

PersoSim – simulate your eID card

Jens Bender

Secure Document World / 09.06.2015

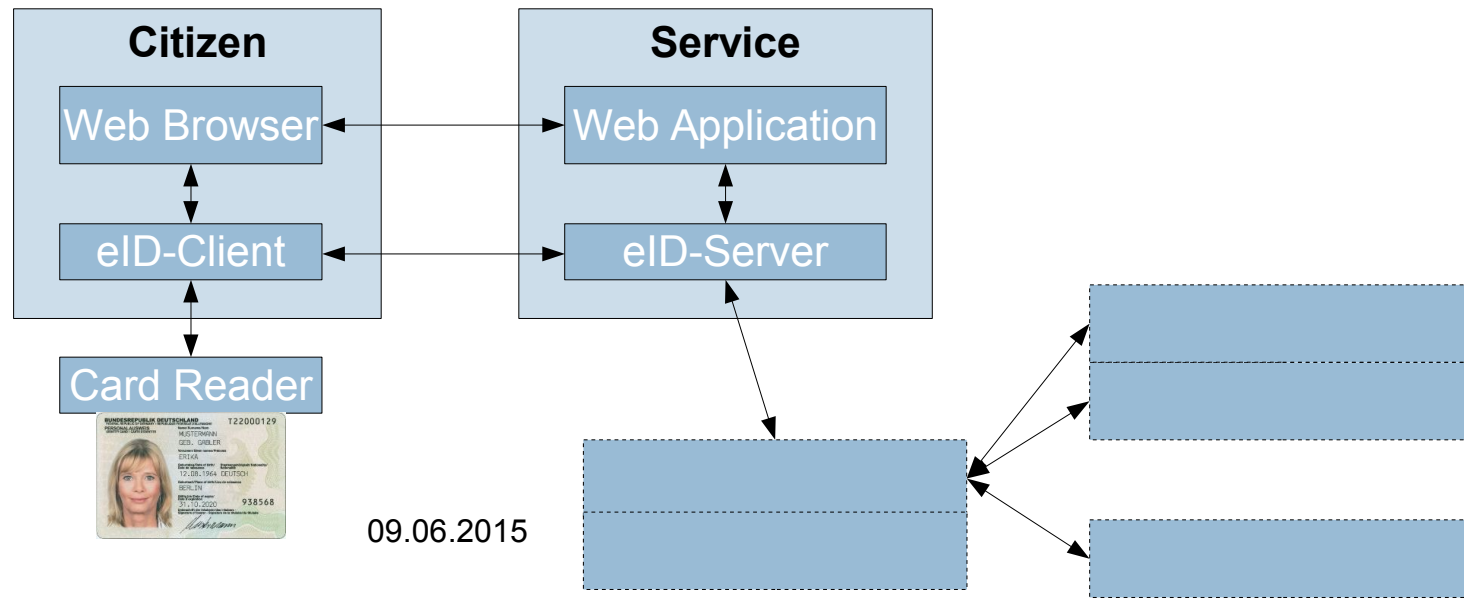
PersoSim

- ❑ Common project of
 - ❑ Bundesamt für Sicherheit in der Informationstechnik (BSI)
 - ❑ HJP Consulting GmbH

- ❑ Goals
 - ❑ Provide an example implementation of crypto/access protocols for eID
 - ❑ Simulate chip functionality (Layer 6/7)
 - ❑ Replace test cards by software simulation
 - ❑ Testbed for new features

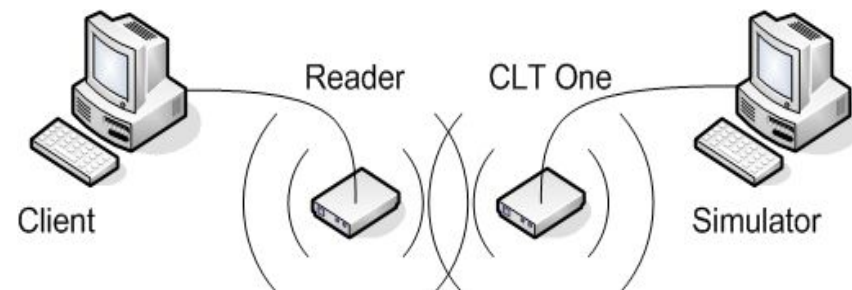
Current Situation – Integration Testing –

- eID scheme consists of/utilizes many components
 - Browser, Application, eID Client, eID Server, ...
 - For most of them several implementations / different vendors
- Currently: Integration tests done with test cards
 - Many different flavours
 - Chip version/vendor; COS version/vendor; different generations, ...
 - → combinatorial explosion



Current Situation

- ❑ New protocols/features
 - ❑ Specification → Implementation → Testing → and back
 - ❑ Currently: Implement on chip
 - ❑ Many players involved – chip vendor, COS vendor, ...
- ❑ Conformity testing of card reader, client software, ...
 - ❑ Currently: Use (commercial) hardware based card simulator
 - ❑ Hardware simulator provides ISO 14443 layer
 - ❑ Great for Layer 1-4 reader tests, but unnecessary for higher layer tests



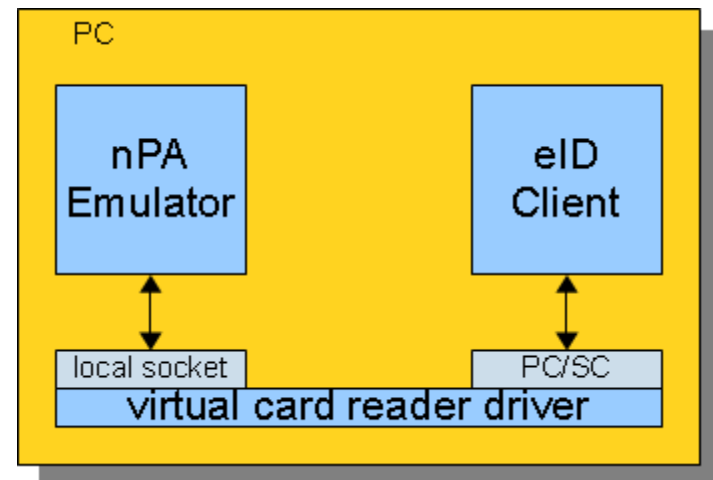
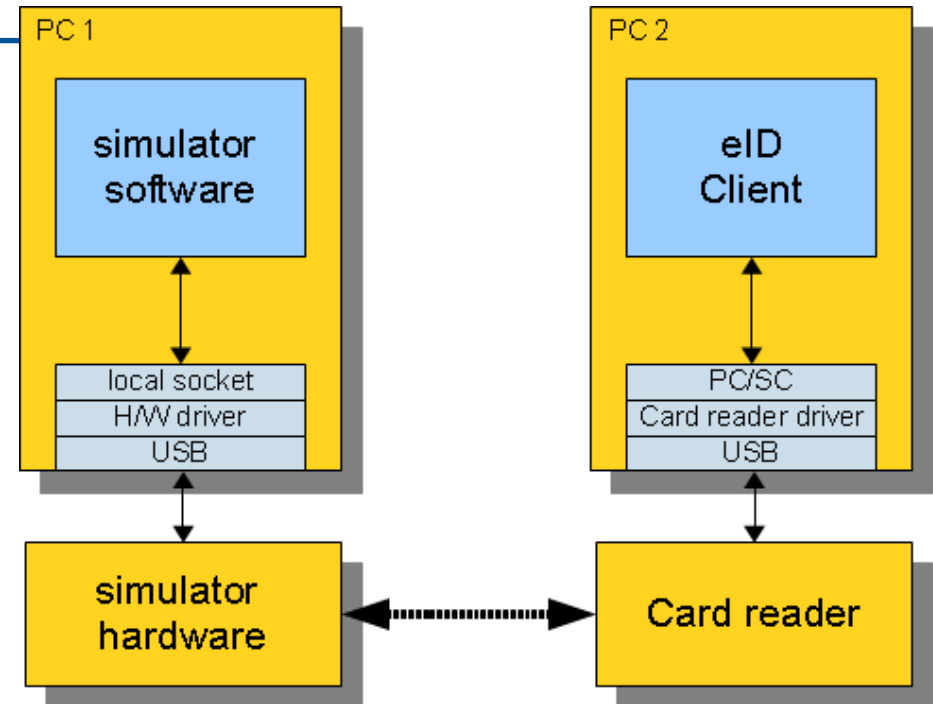
PersoSim

- ❑ Software simulation of complete German eID Card as specified in BSI TR-03110, including
 - ❑ PACE
 - ❑ Terminal Authentication
 - ❑ Chip Authentication
 - ❑ Restricted Identification
 - ❑ Age verification
- ❑ Personalisation files for
 - ❑ Beta-PKI / Test-PKI (same PKI as test cards)
 - ❑ Different data sets, “edge cases”, ...
- ❑ Certified according to TR-03105 for conformity to TR-03110
- ❑ Open Source (GPL)



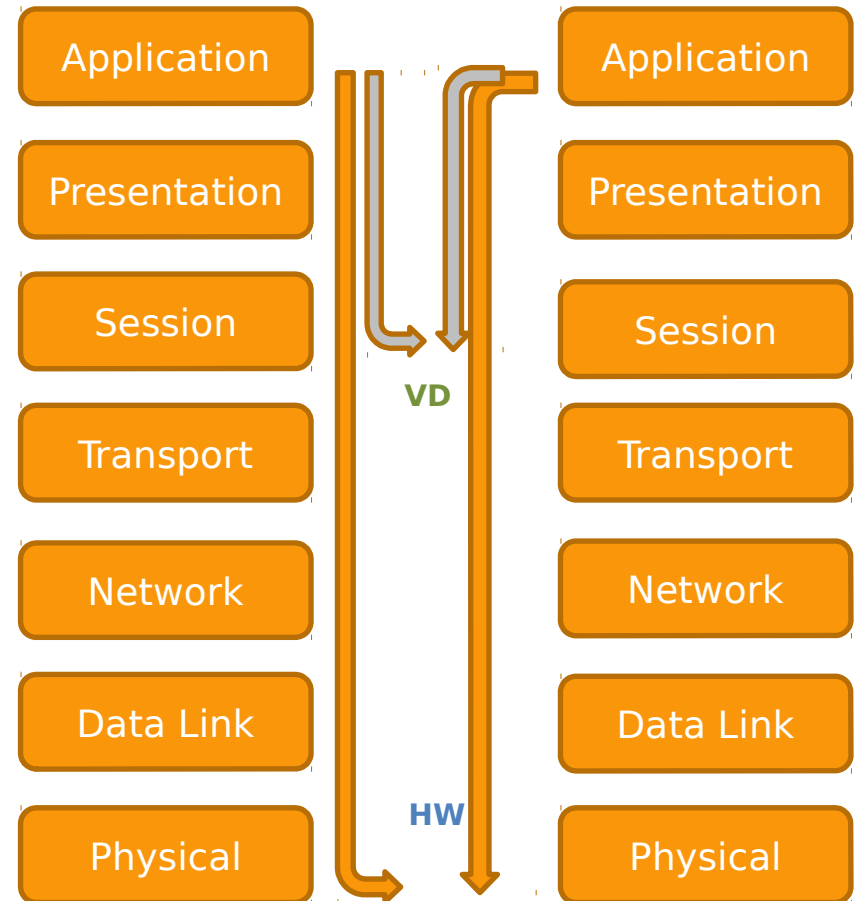
Communication

- ❑ Virtual card reader
 - ❑ Instead of HW simulator
- ❑ PC/SC interface to client software
- ❑ No (physical) card reader necessary
- ❑ Simplified setup

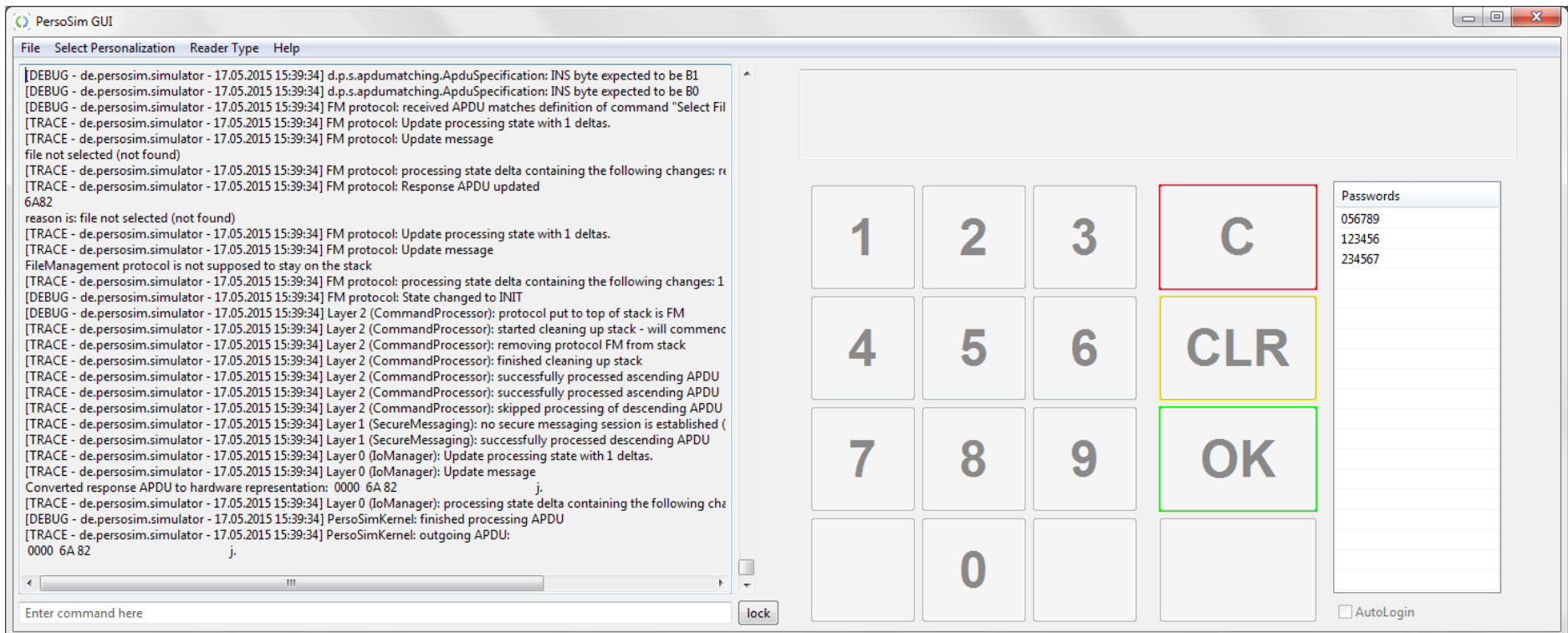


Communication

- ❑ Virtual card reader
 - ❑ Instead of HW simulator
- ❑ PC/SC interface to client software
- ❑ No (physical) card reader necessary
- ❑ Simplified setup



- ❑ Simulator provides full trace of commands/responses
- ❑ Virtual card reader with/without PIN pad



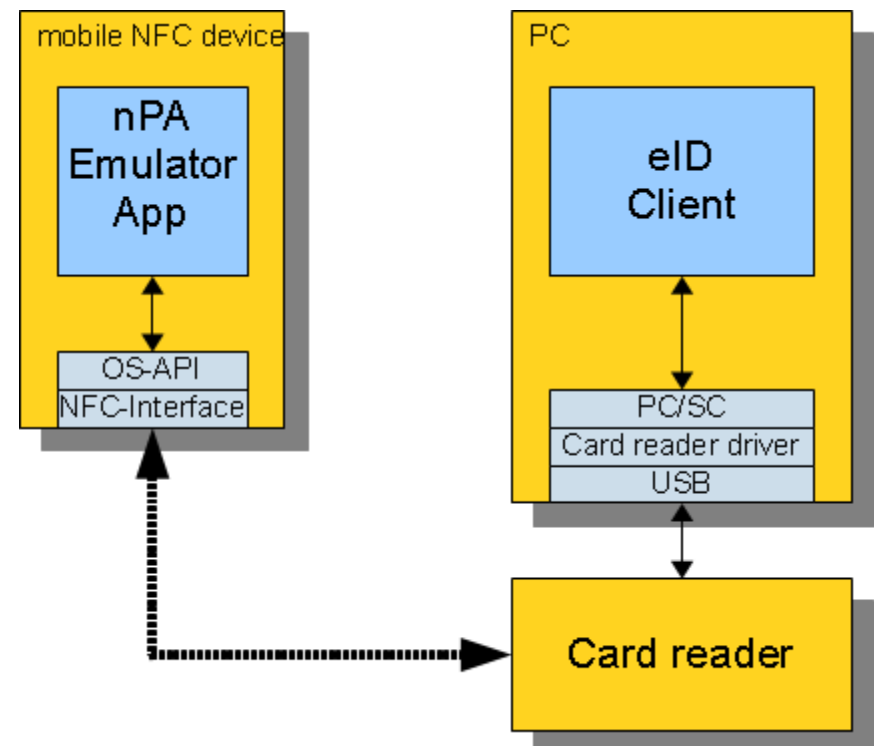
Smartphone as Card

- ❑ PersoSim ported as Android App
- ❑ Communication via NFC interface
- ❑ Allows testing the full setup including reader
 - ❑ But no separate simulator hardware necessary
- ❑ Full personalization flexibility
 - ❑ ... as opposed to test cards



Smartphone as Card

- ❑ PersoSim ported as Android App
- ❑ Communication via NFC interface
- ❑ Allows testing the full setup including reader
 - ❑ But no separate simulator hardware necessary
- ❑ Full personalization flexibility
 - ❑ ... as opposed to test cards



Future

- ❑ Possible enhancements (some of them already in progress)
 - ❑ Nice GUI for the android simulator
 - ❑ Integration of additional/new protocols / testing of new ideas
 - ❑ ePassport, eIDAS Token
 - ❑ Bugfixes
 - ❑ ...
- ❑ Join the community!
 - ❑ Users → www.persosim.de
 - ❑ Ready to use binaries, manuals, personalisation files, ...
 - ❑ Developers → <https://github.com/PersoSim>
 - ❑ Source code, style guide, wiki, ...

Contact

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185 – 189
53175 Bonn

Tel: +49 (0)22899-9582-5051
Fax: +49 (0)22899-10-9582-5051

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

