PersoSim – Der Open-Source-Simulator für den Personalausweis
14. Deutscher IT-Sicherheitskongress 2015

Bundesamt
für Sicherheit in der
Informationstechnik

BSI
Tobias Senger

HJP Consulting
Holger Funke

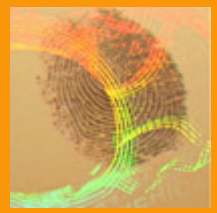
Navigating the complexities of *e-identity* is a challenge
WE FIND WAYS

HJP CONSULTING.

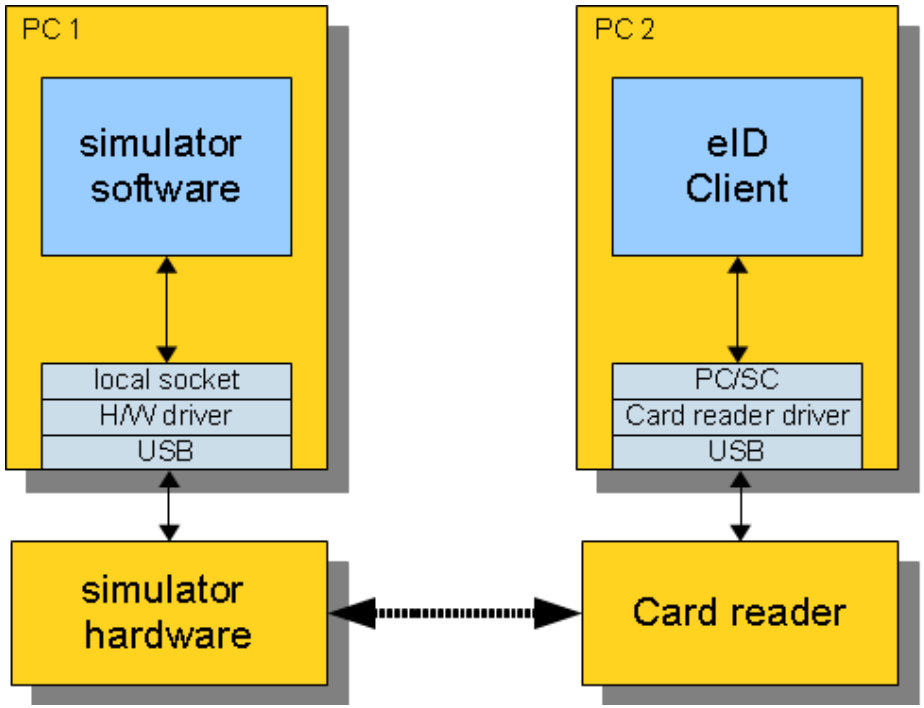
Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

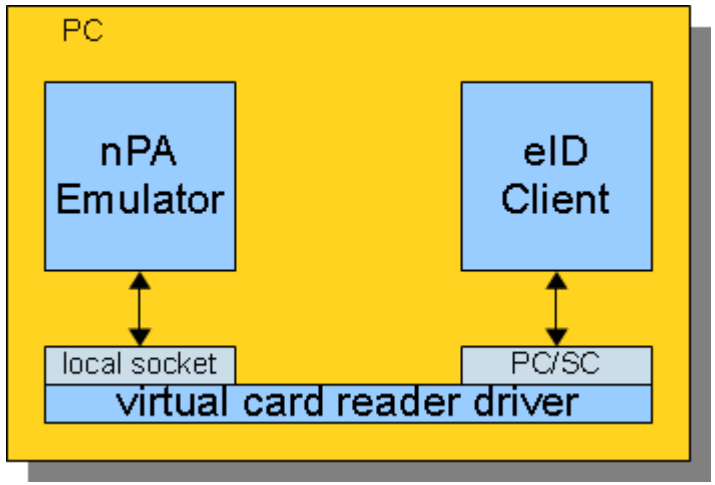
- **Anforderungen des BSI**
- Bisherige Vorgehensweise
- Simulator
- Virtuelle Kartenleser
- Simulation auf Mobilgeräten
- Communities
- Roadmap / Nächste Schritte



Anforderungen: Bisheriger Status und Ziele

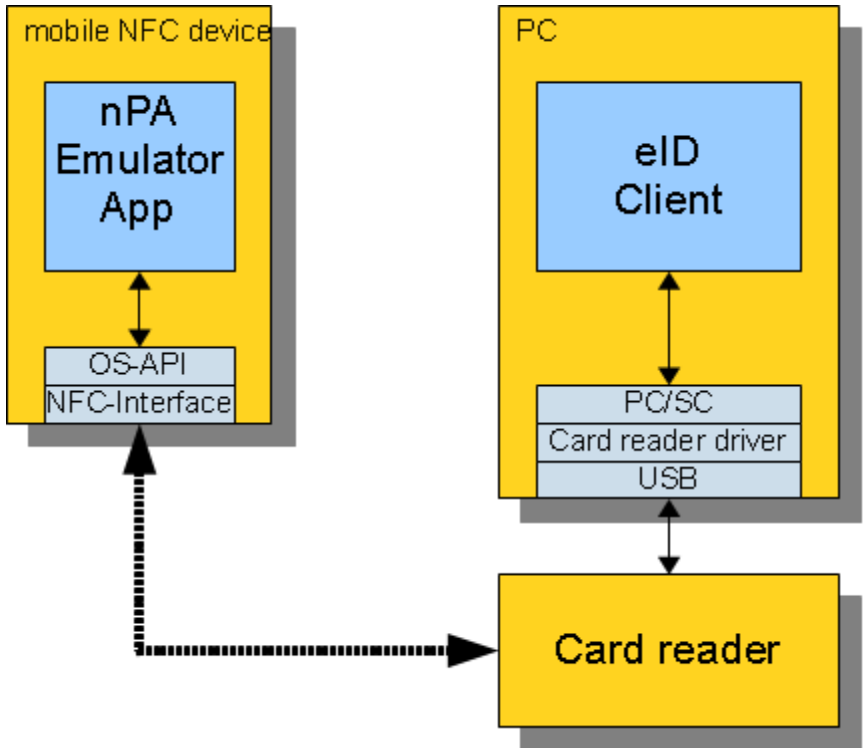


Bisheriger Status



Zielstatus

Anforderung: Simulation auf mobilen NFC-Geräten

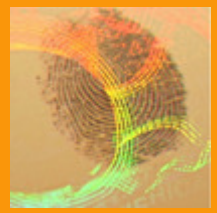


HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Anforderungen des BSI
- **Bisherige Vorgehensweise**
- Simulator
- Virtuelle Kartenleser
- Simulation auf Mobilgeräten
- Communities
- Roadmap / Nächste Schritte



Aktueller Status: Entwicklung neuer Smart Card-Protokolle

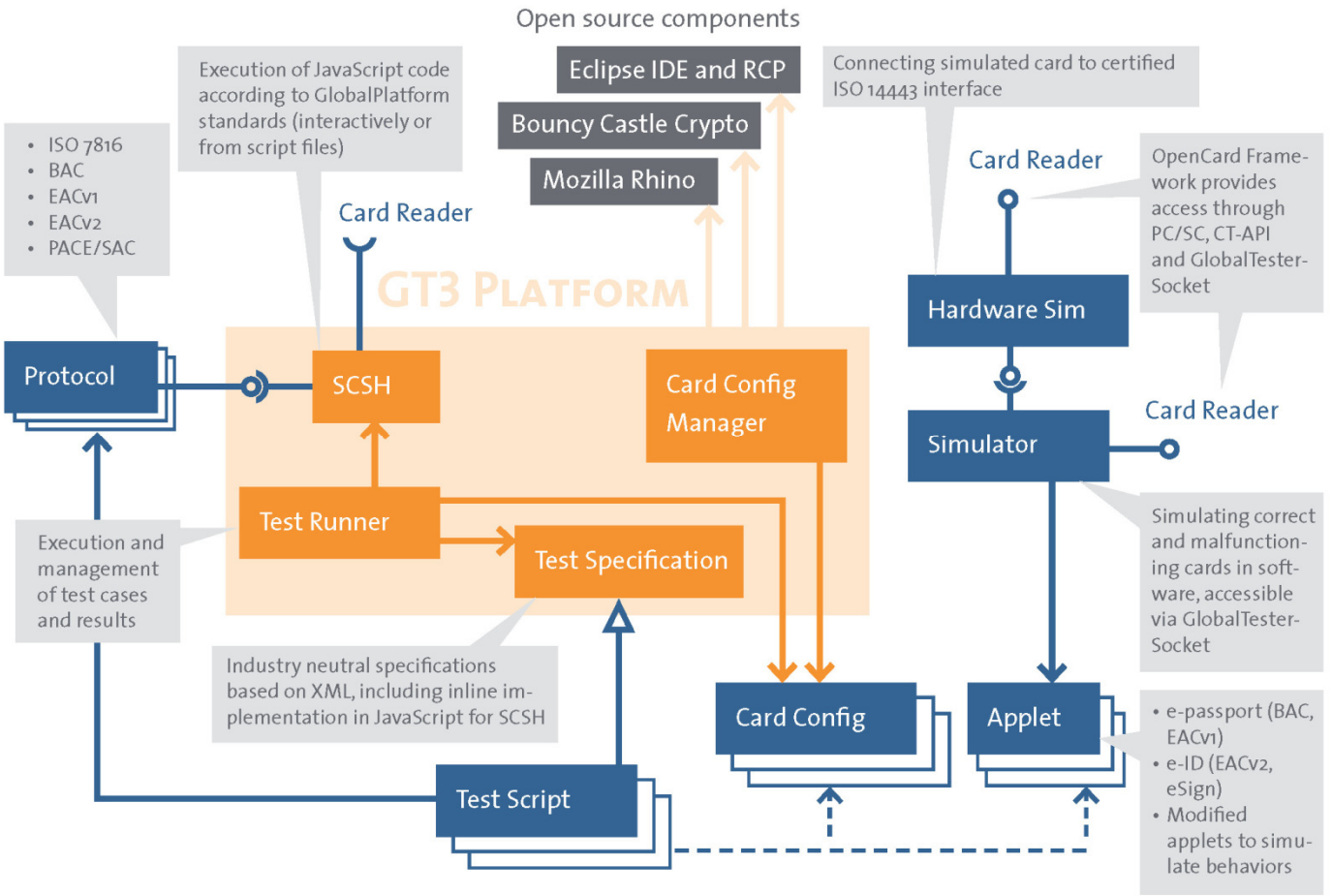
- Zeitintensiv:
  - Zahlreiche Mitspieler:
    - Chip-Entwickler und -hersteller
    - COS Entwickler
    - Applikations-Entwickler
    - Systemintegratoren
  - Chip muss produziert werden, um damit zu arbeiten
  - Lebenszyklus während der Entwicklung kurz, Spezifikationen ändern sich häufig
  - Unterschiedliche Konfigurationen müssen betrachtet werden
  - Unterschiedliche Zertifikate müssen zur Verfügung stehen
    - Benötigt werden aktuelle Test-Zertifikate
- Teuer:
  - Musterkarten sind teuer in der Produktion
  - Unterschiedliche Mitspieler müssen an Bord geholt werden

Aktueller Status: GlobalTester Testwerkzeug und -plattform

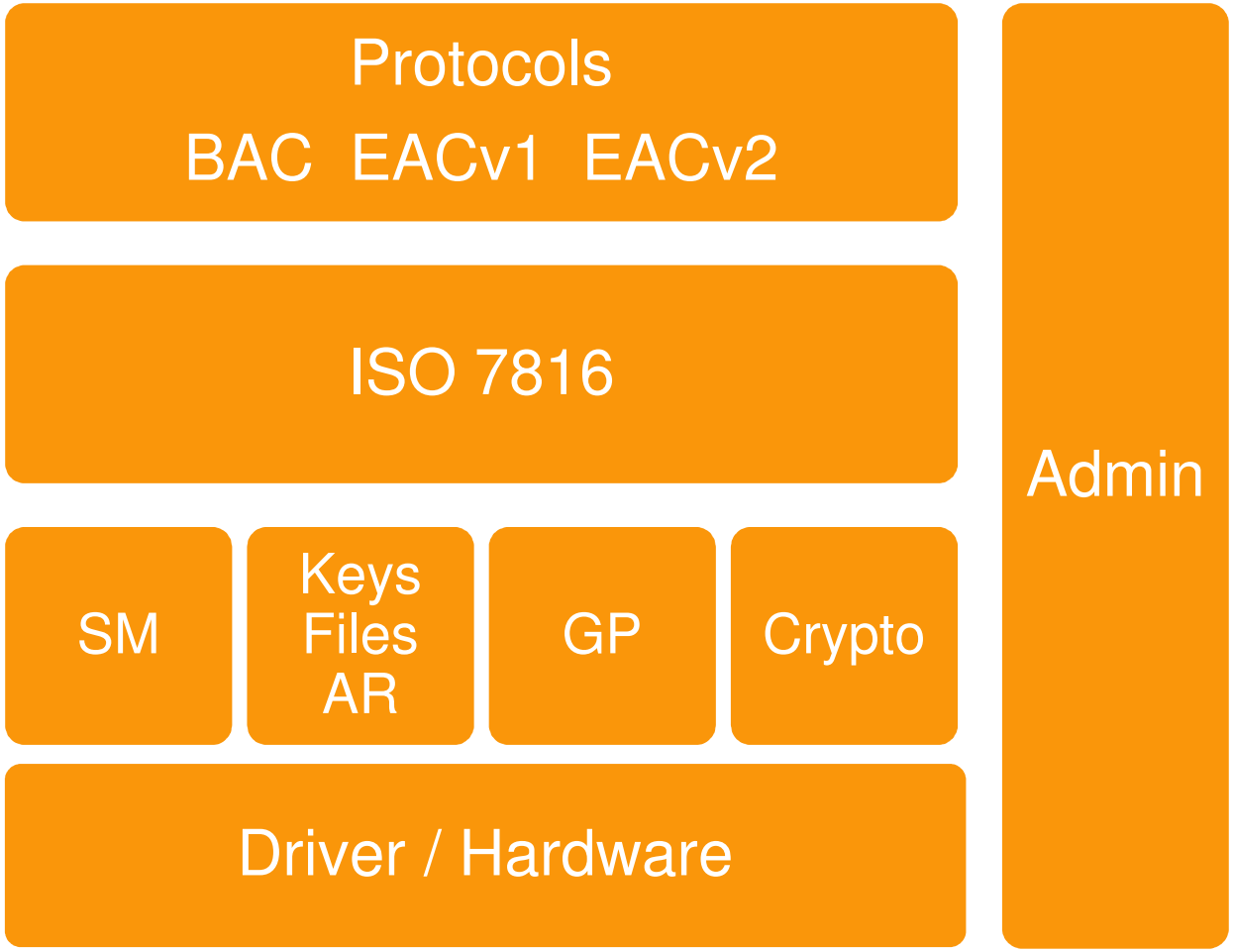
- GlobalTester
  - Open Source Testwerkzeug für Chipkarten und Lesegeräte
    - Eclipse Framework
    - Rhino Engine
    - Bouncy Castle Crypto Bibliothek
    - Smart Card Shell
  - Erste Version bereits 2005 (www.globaltester.org)
    - Open community
    - Closed community

- GlobalTester Prove IS / ePA-R:
  - Um Lesegeräte zu testen, muss der Chip simuliert werden
  - Vollständige Implementierung der BSI TR-03110
    - Quell-Code steht zur Verfügung

Architektur der GlobalTester Plattform

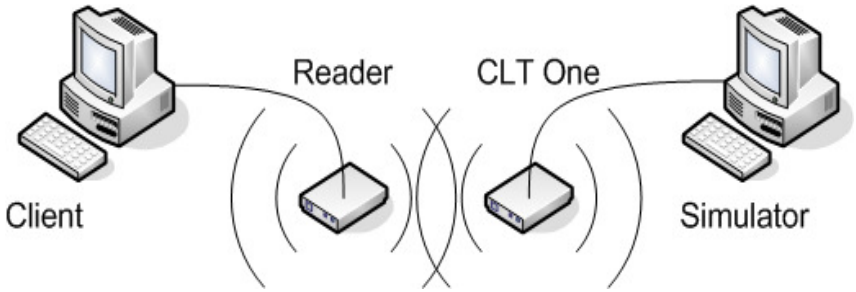


Architektur des Simulators



Kommunikation mit Simulator via Hardware

- Fehlendes Verbindungsglied zwischen Software-Simulator und Terminal
- Bisherige Lösung benötigt
  - Comprion CLT one (kommerzielle Hardware)
  - Handling der ISO 14443-Kommunikation (transfer speed, modulation type, etc.)
  - Anschaffung der Hardware als Einstiegshürde für Open Source-Projekte



Zusammengefasste Projektziele für PersoSim

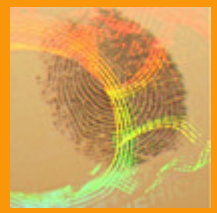
- Simulation der Personalausweisfunktionen in Open-Source-Software
- Umgehung des Hardware-Kartenlesers
- Aufbau einer Community zum Einsatz / Entwicklung der Software
- Simulation des Personalausweis auf mobilem NFC-Gerät

HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Anforderungen des BSI
- Bisherige Vorgehensweise
- **Simulator**
- Virtuelle Kartenleser
- Simulation auf Mobilgeräten
- Communities
- Roadmap / Nächste Schritte



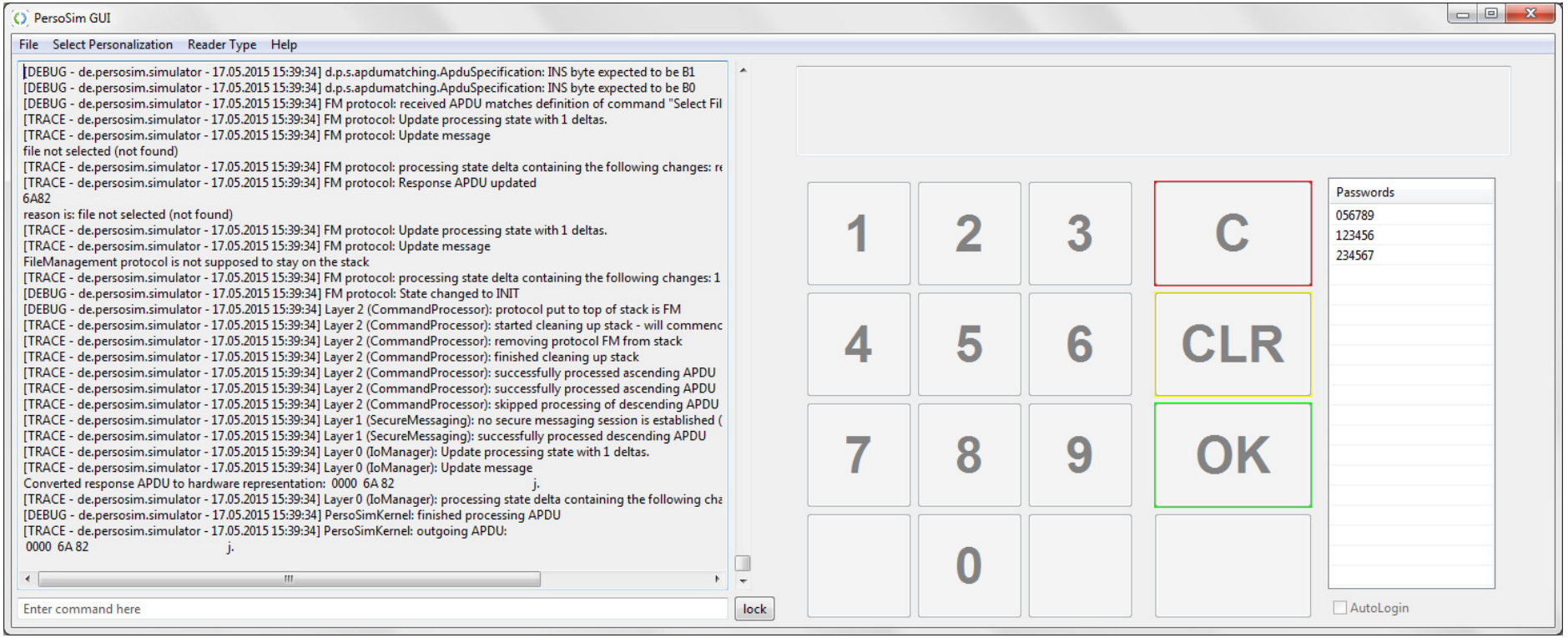
Simulator: Umsetzung in Software

- Funktionalität des elektronischen Personalausweis gemäß TR-03110 umgesetzt:
  - PACE
  - Chip Authentication
  - Terminal Authentication
  - Restricted Identification
  - Altersverifikation
- Integration in die Test-PKI und Beta-PKI des BSI
  - Signieren der Daten
  - Zertifikate gemäß PKI
- Zertifiziert durch BSI gemäß TR-03110 bzw. TR-03105

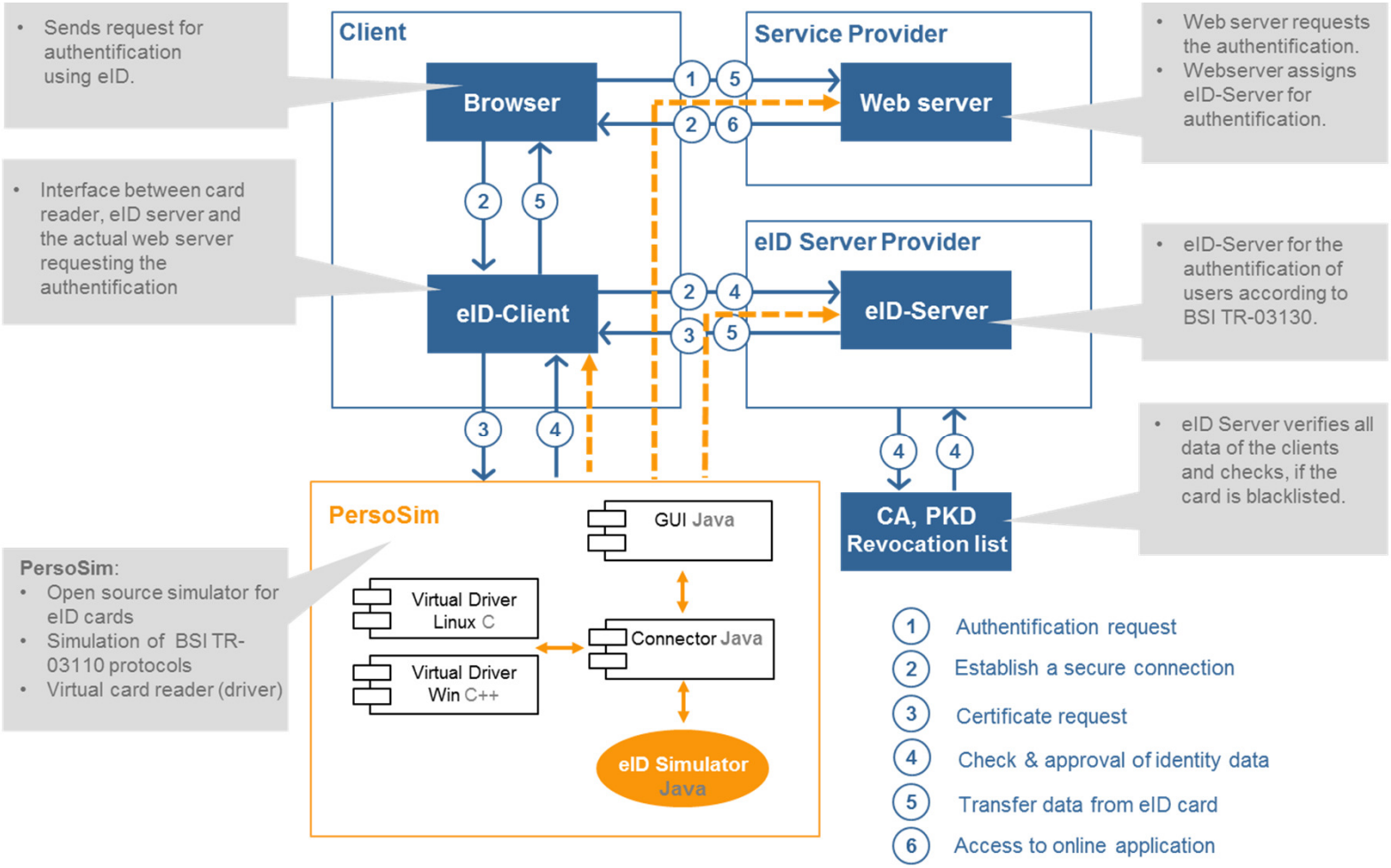
Simulator: Personalisierungsdaten

- Personalisierung orientiert an „Familie Mustermann“ der BDr
- 10 Personalisierungsprofile werden mitgeliefert, eigene Profile können erstellt werden
- Varianten bzgl. Inhaber-Daten:
  - Geburtsdatum, z.B. zwischen 16 und 18
  - Lange Dateninhalte, z.B. Familiennamen
  - Unvollständige Geburtsdaten
  - Gesperrte Ausweise
- Varianten bzgl. nPA-Daten:
  - Varianten des Personalausweise seit 11/2010
    - PrivilegedTerminalInfos fehlten bis Q3/2011
    - Datengruppe „Geburtsname“ hinzugefügt
    - Datengruppe „Nationalität“ hinzugefügt

Simulator: Screenshot



Simulator: Einordung in deutsche eID-Landschaft

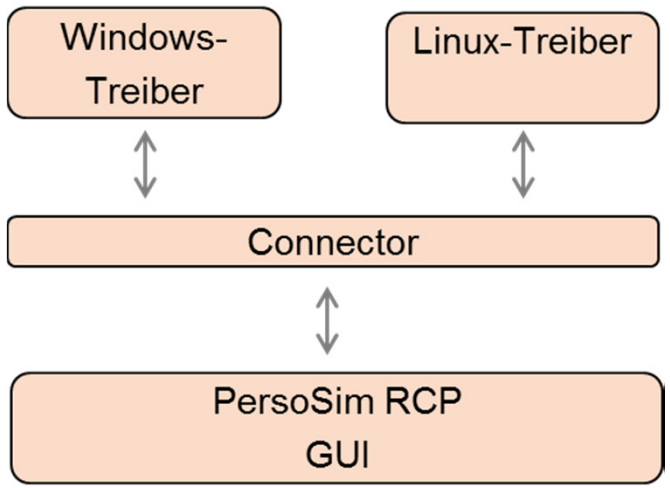


Agenda

- Anforderungen des BSI
- Bisherige Vorgehensweise
- Simulator
- **Virtuelle Kartenleser**
- Simulation auf Mobilgeräten
- Communities
- Roadmap / Nächste Schritte

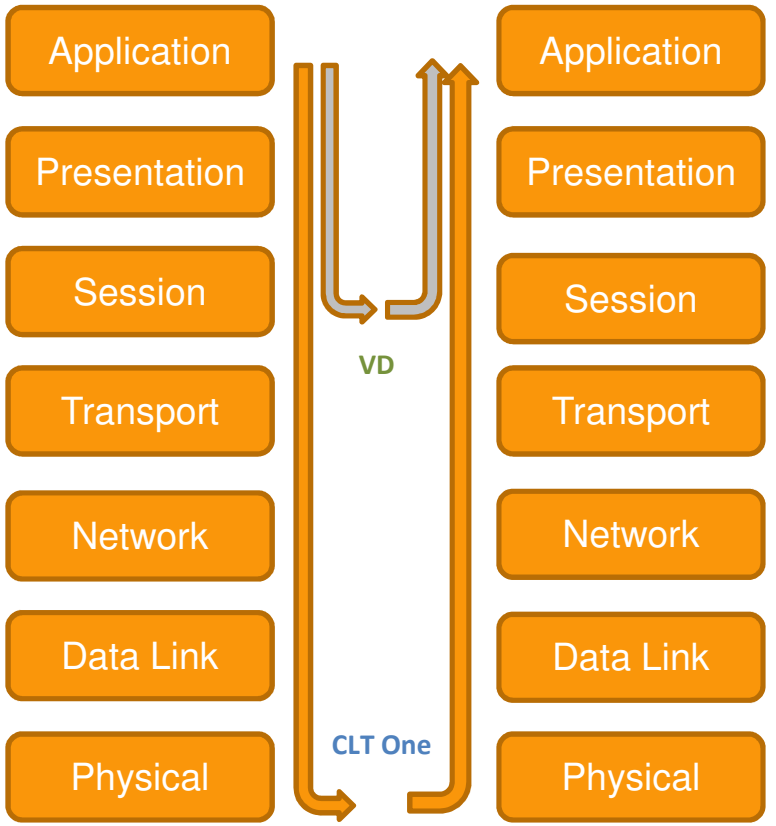
Virtuelle Kartenleser (I)

- Virtueller Kartenleser als Ersatz für Hardware
- Implementierung der PC/SC-Funktionen
- Simulation in Kontext des Personalausweises:
  - Basisleser
  - Standard-/Komfortleser inkl. PIN-Pad (gemäß TR-03119)
- Unterstütze Plattformen:
  - Windows 7 und Windows 8 (32 und 64 Bit)
  - Ubuntu Linux (32 und 64 Bit)
- Schlanke Treiber, Logik im Connector



Virtuelle Kartenleser (II)

- Virtueller Kartenleser integriert sich in das Betriebssystem wie ein gewöhnlicher Hardware-Kartenleser
- Kann als Kartenleser von üblichen Programmen (z.B. AusweisApp) adressiert werden
- Source Code basiert auf
  - Projekt von Fabio Ottavi
  - Microsoft-Sample für UMDF

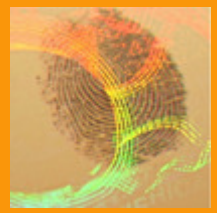


HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

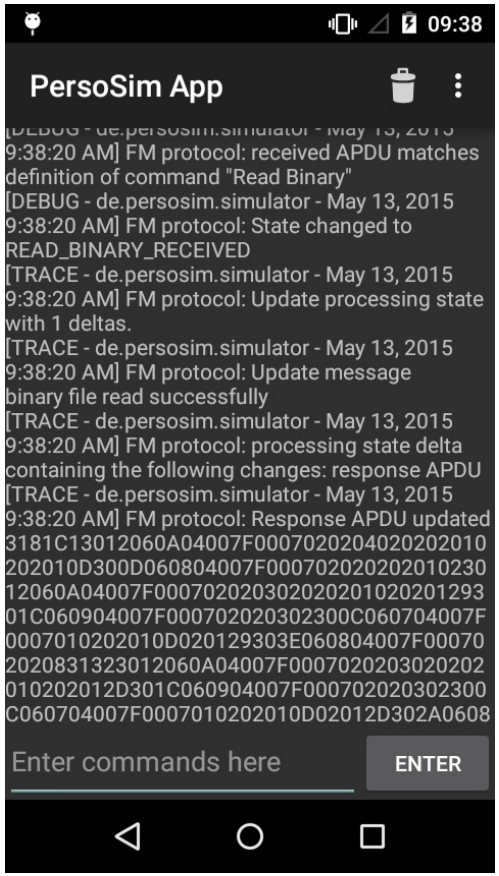
Agenda

- Anforderungen des BSI
- Bisherige Vorgehensweise
- Simulator
- Virtuelle Kartenleser
- **Simulation auf Mobilgeräten**
- Communities
- Roadmap / Nächste Schritte



Simulation auf Mobilgeräten

- Portierung des Simulators auf Android
- Nutzung der NFC-Schnittstelle zur Kommunikation
- Adressierbar über Standard-Kartenleser
- Auswahl zwischen zehn Personalisierungen
- Modifikation der LibNFC (Android) notwendig
- Source Code steht ebenfalls zur Verfügung
- Verwendete Hardware:
  - Nexus 7
  - Sony E3

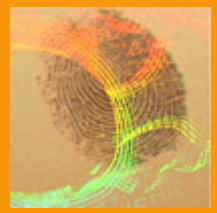


HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Anforderungen des BSI
- Bisherige Vorgehensweise
- Simulator
- Virtuelle Kartenleser
- Simulation auf Mobilgeräten
- **Communities**
- Roadmap / Nächste Schritte



Communities

- Anwender-Community
  - Manuals zum Einsatz des Simulators
  - Installationsanleitungen
  - Informationen zu den zehn Personalisierungen
  - Referenzen auf weitere eID-Projekte (Open Source)
  - Informationen zu Varianten des Personalausweises
  - Website: www.persosim.de

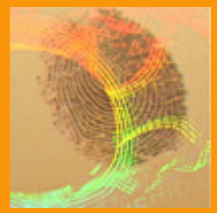
- Entwickler-Community
  - Wikis mit Informationen zur Architektur des Simulators
  - Source Code für Simulator, virtuelle Kartenleser, Android
  - Issue-Tracking, Source-Code-Verwaltung
  - Kommunikation/Integration der Entwickler
  - Website: https://github.com/PersoSim

HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Anforderungen des BSI
- Bisherige Vorgehensweise
- Simulator
- Virtuelle Kartenleser
- Simulation auf Mobilgeräten
- Communities
- **Roadmap / Nächste Schritte**



Roadmap / Nächste Schritte

- Projektstart: Ende 2013
- Erste Version der virtuellen Treiber (Basisleser) und Simulator: Dezember 2013
- Basis-/Komfortleser-Funktionalität: März 2015
- Stetige Erweiterung des Simulators
  - Speichern von PINs, Automatische PIN-Eingabe, Bugfixes
- Januar 2015: Zertifizierung des Simulators
- Android-Portierung: Mai 2015
- Weiterhin Betreuung der Communities

JOIN NOW!

- Zukunft (seit Mai 2015):
  - Implementierung von eIDAS-Funktionen für den Simulator
    - Chip Authentication Version 3
    - Pseudonyme Signaturen

HJP CONSULTING.

Bundesamt
für Sicherheit in der
Informationstechnik

Fragen?

HJP Consulting GmbH
Holger Funke
Hauptstraße 35
33178 Borchen, Germany

tel: +49 5251 41 77 633
fax: +49 5251 41 77 666
e-mail: holger.funke@hjp-consulting.com
web: www.hjp-consulting.com
www.globaltester.org
www.persosim.de