

The truth about ABN-AMRO's e.dentifier2

Arjan Blom, Gerhard de Koning Gans, Erik Poll,
Joeri de Ruiter & Roel Verdult

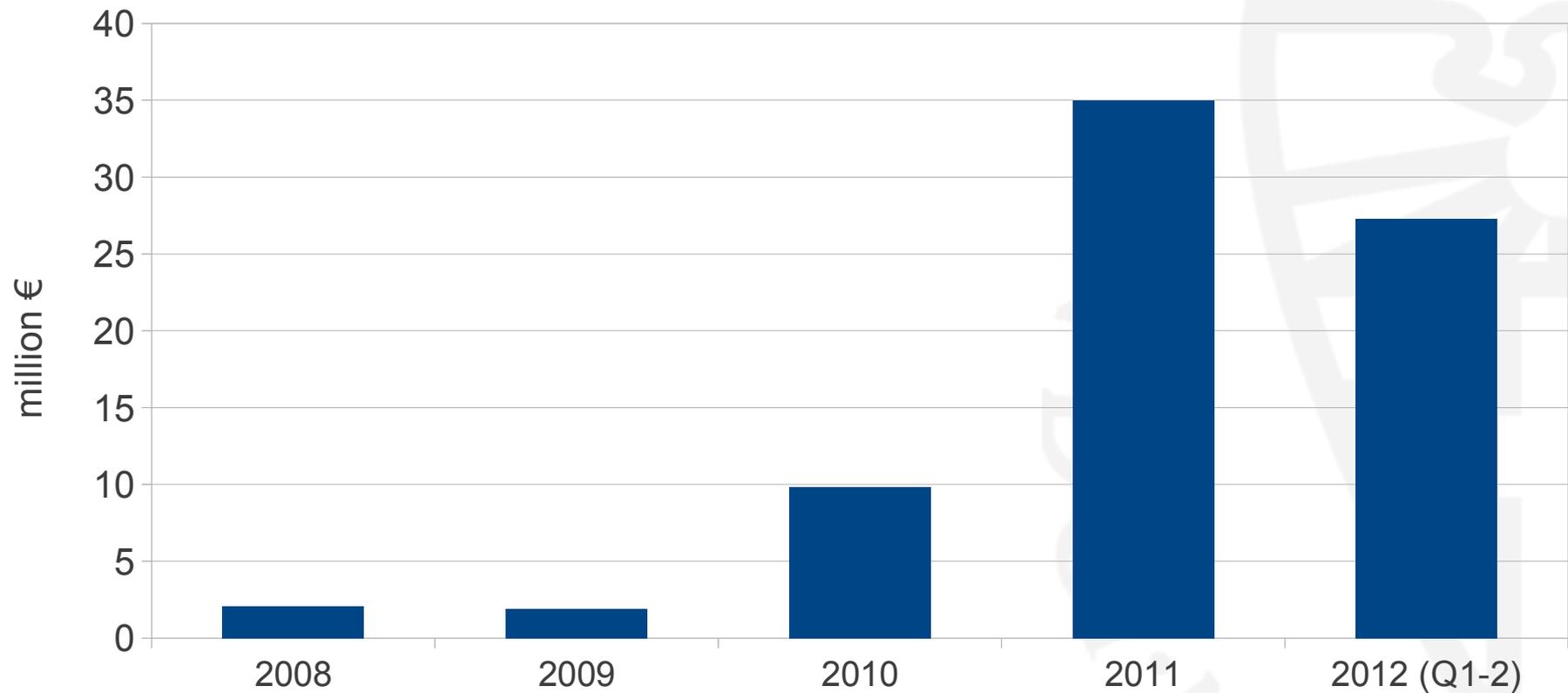
Digital Security, Radboud University Nijmegen

E-banking in the Netherlands

- 93% of all transactions
- 3 billion transactions a year
(€ 3.200 billion)



Fraud figures in the Netherlands



EMV-CAP

- Based on EMV
- Not public
- Reverse engineered
- Handheld readers
- Challenge-response

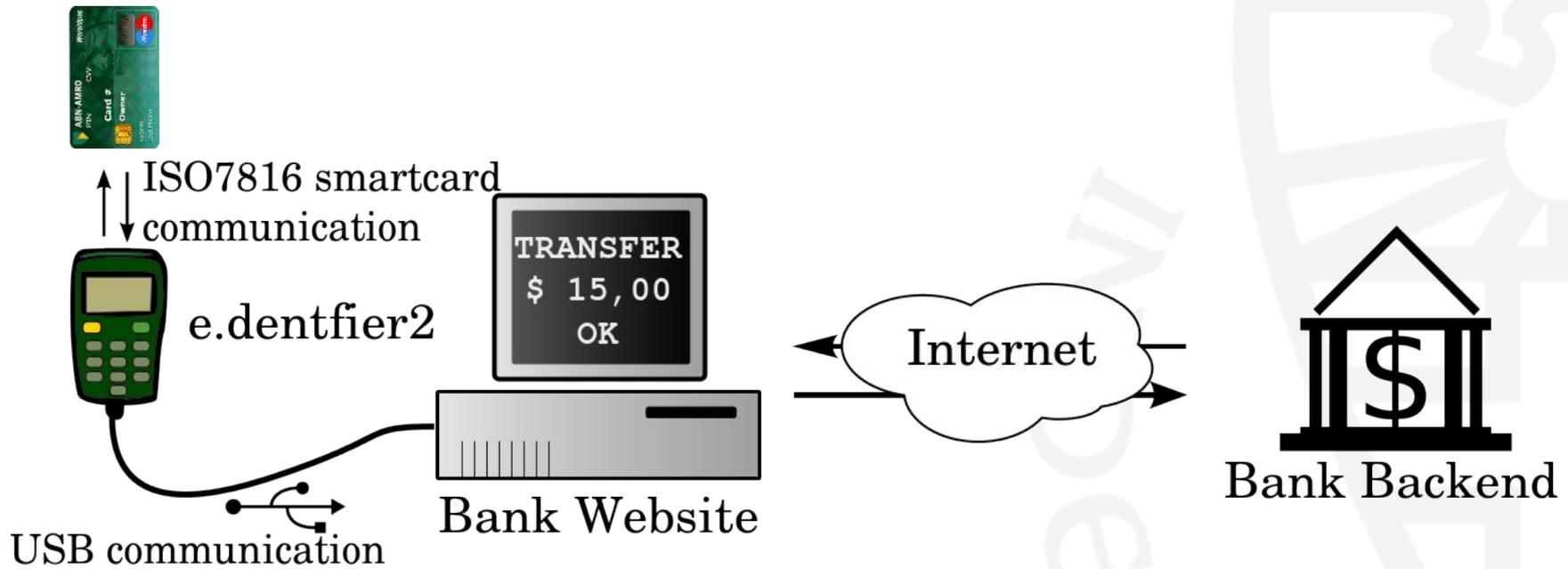


e.dentifier2

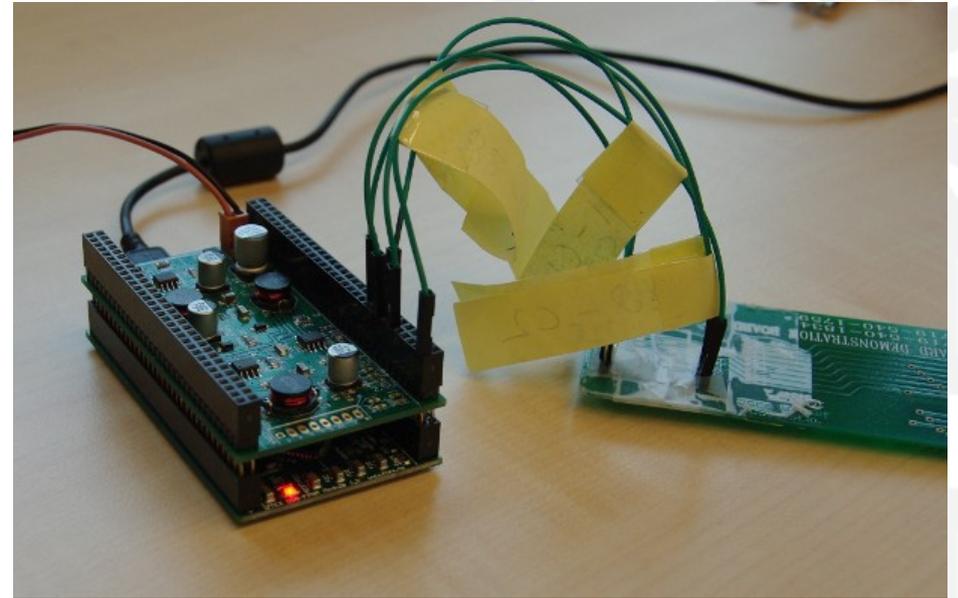
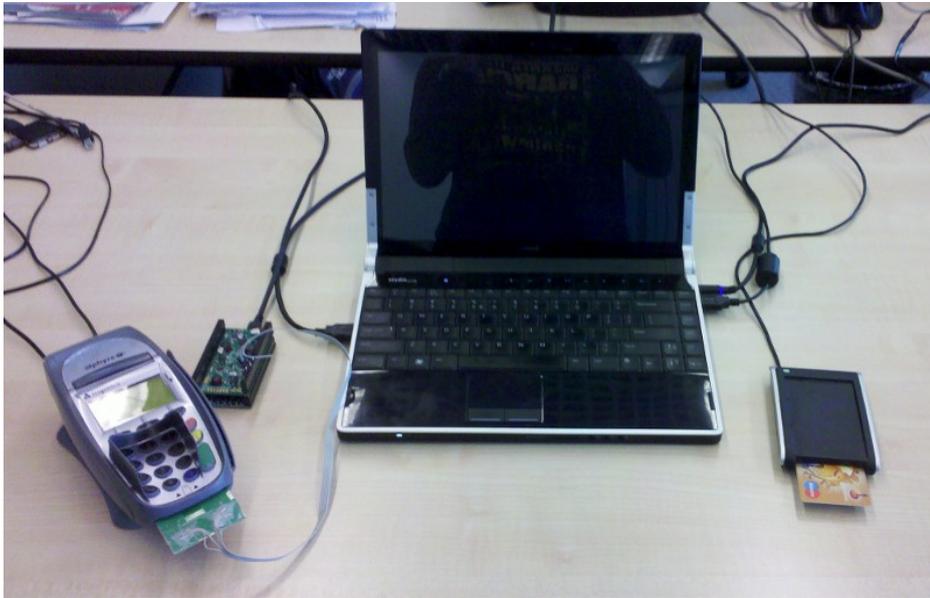
- Developed by Todos (now Gemalto)
- Can be with or without USB
- With USB:
 - See-What-You-Sign
 - “the most secure sign-what-you-see end user device ever seen”
 - Good idea!



Analysis



Smartcard ↔ Reader (ISO 7816): SmartLogic



Reader ↔ PC (USB): Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
135	120.736169	host	2.2	USB	72	URB_BULK out
154	120.738247	2.2	host	USB	64	URB_BULK out
155	120.740244	host	2.2	USB	72	URB_BULK out
156	120.740321	2.2	host	USB	64	URB_BULK out
157	120.743075	host	2.2	USB	72	URB_BULK out
158	120.743122	2.2	host	USB	64	URB_BULK out
159	120.746060	host	2.2	USB	72	URB_BULK out
160	120.746112	2.2	host	USB	64	URB_BULK out
161	120.748110	host	2.2	USB	72	URB_BULK out
162	120.748150	2.2	host	USB	64	URB_BULK out
163	120.750099	host	2.2	USB	72	URB_BULK out
164	120.750170	2.2	host	USB	64	URB_BULK out
165	120.752132	host	2.2	USB	72	URB_BULK out
166	120.752186	2.2	host	USB	64	URB_BULK out
167	120.754168	host	2.2	USB	72	URB_BULK out
168	120.754228	2.2	host	USB	64	URB_BULK out
169	120.756068	host	2.2	USB	72	URB_BULK out
170	120.756111	2.2	host	USB	64	URB_BULK out

▶ Endpoint: 0x02, Direction: OUT
Device: 2
URB bus id: 3
Device setup request: not relevant ('-')
Data: present (0)
URB sec: 1328621395
URB usec: 216521
URB status: Operation now in progress (-EINPROGRESS) (-115)
URB length [bytes]: 8
Data length [bytes]: 8
[\[Response in: 166\]](#)
[bInterfaceClass: Unknown (0xffff)]
Leftover Capture Data: 0006455552203132

```
0000 00 b6 29 4a 00 88 ff ff 53 03 02 02 03 00 2d 00  ..)J.... S.....
0010 53 27 31 4f 00 00 00 00 c9 4d 03 00 8d ff ff ff  S'10.... .M.....
0020 08 00 00 00 08 00 00 00 00 00 00 00 00 00 00  ..00000000000000
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..00000000000000
0040 00 06 45 55 52 20 31 32  ..EUR 12
```

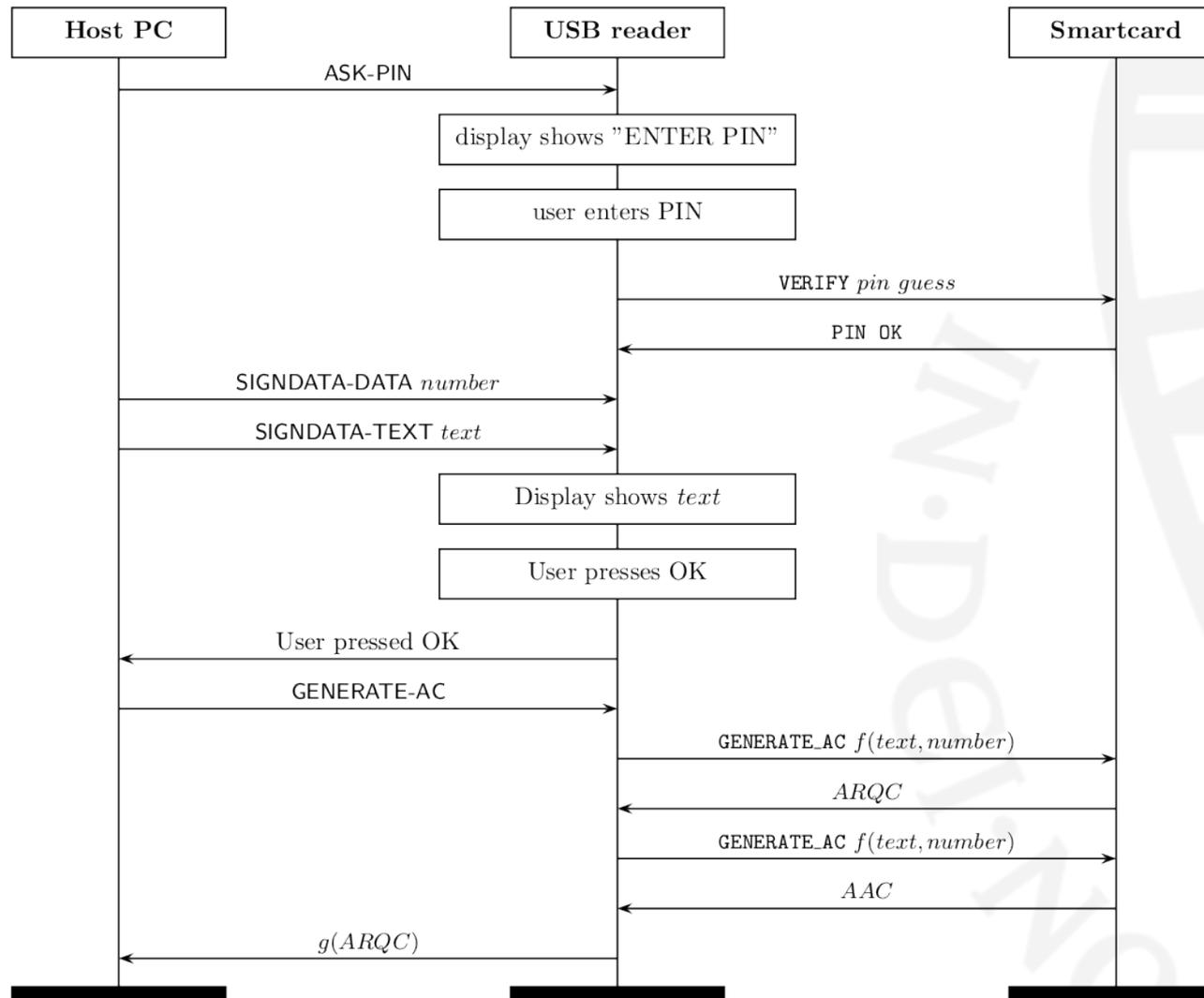
© Padding added by the USB captur... Packets: 216 Displayed: 216 Marked: 0 Load time: 0:00.002 Profile: Default

Analysis

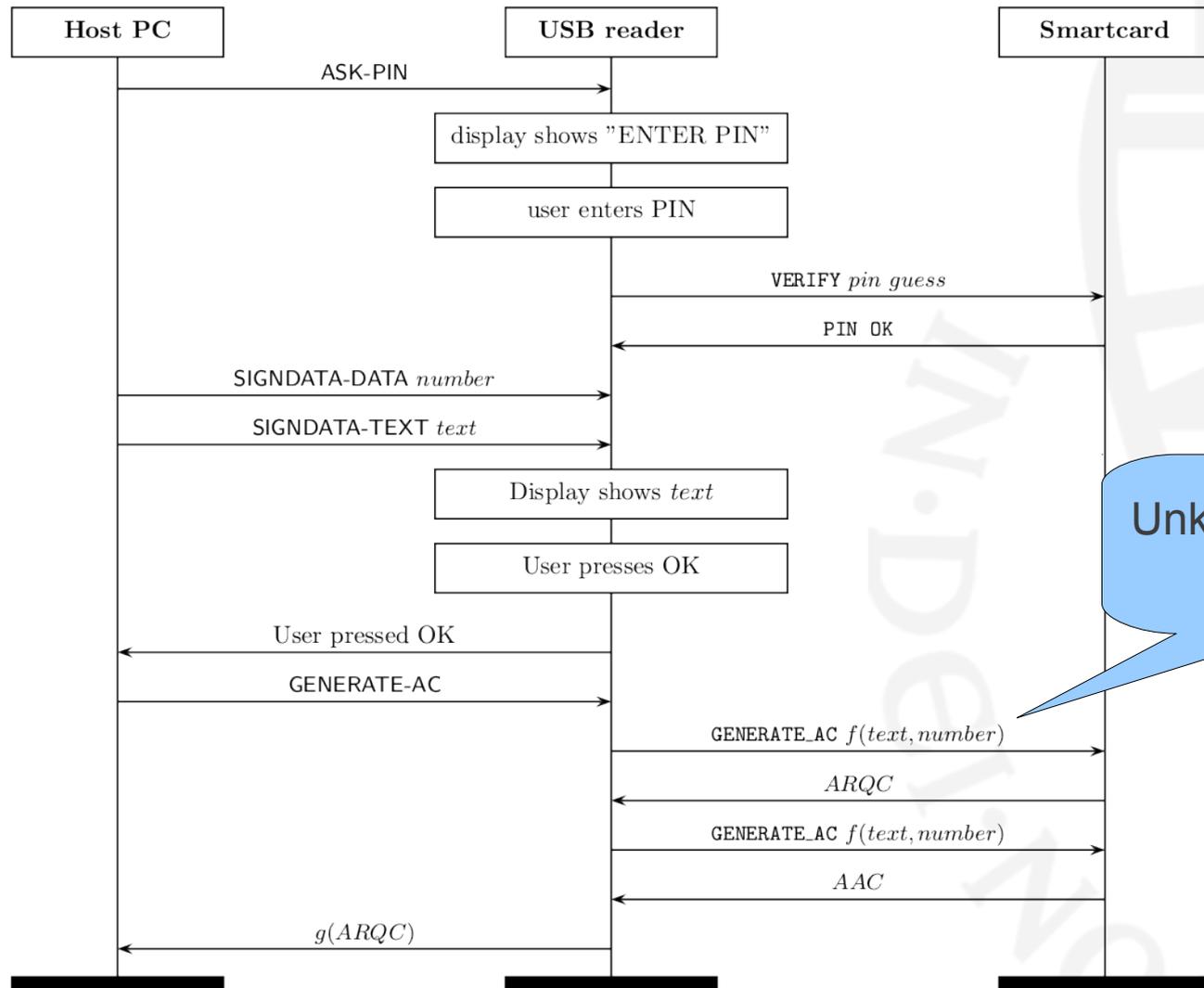
- PC can show
 - messages predefined in the e.dentifier2
 - any message that it wants to be signed



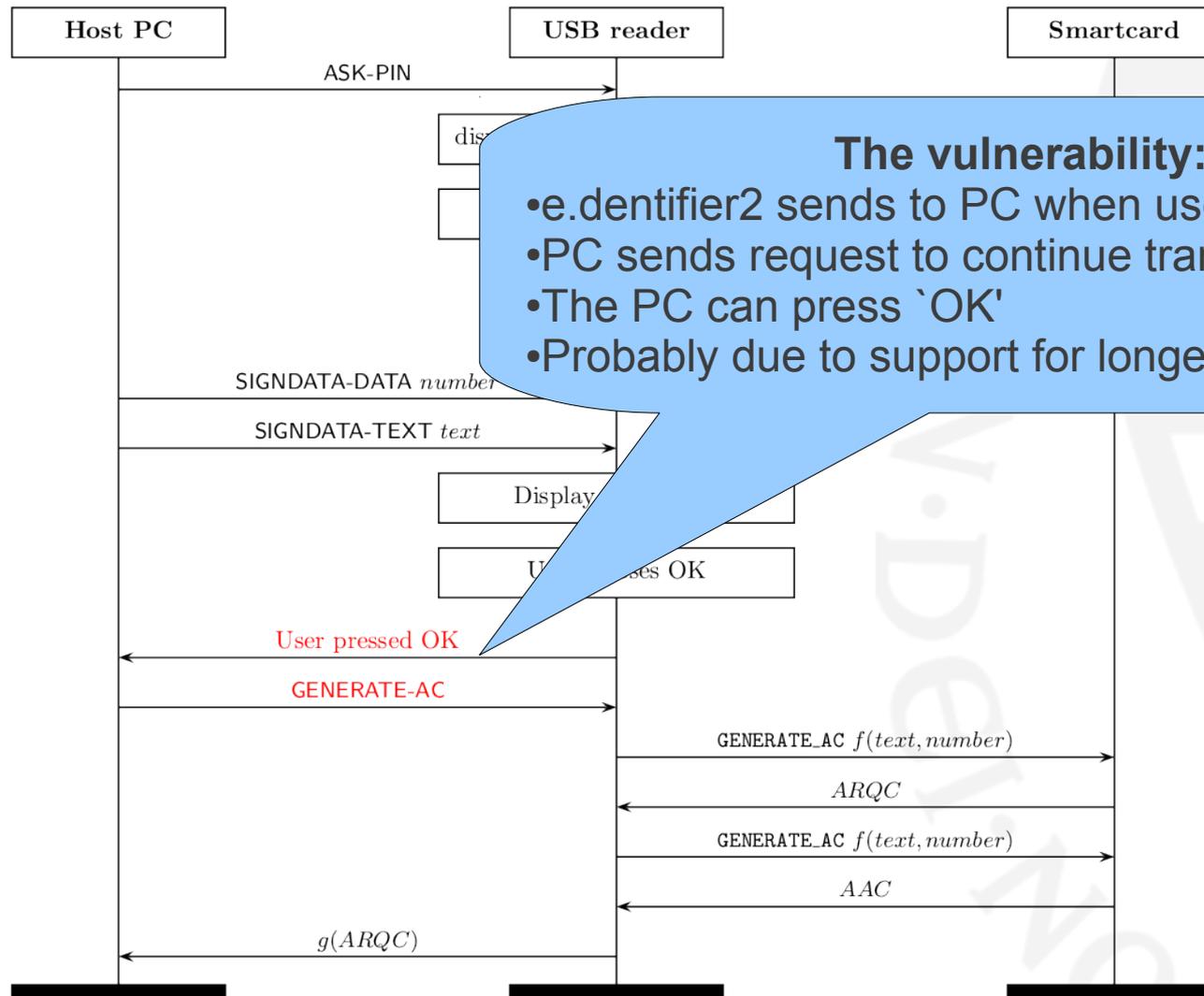
Protocol



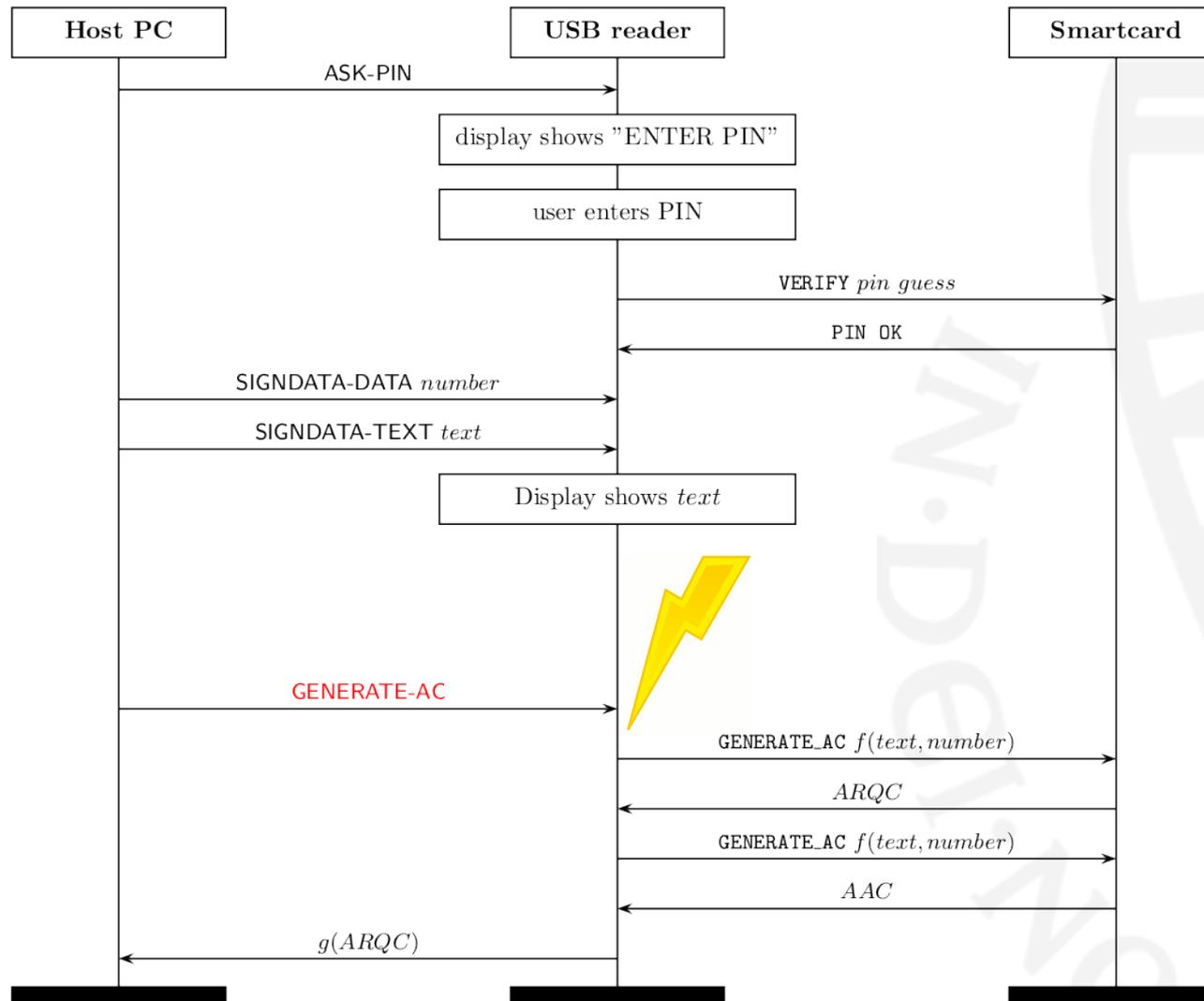
Protocol



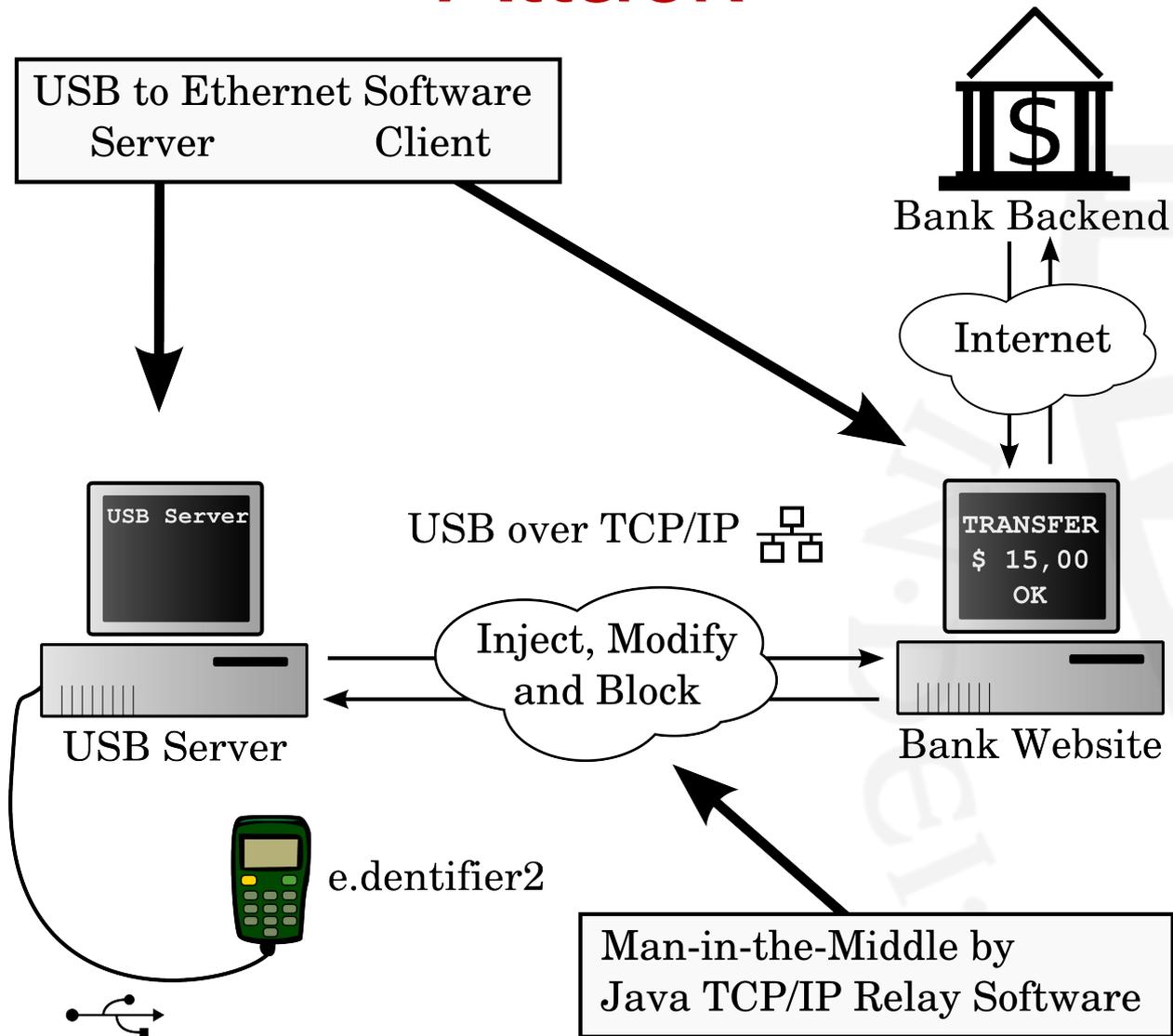
Protocol



Protocol



Attack



Video



Reaction bank

- Existing devices cannot be patched
- Visited us a few days after the discovery
- Informed their supplier
- Production was stopped and an improved version developed
- We were asked to investigate the improved version, but this proved problematic due to NDAs

Implications

- Handelsbanken uses same device
- Is the e.dentifier2 more secure with or without USB?
 - Using USB it should have been more secure
 - Now equally “secure” depending on challenges, however USB attack requires ABN-AMRO specific malware

Conclusion

- If implemented correctly What-you-see-is-what-you-sign is a good idea
- How could this ever have been introduced in development & missed in security review??
- Reduce control of PC over the device to minimum
- Stick to Kerckhoffs' principle (no NDAs)

Conclusion

- If implemented correctly What-you-see-is-what-you-sign is a good idea
- How could this ever have been introduced in development & missed in security review??
- Reduce control of PC over the device to minimum
- Stick to Kerckhoffs' principle (no NDAs)

Thanks for your attention!