The truth about ABN-AMRO's e.dentifier2

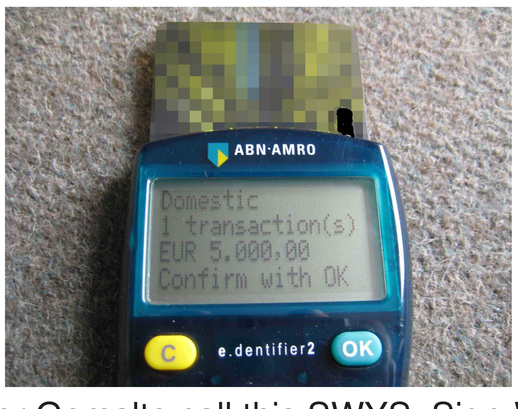
Digital Security group - Radboud University Nijmegen

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

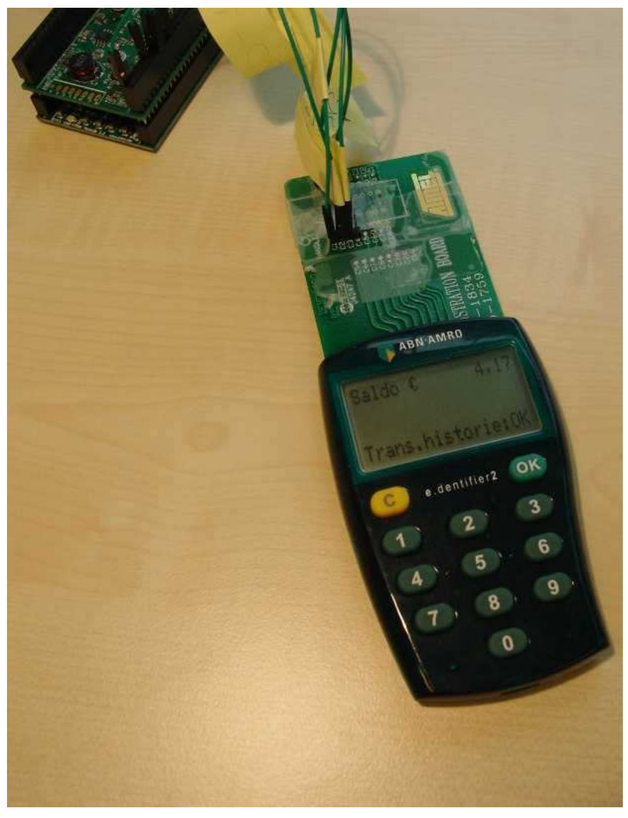
The *good* idea behind the USB-connected e.dentifier2

The e.dentifier2 is used to secure internet banking:
smartcard & PIN needed to login or approve transaction.
It can be used *with* or *without* USB cable.

- Without USB cable: user has to trust the display of his PC to know what he is approving, and could fall victim to a Man-in-the-Browser attack on an infected PC.
- With USB cable: the user sees the transaction details on the e.dentifier2 before approving it (see photo below).
  This can defeat Man-in-the-Browser attacks!

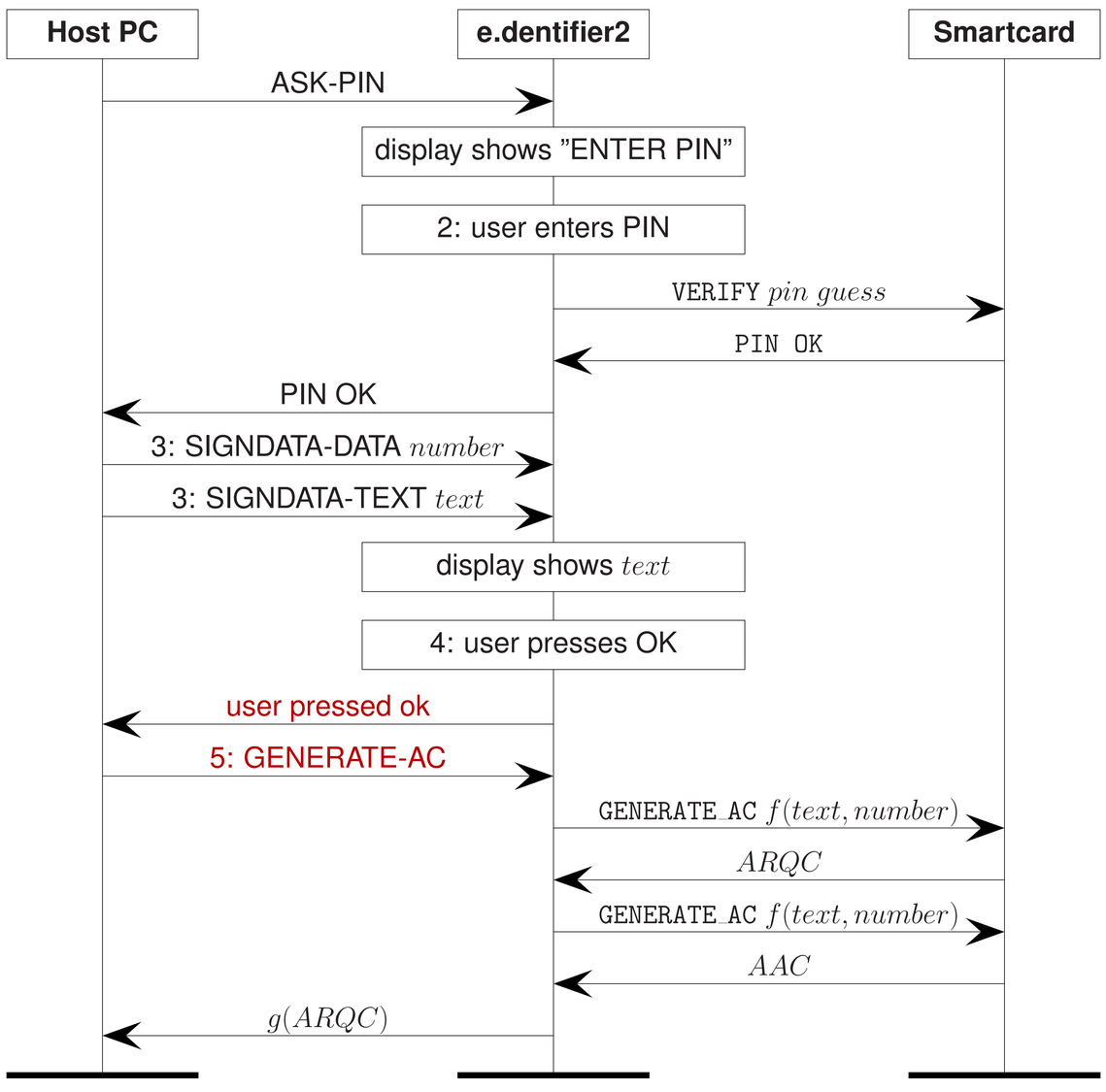


Manufacturer Gemalto call this SWYS: Sign-What-You-See.
However . . .



Our SmartLogic tool for observing smartcard communication.

The *bad* realisation of this idea in the protocol . . .



The protocol, reverse-engineered using Wireshark for observing USB communication and the Smartlogic for the smartcard communication

The protocol:

1. The user starts a transaction on the bank's website.
2. He is asked to enter his PIN code on the e.dentifier2.
3. The PC sends the transaction details to the e.dentifier2.
4. The e.dentifier2 displays the text and waits for user approval.
5. The PC sends a command to sign the transaction details.

The vulnerability

- The problem: the e.dentifier2 sends a message to the PC that the user pressed 'OK' and *the PC* then gives the go-ahead for the smartcard to sign the transaction.
- An infected PC can give the go-ahead without waiting for the user to press 'OK'. In other words: the PC can press 'OK'!
- Hence: an infected PC can choose transaction details and then carry out a bank transfer without confirmation by the user.

Details in: *Designed to fail: a USB-connected reader for online banking*, NORDSEC 2012.

Moral of the story: banks and their suppliers should not design their own secret proprietary protocols, but stick to Kerckhoffs' principle!

k3rckhoffs 1nst1tute

Radboud Universiteit Nijmegen