Agenda of Constitutive Advisory Board Meeting

Wednesday, September 4, 2013

12:30-12:45 **Welcome:** Ministerialrat Achim Hildebrandt (BMI) – Head of Division Passports and Identity Documents, Identification Systems

12:45-13:00 **Introduction to PersoApp & Advisory Board:**
Prof. Dr. Ahmad-Reza Sadeghi and Dr. Sven Wohlgemuth (TU Darmstadt/CASED)

13:00-13:30 **Introducing "PersoApp – Secure and User-Friendly Internet Applications":**
Prof. Dr. Ahmad-Reza Sadeghi and Dr. Sven Wohlgemuth (TU Darmstadt/CASED)

13:30-13:45 **Break**

13:45-14:15 **Introducing "PersoApp – Pre-Release and Open Source Software Library":**
Christian Bruntsch (AGETO Service GmbH)

14:15-14:45 **Introducing "PersoApp – Guidelines for Secure Integration of the PersoApp Open Source Software Library"**: Dr. Thorsten Henkel (Fraunhofer SIT)

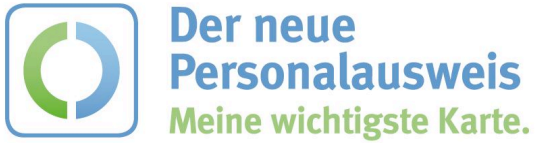
14:45-15:15 **Expectations of Advisory Board Members & Discussion:** Everyone

15:15-15:20 **Election of Chairman of the Advisory Board:** Everyone

15:20-15:30 **Miscellaneous**

PersoApp

An Open Source Community for the new German national ID Card



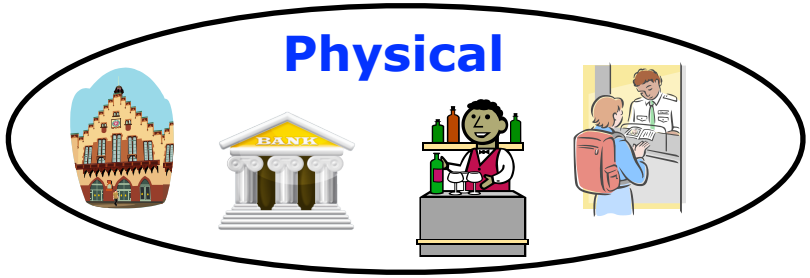
Constitutive Meeting of the PersoApp Advisory Board
Berlin, September 4, 2013

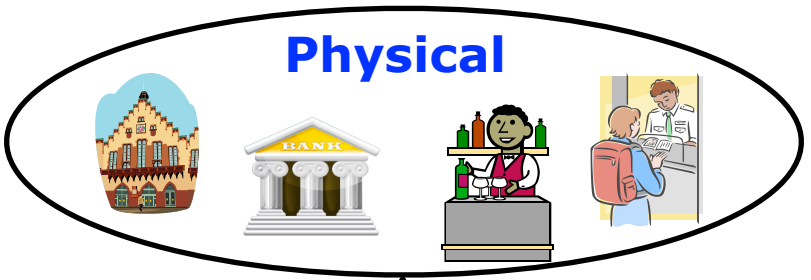
Prof. Dr. Ahmad-Reza Sadeghi
Dr. Sven Wohlgemuth

Head of PersoApp Consortium
Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt (CASED)

System Security Lab · Fraunhofer SIT · Technische Universität Darmstadt · CASED

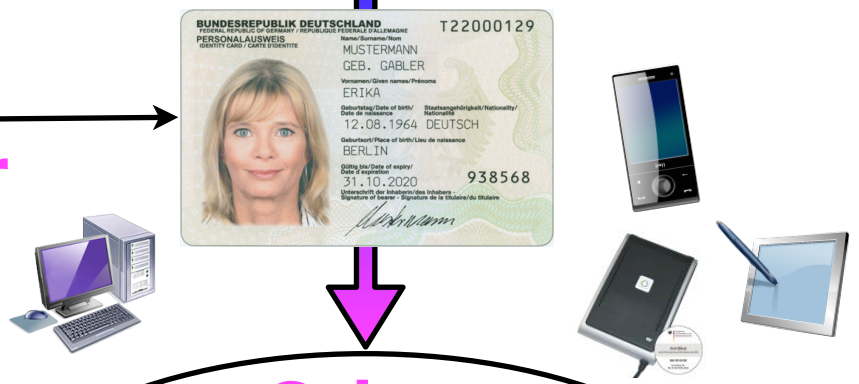
Electronic Identity and Applications





Physical

+ Cyber



Societal benefit

Re-using the existing national infrastructure of electronic identity for value-added services

PersoApp – Open Source Community

Citizen, Government, Industry, and Academia

Federal Ministry of the Interior (BMI):

- **Introduced** new German national ID card in November, 2010
- **Project PersoApp:** € 684.880,- (without VAT) until Dec. 31, 2015
- **Objectives:** 1. Establishment of an open source community
  2. Alternative for eID client of the Government (AusweisApp)
  3. Experimental platform for new requirements, services, ...

Core Team of PersoApp:

AGETO

- **AGETO Service GmbH:** Open source library for electronic identification
- **Fraunhofer SIT:** Guidelines for security engineering

Fraunhofer SIT

- **TUD/CASED:** Community building with user survey, use cases, workshops, …

TECHNISCHE UNIVERSITÄT DARMSTADT

Center for Advanced Security Research Darmstadt (CASED)

www.cased.de

CASED

Secure Software Engineering		
Cryptography	Identity, Privacy, Trust	Usable Security
Cloud Security		
Mobile and Cyberphysical System Security		
Internet and Infrastructure Security		

Fraunhofer SIT · Technische Universität Darmstadt · h_da Hochschule Darmstadt University of Applied Sciences

- 33 professorships
- 30 Post Docs
- 102 PhD students
- > 80 guest scientists p.a.
- #1 University in Germany for computer science/ security and privacy[1]; 31 awards (2011-2013)

Third-party funding since 07/2008: > € 60 Mio.

LOEWE Exzellente Forschung für Hessens Zukunft · Bundesministerium des Innern · Bundesministerium für Bildung und Forschung · DFG · + industry

Some projects and joint institutes

EC SPRIDE European Center for Security and Privacy by Design · eit European Institute of Innovation & Technology · Software-Cluster · intel Intel Collaborative Research Institute for Secure Computing · acm SIGSAC CCS 2013 November 4-8

RS³ — DFG Priority Program "RS³ - Reliable secure software systems (coordination)"

Security evaluation of PACE protocol; PersoApp (coordination)

acatech National Academy of Science and Engineering — Internet privacy

[1] #publications at TOP25 conferences; Microsoft Academic Search

Working Groups

WG1 Open eID Client

Lead: AGETO

- Development of an Open Source library for eID Client
- Interoperable with eID infrastructure and test as well as demo site
- Improvement
- Release management

W2 Quality Assurance

Lead: Fraunhofer SIT

- Specification of processes for quality assurance for compliance with BSI technical guidelines for eID infrastructure
- Programming guidelines
- Review environment

WG3 Open Community

Lead: TU Darmstadt/ CASED

- Community Portal
- Survey
- Design of use cases
- Roadshow
- Workshop
- Teaching

WGs TBD.

Lead: N.N.

- Extension of base modules by community

WG4 Management

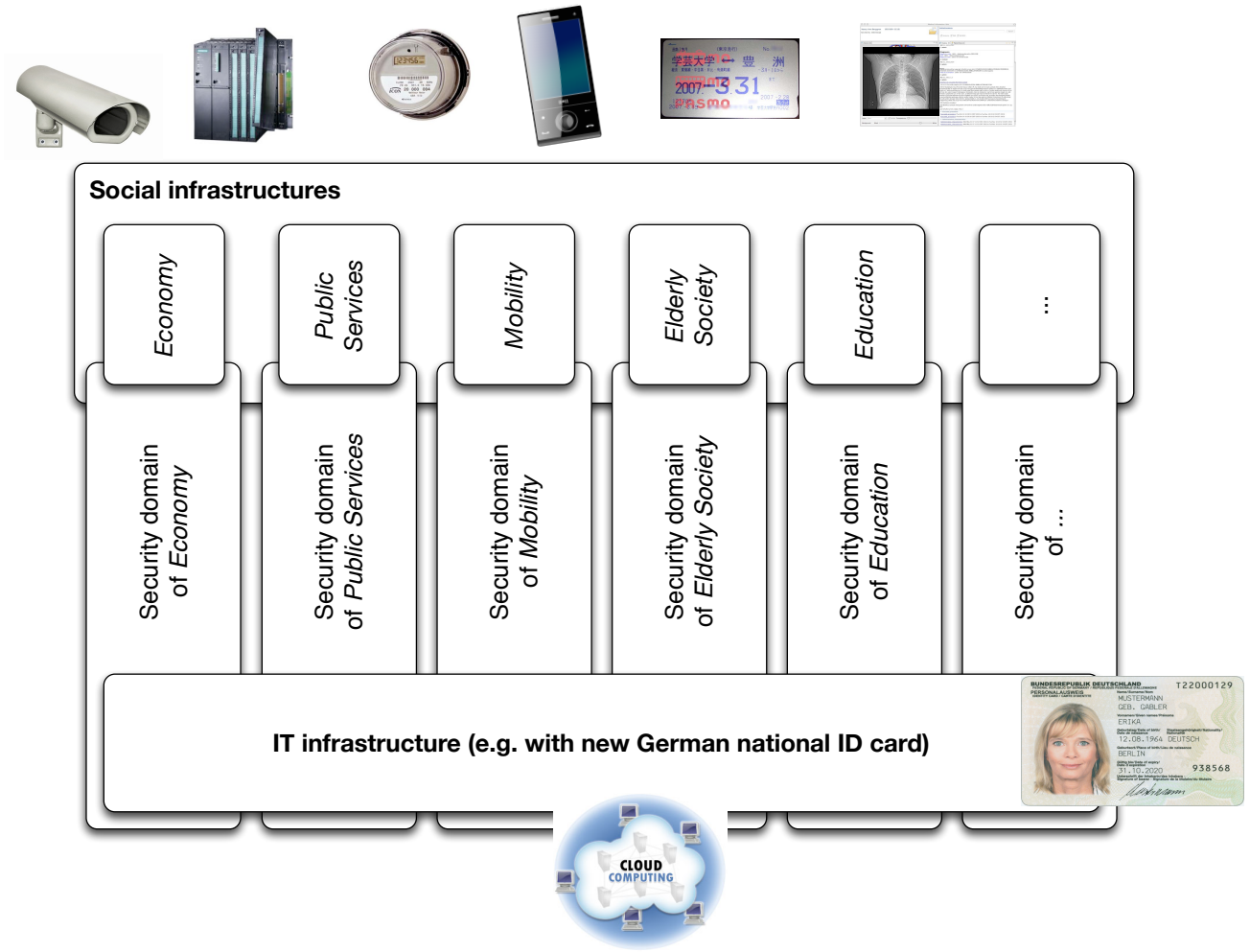
Lead: TU Darmstadt/CASED

- Discussion of content and results for usage of electronic ID card
- Reporting to Project Management Board
- Reporting to Steering Committee
- Interacting with Advisory Board

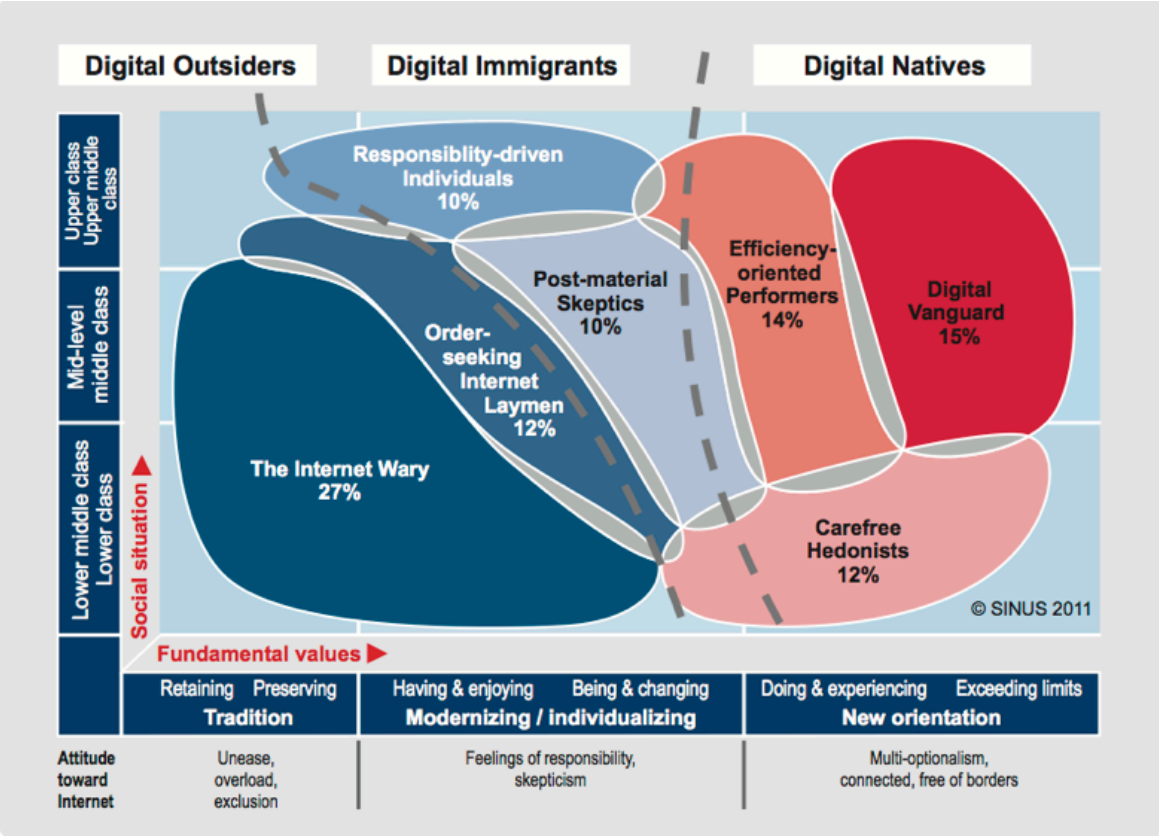
Focus Areas of PersoApp

ICT support for social infrastructures:

- Efficiency of service processes, security measures, and coordination activities
- Observing, evaluating, forecasting, coordinating, and optimizing flows of a city



Participants in Germany: Internet Milieus



https://www.divsi.de/sites/default/files/DIVSI_Milieu_Study_Summary.pdf

Digital Natives:

- "Always on-line" for personal benefit
- Hardly aware of risks

Digital Immigrants:

- Selective Internet usage for personal benefit
- Highly aware of security and privacy risks

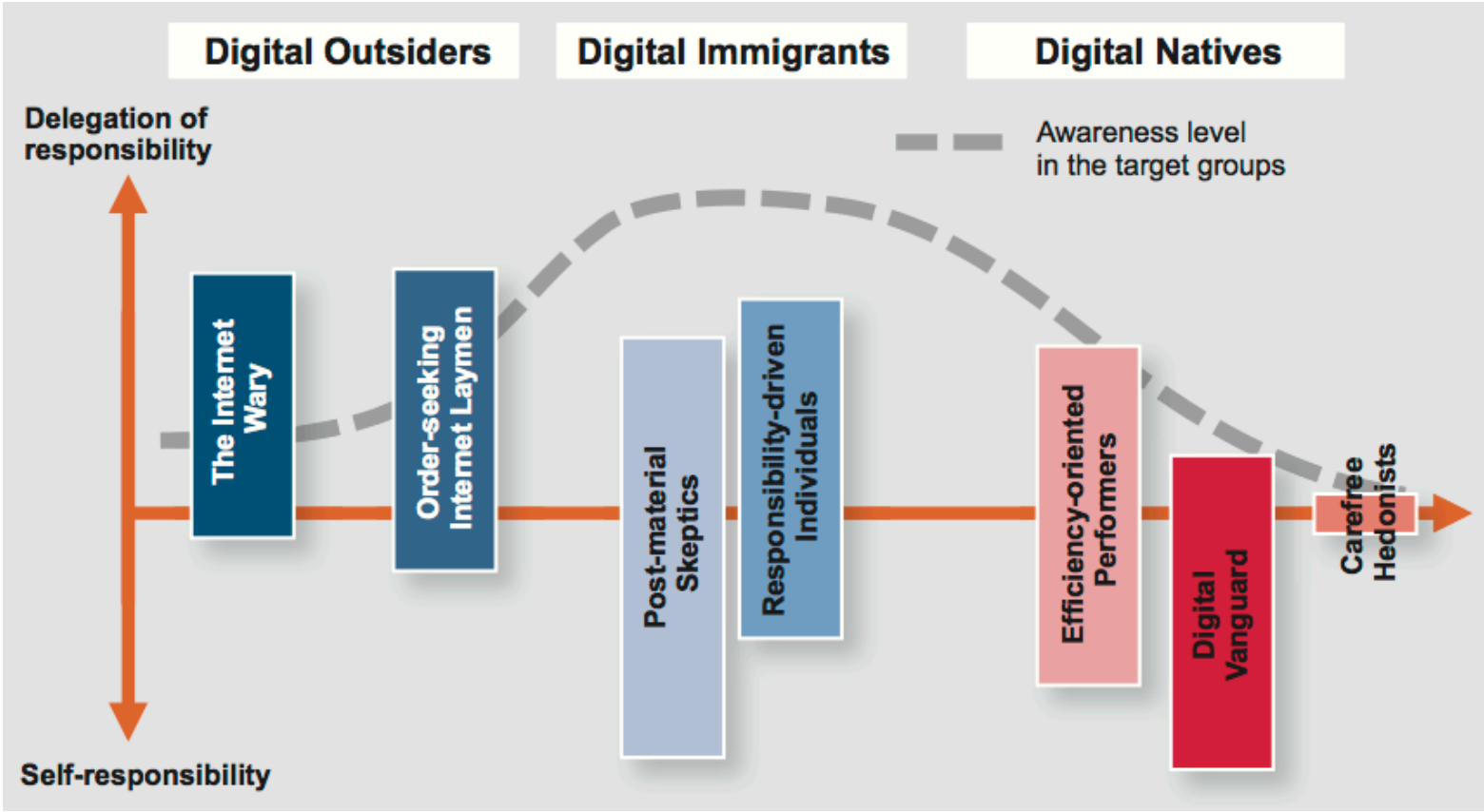
Digital Outsiders:

- Personal benefit of Internet usage is not clear
- Strongly uncertain for security and privacy risks

- **People selectively or not participating: 59% / 41 million**
- **Main concern: Threats by misuse of personal data**

Risk Awareness and Responsibility

Main concern: **Threats by misuse of personal data**



https://www.divsi.de/sites/default/files/DIVSI_Milieu_Study_Summary.pdf

"Those who have less Internet expertise demand protection by regulation and control; those who feel secure, demand no regulation and no control."

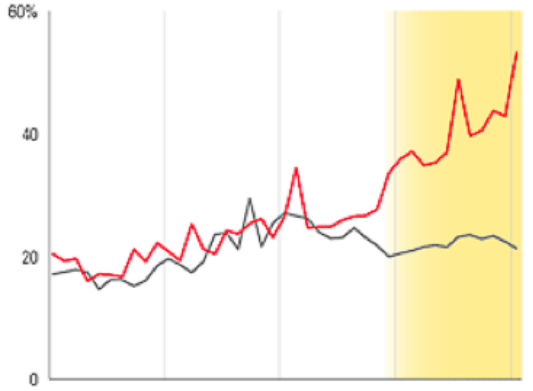
Online Identification & Individualization

Infrastructure of online identification with new German national ID card

- Secure identities with mutual (pseudonymous) authentication via third party
- Standardized IT security system (BSI technical guidelines)
- Currently: Used for standardized processes (opening bank account, registration, ...)

„Productivity paradoxon" (MIT)

- Difference in productivity of companies even though using standardized IT system
- Higher productivity due to individualization of services



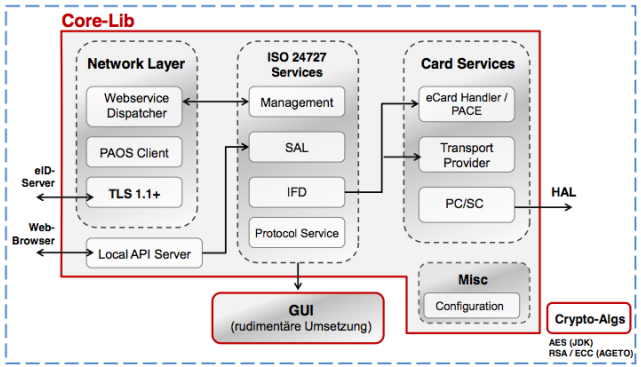
McAfee & Brynjolfsson. Investing in the IT That Makes a Competitive Difference, 2008

Security and individualization

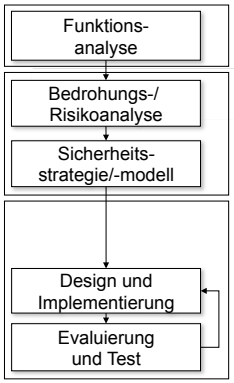
- Online identification for individualized services
- Security of **integrated** IT systems

What we offer ...

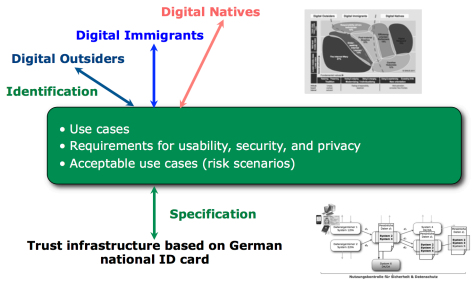
Open Source Software Library

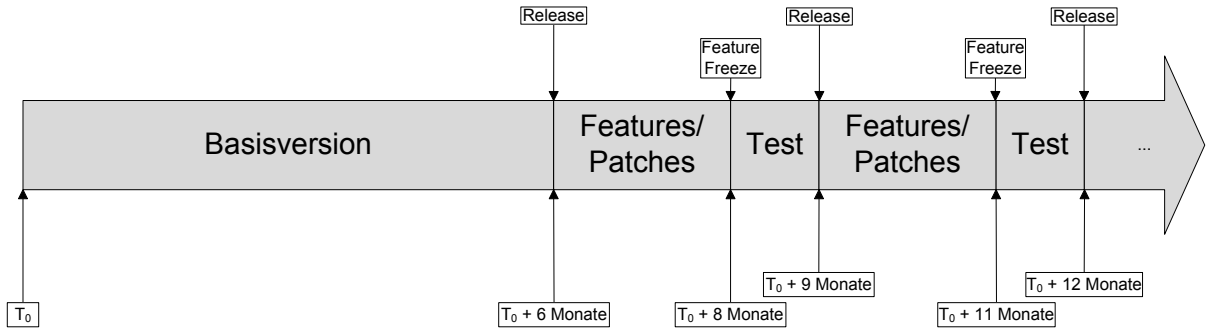


Security Engineering



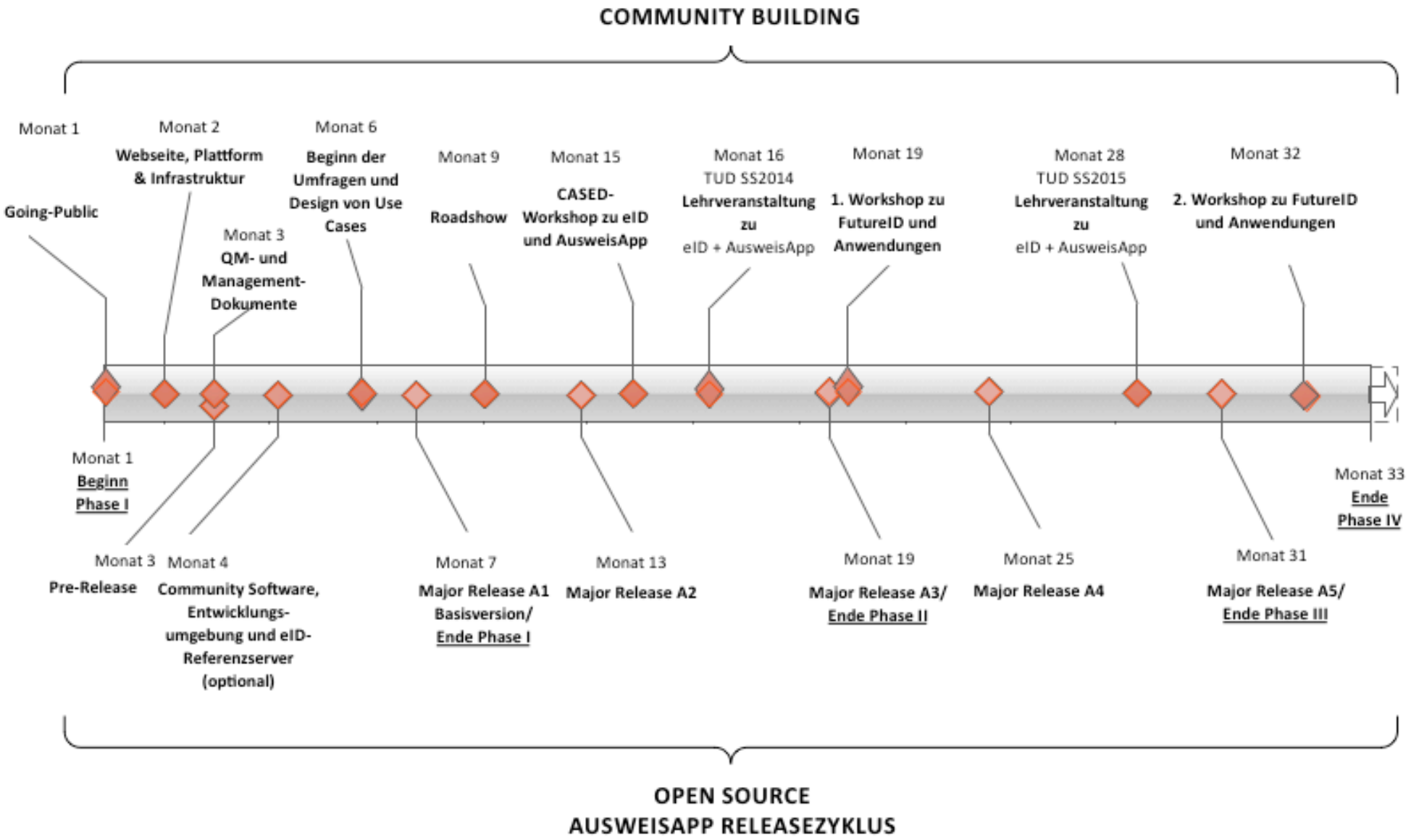
Individualization





User-Centric Security Engineering

Time Plan


COMMUNITY BUILDING
Monat 1
Going-Public
Monat 2
Webseite, Plattform & Infrastruktur
Monat 3
QM- und Management-Dokumente
Monat 6
Beginn der Umfragen und Design von Use Cases
Monat 9
Roadshow
Monat 15
CASED-Workshop zu eID und AusweisApp
Monat 16
TUD SS2014
Lehrveranstaltung zu
eID + AusweisApp
Monat 19
1. Workshop zu FutureID und Anwendungen
Monat 28
TUD SS2015
Lehrveranstaltung zu
eID + AusweisApp
Monat 32
2. Workshop zu FutureID und Anwendungen
Monat 1
Beginn Phase I
Monat 3
Pre-Release
Monat 4
Community Software, Entwicklungs-umgebung und eID-Referenzserver (optional)
Monat 7
Major Release A1 Basisversion/ Ende Phase I
Monat 13
Major Release A2
Monat 19
Major Release A3/ Ende Phase II
Monat 25
Major Release A4
Monat 31
Major Release A5/ Ende Phase III
Monat 33
Ende Phase IV
OPEN SOURCE
AUSWEISAPP RELEASEZYKLUS

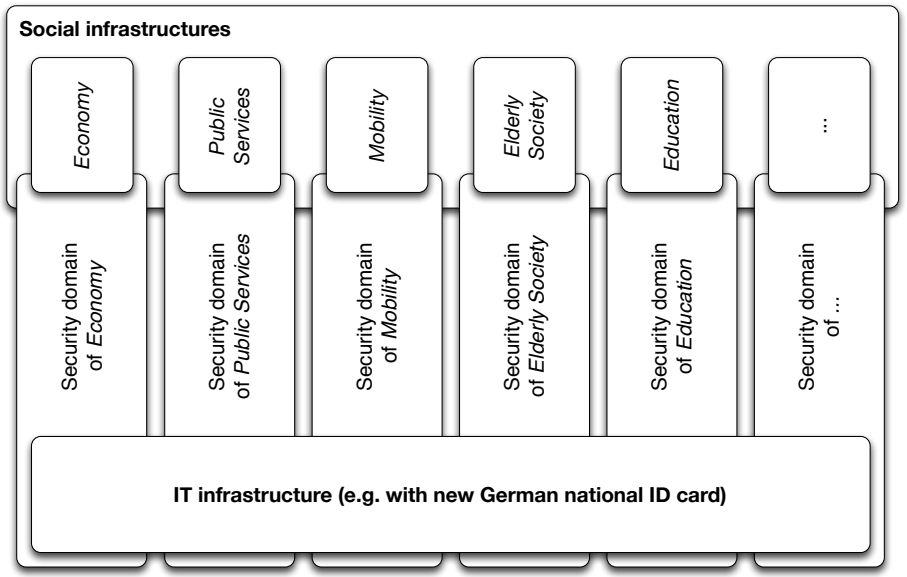
Advisory Board

Advisory Board:

- Consulting steering committee with expertise, best practices, trends, etc.
- Annual meetings (Constitutive meeting on September 4, 2013 at BMI, Berlin)

Call for Apps (incl. received expectations):

- Use cases, e.g. for mobility, social networks, etc.
  - Employee card, payments, eCommerce
  - University, Cloud Computing
  - etc.
- Security requirements from service providers
  - Authentic (customer) data
  - Security of services
  - Reliable PKI services
  - Usability
  - etc.



Cooperate via PersoApp!

Internet Portal at https://www.persoapp.de
- Forum
- Pre-Release
- Demo and test service
- Documentation
- Event calendar

Code Repository at https://persoapp.googlecode.com/
- SVN repository
- Issue tracker

E-Mail Listings
- Contact: persoapp@trust.cased.de
- Project leaders: persoapp-projects@trust.cased.de
- Software developers: persoapp-devel@trust.cased.de
- Project members: persoapp-broadcast@trust.cased.de
- Steering committee: persoapp-steering@trust.cased.de
- Advisory board: persoapp-advisory@trust.cased.de

Twitter at https://www.twitter.com/persoapp
- Publication of news about PersoApp

Appendix: Some Expectations and Interests

Expectation A

Im Bereich elektronischer Vertrieb pilotieren wir häufig Themen der Finanz-Informatik und arbeiten auch in Projekten des DSGV mit und verstehen uns als eine der innovativen Sparkassen in diesem Bereich. Deshalb sind wir auch interessiert, inwieweit PersoApp in diesem Bereich zukünftig eine Rolle spielen wird.

Expectation B

- Anwendungsmöglichkeiten des Personalausweises für den Handel (Kundenbeziehungen): Bspw. Unterstützung der Bezahlfunktion: Anwendung im Rahmen des Lastschriftverfahrens (Nutzen/ Risiken), Anwendung im Rahmen des Online-Handels
- Anwendungsmöglichkeiten für die interne Organisation Bspw. Mitarbeiterausweis (Zutrittsschutz, Zeiterfassung etc.)
- Kosten der Nutzung
- Kosten für den Händler, Kosten für den Kunden / Infrastrukturelle Voraussetzungen etc.
- Sicherstellung des Schutzes persönlicher Daten & rechtssichere Anwendung für Unternehmen
- Strategien zur Durchsetzung am Markt

Expectation C

We have several projects ongoing where we are cooperating with private sector. Today I can't name any specific expert. But what I had in my mind was, that if we going to need, in our cooperation with you, some deeper technical knowledge about ... eID products (like mobile-ID) then we can use technical experts from private sector (for example certification authority).

Appendix: Some Expectations and Interests

Expectation D

Allgemeine Ziele: Deutliche Verbesserung der Usability der eID-Funktion, Kernel kompatibel zu allen Betriebssystemen, klarer Schwerpunkt auf Nutzerorientierung

Mit Blick auf die jetzige Nutzung von Sozialen Netzwerken erschließt sich mir das Einsatzfeld noch nicht. Ich würde es zwar begrüßen, von Facebook sich für die Nutzung der eID-Funktion entscheidet. Allerdings kann ich mir derzeit nicht vorstellen, dass sich Facebook auch dazu entschließt, deutsches Datenschutzrecht zu akzeptieren. Der Versuche mit studiVZ sind im Sande verlaufen.
Soweit der Schwerpunkt eher auf dem Thema Cloudnutzung liegt, lohnt es sich aus meiner Sicht, mit dem Projekt „Trusted Cloud" (http://trusted-cloud.de/de/1474.php) Kontakt aufzunehmen.
Ein Pilotprojekt mit einer großen Universität unter dem Stichwort „Studentenkonto" (vgl. z.B. http://www.hs-harz.de/9152.html) halte ich für sehr sinnvoll.

Expectation E

Gerne schildere ich Ihnen meine Vorstellung / Erwartung an die PersoApp. Aus meiner Sicht ist für uns als eCommerce Unternehmen vor allem die Nutzung der Authentifizierung von Kunden in der privaten Wirtschaft interessant. Dabei ist es aus meiner Sicht vor allem wichtig, die „Echtheit" der digitalen Identität sicher zu stellen, der Sicherheitsgedanke steht absolut im Vordergrund. Als OpenSource Software sollte es eine unabhängige Möglichkeit der Zertifizierung von Implementierungen geben. Einem Bürger muss vermittelt werden, dass die PersoApp im Rahmen von sicherheitstechnischen und rechtlichen Aspekten unbedenklich ist. Eine nicht zertifizierte Nutzung muss als solche erkennbar sein. Somit ist der informations-/Aufklärungsaspekt neben der technischen Betrachtung essentiell für den Erfolg der PersoApp.

Appendix: Some Expectations and Interests

Expectation F

Sowohl in der Sozialwirtschaft mit unserer Lösung ... als auch im klinischen Bereich mit unserer elektronischen Patientenakte auf dem iPad (...) haben wir es viel mit Benutzerkonten zu tun. Diese erhalten wir i.d.R von einem führenden System, z.B. aus dem KIS (Krankenhausinformationssystem). Beim Aktivieren des Kontos für einen Arzt würden wir gerne sicherstellen, dass es sich auch tatsächlich um diese oder jene Person handelt. Das muss dann zu späteren Zeitpunkten nicht mehr geprüft werden, jedoch wäre es für die initiale Freischaltung perfekt.

Einen ähnlichen Sachverhalt haben wir in der ambulanten Pflege. Dort haben wir eine App in Vorbereitung die es erlaubt Angehörigen von Pflegekunden nach Freigabe durch die Pflegekunden den Zugang zu einigen wenigen, ausgesuchten Daten zu ermöglichen. Wie bei vielen anderen Anwendern auch wird hier die Rufnummer der SIM-Karte als Authentifizierungsmerkmal verwendet, was natürlich nicht sehr 'sicher' ist. Gerade für den Vertriebskanal 'AppStore' und 'PlayStore' wäre eine leichtgewichtige Identitätsprüfung sehr von Vorteil.

Expectation G

1. Als primäre Zielsetzung der konstituierenden Sitzung sehe ich die Verständigung der Beiratsmitglieder auf einen gemeinsamen Kriterienkatalog, der den Beirat in seiner zukünftigen Arbeit durchgängig und konsistent leitet. Dieser Katalog sollte sich aus meiner Sicht an den Leitkriterien a) Nutzbarkeit, b) Sicherheit und c) Datenschutz orientieren und diese Kriterien operationalisieren, indem 1) sowohl für einzelne Stakeholder als auch Stakeholder-übergreifend Erwartungen/Anforderungen an das Projekt formuliert werden und 2) diese Erwartungen/Anforderungen durch Indikatoren konkretisiert werden, mit denen sich im Verlauf des Projekts die Erwartungen des Beirats mit den Ergebnissen des Projekts abgleichen lassen.
2. Aus inhaltlicher Sicht halte ich die zum einen die Integration in PKIs bzw. die Nutzbarkeit von digitalen Signaturen und von Verschlüsselungen für wichtig (bislang sind im privaten Bereich PKIs gescheitert), zum anderen den Schutz der Daten, die auf dem Pers.ausweis gespeichert sind und an Applikationen weitergereicht werden.

Appendix: Some Expectations and Interests

Expectation H

Ich erwarte mir von PersoApp eine transparente, für jeden nachvollziehbare/überprüfbare Technologie zur (pseudonymisierten - WICHTIG) Identitätsfeststellung im Internet. Die Sicherheit der dabei verarbeiteten personenbezogenen Daten sowie die Sicherheit des eigentlichen Dienstes haben für mich höchste Wichtigkeit.

Expectation I

"Wie kann das Projekt zusätzlich zu dem primären Fokus auf Sicherheitsaspekte auch Prinzipien des Datenschutzes in Richtung eines aktiven Angebots zur Selbstkontrolle der eigenen Daten und der Privatsphärenpräferenzen einbeziehen? Ich denke hier z.B. an Zweckbestimmung und Zweckbindung, Transparenz, Korrekturmöglichkeiten, Datenminimierung, vielleicht aber auch neu eingeführte Aspekte wie z.B. die Datenportabilität etc. "

Expectation J

Ich würde mir wünschen, dass das PersoApp-Projekt einen praktischen Beitrag zur Verbesserung der Benutzbarkeit des neuen Personalausweises und ähnlicher Ausweisweis- und Signaturkarten liefern würde. Dies scheint mir in Anbetracht der existierenden AusweisApp des Bundes leider dringend notwendig und für die Steigerung der Akzeptanz des nPA geradezu essentiell.

Vor diesem Hintergrund ist es mir offen gestanden ein wenig unverständlich, warum im PersoApp-Projekt scheinbar die existierende Ageto-AusweisApp zu einer für den sicheren elektronischen Identitätsnachweis nicht mehr unmittelbar nutzbaren Bibliothek zurückgebaut werden soll. Warum veröffentlicht man denn nicht die existierende App? Ich bin sehr darauf gespannt, im Rahmen der Beiratssitzung mehr über Ihre mit dem PersoApp-Projekt verbundenen Vorstellungen, Erwartungen und Ziele zu erfahren.

Appendix: Some Expectations and Interests

Expectation K

Die ... hat sich schon sehr früh mit dem neuen Personalausweis (eID) auseinandergesetzt und Szenarien erörtert, bei der die eID zum Einsatz kommt. Die wichtigste Anwendung sind hier zweifelsohne die Online-Dienst, die es dem Bürger nach vorheriger Registrierung erlauben, seine RKontendaten anzusehen und verschiedene Druckprodukte (Auskunft, Info, etc.) in Echtzeit anzufordern. Weitere Szenarien wie der Einsatz bei der Online-Antragsstellung sind angedacht.

Erhebliche Probleme auf Versichertenseite macht zurzeit die technische Infrastruktur der AusweisApp, so wie sie im Moment im Einsatz ist. Plugin und Komplexität machen es dem angesprochenen Kundenkreis nicht einfach, Dienste die mit dem neuen Personalausweis angeboten werden zu nutzen. Ziel muss es hier aus unsere Sicht sein, eine Möglichkeit zu schaffen, eine hohe Benutzerfreundlichkeit zu erreichen, die die entsprechende Sicherheit der Daten bietet und auf einem breiten Spektrum von Plattformen ablauffähig ist (Windows, Linux, iOS, MacOS. Android etc.).

Die ... hat ebenfalls erkannt, dass die Zukunft nicht mehr den Desktop-PCs bzw. den Notebooks gehört, sondern die Entwicklung sich in Richtung leistungsfähiger Kleingeräte (Smartphones, Tablets etc.) verändert. Aus diesem Grund versuchen wir unseren Versicherten eine Infrastruktur zur Verfügung zu stellen, die es ihnen erlaubt, ihre gewohnten Endgeräte für den Zugang zu unseren Diensten auch von unterwegs nutzen können.

Appendix: Some Expectations and Interests

Expectation L

Der Erfolg des neuen Personalausweises hängt meiner Meinung nach zum einen von den vorhandenen Szenarien ab. Gerade Szenarien des Bundes, der Länder und der Kommunen haben die Möglichkeit die Bürger zur Nutzung der online Ausweisfunktion zu animieren. Ein attraktives Szenario wäre beispielsweise die Option an der Wahl auch online teilnehmen zu können. Zudem ist es wichtig bestehende Szenarien, wie den Abruf des Punktekontos in Flensburg, medienbruchfrei zu ermöglichen, sprich die Informationen direkt online zu erhalten und nicht durch einen Brief.

Des Weiteren müssen die Bürger besser über den nPA informiert werden. Dass die zur Einführung des nPAs geplanten Werbungen eingestellt wurden, hat nun die Auswirkung, dass die Bürger immer noch mangelnde und falsche Informationen über den nPA haben. Zudem sollten Mitarbeiter in den Einwohnermeldeämtern dem Bürger gegenüber positiv in Bezug auf den neuen Personalausweis gestimmt sein (was häufig nicht der Fall ist) und wichtige und hilfreiche Informationen weitergeben.

Auch den potentiellen Diensteanbietern muss der Einstieg erleichtert werden eine Authentifizierung ihres Dienstes mit dem nPA zu ermöglichen. Dies betrifft zum einen die hohen Investitionskosten und zum anderen den bürokratischen Aufwand und die komplexen Bestimmungen zur Genehmigung eines Berechtigungszertifikats. Zudem müssen die Infrastruktur und die Maßnahmen zum Betrieb und zur Qualitätssicherung dem eines professionellen Software-Dienstleisters und Rechenzentrums entsprechen.

Bezüglich der Client-Software zur Nutzung des neuen Personalausweises erscheint es mir sinnvoll diese zentral bereit zu stellen. Direkt vom Diensteanbieter bereitgestellte Software hat bei Weitem nicht die Vertrauensstellung, wie solche die von einer zentralen, vertrauensvollen Stelle bereitgestellt wird. Gerade bei sensiblen Daten, wie die auf den Personalausweis, sollte die Software von einer Institution bereitgestellt werden, deren Vertrauen der Bürger genießt.

Grundsätzlich stellt sich mir die Frage, wo der Bund in Zukunft sein Aufgabengebiet sieht und welche Aufgaben an die Diensteanbieter delegiert werden. Gerade bei der Aufgabe dem Bürger den neuen Personalausweis nahezubringen, sowie die Infrastruktur bereitzustellen sollte der Bund sich nicht zurückzuziehen.

Appendix: Some Expectations and Interests

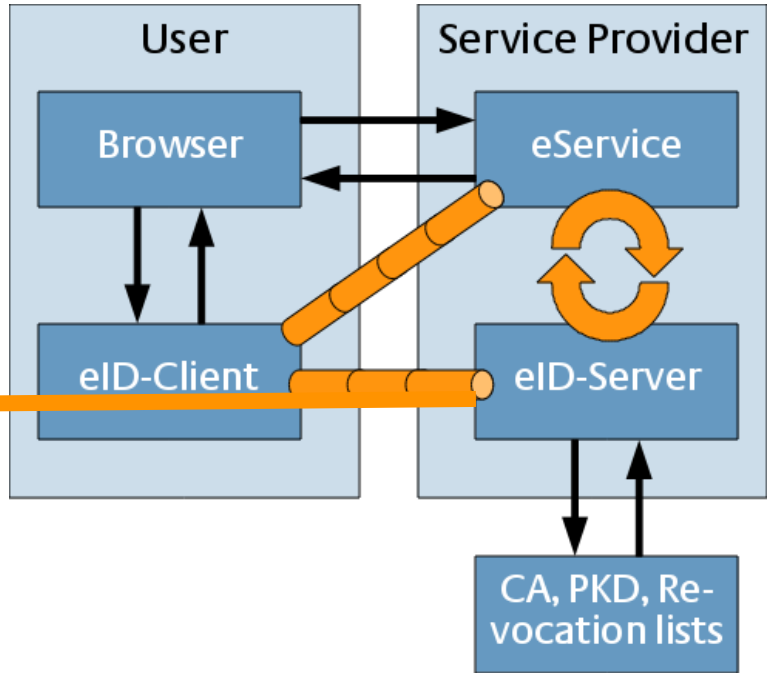
Expectation M

Eine benutzerfreundliche, sichere und transparente Identitätsermittlung in der elektronischen Kommunikation sehe ich auch als vertrauensbildende Maßnahme. Denn neben den technischen Herausforderungen wird vor allem die Akzeptanz bei den Benutzer über den Erfolg des Projekts entscheiden. Dazu denke ich ist es wichtig, dass der einzelne Teilnehmer an dem Verfahren einen unmittelbaren Nutzen erfährt, sprich für Ihn ein Mehrwert generiert wird und sei es nur, so profane Dinge wie, dass es "cool" ist wenn man im Autohaus mit seinem Smartphone über NFC den nPA liest, sich den Verdienstnachweis online abruft, dem Kreditgeber übermittelt und den Kaufvertrag abschließt, ...

Security Properties of new German ID Card

Applications of new German national ID card:

- Biometric authentication (souvereign only)
- **Electronic identity**
- Electronic signature



BSI TR-03130 Technical Guideline eID-Server

Mutual authentication:

- Citizen and service provider show both their identity

Data economy:

- Data disclosure according to authorization certificate of service provider
- Supports pseudonymity of citizen

Trust anchor:

- Access control: Each application is based on own PKI
- Isolation of information flow: Cryptographic protocols, hardware system, and eID server
- Policy: Legal regulation for usage of national ID card