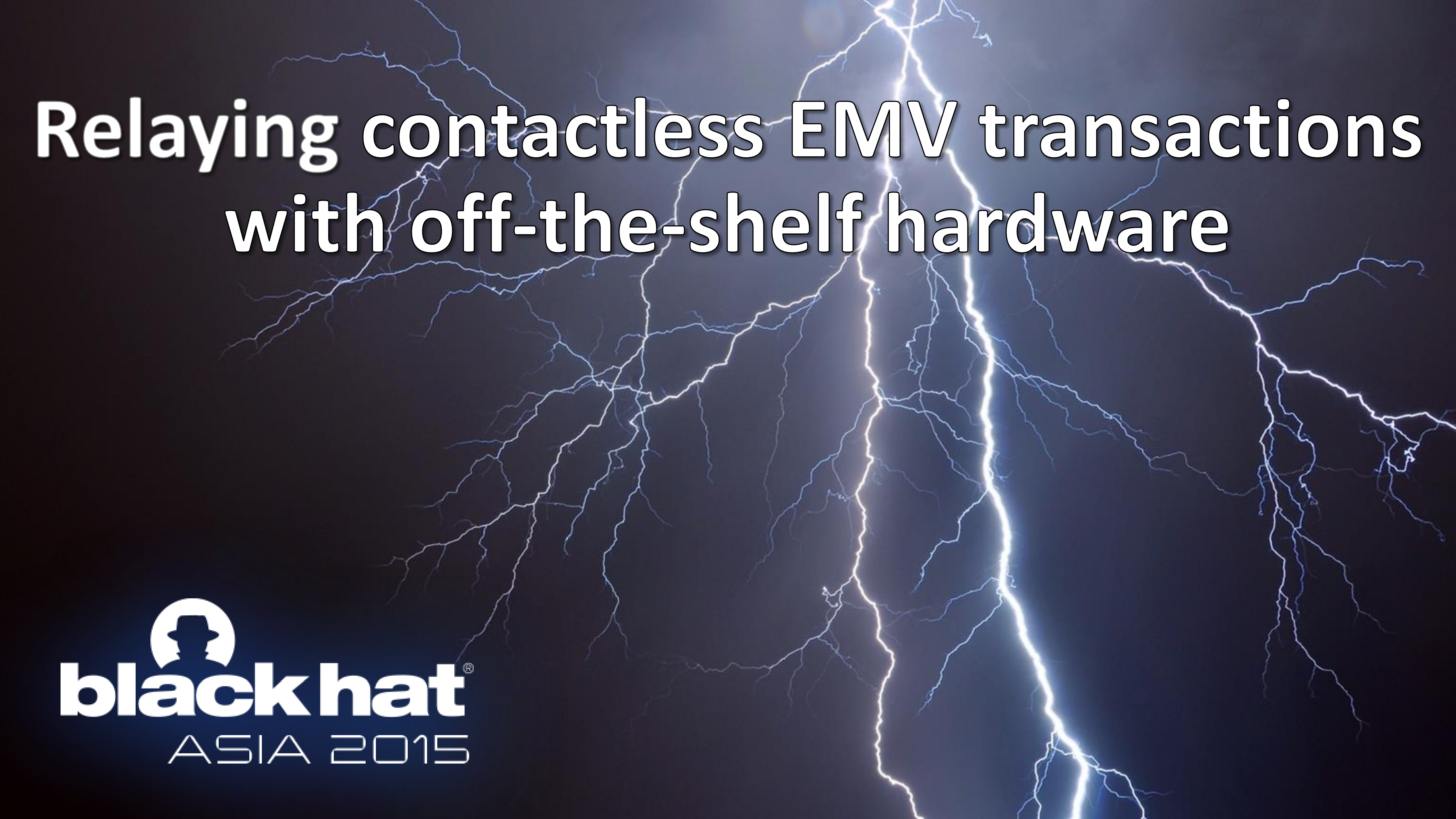


Relaying contactless EMV transactions with off-the-shelf hardware

black hat
ASIA 2015

Something about me

- Jordi van den Breekel (NL)
- Graduation project (2014)
- Security consultant KPMG the Netherlands

KPMG

TU/e Technische Universiteit Eindhoven University of Technology

Dr. Nicola Zannone

Radboud University Nijmegen

Dr. Erik Poll
Dr. Joeri de Ruiter

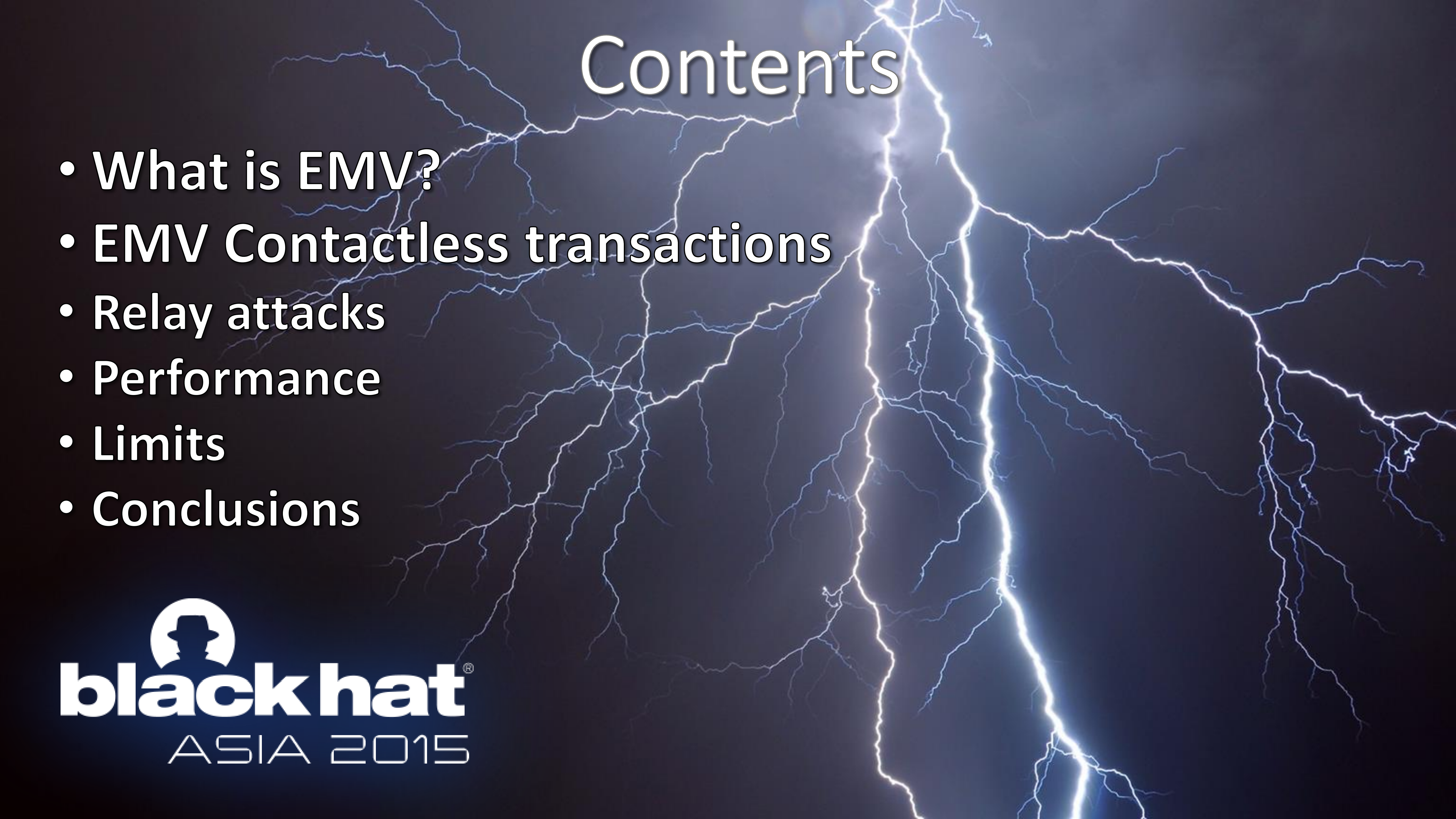
KPMG

Msc. Stan Hegt
Msc. Thijs Timmerman

black hat® ASIA 2015

Contents

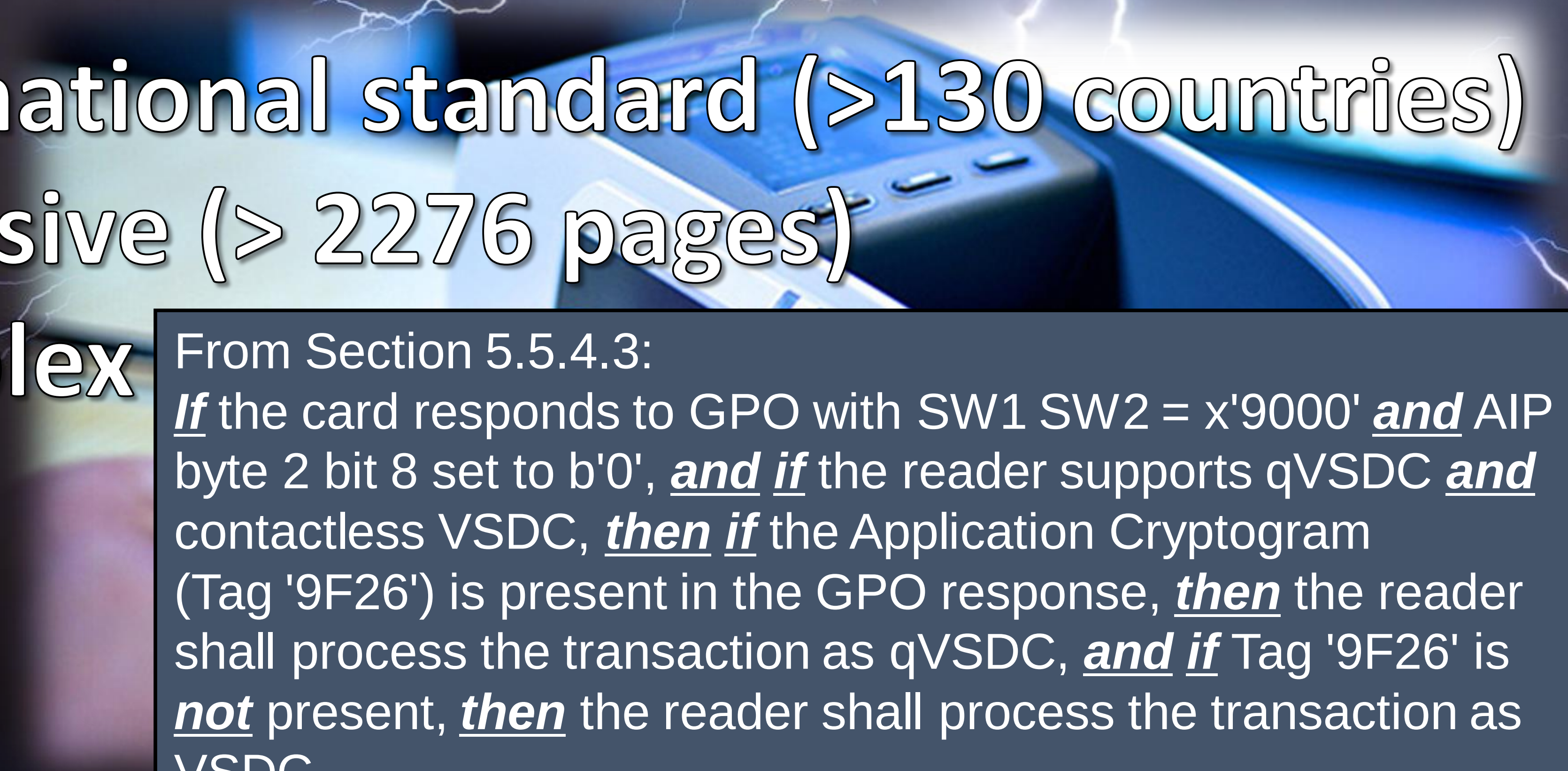
- What is EMV?
- EMV Contactless transactions
- Relay attacks
- Performance
- Limits
- Conclusions



What is EMV?

Europay
Mastercard
Visa

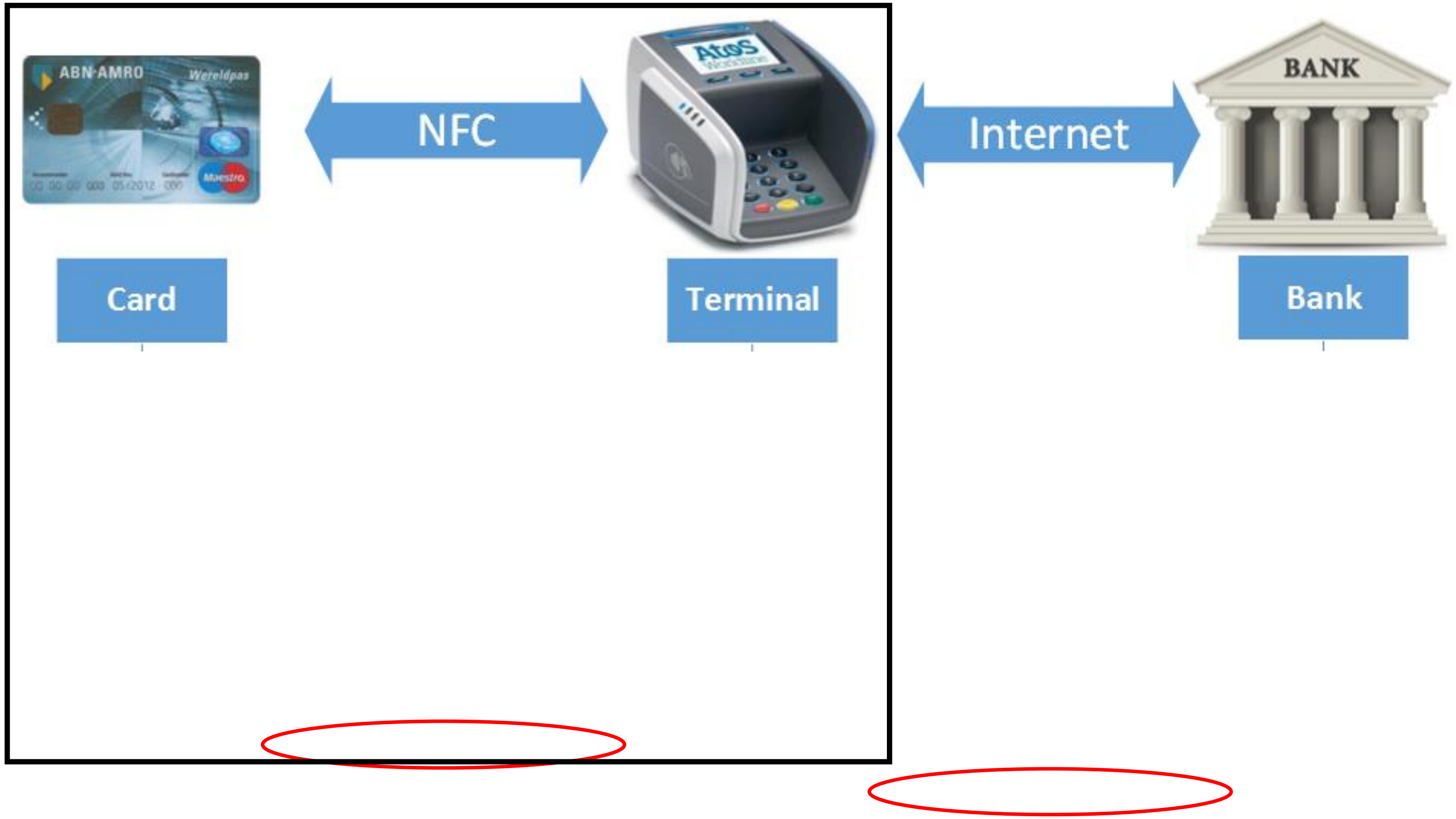
What is EMV?

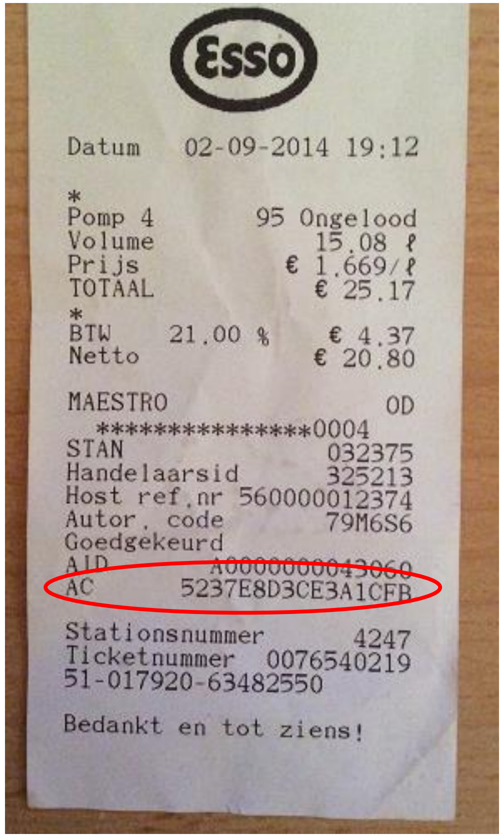


- International standard (>130 countries)
- Extensive (> 2276 pages)
- Complex

From Section 5.5.4.3:
If the card responds to GPO with SW1 SW2 = x'9000' ***and*** AIP byte 2 bit 8 set to b'0', ***and if*** the reader supports qVSDC ***and*** contactless VSDC, ***then if*** the Application Cryptogram (Tag '9F26') is present in the GPO response, ***then*** the reader shall process the transaction as qVSDC, ***and if*** Tag '9F26' is ***not*** present, ***then*** the reader shall process the transaction as VSDC.

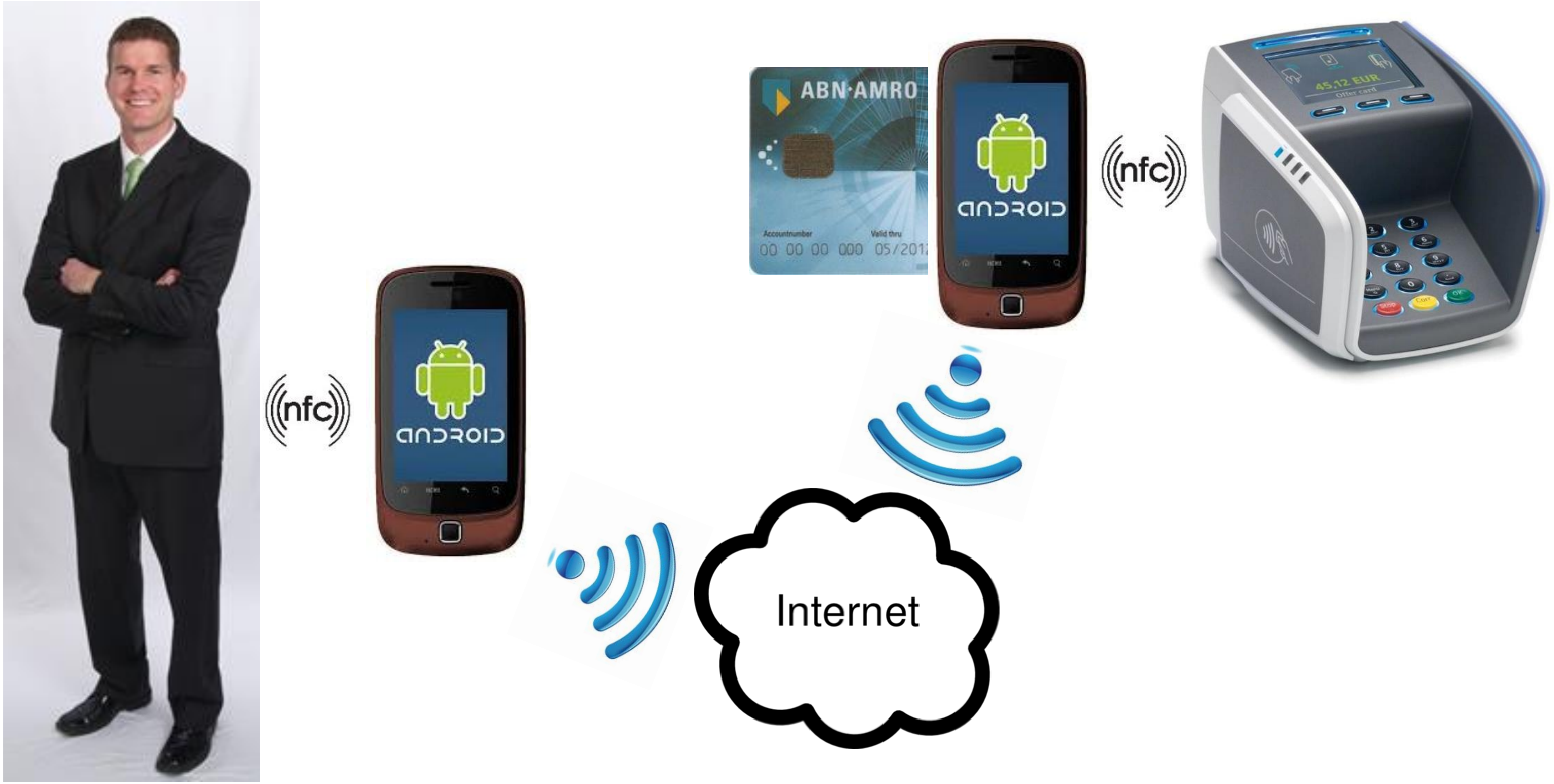
EMV Contactless transaction



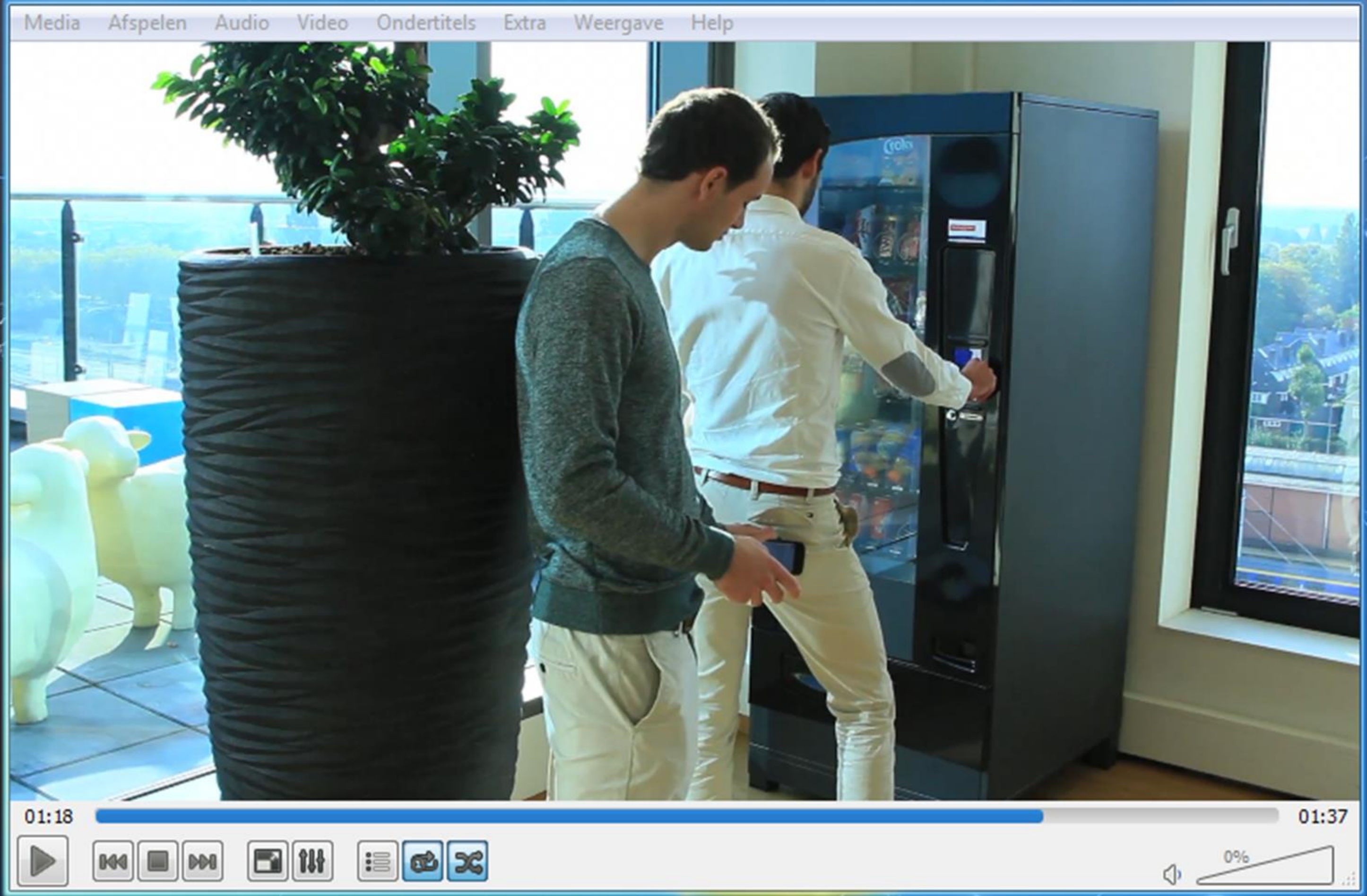


```
Esso

Datum    02-09-2014 19:12

*
Pomp 4           95 Ongelood
Volume               15.08 ℓ
Prijs              € 1.669/ℓ
TOTAAL               € 25.17
*
BTW     21.00 %       € 4.37
Netto                € 20.80

MAESTRO                   OD
  ***************0004
STAN                  032375
Handelaarsid          325213
Host ref.nr 560000012374
Autor. code           79M6S6
Goedgekeurd
AID           A0000000043060
AC              5237E8D3CE3A1CFB

Stationsnummer          4247
Ticketnummer      0076540219
51-017920-63482550

Bedankt en tot ziens!
```

Relay attack scenario



Relay attack demonstration

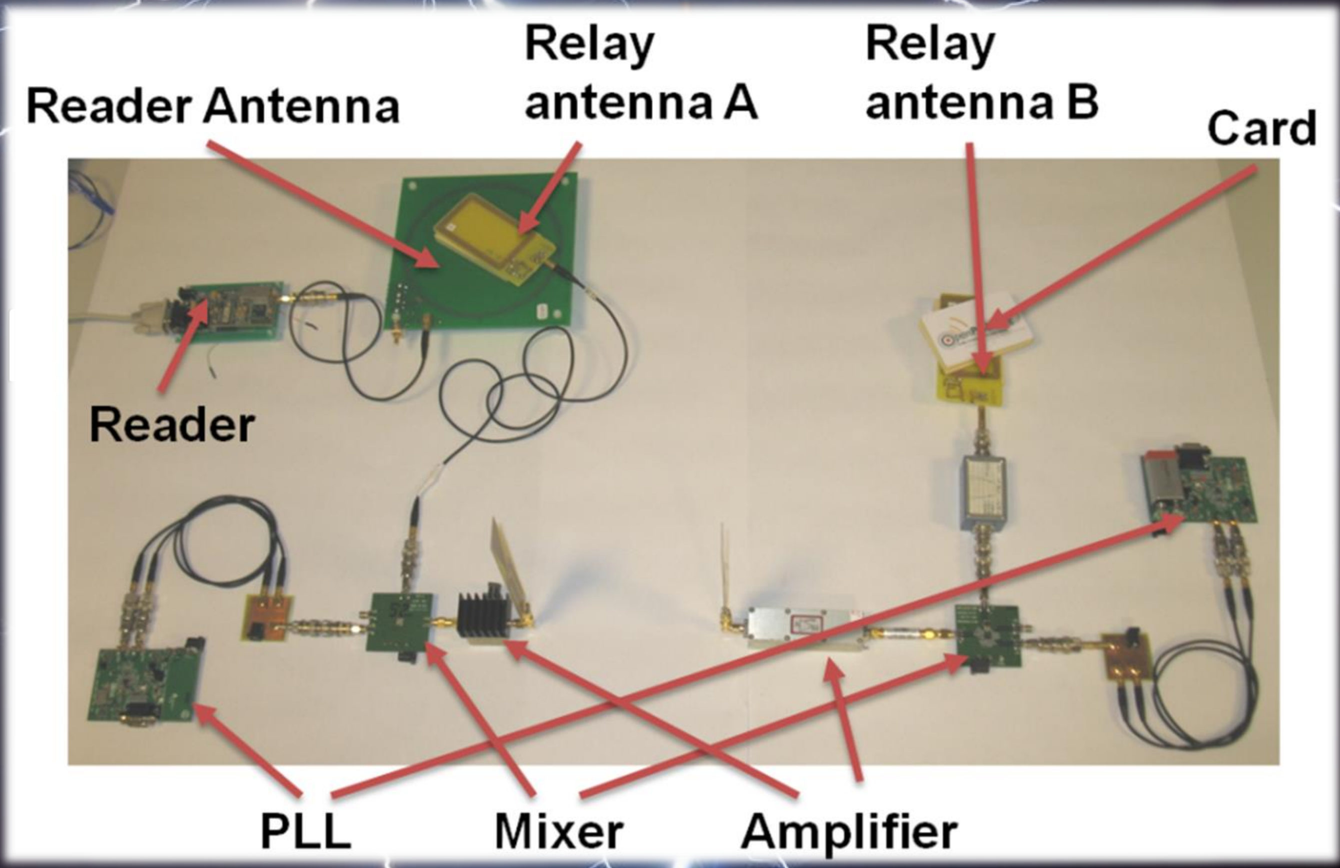


black hat® ASIA 2015

Developments of relay attacks on EMV

- Relay attacks are not new
  - On EMV Contact (2005)
  - On NFC
    - Special hardware
    - Unlocked SE (e.g.
    - Modified Android

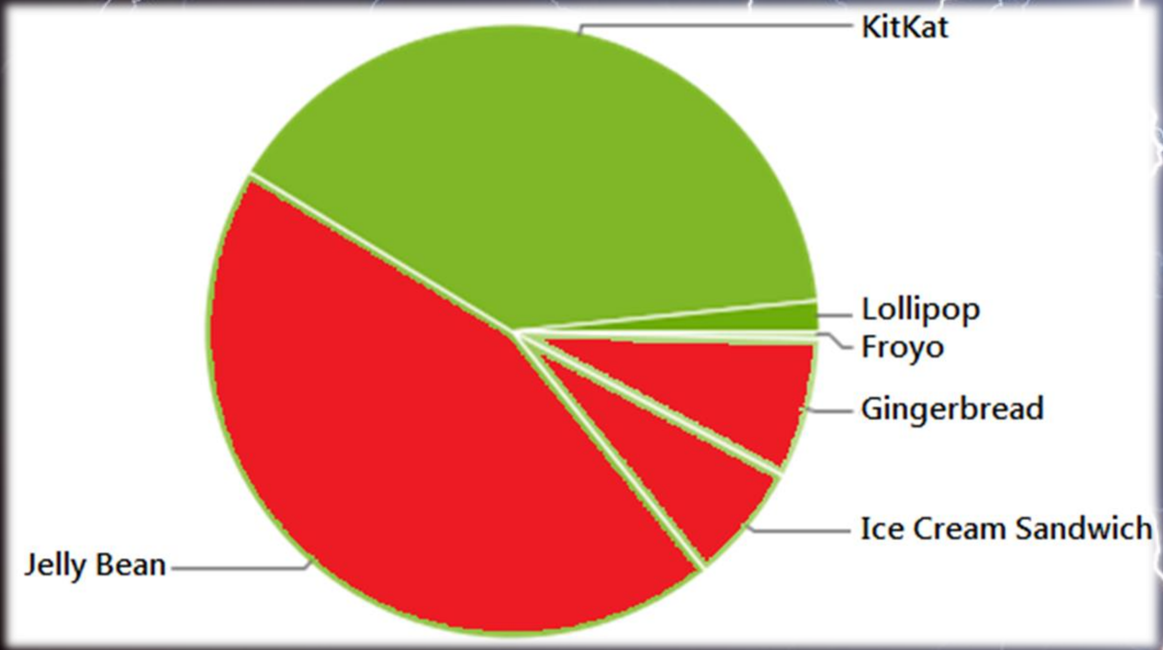
cyanogen(mod)



THERE'S AN APP FOR THAT

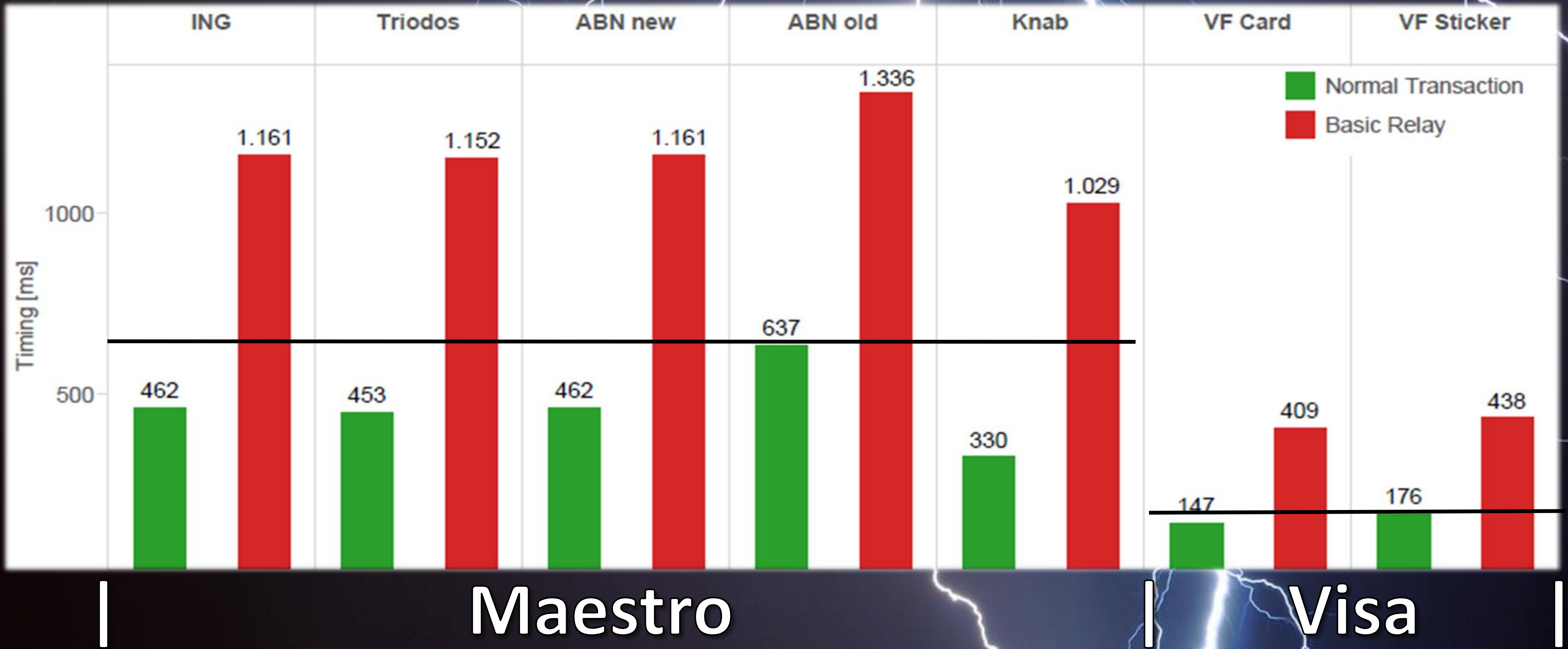
Android 4.4

- Host Card Emulation
- Adoption rate 2015: 41.3%+

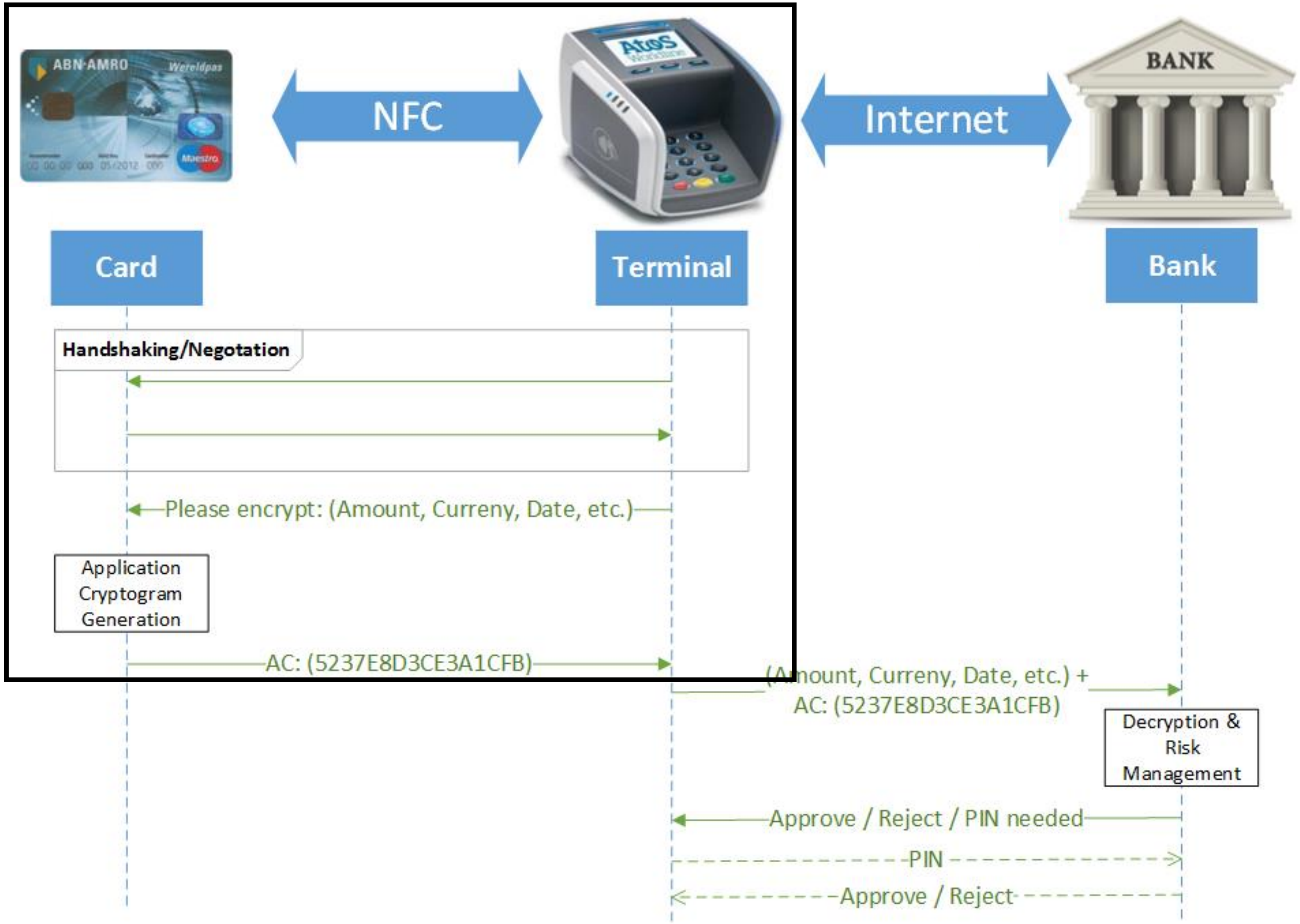


Performance

- Typical Dutch transactions : 330ms – 637ms
- Basic relay transactions: 1152ms – 1336ms
- Max allowed transaction time: 52 <u>seconds</u>



EMV Contactless transaction



NFC

Internet

Card

Terminal

Bank

Handshaking/Negotation

Please encrypt: (Amount, Curreny, Date, etc.)

Application Cryptogram Generation

AC: (5237E8D3CE3A1CFB)

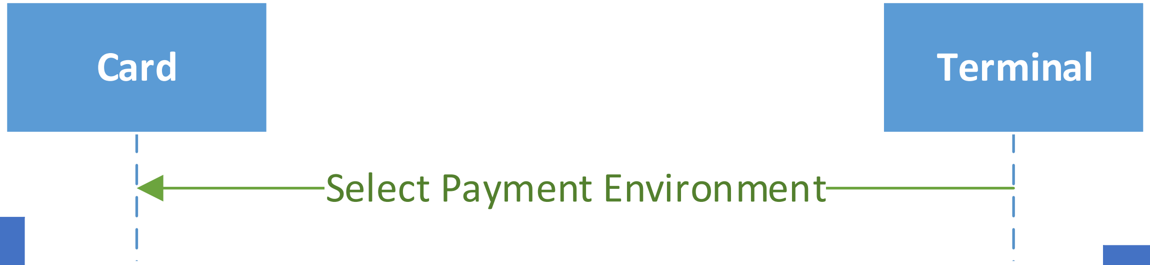
(Amount, Curreny, Date, etc.) + AC: (5237E8D3CE3A1CFB)

Decryption & Risk Management

Approve / Reject / PIN needed

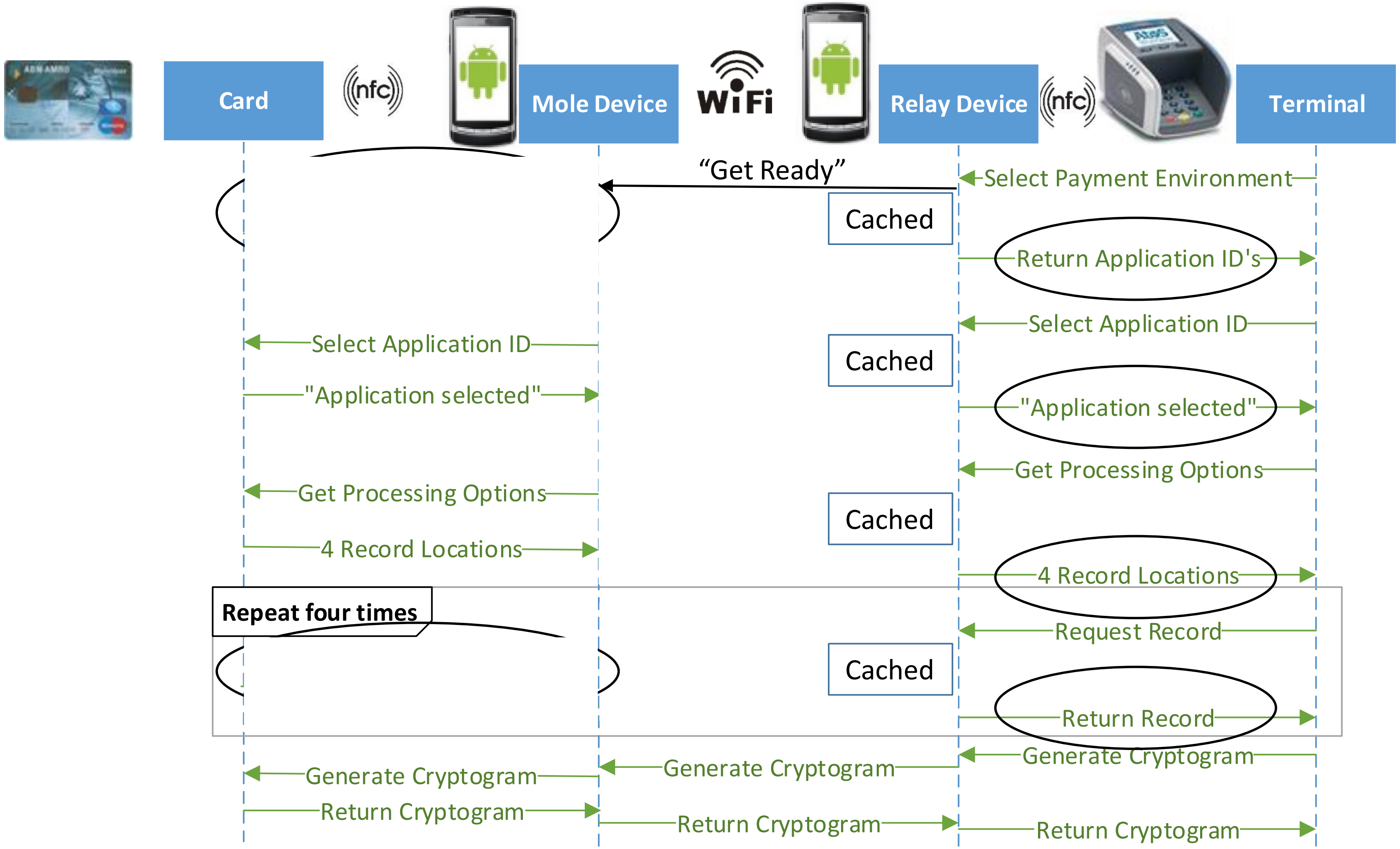
PIN

Approve / Reject



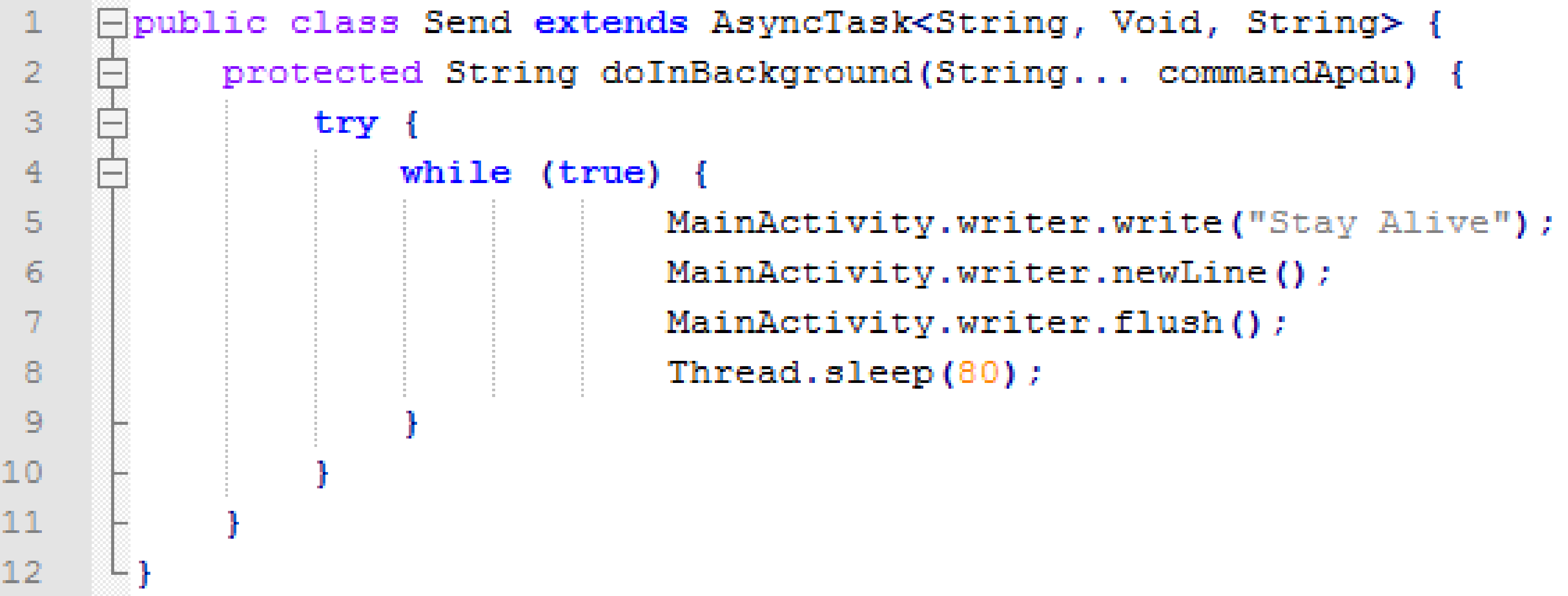
Application ID	Application name	Priority
A0000032010	Visa Electron	1
A0000032020	Visa V Pay	2

Application ID	Application name
A0000004306	Maestro
A0000032020	Visa V Pay
A0000002501	American Express

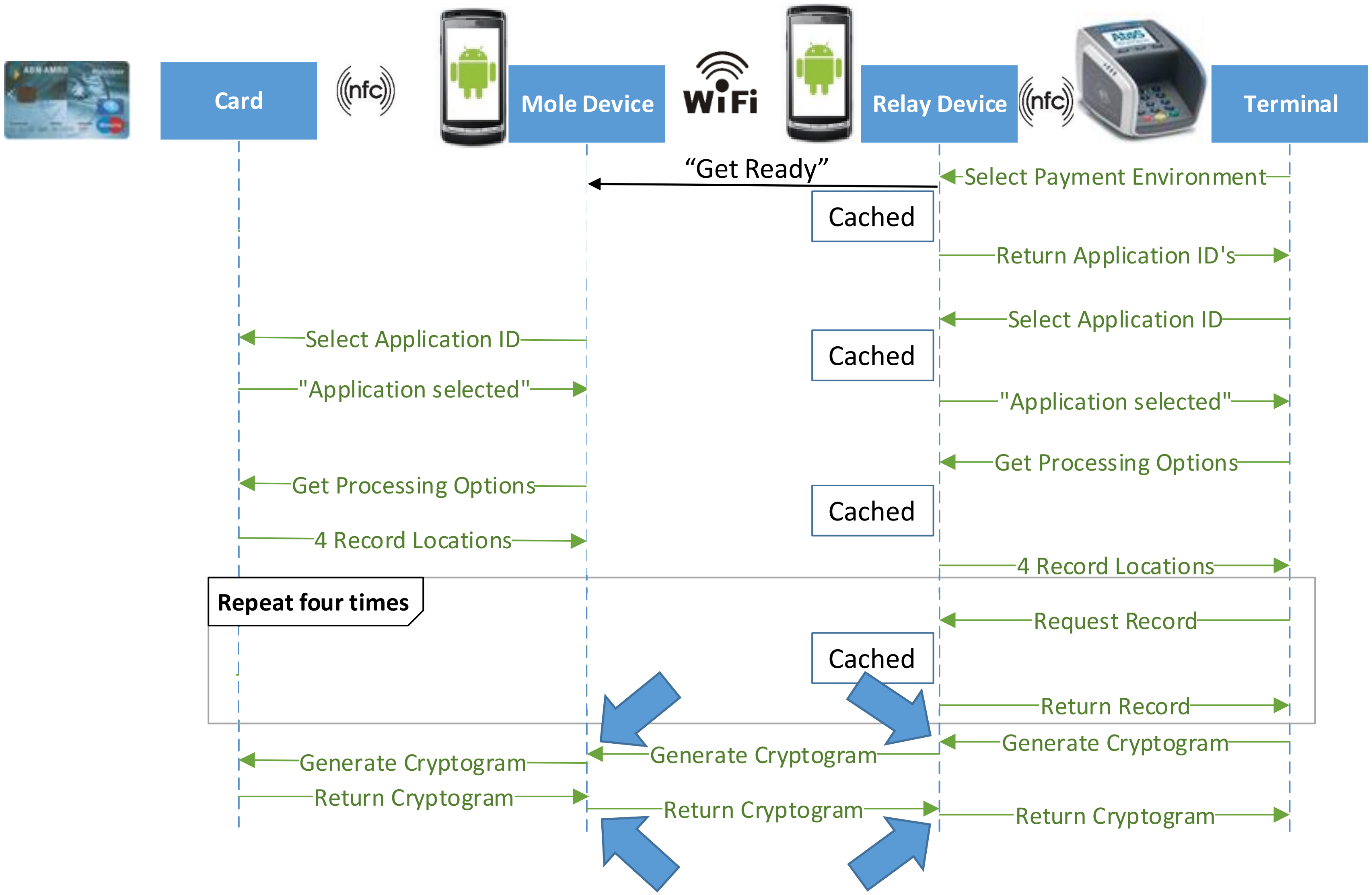

Card
Mole Device
Relay Device
Terminal
WiFi
(nfc)
(nfc)
"Get Ready"
Select Payment Environment
Cached
Return Application ID's
Select Application ID
Select Application ID
Cached
"Application selected"
"Application selected"
Get Processing Options
Get Processing Options
Cached
4 Record Locations
4 Record Locations
Repeat four times
Request Record
Cached
Return Record
Generate Cryptogram
Generate Cryptogram
Generate Cryptogram
Return Cryptogram
Return Cryptogram
Return Cryptogram

Android’s power savings function

- Network adapter
  - After 100ms of inactivity
  - Adds ± 40ms additional delay
- Implement ‘keep-alive’ function



```java
public class Send extends AsyncTask<String, Void, String> {
    protected String doInBackground(String... commandApdu) {
        try {
            while (true) {
                        MainActivity.writer.write("Stay Alive");
                        MainActivity.writer.newLine();
                        MainActivity.writer.flush();
                        Thread.sleep(80);
            }
        }
    }
}
```



Card

Mole Device

Relay Device

Terminal

“Get Ready”

Select Payment Environment

Cached

Return Application ID's

Select Application ID

Select Application ID

Cached

"Application selected"

"Application selected"

Get Processing Options

Get Processing Options

Cached

4 Record Locations

4 Record Locations

Repeat four times

Request Record

Cached

Return Record

Generate Cryptogram

Generate Cryptogram

Generate Cryptogram

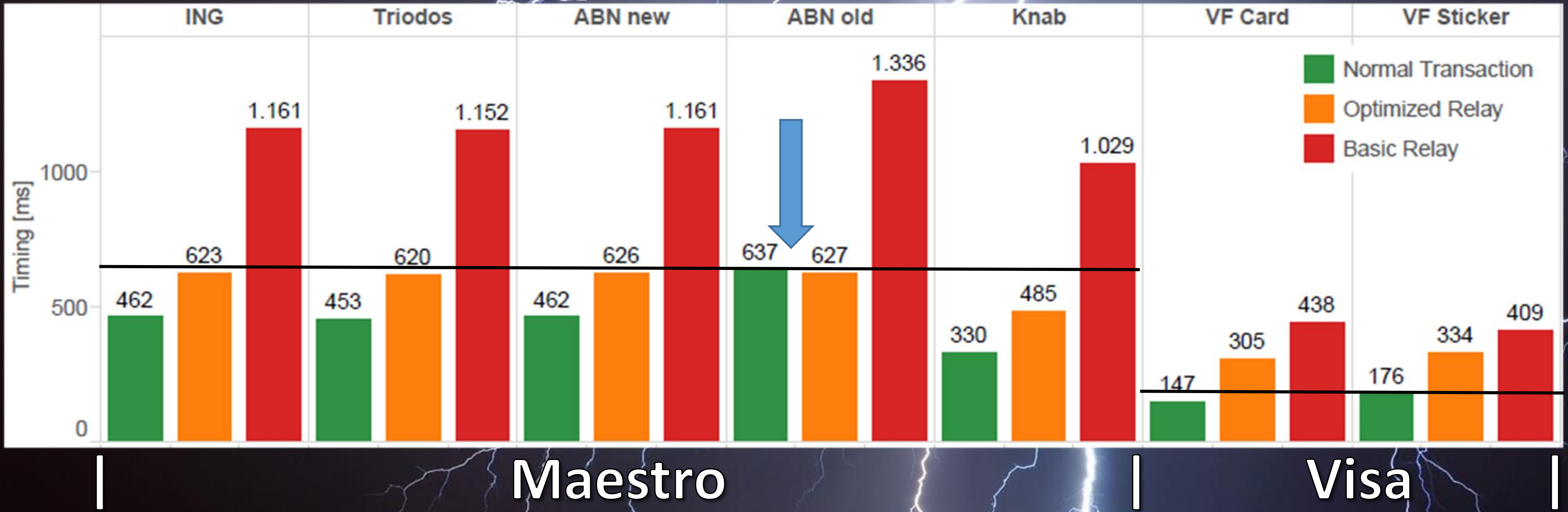
Return Cryptogram

Return Cryptogram

Return Cryptogram

Reduction: ± 160ms

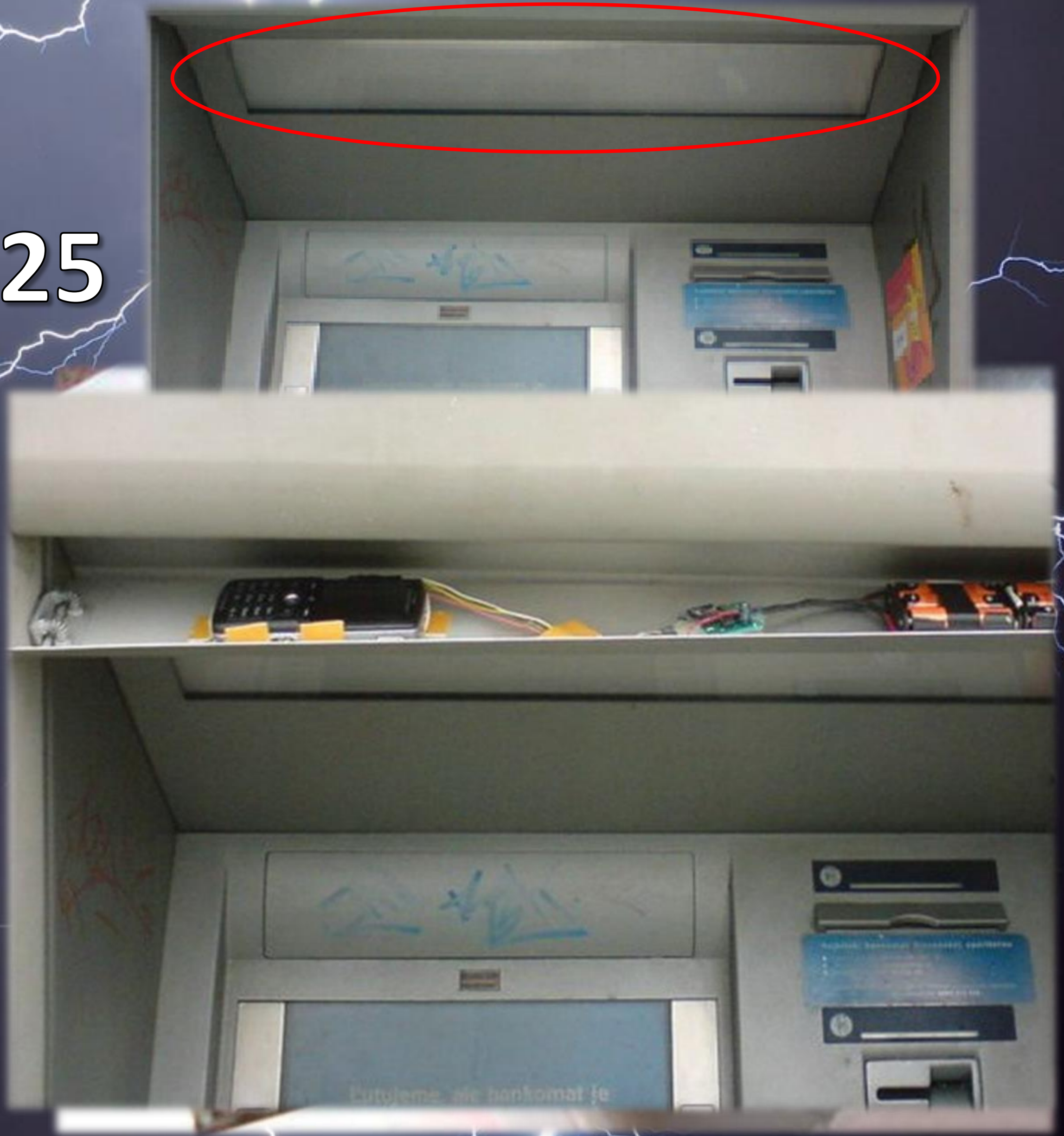
Performance results



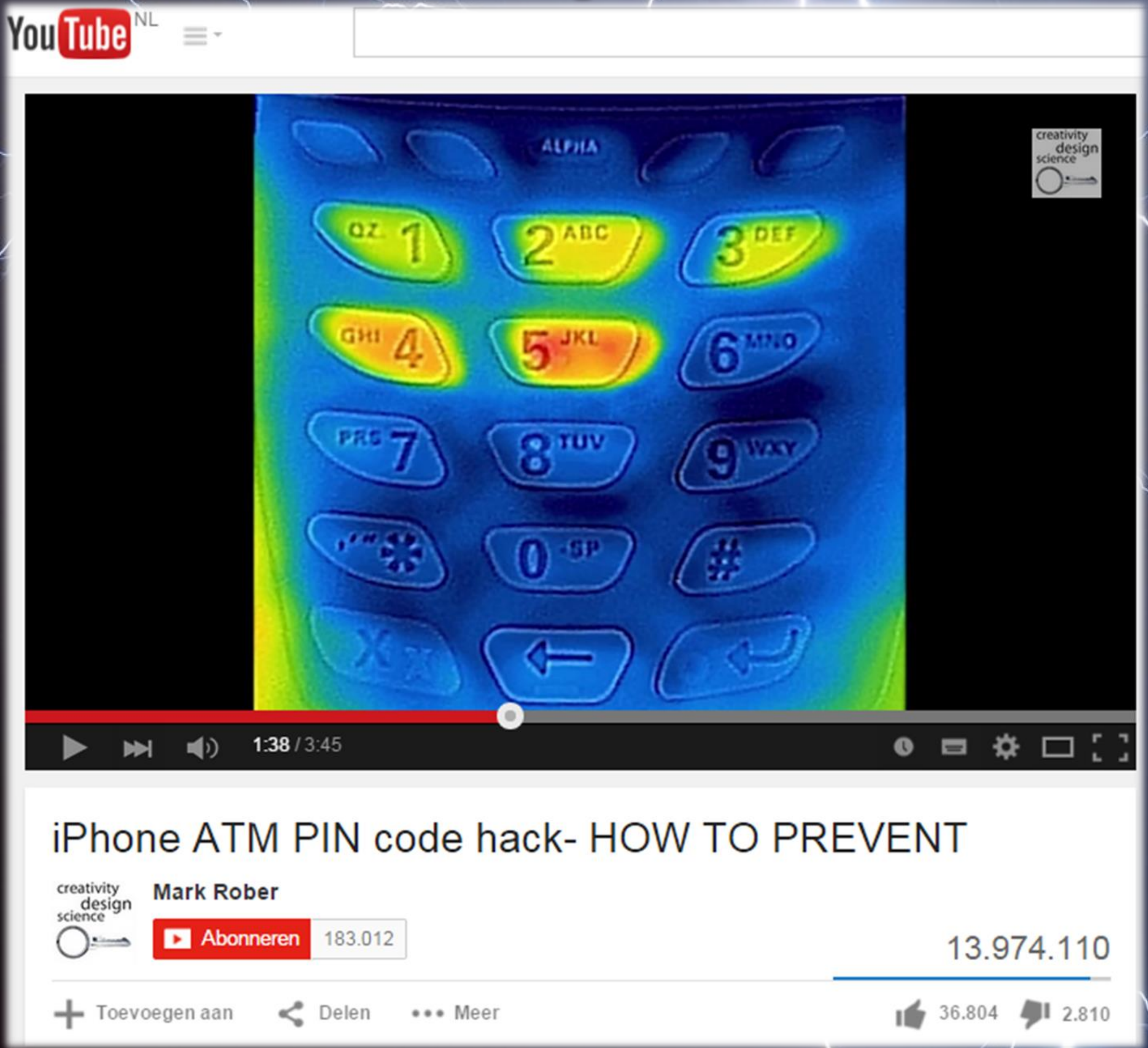
Relayed transaction with slowest card
is faster than normal transaction

Amounts limits

- No PIN for < €25/$25
- Pin needed for > €25/$25
  - Cameras
  - PIN pad
  - Shoulder surfing
  - Infrared pictures (?)



Infrared pictures



iPhone ATM PIN code hack- HOW TO PREVENT

Mark Rober

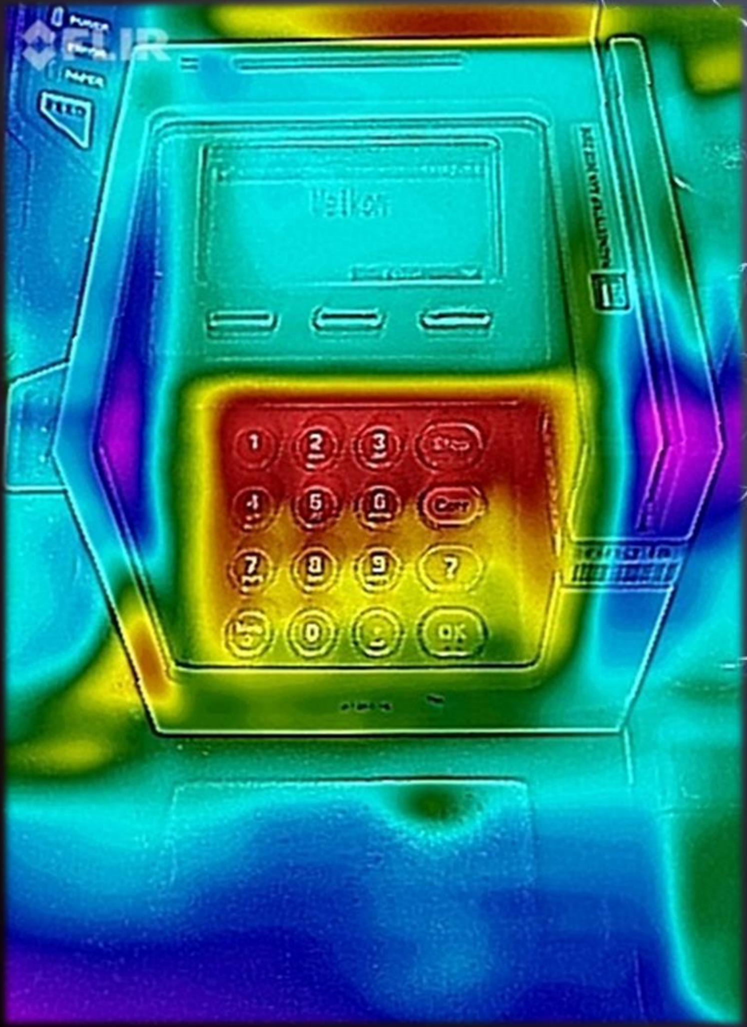
Abonneren 183.012

13.974.110

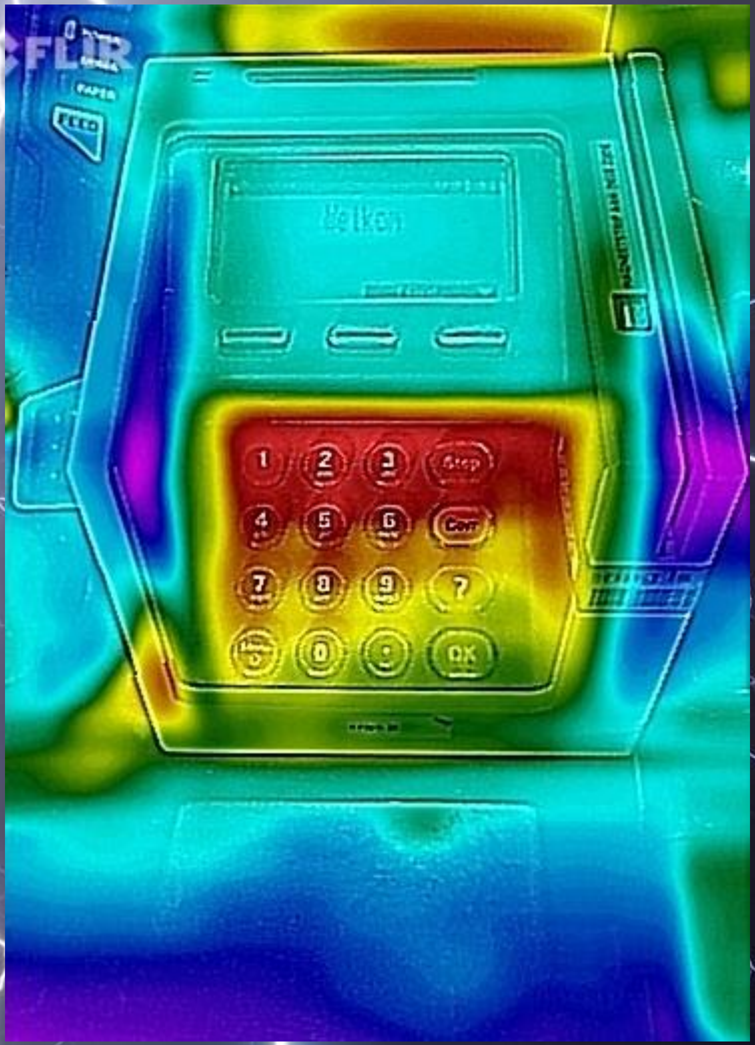
Toevoegen aan Delen ••• Meer 36.804 2.810

Video

Infrared in practice

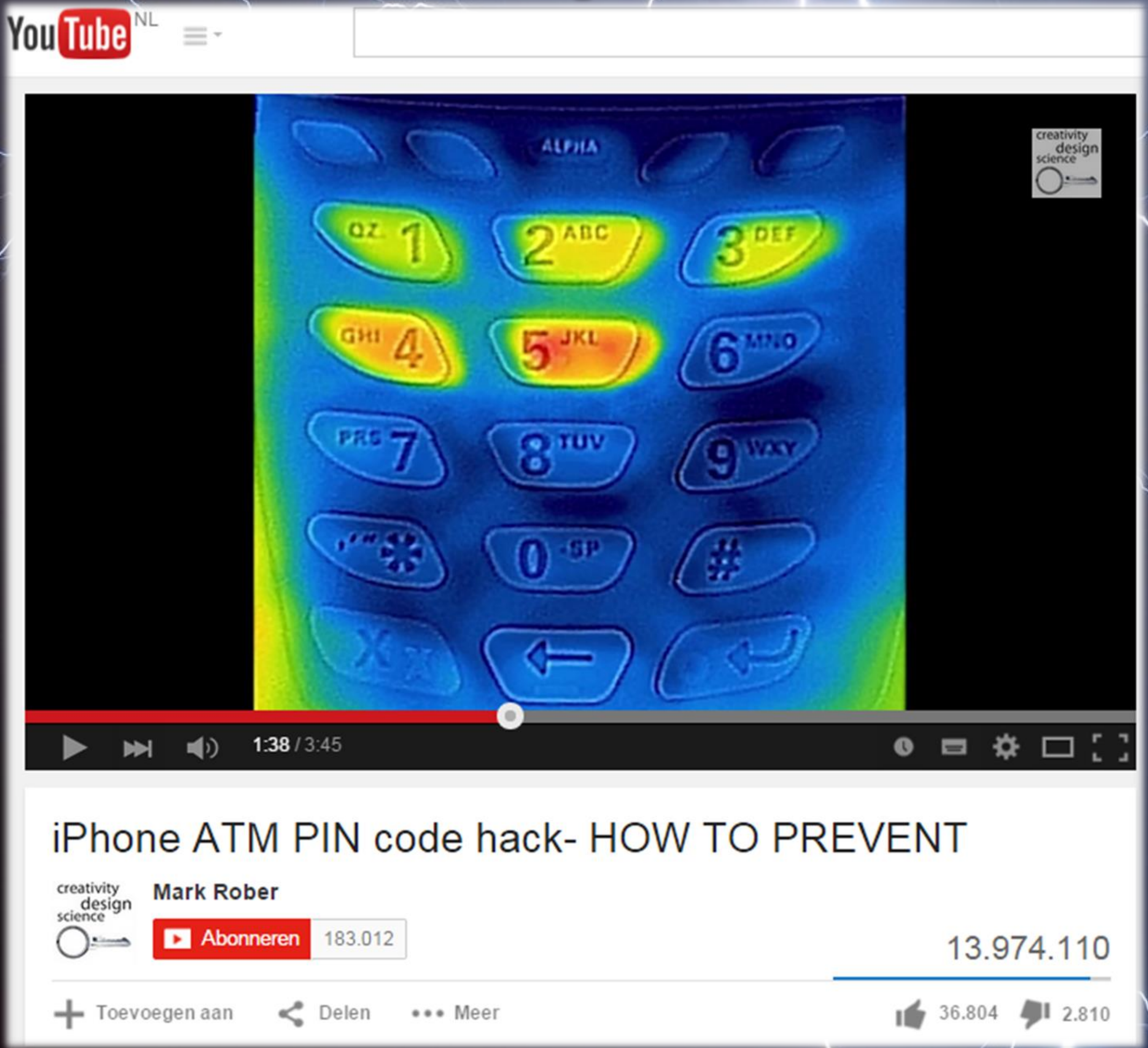


PIN entered: 1-2-3-4-5



PIN entered: 6-7-8-9-0

Infrared pictures



iPhone ATM PIN code hack- HOW TO PREVENT

Mark Rober

13.974.110

Amounts overview

Limit	Without PIN	With PIN
EMV Contact	-	€2500-€5000
EMV Contactless	€25	€2500-€5000

- 1€ contact transactions protected with PIN worth up to €5000
- Contactless transactions up to €5000 allowed

Conclusion

- Relay setup possible with 2 OTS Android devices
- Simple application needed (± 2 days developing)
- No effective countermeasures existent
  - Probably difficult to realize
- Payment limits should be optimzed

Thank you!

Contact: vandenBreekel.Jordi@KPMG.nl