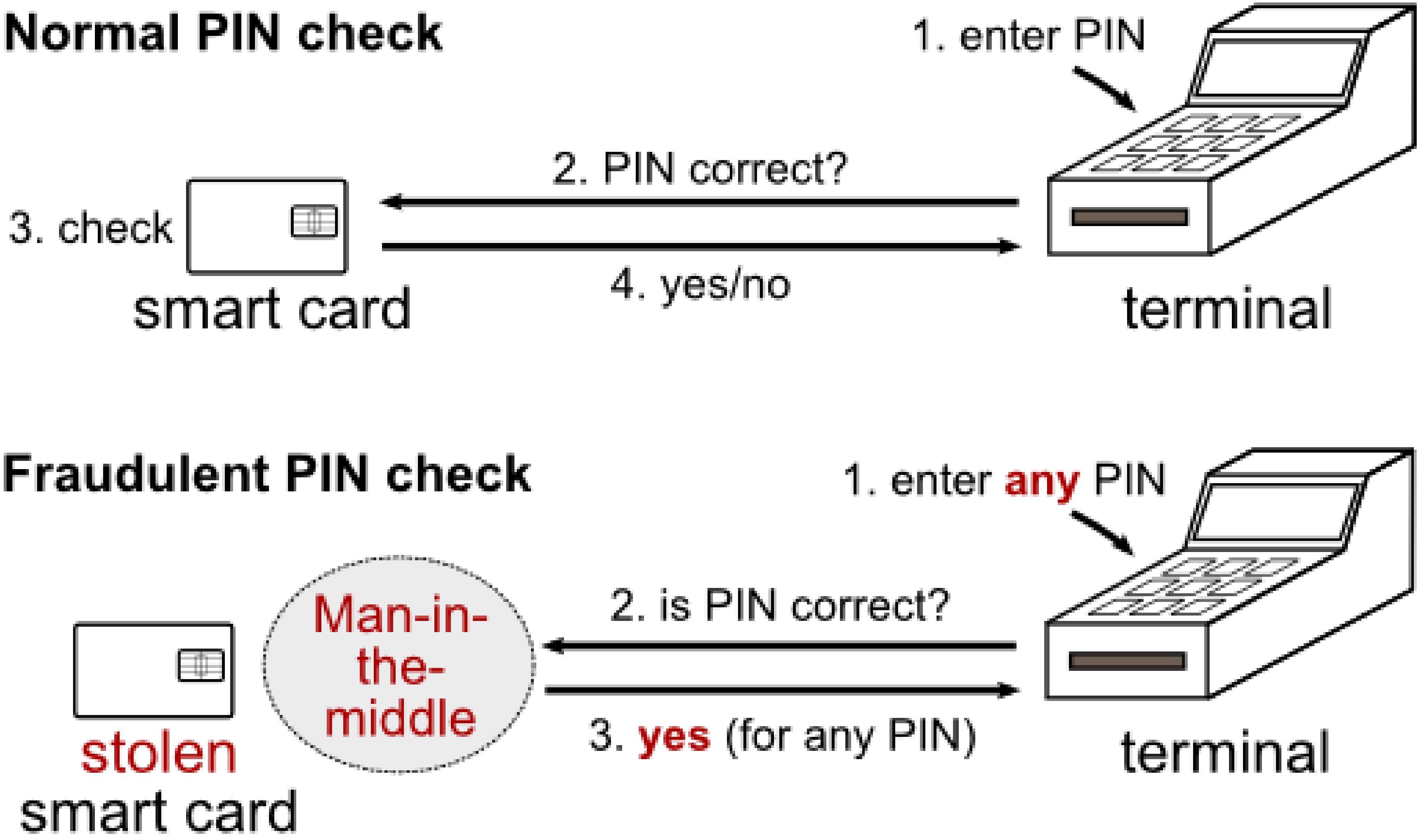
MitM

Known weaknesses

“Chip & PIN is broken” [Murdoch et al. 2010]

- Possible for both offline and online transactions
    - If card is not blocked
    - If transaction without PIN are accepted
- Man-in-the-middle attack
- All PIN codes accepted

Known weaknesses

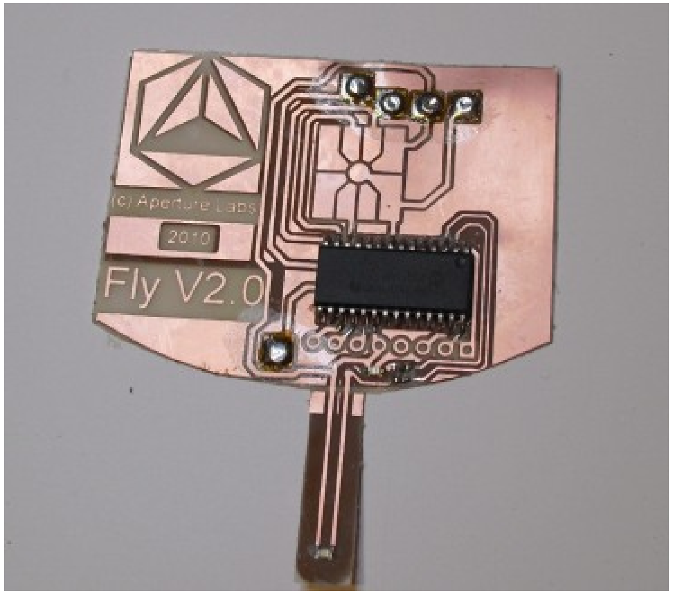


Source: https://www.cl.cam.ac.uk/research/security/banking/nopin/

Known weaknesses

"Chip & PIN is definitely broken" [Barisani et al. 2011]

- Rollback to plaintext PIN by modifying the CVM List
- Possible to perform an online transaction in case of failed data authentication
- Terminals in the Netherlands patched
- Attack was still possible
  - Detected in backend



EMV-Contactless

- 4 books
  - Book A: Architecture and General Requirements
  - Book B: Entry Point
  - Book C: Kernel Specification
  - Book D: Contactless Communication Protocol
- 7 variants for book C
- ISO 14443
- All EMV applications listed in 2PAY.SYS.DDF01

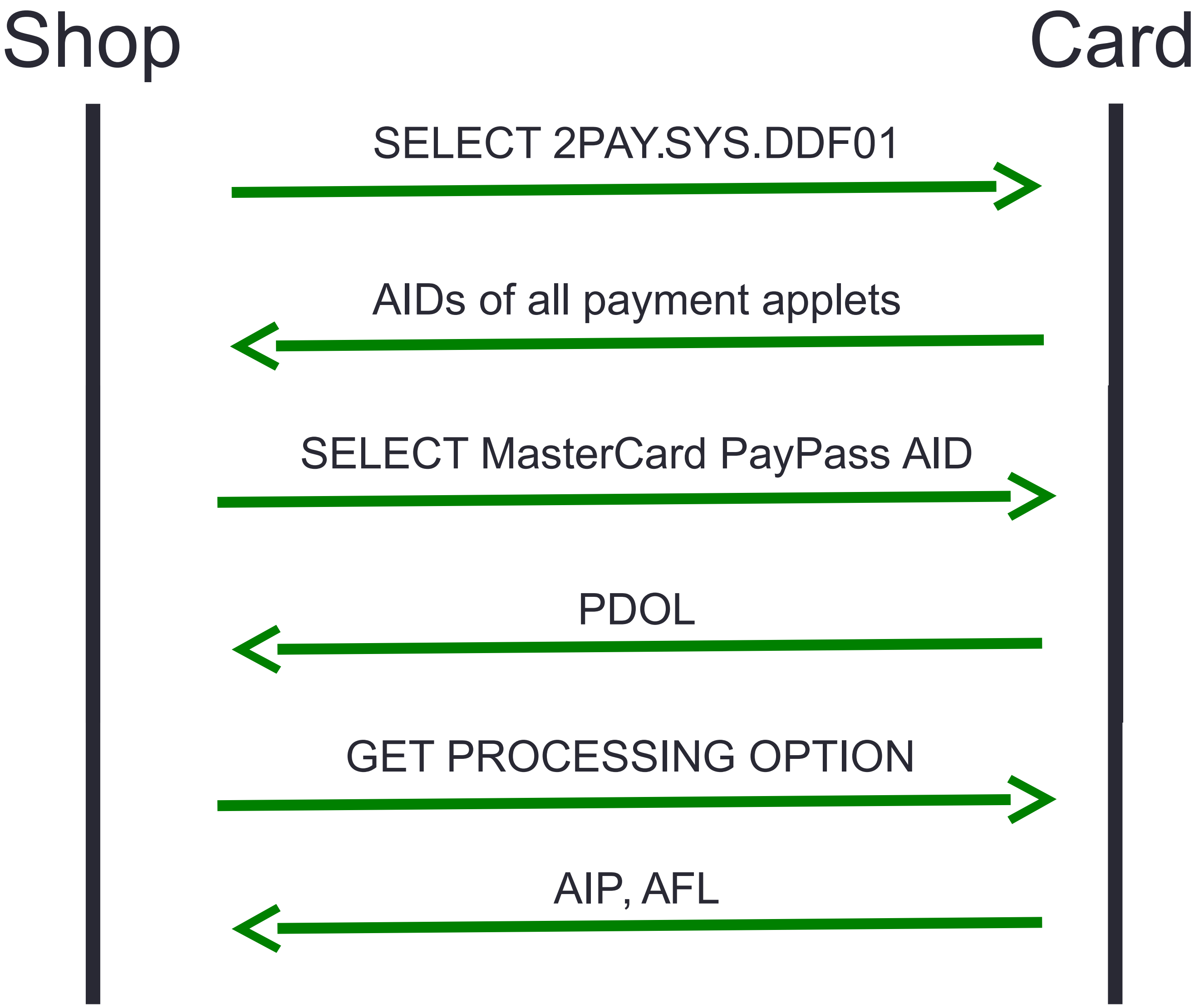
MasterCard PayPass

- Kernel 2
- EMV mode
- Mag-stripe mode

EMV mode

- No DDA
- Only one application cryptogram for online transactions
- Torn transactions can be restored using RECOVER AC command
- Terminal can store data on card in 'scratch pad'

EMV mode



Shop

Card

SELECT 2PAY.SYS.DDF01

AIDs of all payment applets

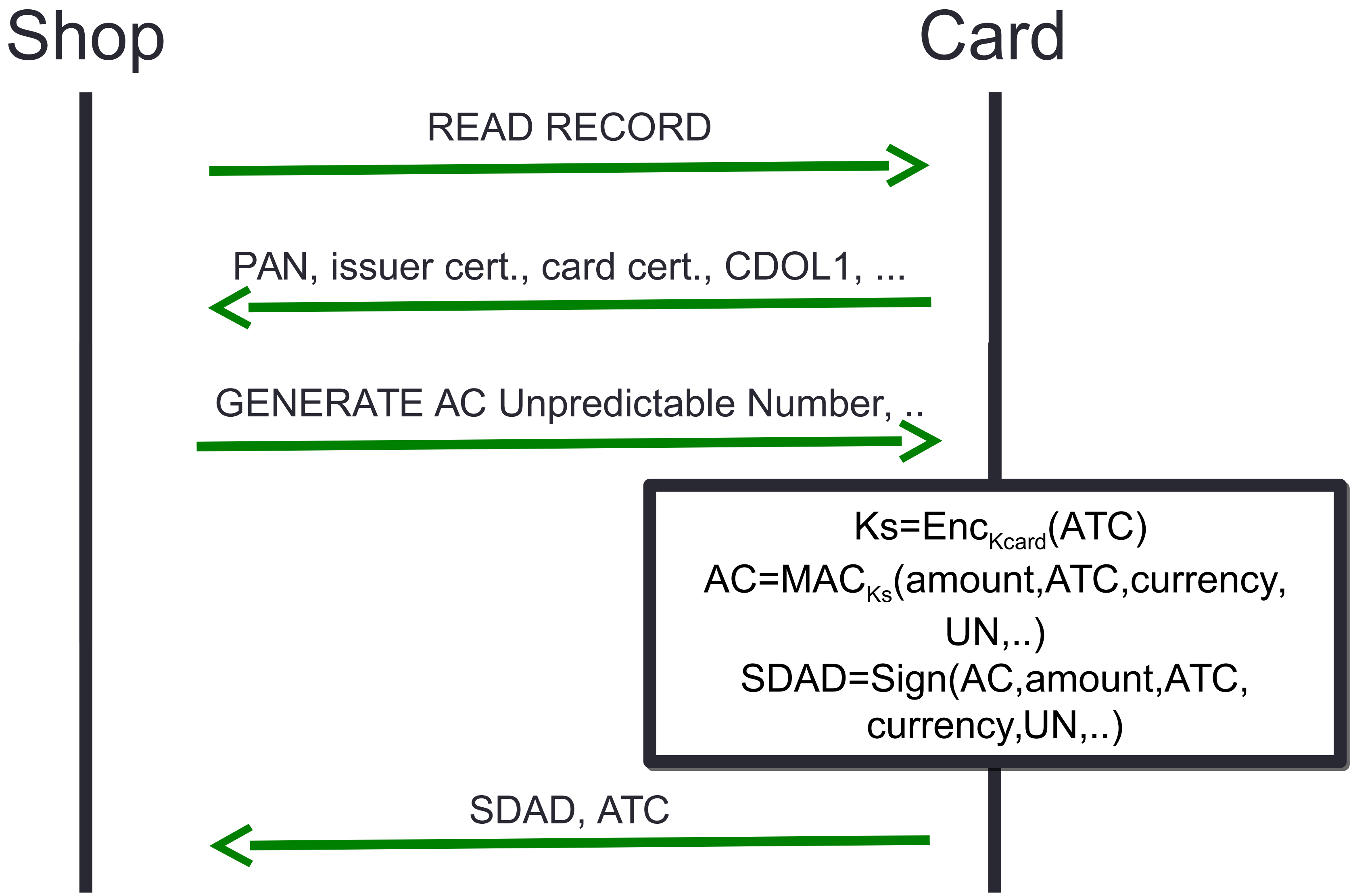
SELECT MasterCard PayPass AID

PDOL

GET PROCESSING OPTION

AIP, AFL

EMV mode



Shop

Card

READ RECORD

PAN, issuer cert., card cert., CDOL1, ...

GENERATE AC Unpredictable Number, ..

$Ks=Enc_{Kcard}(ATC)$

$AC=MAC_{Ks}(amount,ATC,currency, UN,..)$

$SDAD=Sign(AC,amount,ATC, currency,UN,..)$

SDAD, ATC

Mag-stripe mode

- Backwards compatibility for old mag-stripe systems
- COMPUTE CRYPTOGRAPHIC CHECKSUM command to generate CVC3 (Card Verification Code)
- CVC3 based on
  - Unpredictable Number (UN)
  - Application Transaction Counter
  - Secret Key
- CVC3 and UN used to construct valid mag-stripe data

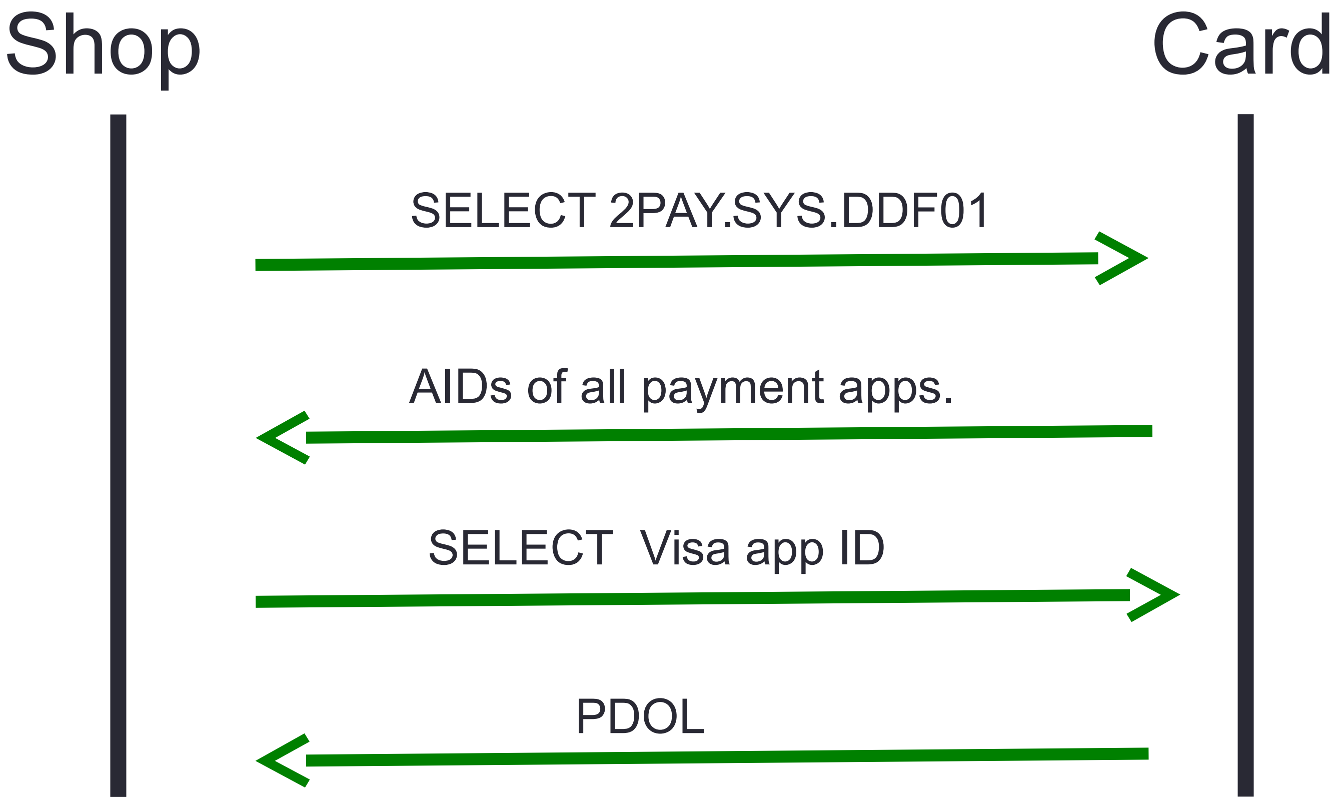
Pre-play attack on mag-stripe mode

- “Cloning Credit Cards: A combined pre-play and downgrade attack on EMV Contactless” [Roland and Langer, 2013]
- Unpredictable Number provided in BCD notation
- Card indicates length of UN
  - 1 to 3 digits in practice
- Fallback possible
  - To mag-stripe mode
  - To shorter UN

Visa payWave

- Kernel 1 and 3
- EMV modes (VSDC and qVSDC)
- Mag-stripe mode (MSD)
- VSDC uses original EMV with minor changes
- qVSDC quite different from original EMV
  - Minimises number of messages
  - fDDA
  - No separate command for cryptogram generation
- No offline plaintext PIN allowed

qVSDC (offline)



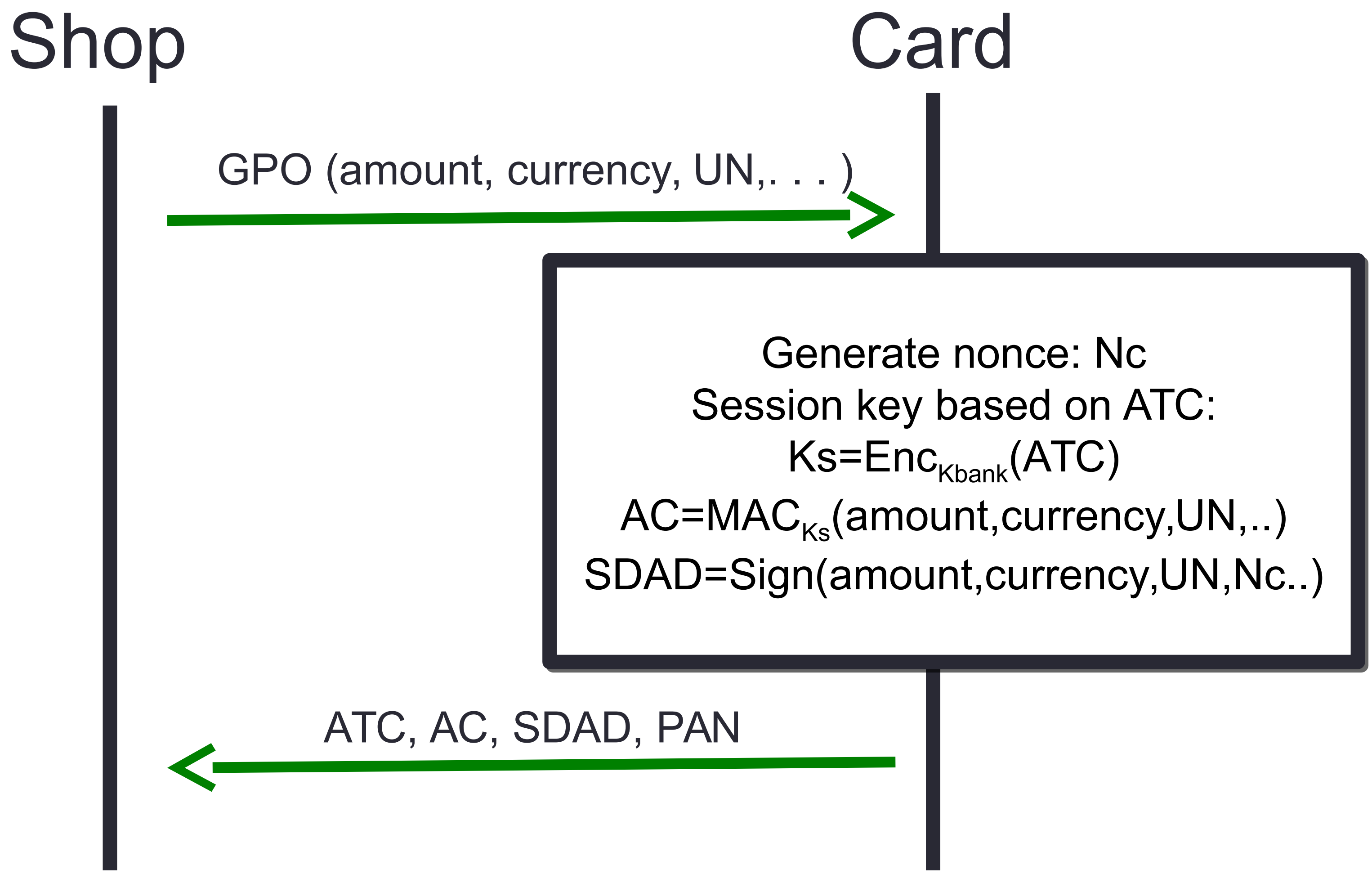
PDOL

```
9F38189F66049F02069F03069F1A0295055F2A029A039C019F37045F
2D02656E9000
```

which parses as:

```
9F38 | len:18    Processing Options Data Object List (PDOL)
    9F66   len:04     Card Production Life Cycle
         9F02   len:06    Amount, Authorised (Numeric)
         9F03   len:06    Amount, Other (Numeric)
         9F1A   len:02    Terminal Country Code
             95   len:05    Terminal Verification Results
         5F2A    len:02   Transaction Currency Code
             9A   len:03   Transaction Date
        9C   len:01    Transaction Type
             9F37   len:04    Unpredictable Number
```

qVSDC (offline)



Shop

Card

GPO (amount, currency, UN,. . .)

Generate nonce: Nc

Session key based on ATC:

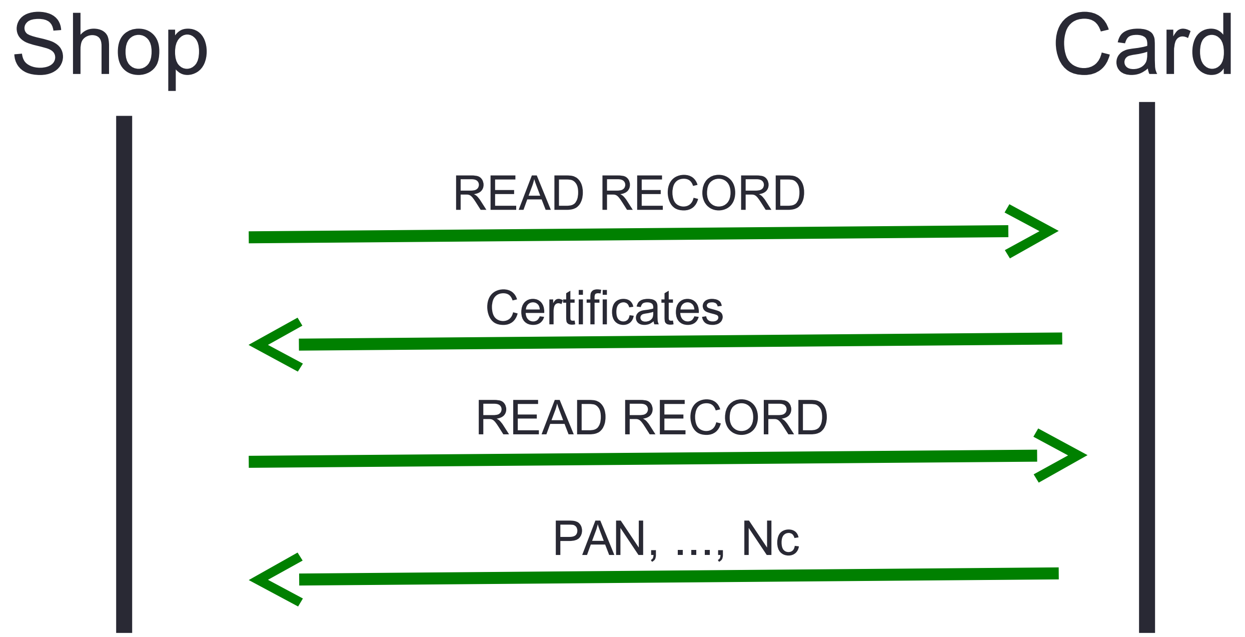
Ks=Enc$_{Kbank}$(ATC)

AC=MAC$_{Ks}$(amount,currency,UN,..)

SDAD=Sign(amount,currency,UN,Nc..)

ATC, AC, SDAD, PAN

qVSDC (offline)



- Shop reader then checks the signature on the SDAD data.
- If this is correct it shop reader accepts the payment and sends the AC to the bank.
- The bank checks the AC and transfers the money.

MSD

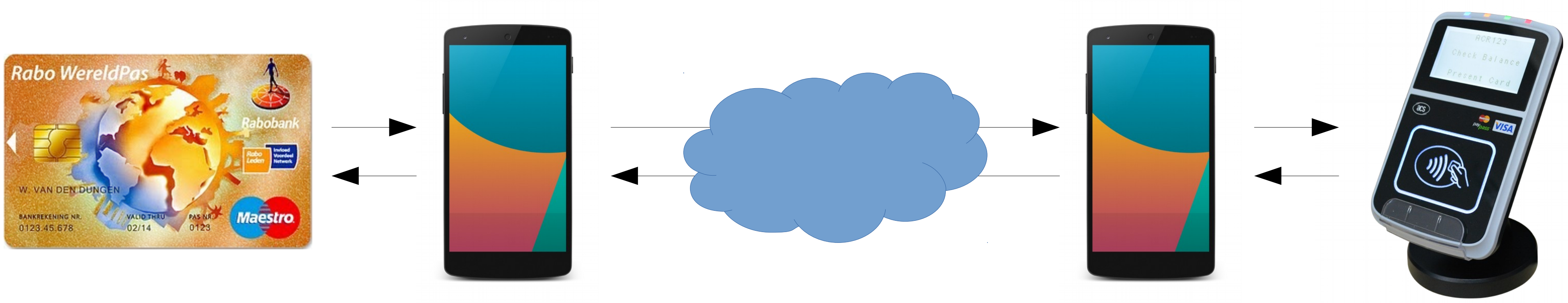
- Mag-stripe data returned in response to GET PROCESSING OPTIONS or READ RECORD command
- Option for dynamic CVV (dCVV)
  - Based on account number and transaction counter

PIN verification

- On certain cards PIN verification still enabled
- Found by Emms et al. and students from Nijmegen
  - "The dangers of verify PIN on contactless cards" [Emms et al. 2012]
- Possible to guess two PIN codes for free
- Or perform denial-of-service attack

Relay attacks

- Reader to interact with victim's card
- Emulator to use at shop's terminal
- Requires good timing
- Demonstrated several times before



Relay attacks

- *Practical NFC peer-to-peer relay attack using mobile phones.*
  - Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis.
  - Proceedings of the 6th International Conference on Radio Frequency Identification: Security and Privacy Issues, RFIDSec'10,

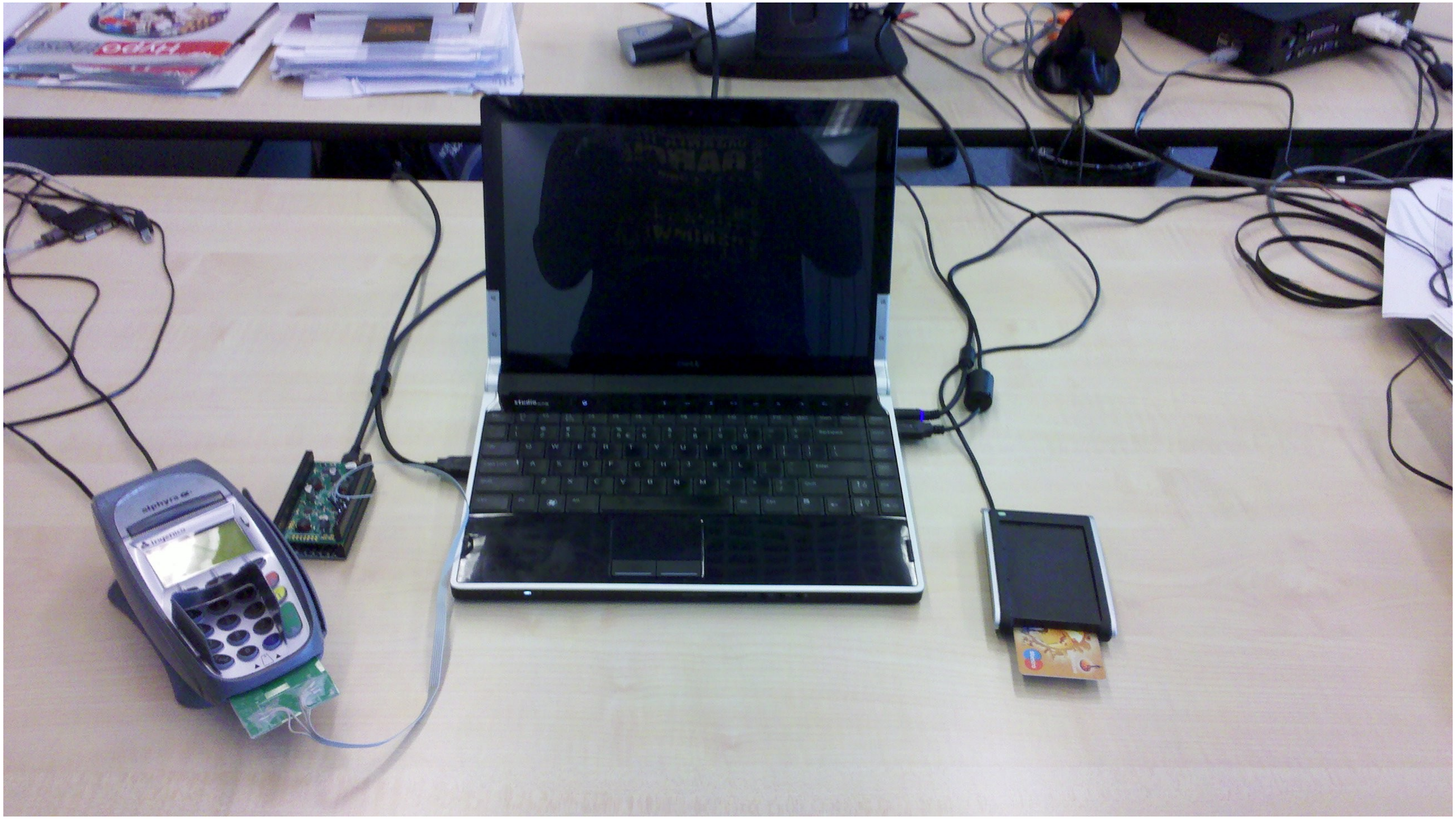
- *The dangers of verify PIN on contactless cards.*
  - M. Emms, B. Arief, T. Defty, J. Hannon, F. Hao, and A. van Moorsel.
  - Technical report. CS-TR-1332.

Relay attacks

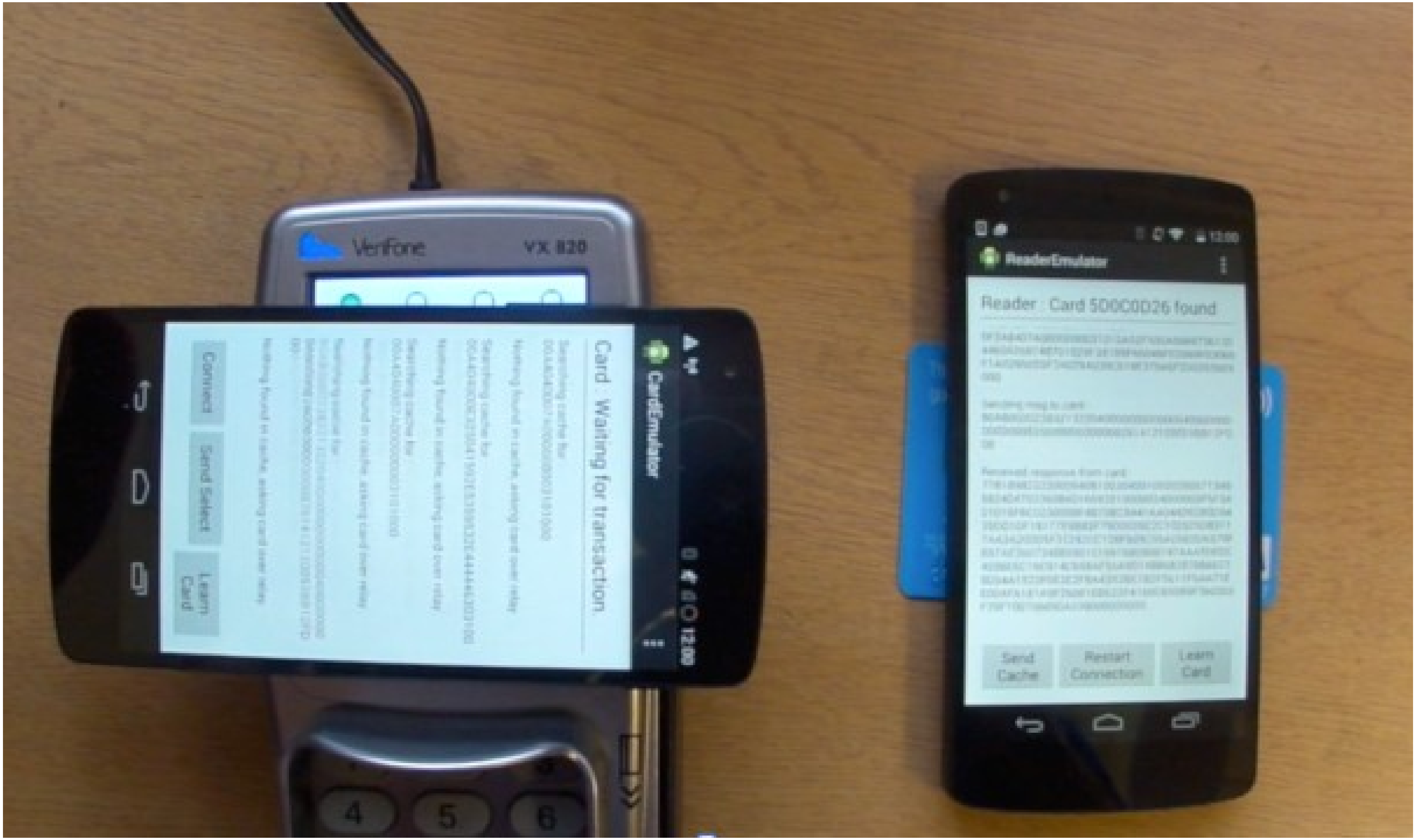
- Two Android devices
  - Before Android 4.4 using CyanogenMod
  - Now using host-based card emulation
- Cheap, easily available, not suspicious
- Students both in Nijmegen en Birmingham
- Relay faster than genuine card using caching (ABN Amro, Dutch)
  - Time for card to complete a purchase: 637ms
  - Time for relay to complete a purchase: 627ms.

Contact relay

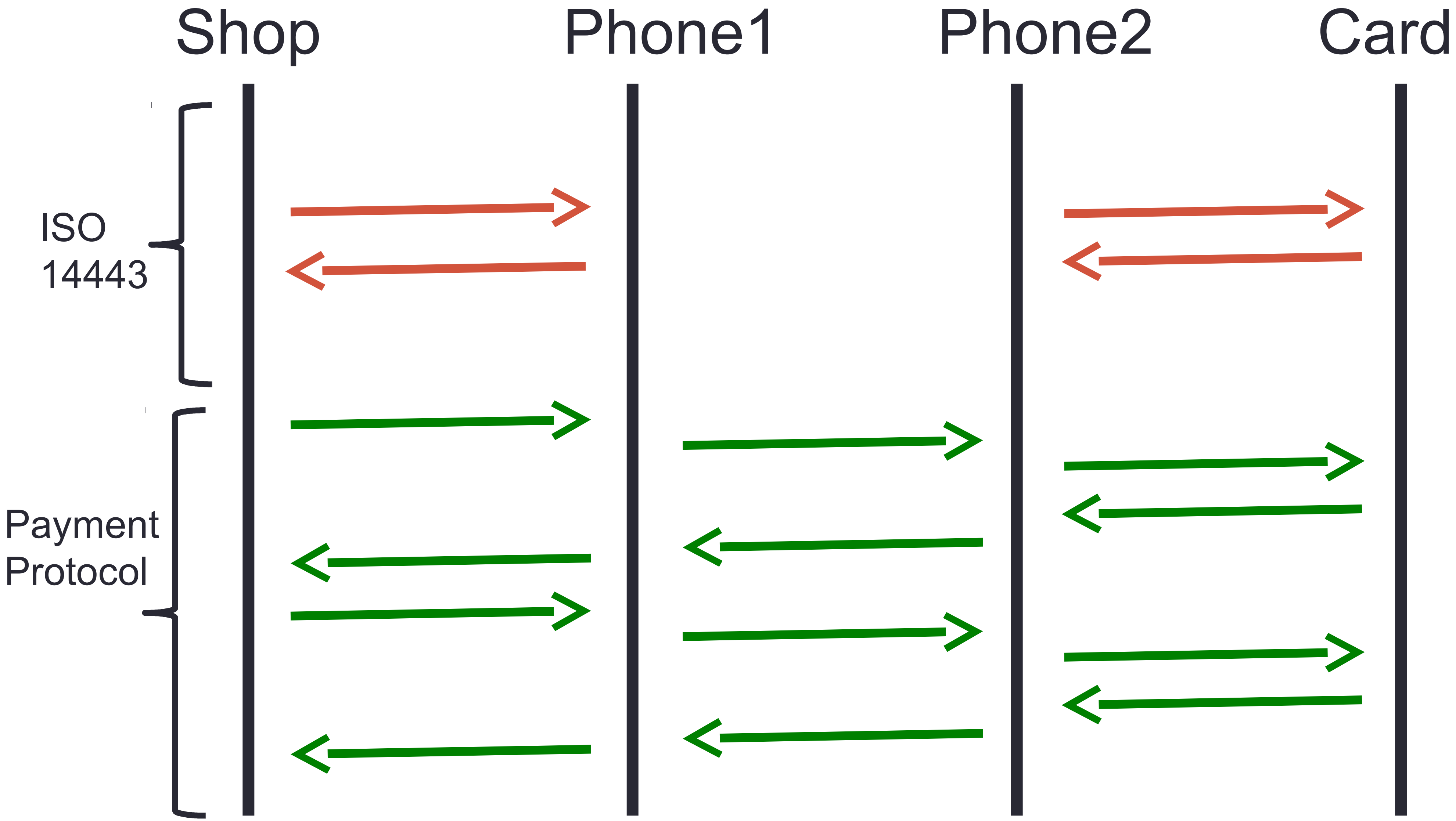
SmartLogic by Gerhard de Koning-Gans

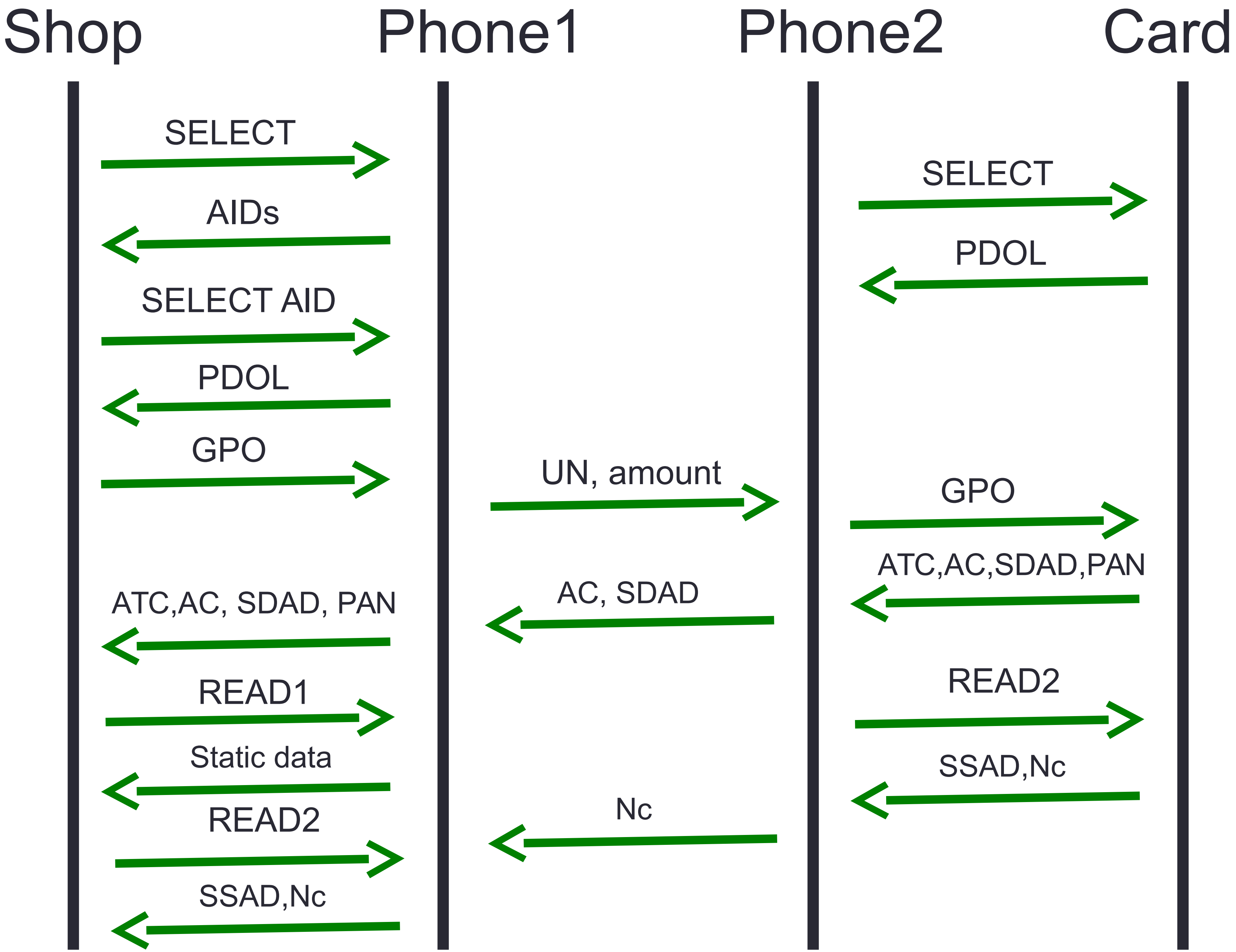


Contactless relay



Relay with phones





Shop

Phone1

Phone2

Card

SELECT

SELECT

AIDs

PDOL

SELECT AID

PDOL

GPO

UN, amount

GPO

ATC,AC,SDAD,PAN

AC, SDAD

ATC,AC, SDAD, PAN

READ2

READ1

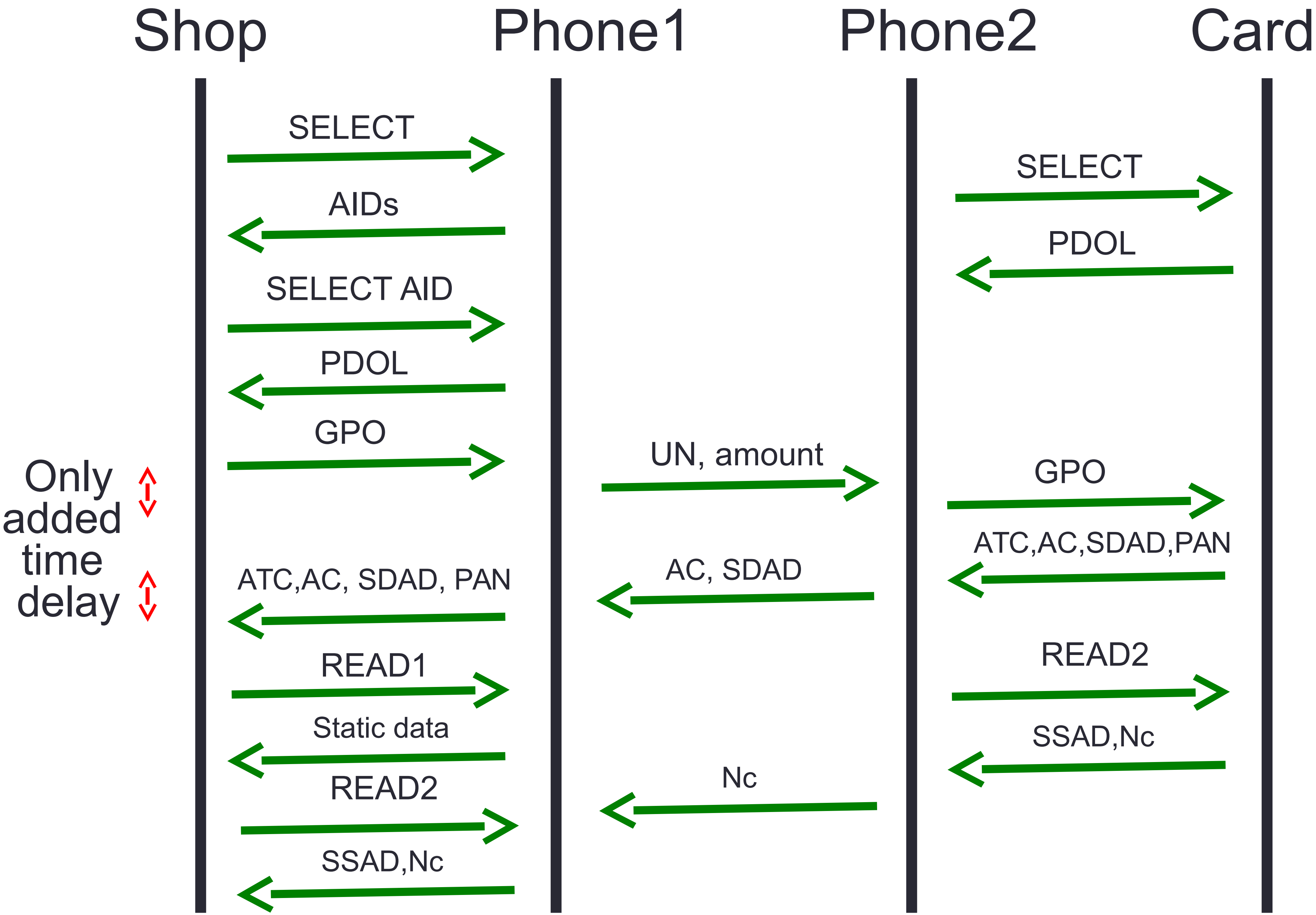
Static data

SSAD,Nc

Nc

READ2

SSAD,Nc



Shop

Phone1

Phone2

Card

SELECT

AIDs

SELECT AID

PDOL

GPO

ATC,AC, SDAD, PAN

READ1

Static data

READ2

SSAD,Nc

UN, amount

AC, SDAD

Nc

SELECT

PDOL

GPO

ATC,AC,SDAD,PAN

READ2

SSAD,Nc

Only added time delay

Demo relay attack

Payment using phones

- Same protocols as before
- Key management on untrusted device
  - Secure element
  - SIM-card
  - Whitebox crypto
- On-device cardholder verification
- EMV tokenisation

Stopping relay attacks

Stopping relays: Idea 1

- Relaying all messages takes over a second.
- The transaction *should* complete in under 500ms.
- Can we stop relay attacks by adding a time out to the reader?

Stopping relays: Idea 2

- Why not just time-bound the important crypto message?
  - GET PROCESSING OPTIONS for Visa’s payWave
  - GENERATE AC for Mastercard’s PayPass

- **Problem**: these are the steps that require the cards to do crypto, which shows more variance than any other messages.
  - Fastest payWave GPO: 105ms
  - Slowest payWave GPO: 364ms

- We were able to relay the fastest response in 208ms.

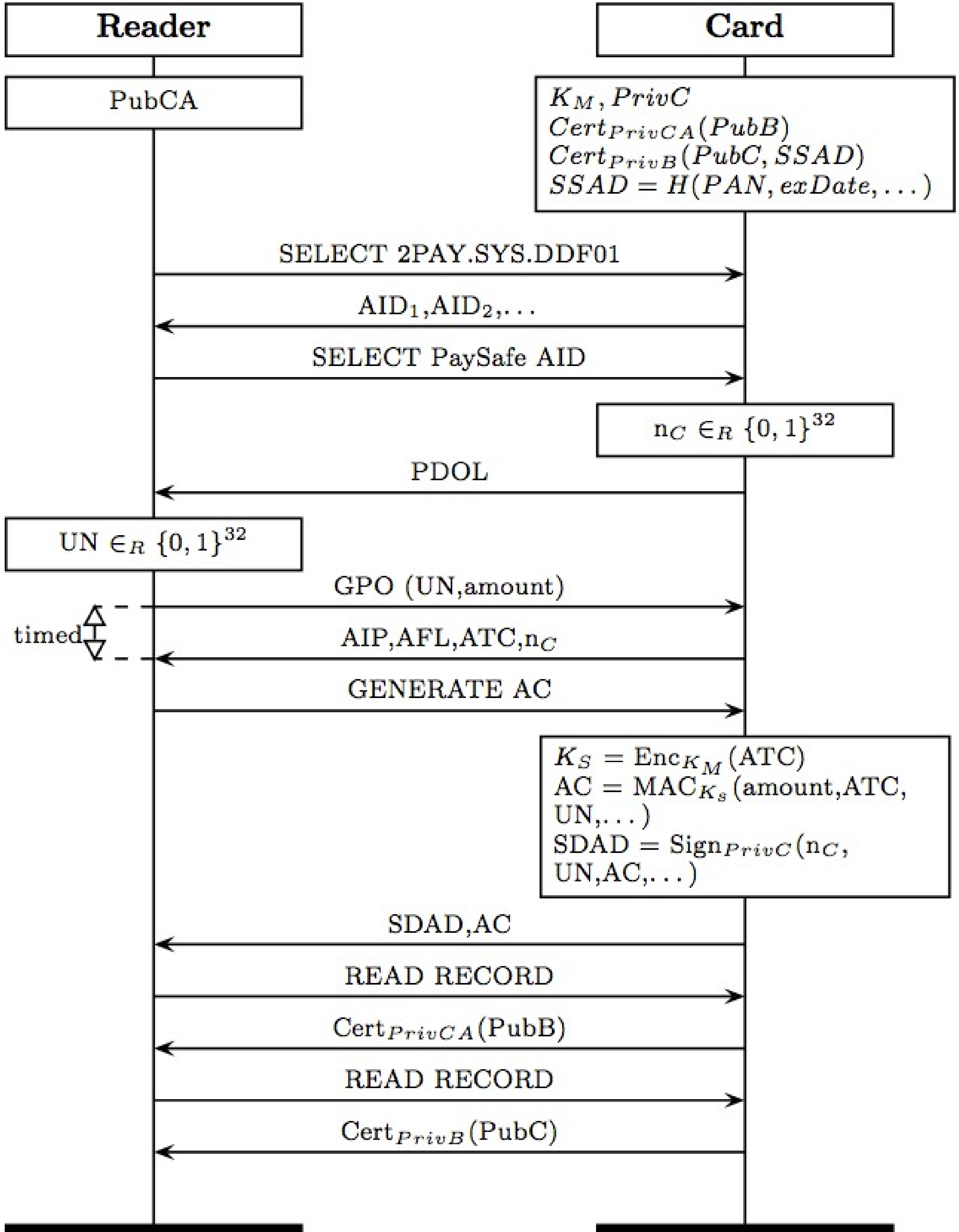
Key Observation Protocol

- The non-crypto messages are predictable and therefore can be time bound.

- But in the current protocols all non-crypto messages can be cached.

- We tweak the protocol, so there is a non-crypto message that can be time-bound.

PaySafe



Reader

Card

PubCA

K_M, $PrivC$
$Cert_{PrivCA}(PubB)$
$Cert_{PrivB}(PubC, SSAD)$
$SSAD = H(PAN, exDate, \ldots)$

SELECT 2PAY.SYS.DDF01

AID_1,AID_2,...

SELECT PaySafe AID

$\mathrm{n}_C \in_R \{0,1\}^{32}$

PDOL

$\mathrm{UN} \in_R \{0,1\}^{32}$

GPO (UN,amount)

timed

AIP,AFL,ATC,n_C

GENERATE AC

$K_S = \mathrm{Enc}_{K_M}(\mathrm{ATC})$
$\mathrm{AC} = \mathrm{MAC}_{K_s}(\mathrm{amount,ATC,}$
$\mathrm{UN},\ldots)$
$\mathrm{SDAD} = \mathrm{Sign}_{PrivC}(\mathrm{n}_C,$
$\mathrm{UN,AC},\ldots)$

SDAD,AC

READ RECORD

$\mathrm{Cert}_{PrivCA}(\mathrm{PubB})$

READ RECORD

$\mathrm{Cert}_{PrivB}(\mathrm{PubC})$

PaySafe Timing

- Time for cards to respond to a message of this length = 28 to 36ms.

- Time to relay a message of this length: 100ms

- So the reader will time out after 80ms.

- No phone or USB reader will be able to relay this message.

- Faster purpose build hardware costs tens of thousands of dollars.

Thanks for your attention!