The Radboud Reader

A minimal trusted smartcard reader for securing online transactions

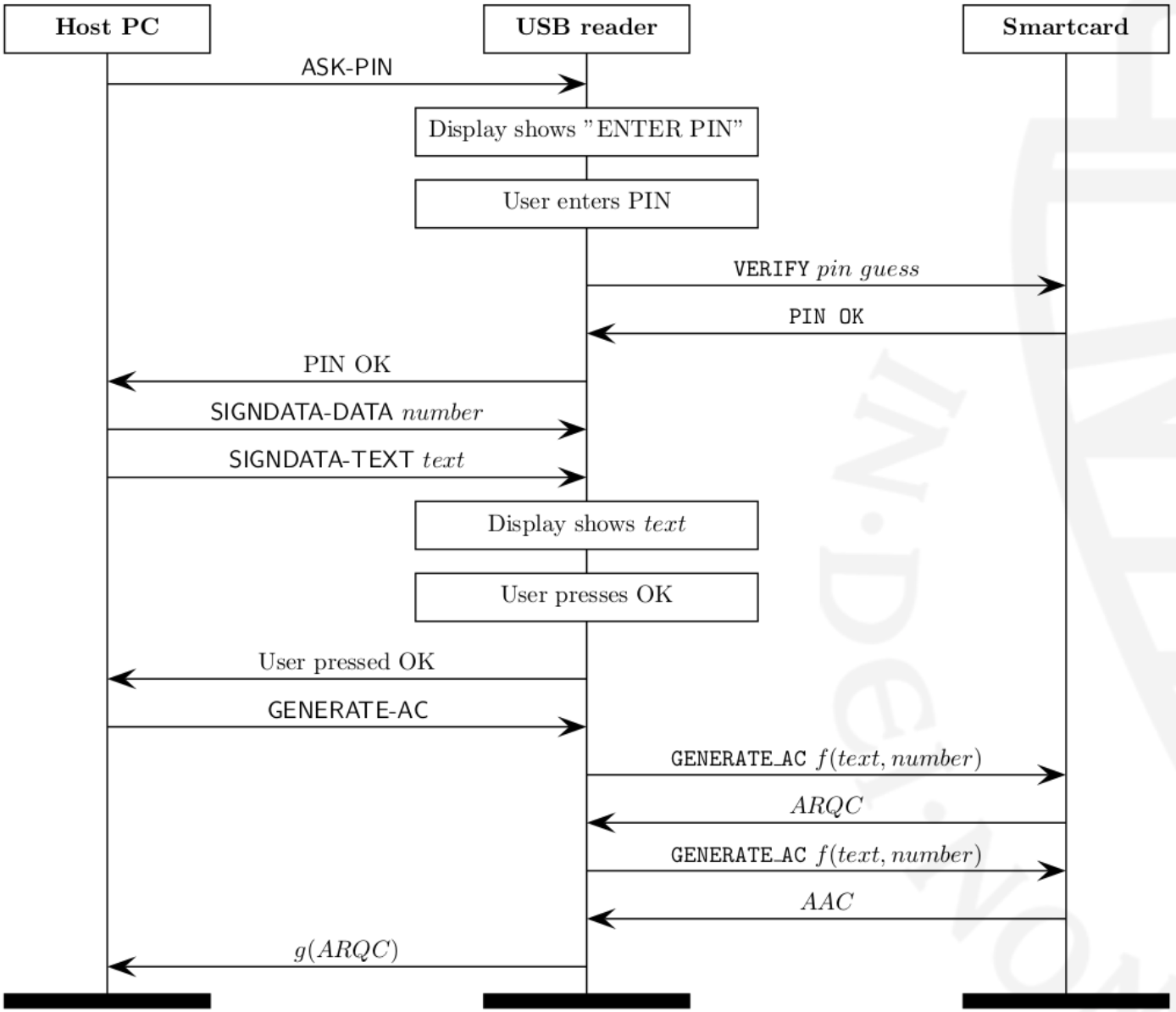
Erik Poll and Joeri de Ruiter

Digital Security, Radboud University Nijmegen

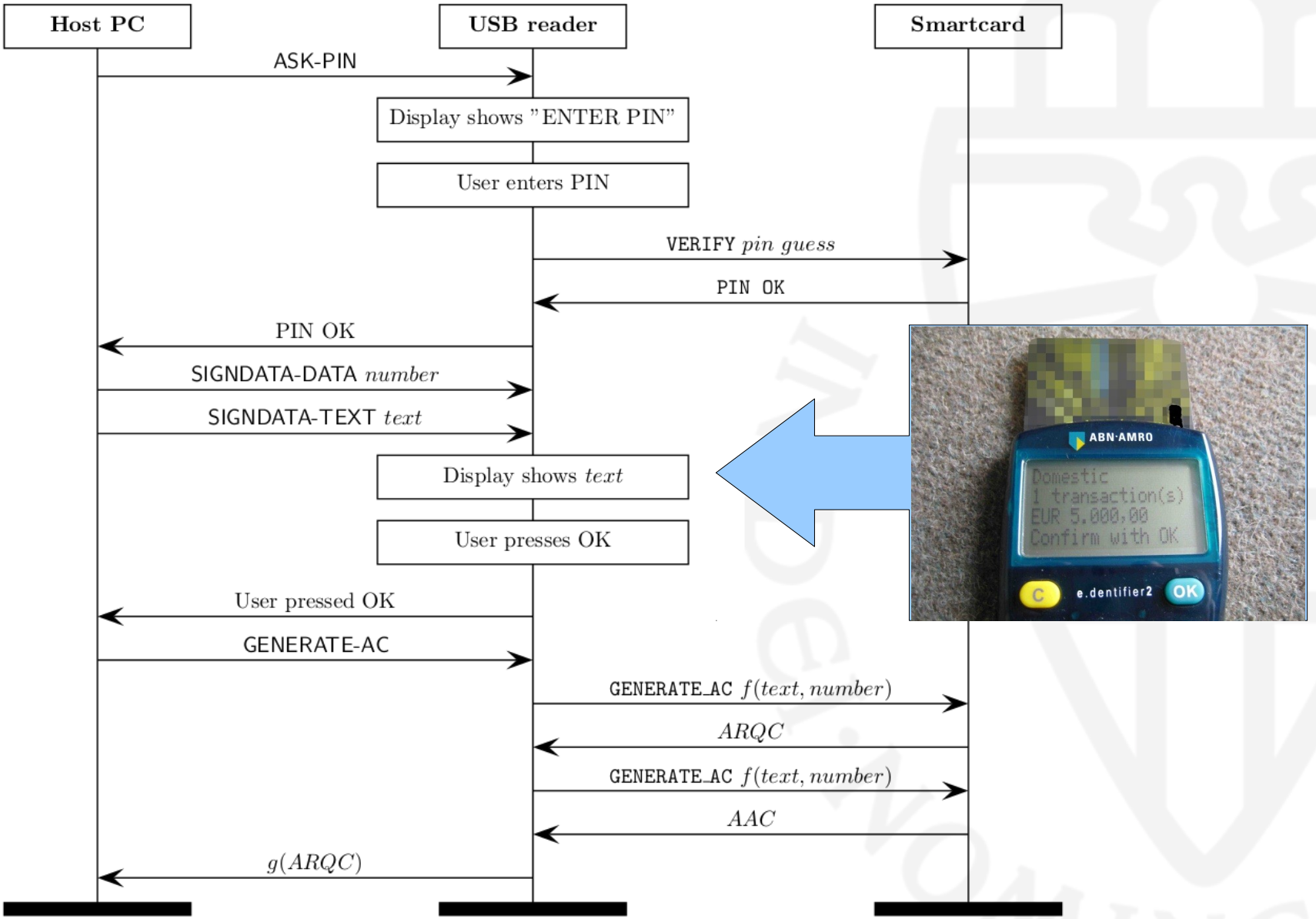
Motivation: e.dentifier2

- Developed by Todos (now Gemalto)
- Can be used with or without USB
- With USB:
  - See-What-You-Sign
  - “the most secure sign-what-you-see end user device ever seen”

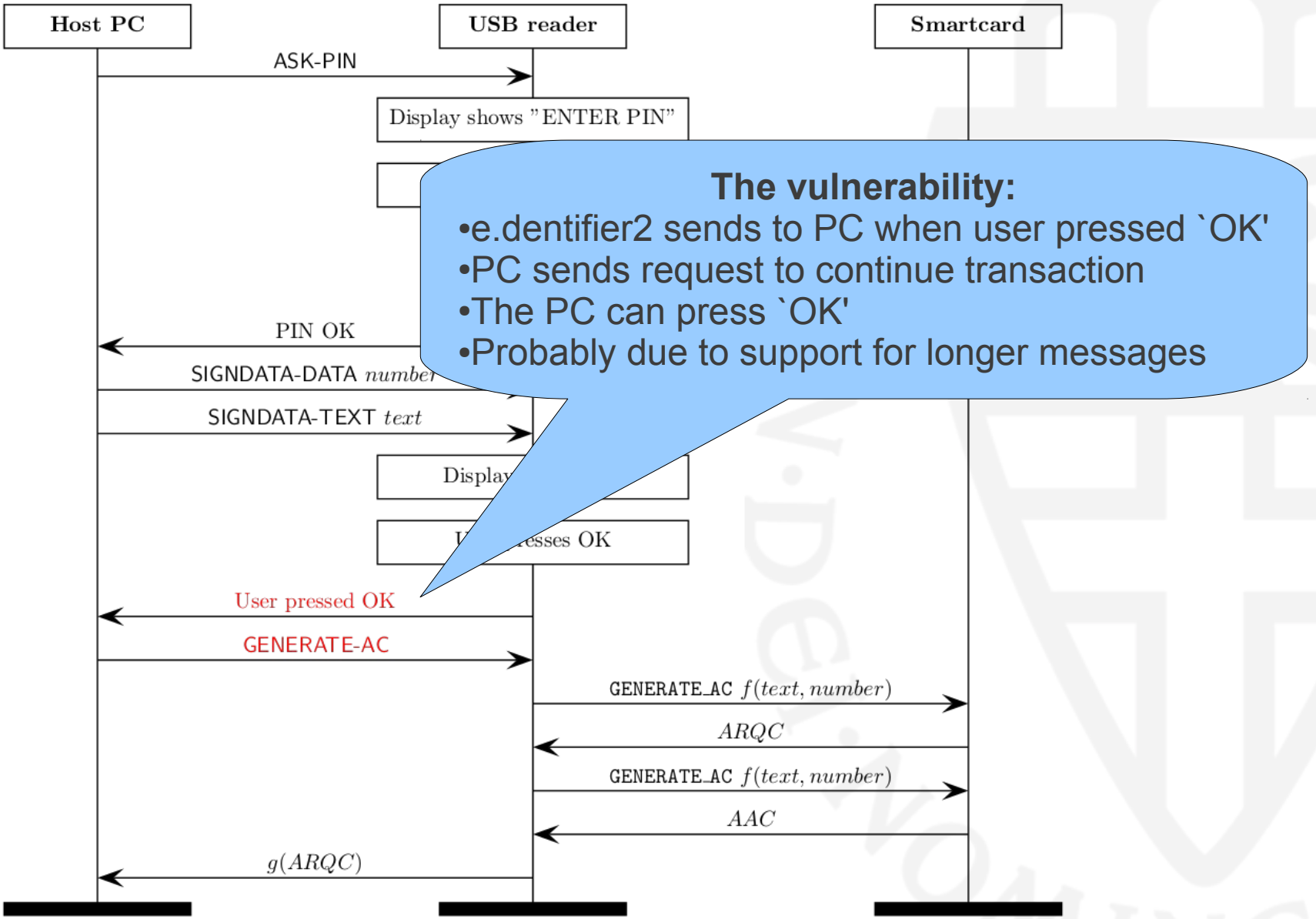
Protocol


Host PC
USB reader
Smartcard
ASK-PIN
Display shows "ENTER PIN"
User enters PIN
VERIFY pin guess
PIN OK
PIN OK
SIGNDATA-DATA number
SIGNDATA-TEXT text
Display shows text
User presses OK
User pressed OK
GENERATE-AC
GENERATE_AC f(text, number)
ARQC
GENERATE_AC f(text, number)
AAC
g(ARQC)

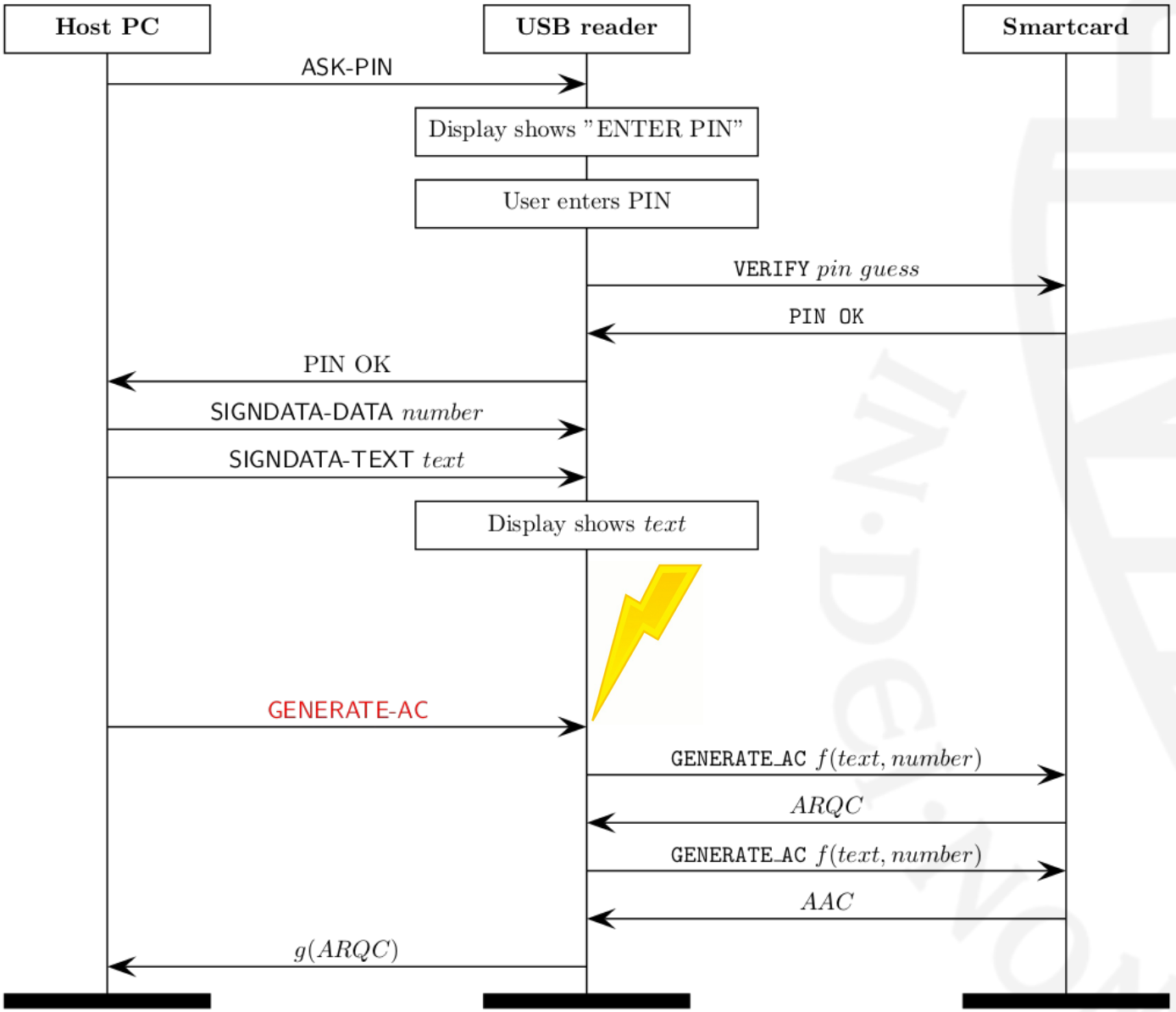
Protocol


Host PC
USB reader
Smartcard
ASK-PIN
Display shows "ENTER PIN"
User enters PIN
VERIFY pin guess
PIN OK
PIN OK
SIGNDATA-DATA number
SIGNDATA-TEXT text
Display shows text
User presses OK
User pressed OK
GENERATE-AC
GENERATE_AC f(text, number)
ARQC
GENERATE_AC f(text, number)
AAC
g(ARQC)
ABN·AMRO
Domestic
1 transaction(s)
EUR 5.000,00
Confirm with OK
C
e.dentifier2
OK

Protocol


Host PC
USB reader
Smartcard
ASK-PIN
Display shows "ENTER PIN"
PIN OK
SIGNDATA-DATA number
SIGNDATA-TEXT text
User pressed OK
GENERATE-AC
GENERATE_AC f(text, number)
ARQC
GENERATE_AC f(text, number)
AAC
g(ARQC)
The vulnerability:
•e.dentifier2 sends to PC when user pressed `OK'
•PC sends request to continue transaction
•The PC can press `OK'
•Probably due to support for longer messages

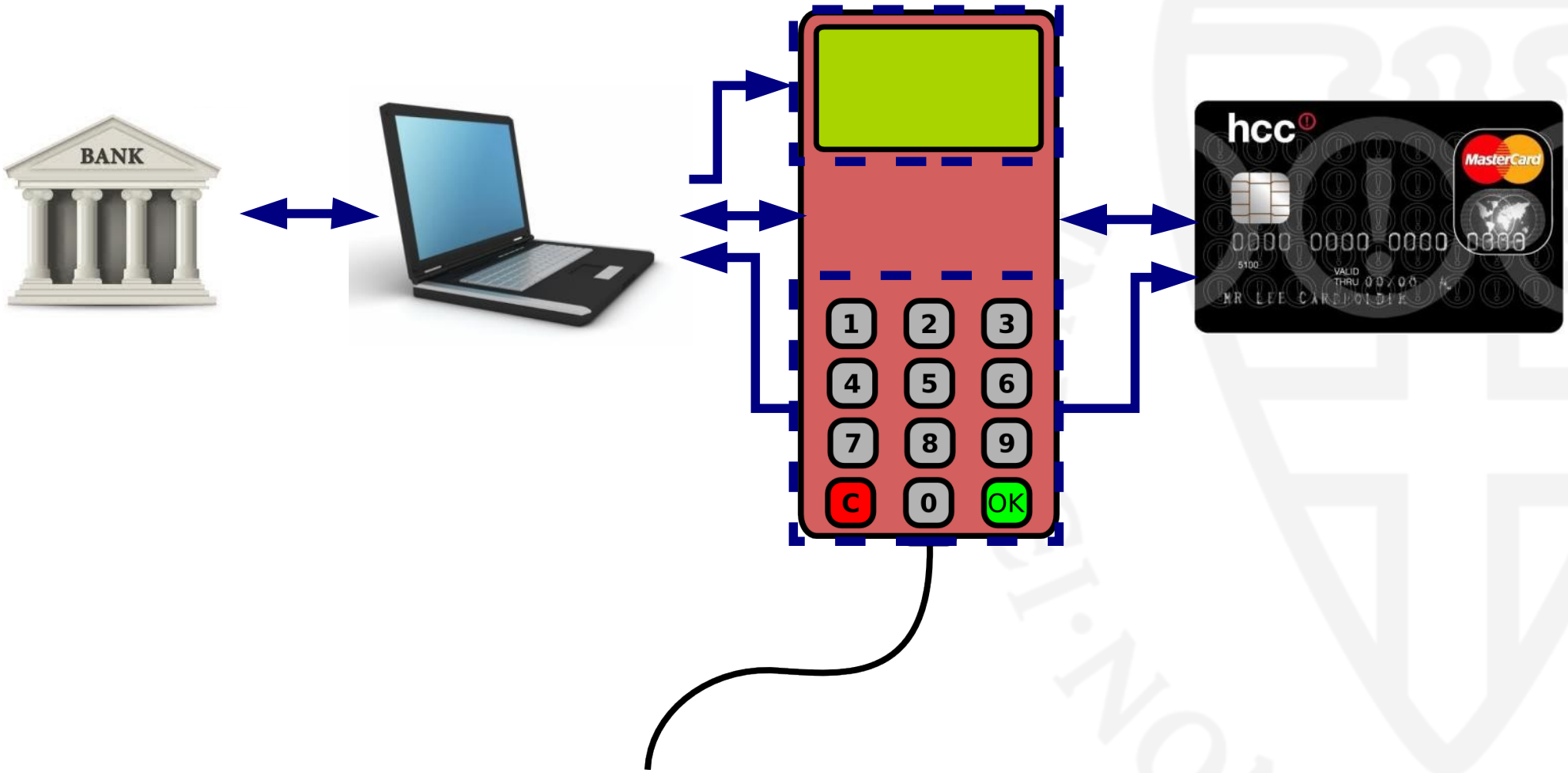
Protocol


Host PC
USB reader
Smartcard
ASK-PIN
Display shows "ENTER PIN"
User enters PIN
VERIFY pin guess
PIN OK
PIN OK
SIGNDATA-DATA number
SIGNDATA-TEXT text
Display shows text
GENERATE-AC
GENERATE_AC f(text, number)
ARQC
GENERATE_AC f(text, number)
AAC
g(ARQC)

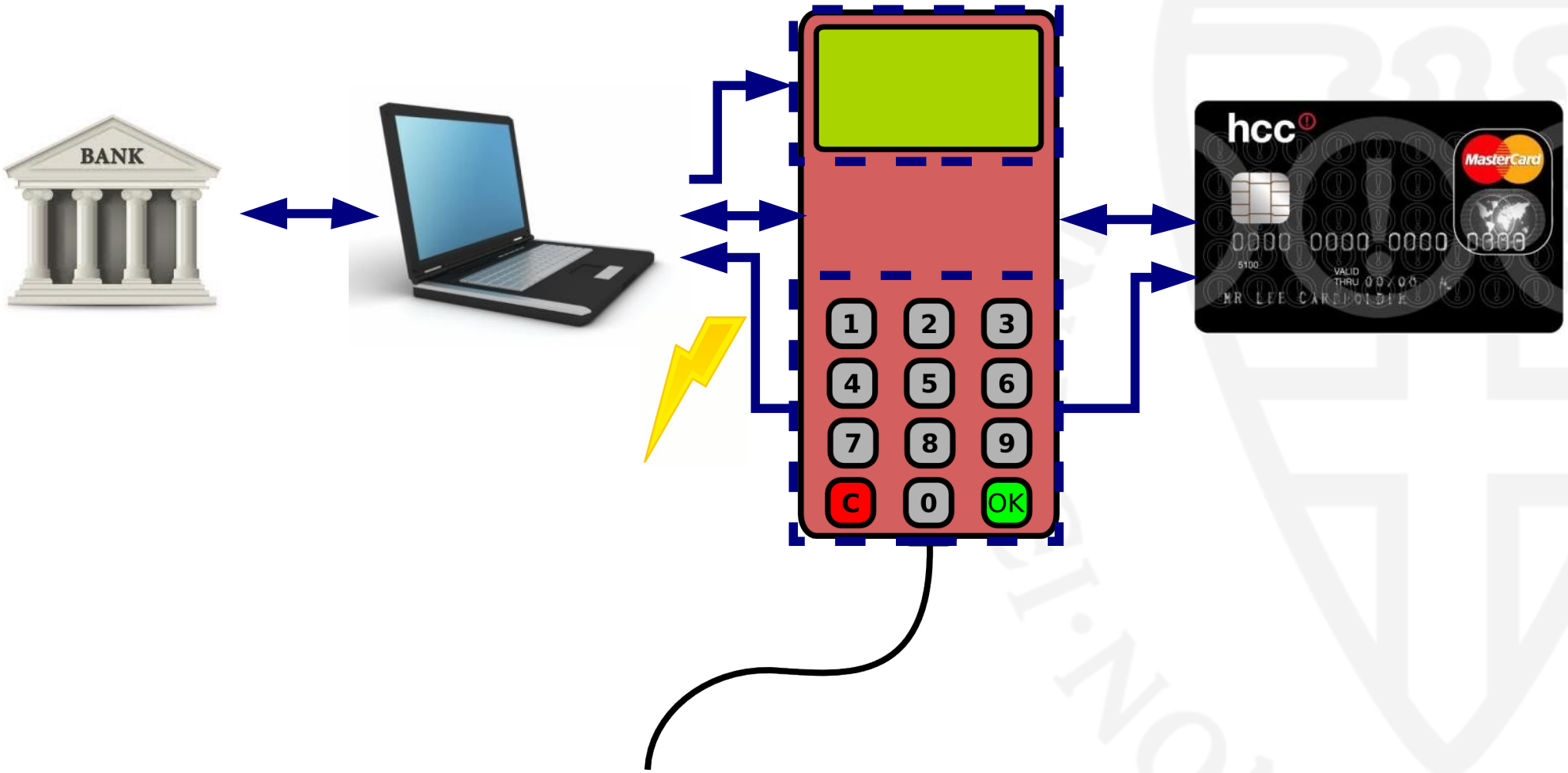
Better solution? Radboud Reader

- Minimal functionality in reader
- Connected via USB, to allow meaningful messages
- Data from PC directly forwarded to card
- Reader controlled by smartcard
  - Display text
  - Request input
  - Send data to PC

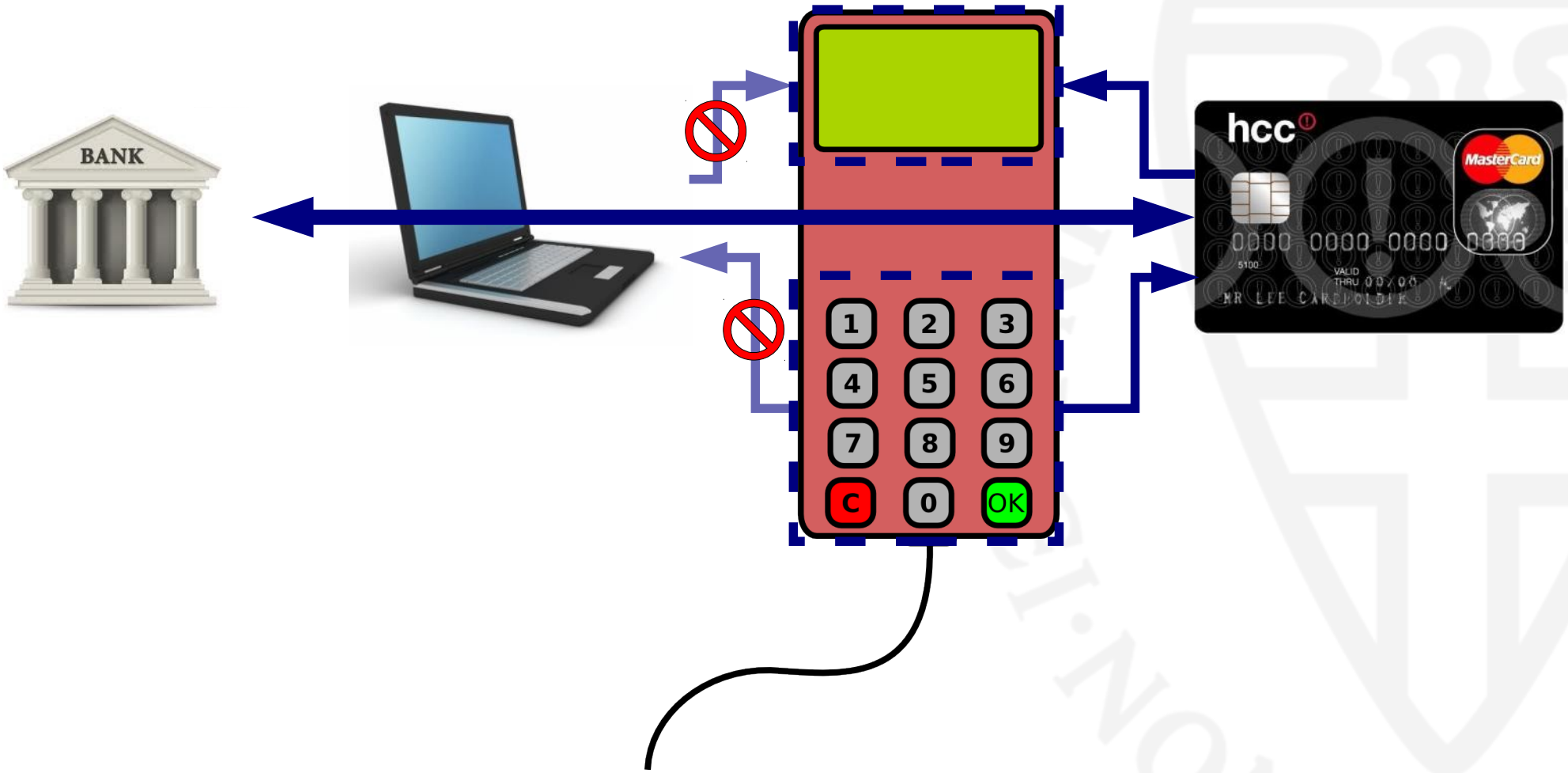
Information flows e.dentifier



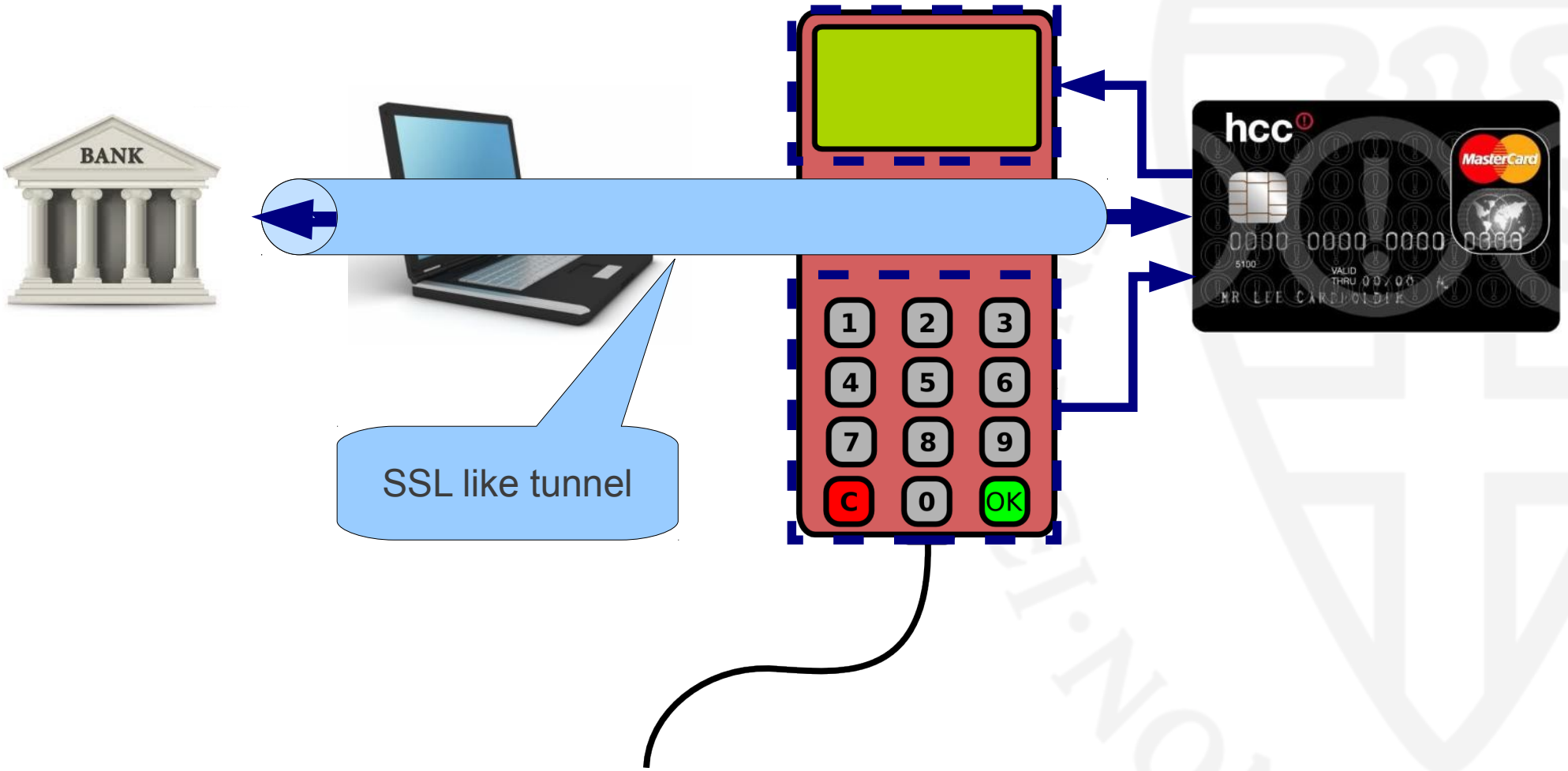
Information flows e.dentifier



Information flows Radboud Reader



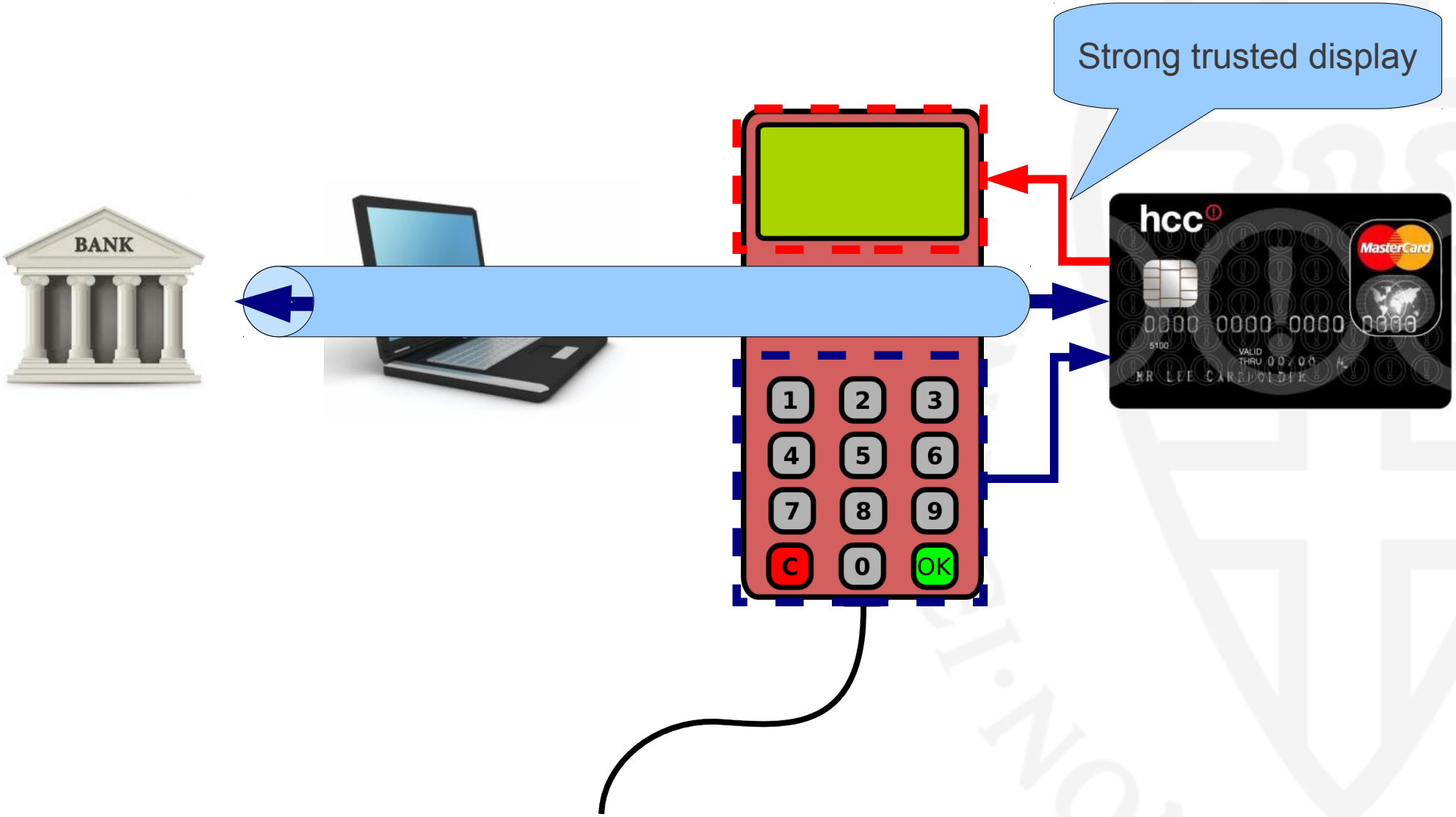
Information flows Radboud Reader



What you see is what you sign

- Weak trusted display
  - Displayed text is signed
- Strong trusted display
  - Displayed text authenticated

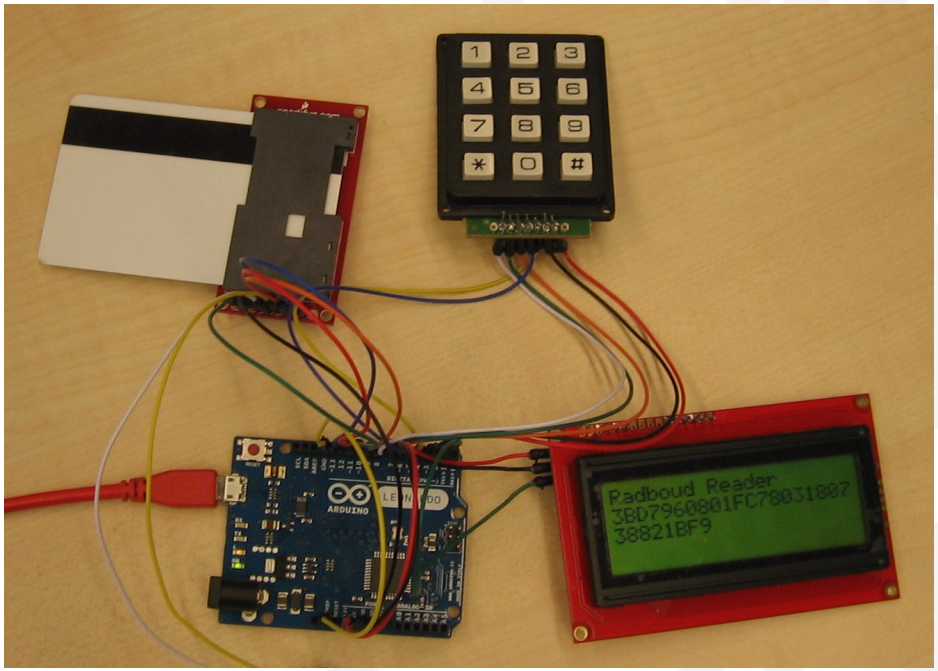
Information flows Radboud Reader



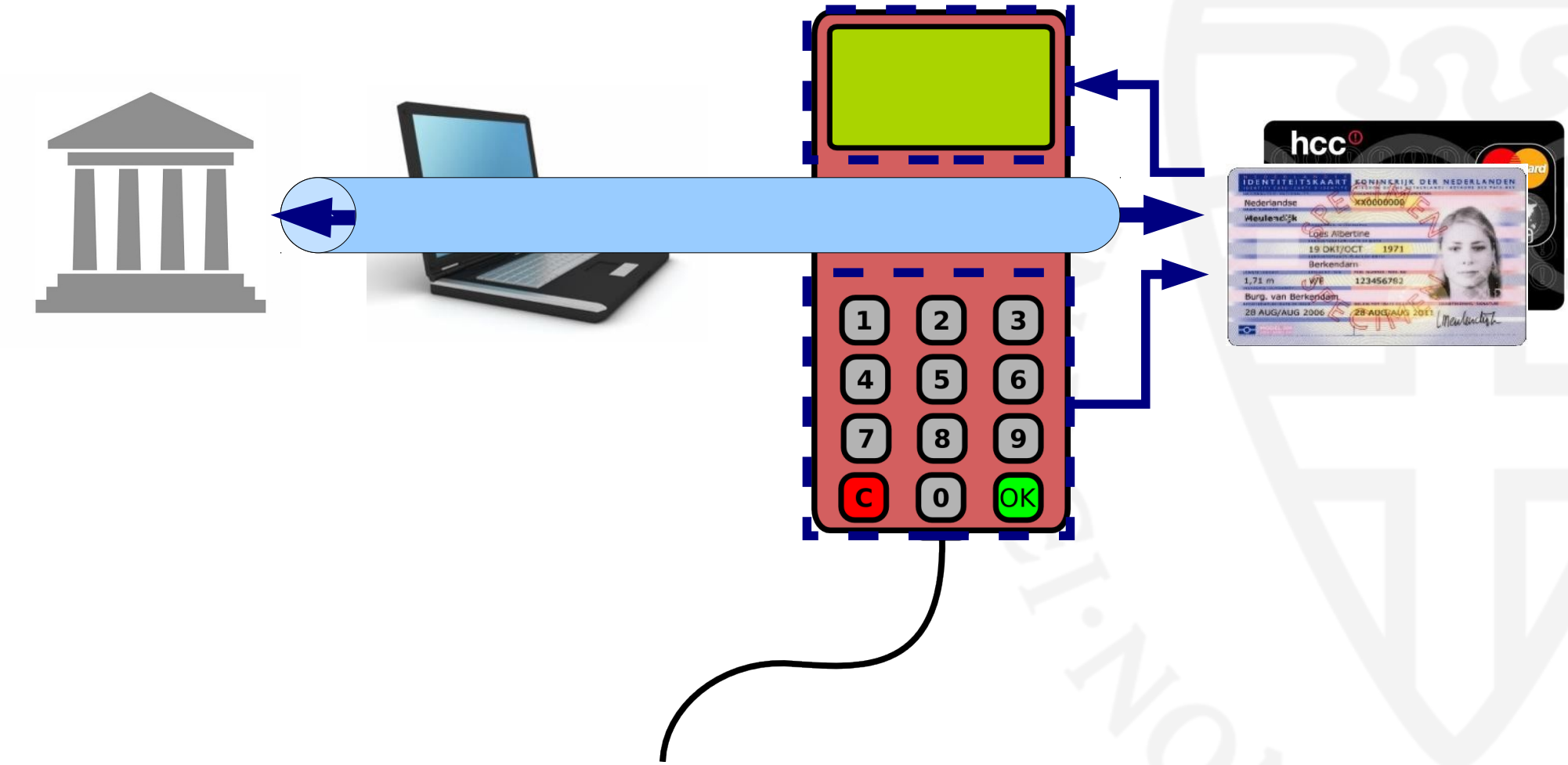
Prototype

- Arduino
- Around $80
- 300 loc

- Smartcard application
- Browser plugin
- Webapplication



Genericity for free

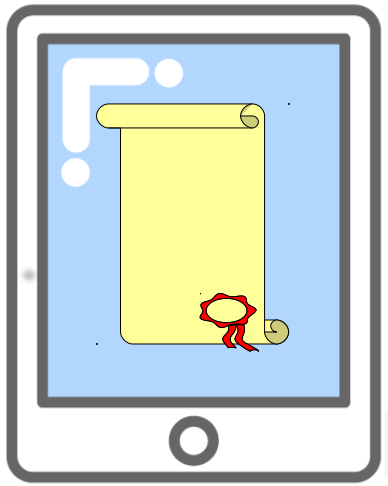


Comparison

- ZTIC (IBM)
  - Secure tunnel between device and back-end
  - Cryptographic operations in device
  - Configuration needed for different usage
- SmartTAN optic
  - PC cannot control device
  - For every message from the back-end a barcode needs to be scanned
  - Use still has to enter response manually on PC

Future

- Trusted devices necessary
- Possible solutions
  - Dedicated device?
  - Integration in untrusted devices?
    - Trusted execution modes
    - How do you recognise trusted mode?



Conclusion

- Radboud Reader can be used to secure online transactions
  - Generic
  - Minimal functionality in reader
  - Provides strong trusted display
  - No arbitrary commands directly to smartcard
- Code for prototype available online

Conclusion

- Radboud Reader can be used to secure online transactions
  - Generic
  - Minimal functionality in reader
  - Provides strong trusted display
  - No arbitrary commands directly to smartcard
- Code for prototype available online

Thanks for your attention!