An Open Source eID Simulator
Open Identity Summit
9th -11th September 2013

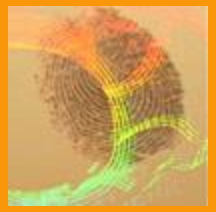
Bundesamt
für Sicherheit in der
Informationstechnik

BSI
Tobias Senger

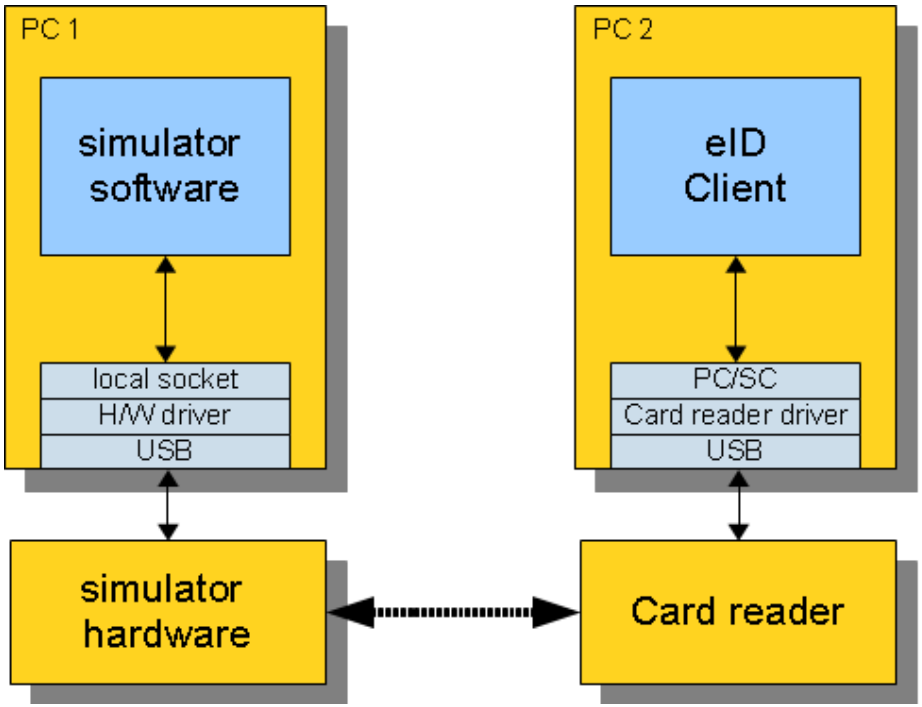
HJP Consulting
Holger Funke

Agenda

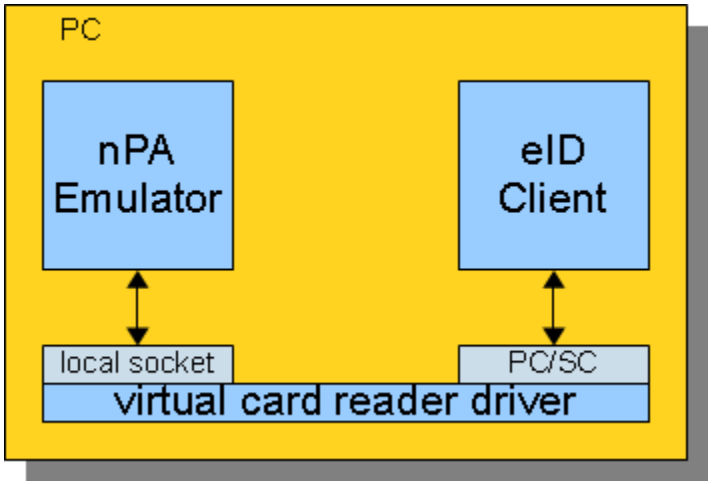
- **Requirements of BSI**
- Current state
- Simulator
- Virtual Smart Card Reader
- Community
- NFC Device
- Planned Roadmap
- Next steps



Requirements: Actual state and target state

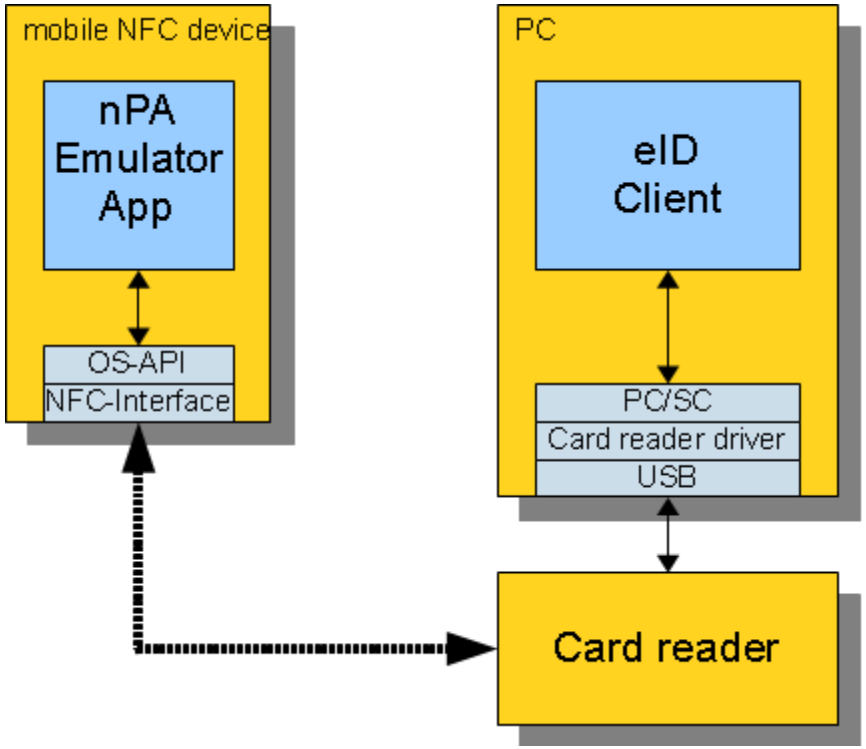


Actual state



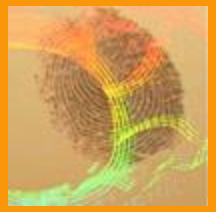
Target state

Requirements: Simulator on mobile NFC device



Agenda

- Requirements of BSI
- **Current state**
- Simulator
- Virtual Smart Card Reader
- Community
- NFC Device
- Planned Roadmap
- Next steps



Current state: Developing new smart card protocols

- Time consuming:
  - Several stakeholder:
    - Chip developer / manufacturer
    - COS developer
    - Application developer
    - Integrator
  - Chip must be produced to work with
  - Life cycle during development very short, „living“ specifications
  - Handling of various configurations (data groups, keys, etc)
  - Handling of certificates (Extended Access Control, EAC)
    - Need of „fresh“ test certificates
- Expensive:
  - Sample cards are expensive
  - Several stakeholders
  - Hardware „chip“ must be produced

Current state: GlobalTester test tool

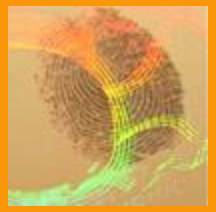
- GlobalTester
  - Open Source test tool for smart cards and inspection systems
    - Eclipse framework
    - Rhino Engine
    - Bouncy castle crypto lib
    - Smart Card Shell
  - Started in 2005 (www.globaltester.org)
    - Open community (test manager, sample scripts)
    - Closed community (commercial: test scripts, simulator)

- GlobalTester Prove IS / ePA-R:
  - To test the inspection system, chip must be simulated
  - Currently implementation of BSI TR-03110 V2
    - Code available

Agenda

- Requirements of BSI
- Current state
- **Simulator**
- Virtual Smart Card Reader
- Community
- NFC Device
- Planned Roadmap
- Next steps

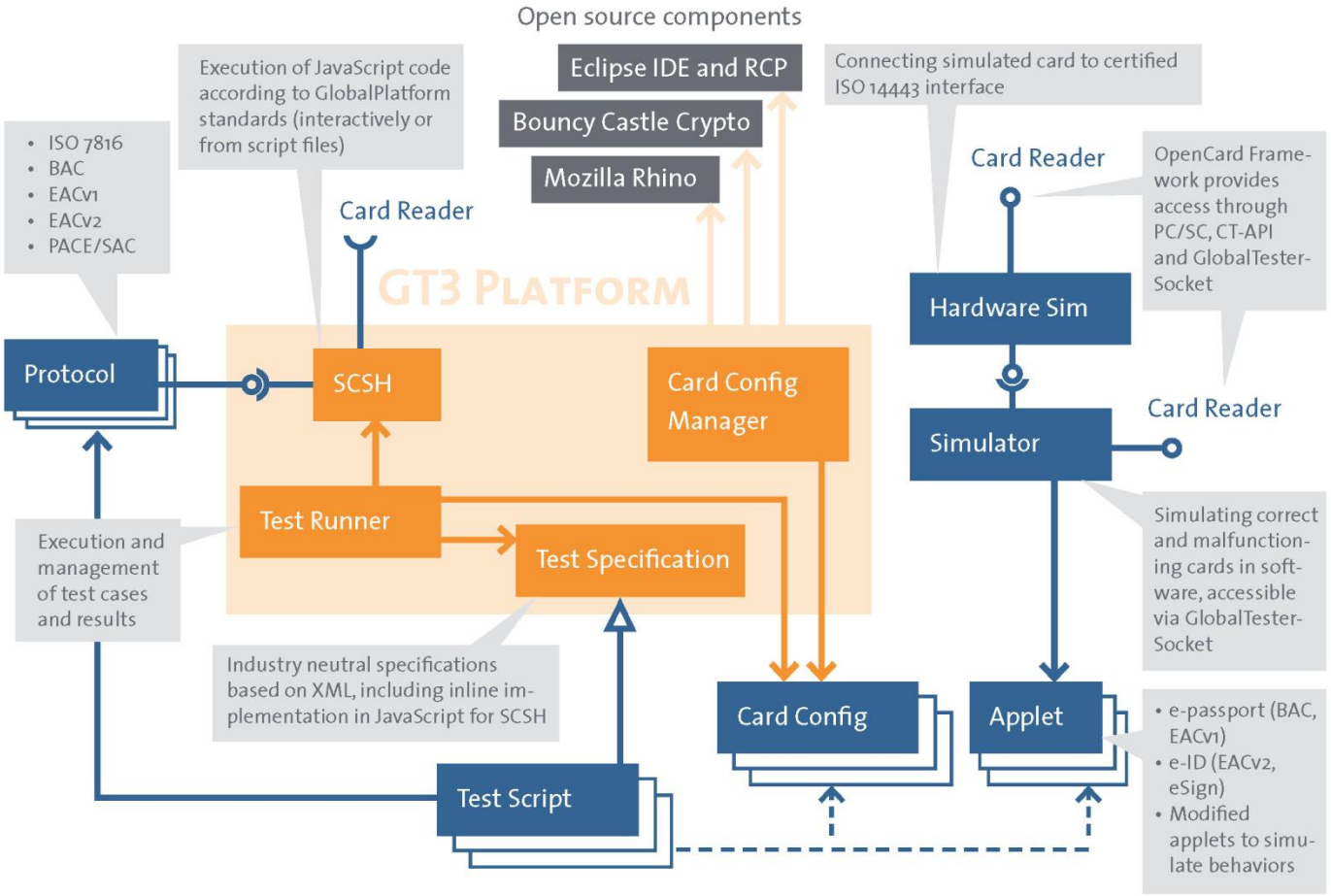





Current state: Software-Simulator (I)

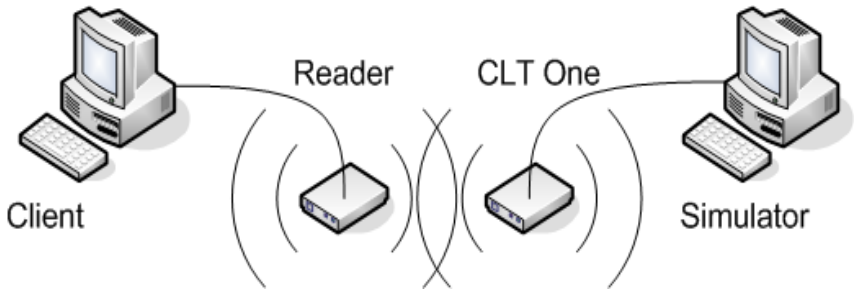
- Implementation (close to Java Card)
  - All protocols, algorithms of BSI-TR-03110 V2 ready
    - EACv1:
      - » Basic Access Control
      - » Chip Authentication v1
      - » Terminal Authentication v2
      - » Active / Passive Authentication
    - EACv2:
      - » PACE / SAC
      - » Chip Authentication v2
      - » Terminal Authentication v2
      - » Restricted Identification
      - » (Qualified electronic signature)
- Configuration via scripts (easy to personalize different cards)

GlobalTester Architecture

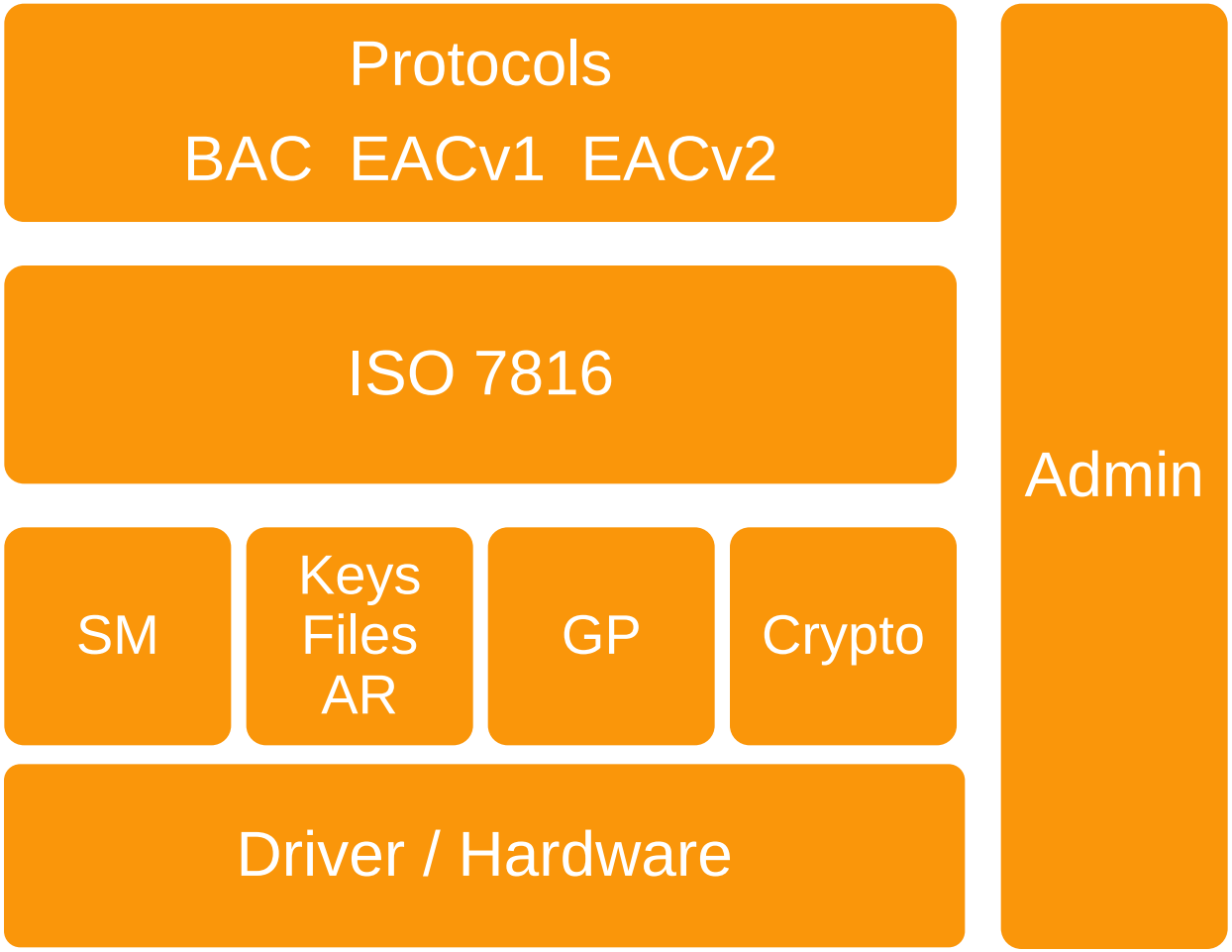


Current state: Software-Simulator (II)

- Missing link between Software-Simulator and Terminal (IS)
- Current solution needs piece of hardware
  - Comprion CLT one (commercial)
  - Handling of ISO 14443 communication (transfer speed, modulation type, etc.)
  - Hardware is expensive -> problem for Open Source projects



Simulator: Architecture



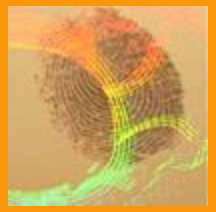
Benefits of Open Source eID Simulator

- Use simulator for testing
  - eID stakeholder like
    - eID Client developers, like Open eCard
    - eID Server developers
    - Solution developers, like eCommerce
- Use simulator to analyze protocols
  - Adapt protocols and test consequences
  - “Experimental platform”
- Easy to configure your eID card
  - In future: CardInfo files (?)
- Easy to understand protocols
  - Participation in “eID world” -> For example: Universities

Agenda

- Requirements of BSI
- Current state
- Simulator
- **Virtual Smart Card Reader**
- Community
- NFC Device
- Planned Roadmap
- Next steps

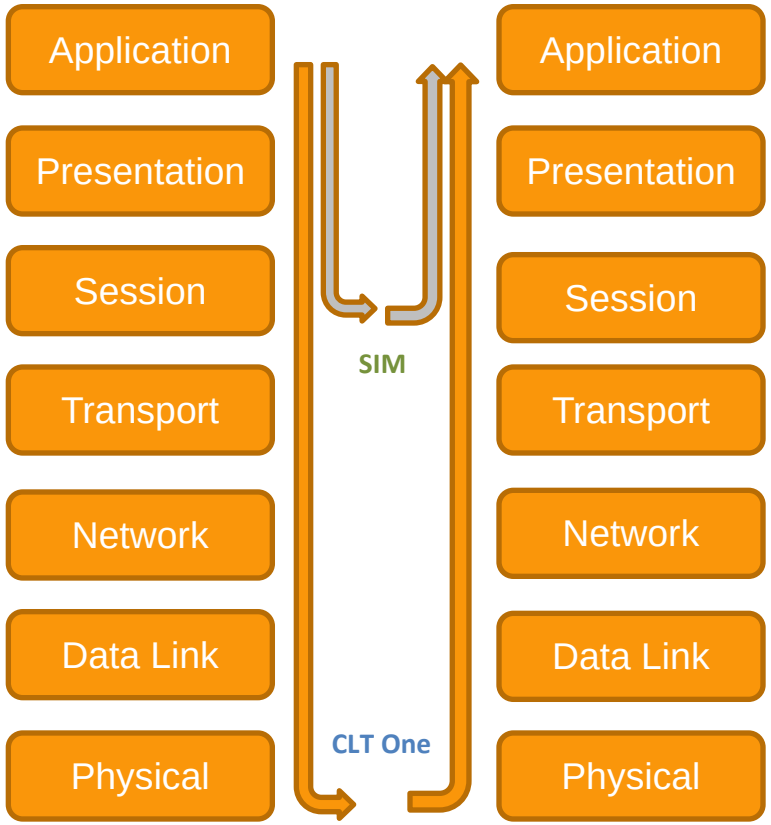





Open Source eID Simulator: Virtual Driver

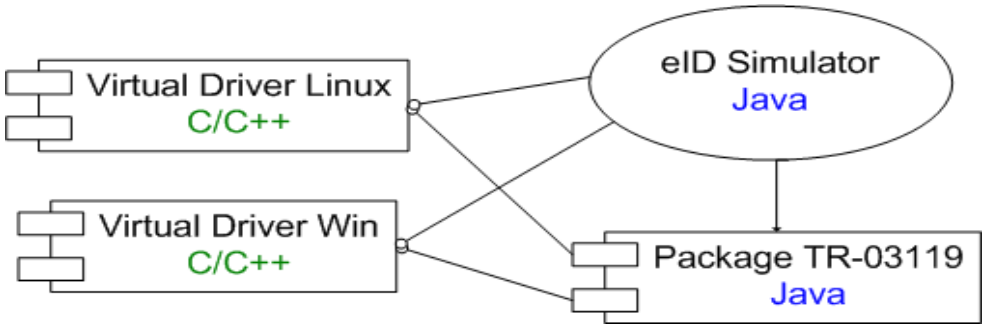
- Code is implemented and tested yet
  - Experience in several tests (e.g. interoperability tests)
  - Simulator can be addressed via TCP/IP-Socket
- Hardware must be substituted:
  - Solution: Virtual Smart Card Reader
    - Runs in operating system as typical physical reader
    - Runs as PC/SC device
    - Can be addressed by typical clients (like eID clients)
    - Handles communication between client and simulator
    - Will be implemented by HJP for operating systems:
      - » Microsoft Windows 7 (32 and 64 bit)
      - » Linux (Ubuntu) (32 and 64 bit)
    - Source Code of drivers will be published under GPL v3

Virtual Driver in ISO-OSI layer model



Simulator: Virtual Reader Driver

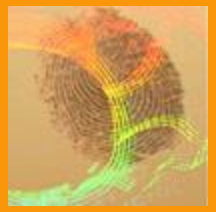
- Simulation of basic reader
  - Only APDU handling: receive APDU and send result
- Standard / Comfort Reader
  - Simulation of PIN-Pad
  - Simulation of TR-03119 functions:
    - EstablishPACEChannel()
    - ModifyPIN(),…



Agenda

- Requirements of BSI
- Current state
- Simulator
- Virtual Smart Card Reader
- **Community**
- NFC Device
- Planned Roadmap
- Next steps

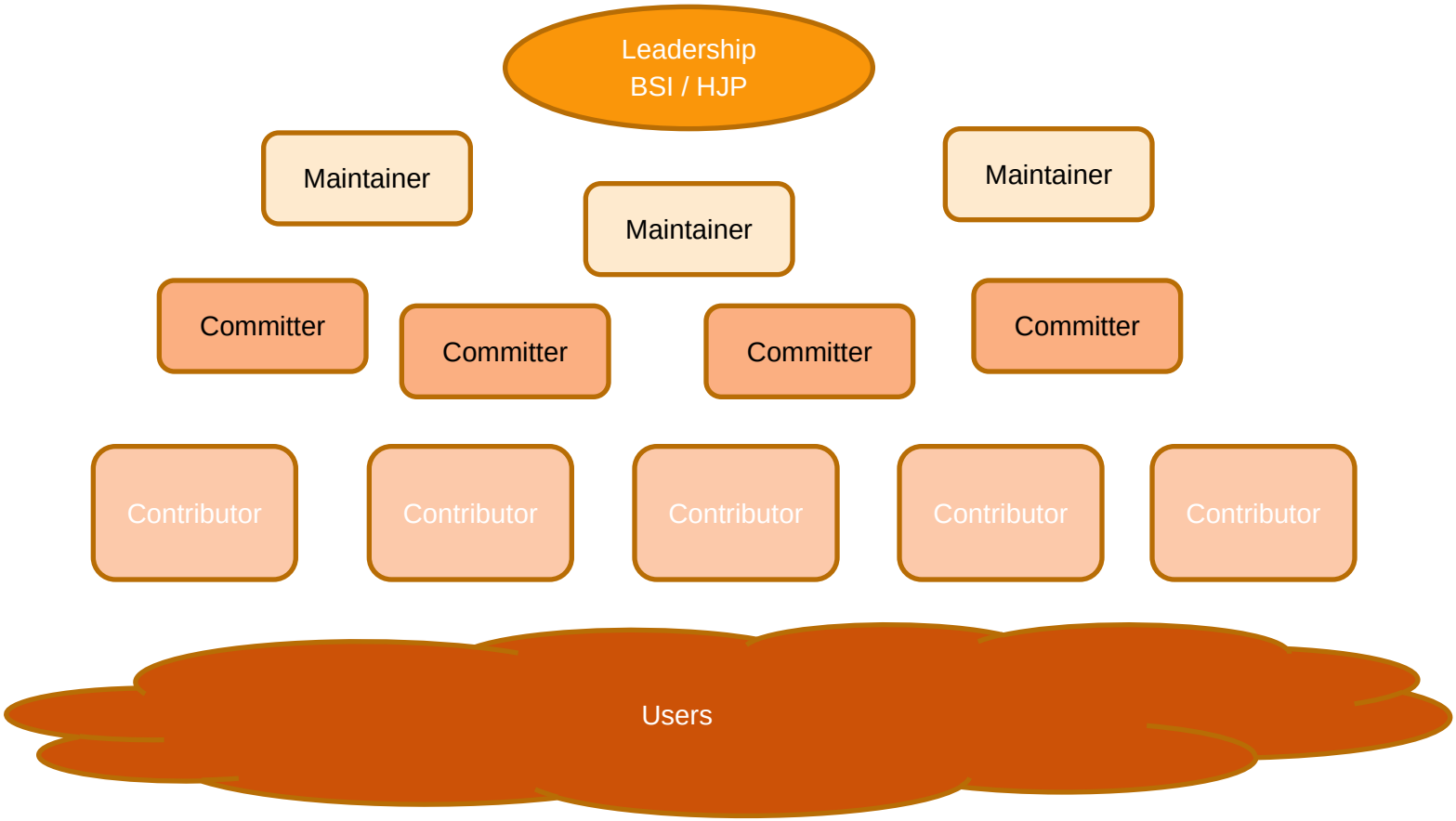





Community

- Web site
  - Basic information, URL is not defined yet ☺
- Code versioning system (repository)
  - First implementation (basic reader) for MS Windows
  - First version of simulator code
- Support for interested users / developers
  - Access to source code
  - Forum
  - Mailing list
  - Wiki
  - Manuals
  - FAQ
  - Bug / Issue tracking
  - Communication of release plan

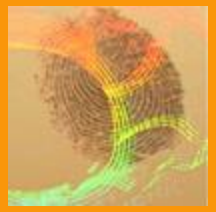
Community: Possible structure



Agenda

- Requirements of BSI
- Current state
- Simulator
- Virtual Smart Card Reader
- Community
- **NFC Device**
- Planned Roadmap
- Next steps



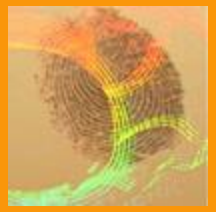



NFC Device

- Some uses cases need physical device (smart card)
- Hardware to simulate also physical characteristics: NFC device
- Use NFC interface to access simulator on smartphone / tablet
- Migration of simulator to NFC device
- Possible platforms
  - Windows Phone
  - Apple iOS
  - Android -> several NFC device, support, established libraries
- BSI has experience in Android applications with NFC:
  - androsmex
  - Student research projects

Agenda

- Requirements of BSI
- Current state
- Simulator
- Virtual Smart Card Reader
- Community
- NFC Device
- **Planned Roadmap**
- Next steps



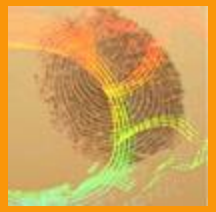
Roadmap

- Project is planned for two years (at least)
  - Lead
    - BSI: Tobias Senger
    - HJP Consulting: Holger Funke
  - Start September 2013
  - First results will be published in 2013
- Virtual Driver
  - First implementation (basic reader) for MS Windows
- Simulator
  - Code adaptions for launching needed
- Community
  - Web site with basic information in 2013, Hoster for Sources
- NFC Device
  - First migration of simulator in 2014

Agenda

- Requirements of BSI
- Current state
- Simulator
- Virtual Smart Card Reader
- Community
- NFC Device
- Planned Roadmap
- **Next steps**






Next steps, Call for Participation

- Simulation of German ID card
- Not only focussing on eID but also on smart card in general
  - Simulation of other applications:
    - eSign
    - Health
    - SIM
    - ….

Questions?

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