PersoApp

Sichere und benutzerfreundliche Internetanwendungen

Der neue
Personalausweis
Meine wichtigste Karte.

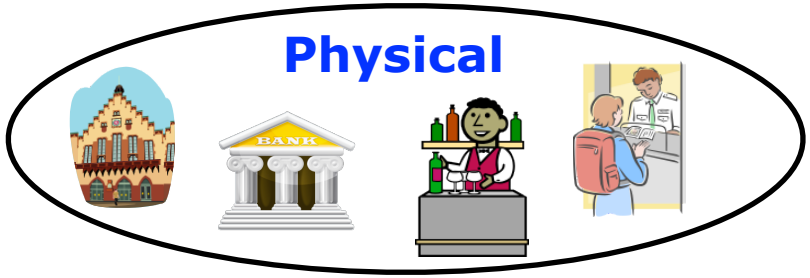
CeBIT 2014
Gemeinschaftsstand des IT-Planungsrates, 13. März 2014

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

Konsortialleitung
Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt (CASED)

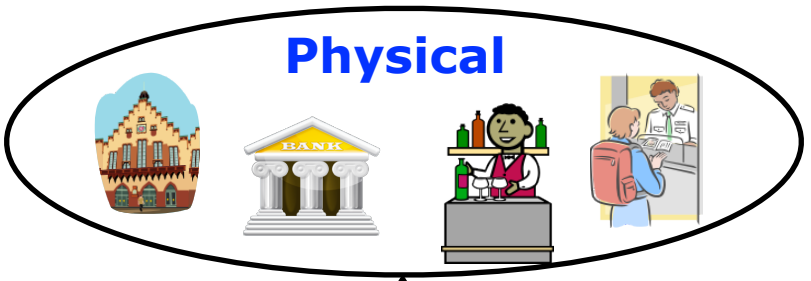
System Security Lab
Fraunhofer SIT
TECHNISCHE UNIVERSITÄT DARMSTADT
CASED

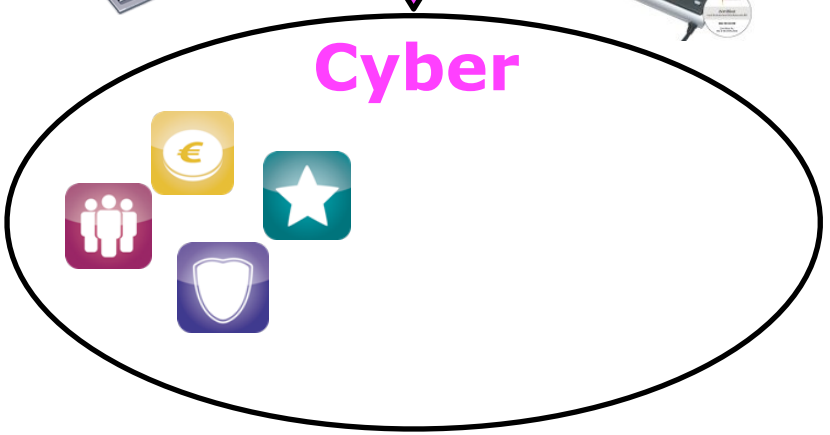
Elektronische Identität und Anwendungen



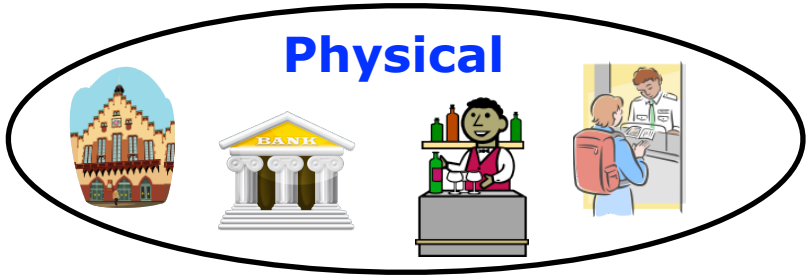
Physical

+ Cyber



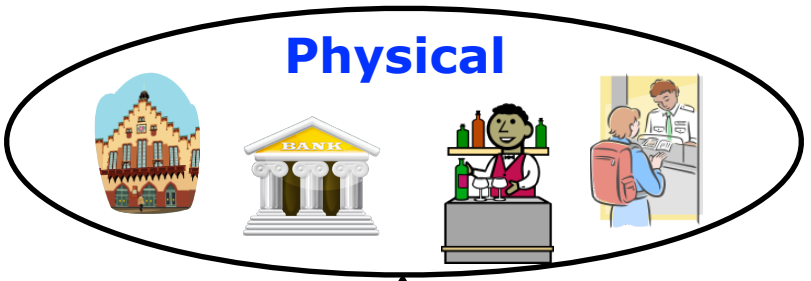


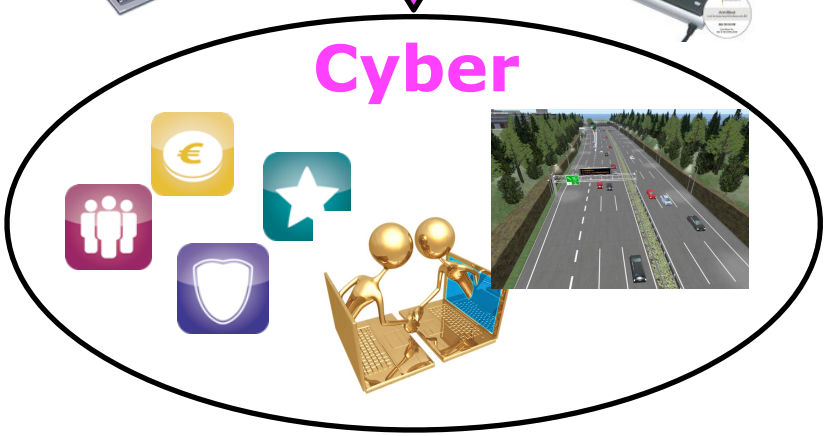
Elektronische Identität und Anwendungen



Physical

+ Cyber





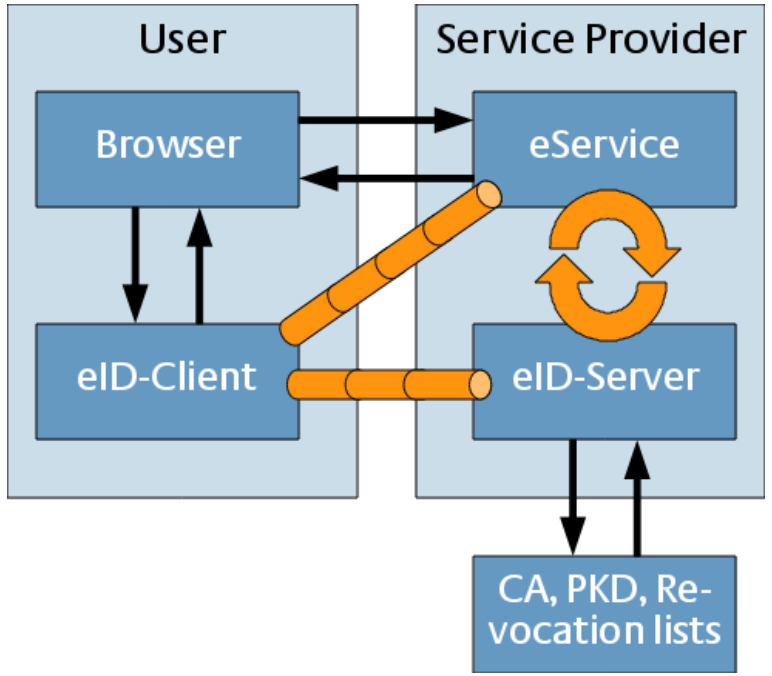
Gesellschaftlicher Beitrag

Wiederverwendung einer existierenden, nationalen Infrastruktur für Mehrwertdienstleistungen

Sicherheitseigenschaften des "Persos"

Anwendungen des neuen Personalausweises

- Biometrische Identitätsfeststellung (hoheitlich)
- **Online Ausweisfunktion**
- Elektronische Signatur



BSI TR-03130 Technische Richtlinie eID-Server

Gegenseitige Identitätsfeststellung

- Bürger und Dienstanbieter weisen ihre Identität nach

Datenschutz

- Datenzugriff nach Berechtigungszertifikat des Dienstanbieters
- Unterstützt Pseudonymität für Bürger (Karteninhaber)

Vertrauensanker

- Zugriffskontrolle basiert auf Public-Key Infrastruktur (PKI)
- Isolation des Datenflusses: Kryptographie und Hardware
- Regulierung durch PAuswG und PAuswV

PersoApp – Open-Source-Community

Bürger, Regierung, Wirtschaft und Wissenschaft

Bundesministerium des Innern (BMI):

Bundesministerium des Innern

- **Einführung** des neuen Personalausweises im November 2010
- **Projekt PersoApp:** € 684.880,- bis 31. Dezember 2015
- **Ziele:**
  1. Aufbau einer Open-Source-Community
  2. Alternative zum eID-Client der Regierung (AusweisApp)
  3. Experimentierplattform für neue Anforderungen, Dienste, …

Kernteam von PersoApp:

AGETO

- **AGETO Service GmbH:** Open-Source-Bibliothek zur Online Ausweisfunktion
- **Fraunhofer SIT:** Handlungsempfehlungen zur sicheren Integration
- **TU DA/CASED:** Aufbau der Community, Umfragen, Use Case, Workshops, …

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

Projektziele

1. Alternative zum eID-Client der Regierung (AusweisApp)

PersoApp Major Release A1

https://persoapp.googlecode.com

2. Aufbau einer Open-Source-Community

- **Internet-Milieus in Deutschland**
- **Beirat**

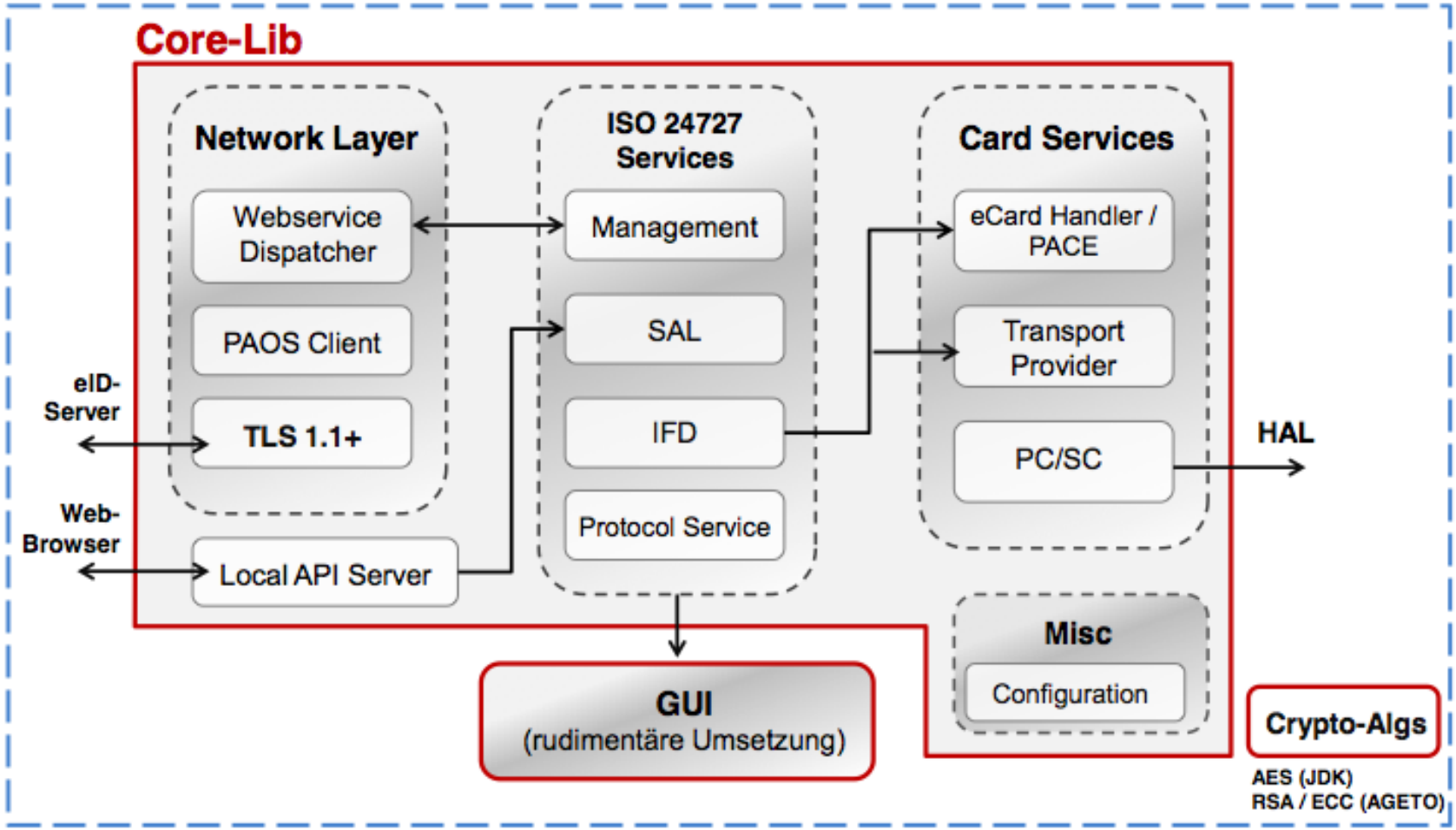
3. Experimentierplattform für neue Anforderungen, Dienste, …

- **Spontaner Informationsaustausch**
- **Kontrolle und Transparenz**

Dokumentation. Austausch, Neuigkeiten, etc. unter

https://www.persoapp.de

1. Alternative zur AusweisApp



- Entsprechend zu den technischen Richtlinien des BSI
- Unterstützt den neuen Aufrufmechanismus (ohne Browser-Plugin)
- LGPLv3, Erweiterung für Android OS geplant

SW-Entwicklung mit dem Personalausweis

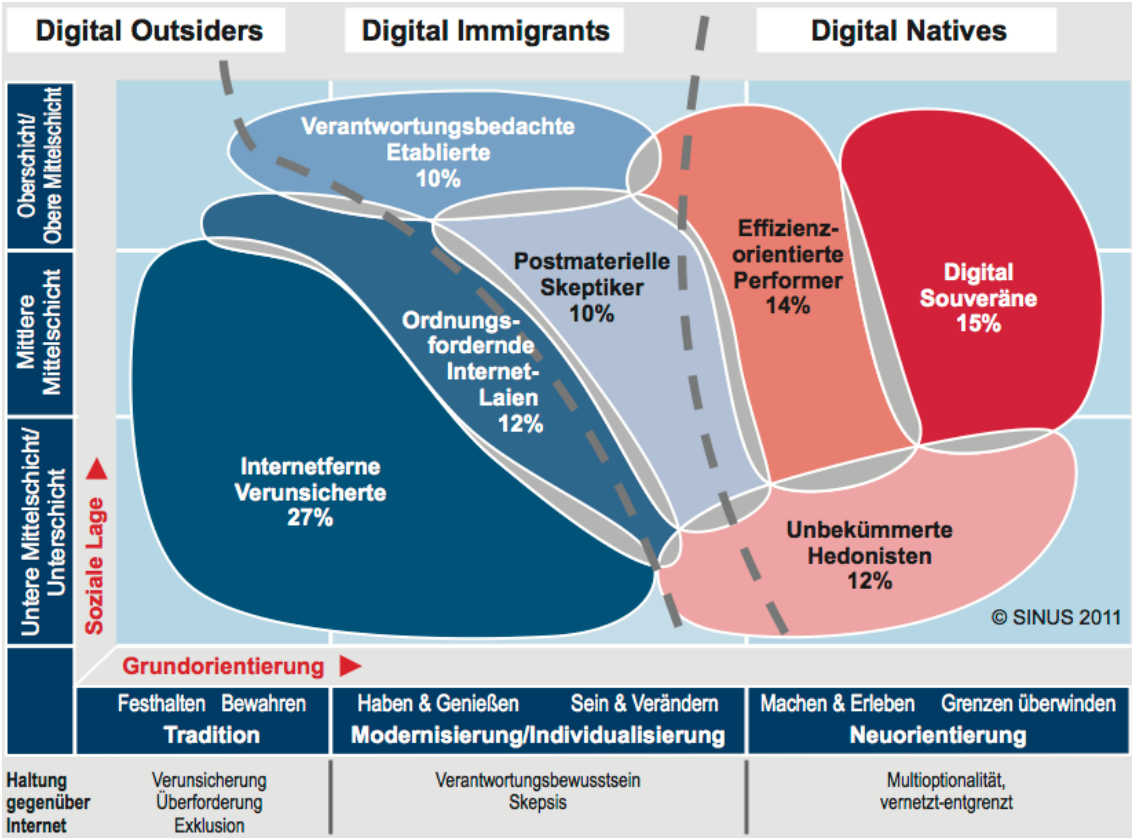
- Unterscheidung: Test-PKI und Wirk-PKI
- Dokumentation und Leitfaden für Review und Release auf www.persoapp.de

	eID-Client	Ausweis	Lesegerät	Berechtigungszertifikat	eID-Server	Gateway eID-Server und Anwendun	Testdienst
Test-PKI	• PersoApp • Autentapp • eIDClientCore • Open eCard • Open eID	a) Testausweis b) PersoSim	a) vgl. Personalausweisportal b) nicht erforderlich	• Betreiben einer eigenen Berechtigungs-CA • Nutzung anderer CA	**eingeschränkt auf PersoApp**	**eingeschränkt auf PersoApp**	**eingeschränkt auf PersoApp**
Wirk-PKI	• AusweisApp • PersoApp • Autentapp • eIDClientCore • Open eCard • Open eID	Personalausweis	vgl. Personalausweisportal	Beantragung bei der VfB (Verfahren s. Personalausweisportal)	• AGETO Service GmbH • Governikus KG • media transfer AG • OpenLimit SignCubes AG	• AGETO Service GmbH • Governikus KG • media transfer AG • OpenLimit SignCubes AG	Selbstauskunft der Stadt Würzburg

Die Tabelle repräsentiert keine Empfehlung und erhebt keinen Anspruch auf Vollständigkeit

2. Aufbau einer Open-Source-Community

Internet Milieus in Deutschland



https://www.divsi.de/publikationen/studien/divsi-milieu-studie/

Digital Natives:

- "Always on-line" für pers. Nutzen
- Hohe Internet-Expertise aber geringe Risikosensibilisierung

Digital Immigrants:

- Kommunikation mit Vertrauten & Recherche
- Stark sensibilisiert für Sicherheit und Datenschutz

Digital Outsiders:

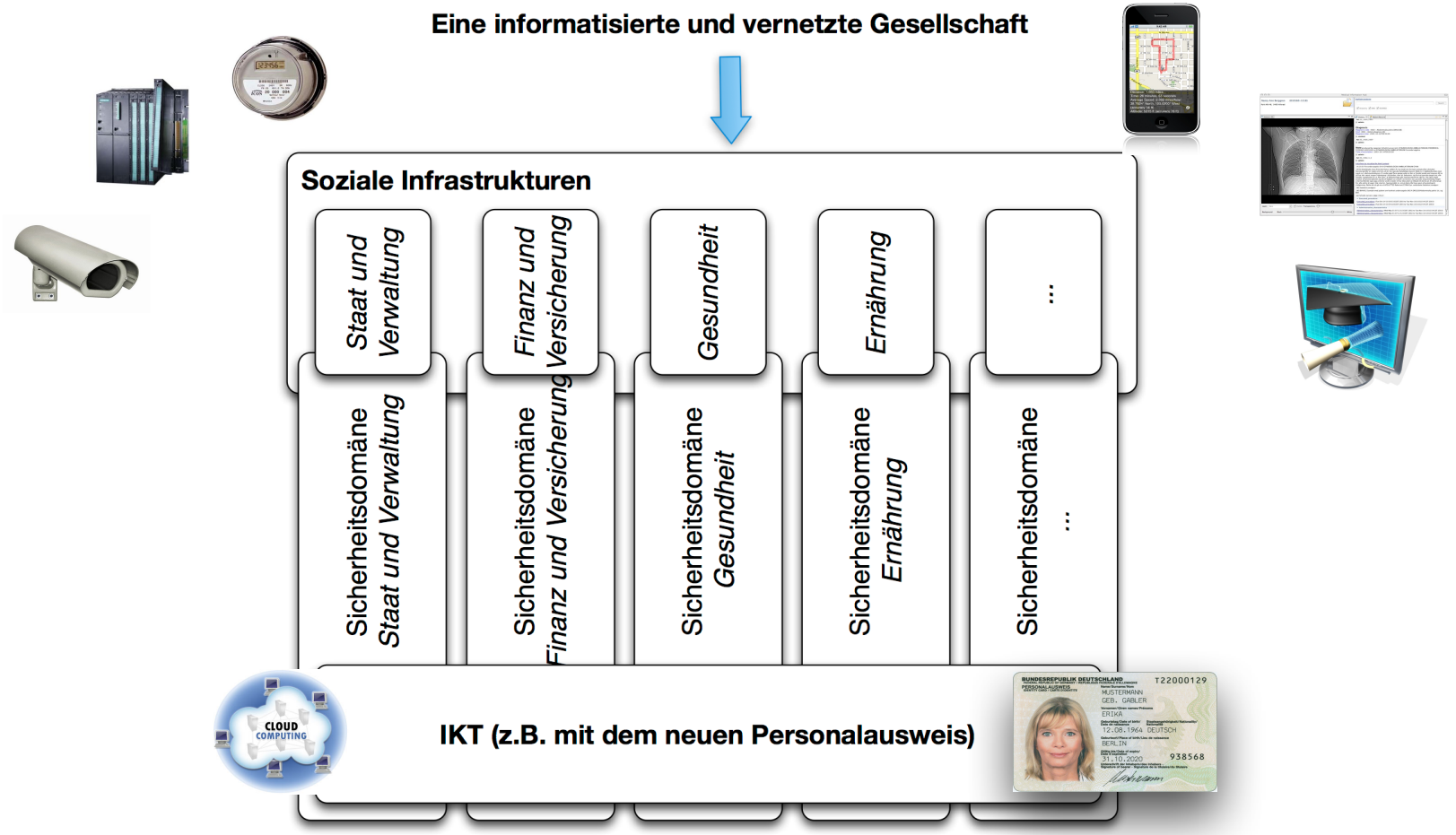
- Pers. Nutzen des Internet nicht ersichtlich
- Stark verunsichert bei Risiken im Internet

- **Digital Natives** bieten Orientierung und sind Multiplikatoren
- **Digital Natives** haben größten Anteil an Fach-/Hochschulqualifikation
- **Initiales Community Building an Gymnasien und Universitäten**

Beratung: Beirat

Ausrichtung:

- Beratung des Lenkungsausschusses in Anforderungen und Interessen
- Internationale Besetzung mit Entscheidungsträgern und Interessensvertretern
- Jährliche Treffen (konstituierende Sitzung im September 2013 beim BMI)



D01-QM Organisation und Rollenverteilung; D10-QM Community Building: Konzept, Maßnahmen und Bewertung

PersoApp Beirat: Ein Netzwerk von Netzen

Bundesministerium des Innern

Bundesverwaltungsamt

Bundesamt für Sicherheit in der Informationstechnik

AGENCE NATIONALE des TITRES SÉCURISÉS

Estonian Information System's Authority

BUNDESDRUCKEREI

Fraunhofer FOKUS

DATEV

Deutsche Rentenversicherung

NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 National Institute of Informatics

secure sba-research.org

Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN

bremen online services

SAP

Kernteam

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

CASED

AGETO

software AG

NXP

Kreissparkasse Ludwigsburg

COMMERZBANK

Swiss Re

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

imc Advanced Learning Solutions

REWE GROUP

otto group

W3C

intel

SIEMENS

MICRONAS

eco

Sirrix AG security technologies

esec

KOBIL secure your identity

Deutsche Telekom

Lohmann & Birkner

TeleTrusT Pioneers in IT security.

UNI FREIBURG

Universität Regensburg

MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG

JOHANN WOLFGANG GOETHE UNIVERSITÄT FRANKFURT AM MAIN

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN · FH MÜNCHEN

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

Anregungen aus dem Beirat

Anwendungen

- „Banking/Payment“ als App für Online-Ausweisfunktion
- Semantik einer Online-Authentifikation, z.B. für finanzielle Transaktionen
- Menschen im Mittelpunkt und Integration in das „Internet of Things“
- Authentische Daten
- Risikoszenario: Gleichgewicht zwischen Sicherheit und Privatsphäre
- eID-Kartensysteme anderer Anwendungsbereichen sollten auch betrachtet werden

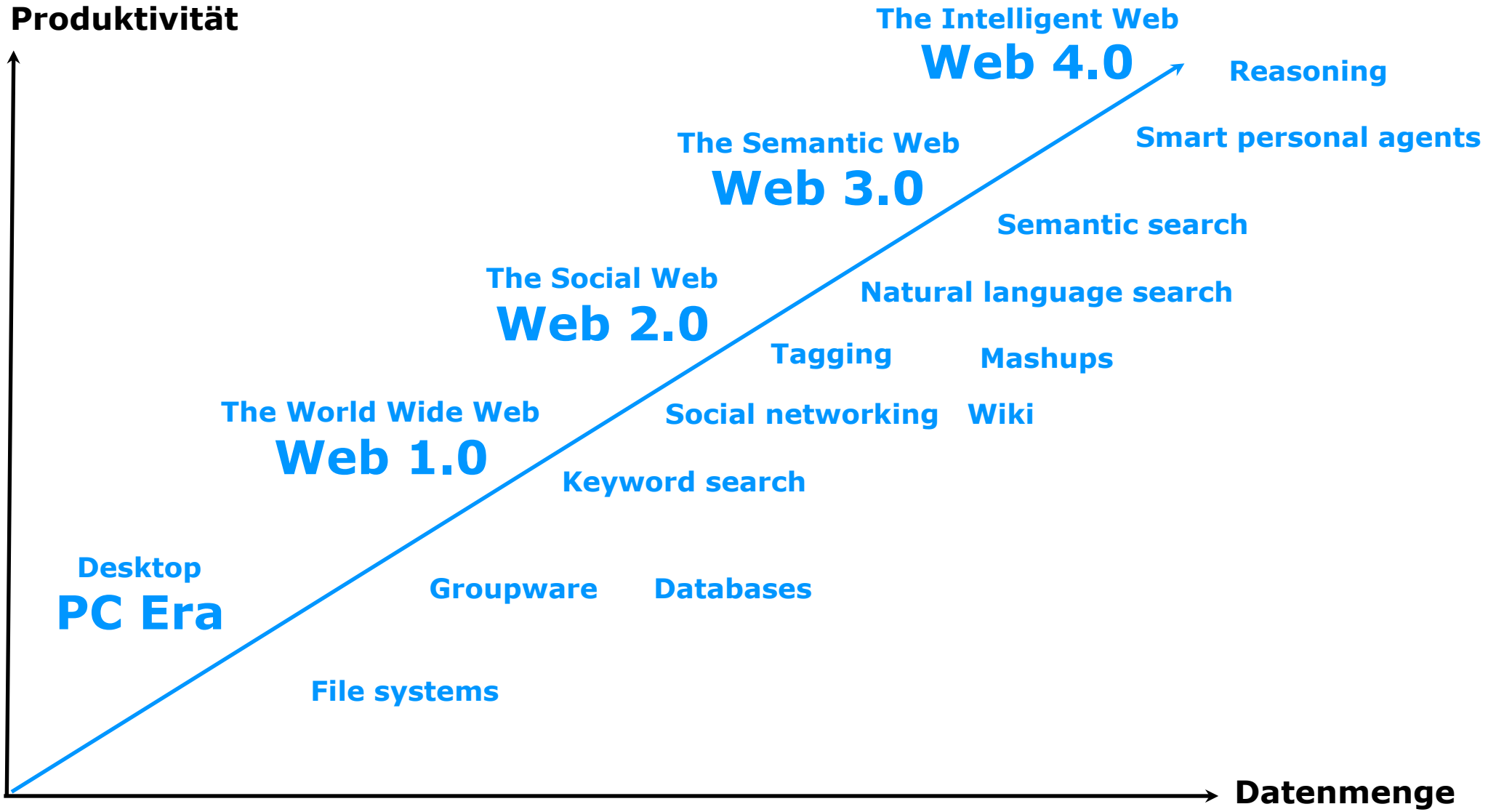
Analyse

- Dokumentation des Datenflusses für Datenschutz
- Abhängige (Analyse-)Software auch als Open Source
- Information eines Nutzers über Durchsetzung gegenwärtiger Sicherheitskonfiguration durch den eID-Client
- Erfahrungen anderer Länder wie Estland, Schweiz, … berücksichtigen und austauschen

Infrastruktur

- Interoperabilität von eID-Systemen und Sicherheitsstufen
- PersoApp-Bibliothek auf mobile Geräte
- eID-Client als Bestandteil eines Webbrowsers
- Treiber fuer Smartcard-Reader sollten auch Open Source sein

3. Experimentierplattform



Eigene Abbildung basierend auf Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011

3. Experimentierplattform

Produktivität

The Intelligent Web
Web 4.0

Reasoning

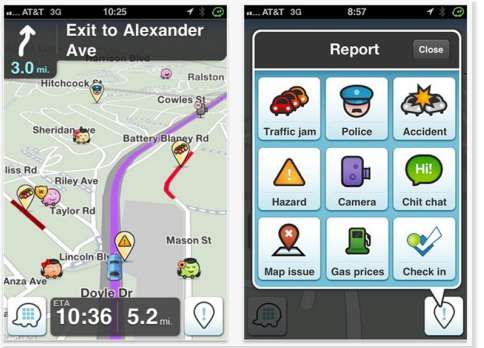
Smart personal agents

ic Web
Web 3.0

Semantic search

The Social Web
Web 2.0

Natural language search



Tagging

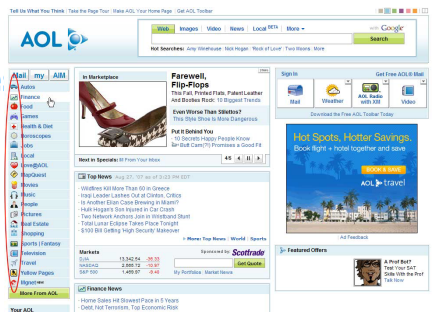
Mashups

The World Wide Web
Web 1.0

Social networking

Wiki

Keyword search



Desktop
PC Era

Groupware

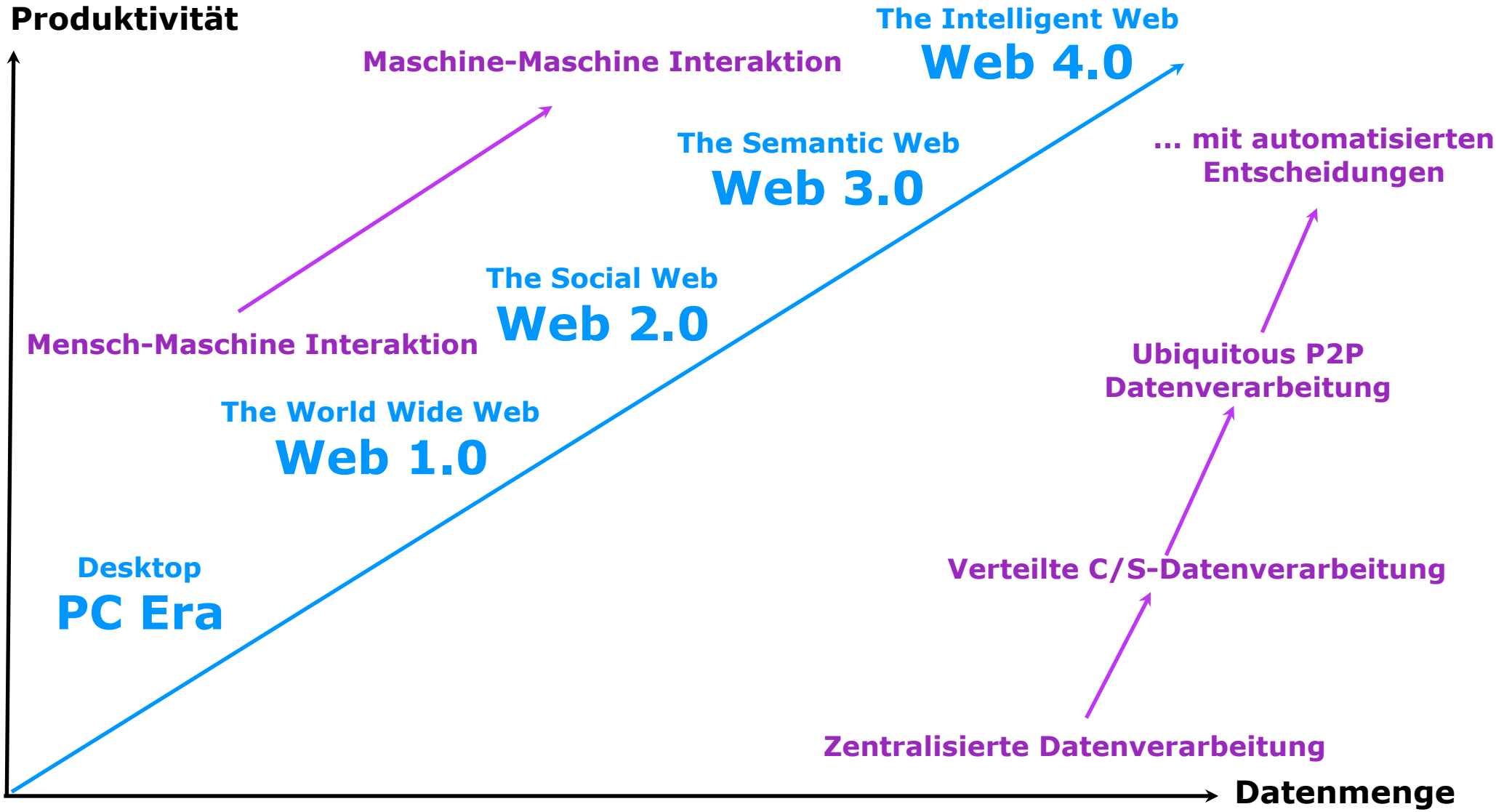
Database

File systems

Datenmenge

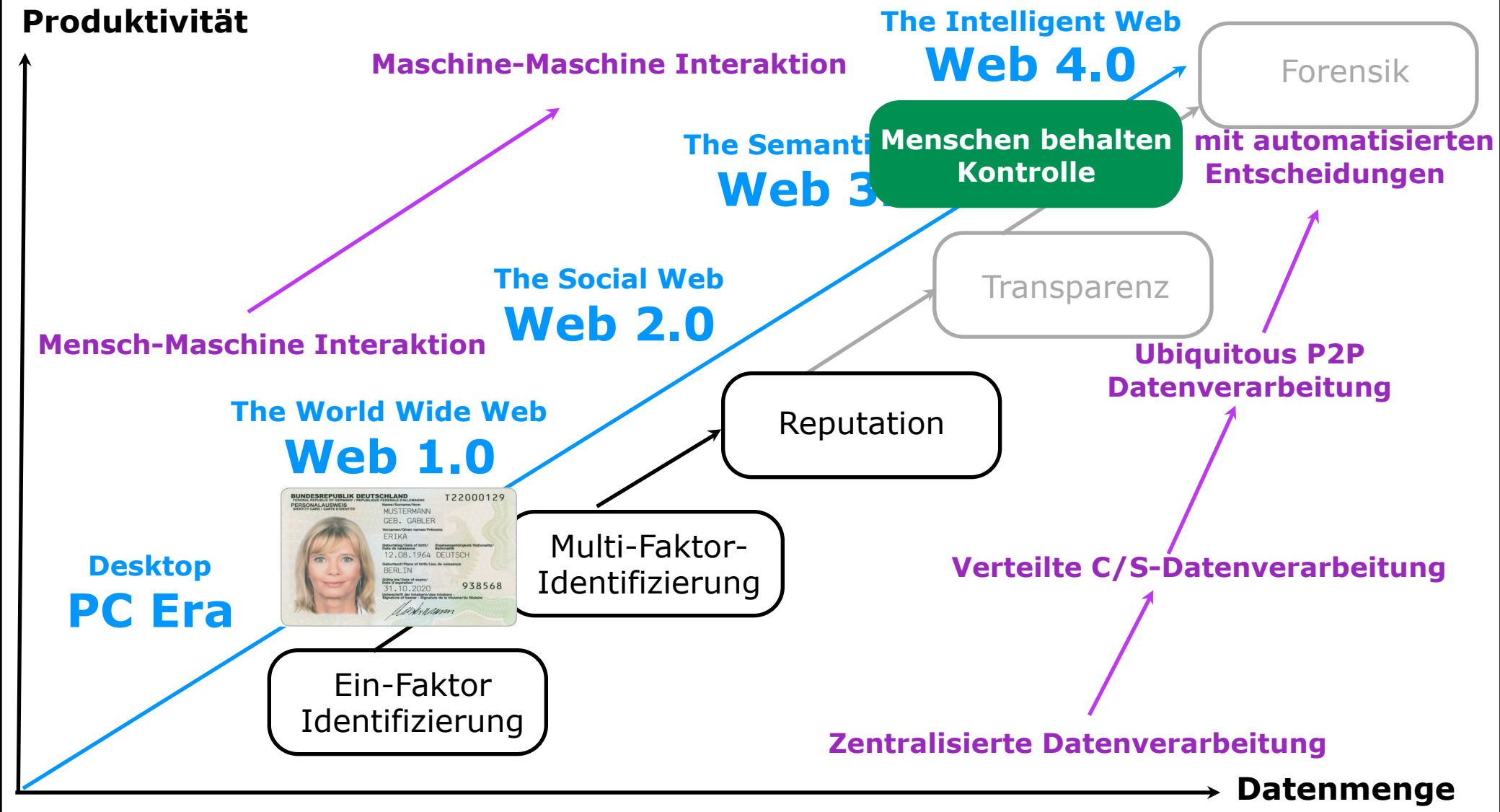
Eigene Abbildung basierend auf Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011

3. Experimentierplattform



Eigene Abbildung basierend auf Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011

3. Experimentierplattform



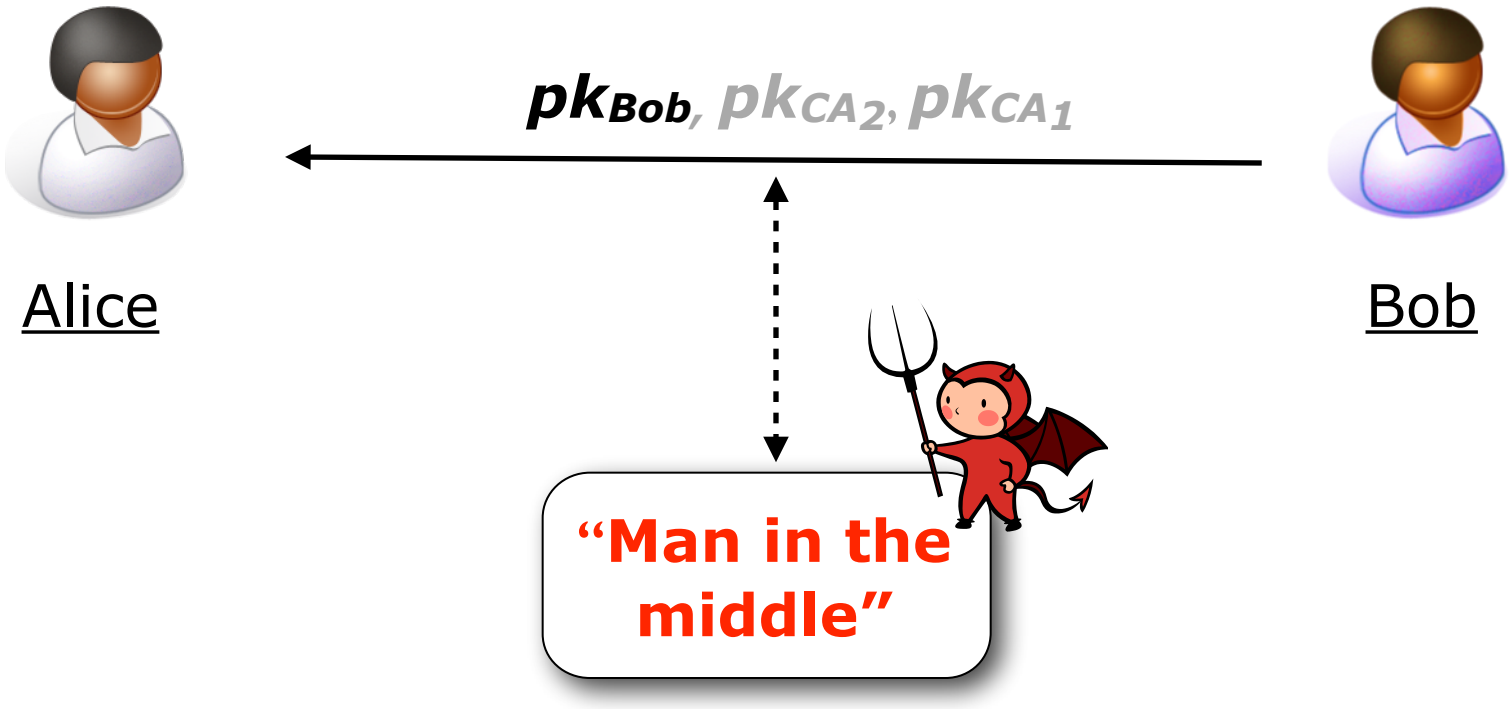
Eigene Abbildung basierend auf Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011

Szenario: Spontaner Informationsaustausch

Beispiel: Schlüsselaustausch

Integrität und Verfügbarkeit von pk_{Bob}

- Voraussetzung ist authentischer Kanal: Persönlicher Austausch, PKI, …

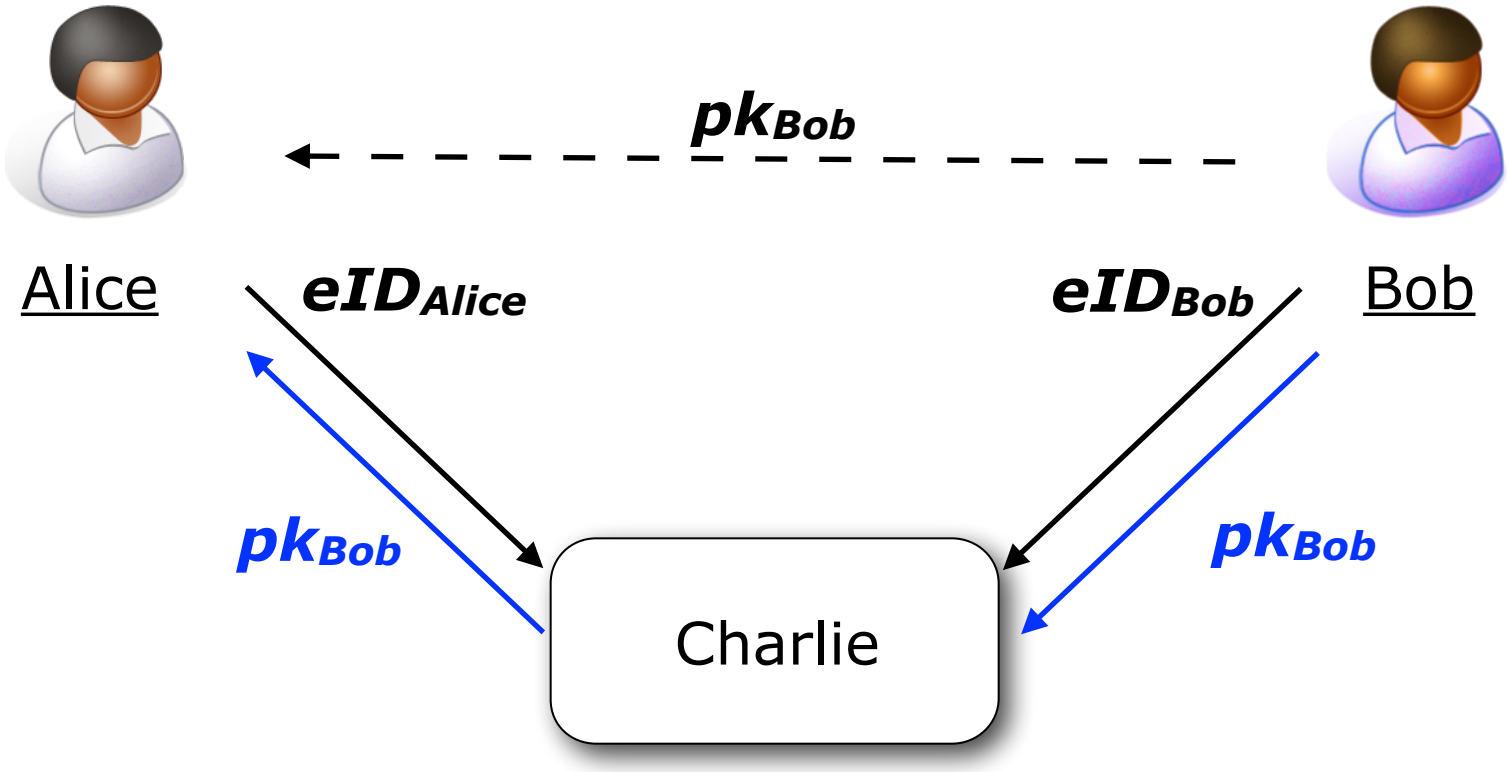


Informatisierte, vernetzte Gesellschaft: Spontaner Informationsaustausch

- Keine globale PKI für Personen
- Mehrseitige IT-Sicherheit: Zurechenbarkeit und Unbeobachtbarkeit explizite Schutzziele
- In Deutschland: 74% möchten ihre Sicherheit an Dritte delegieren

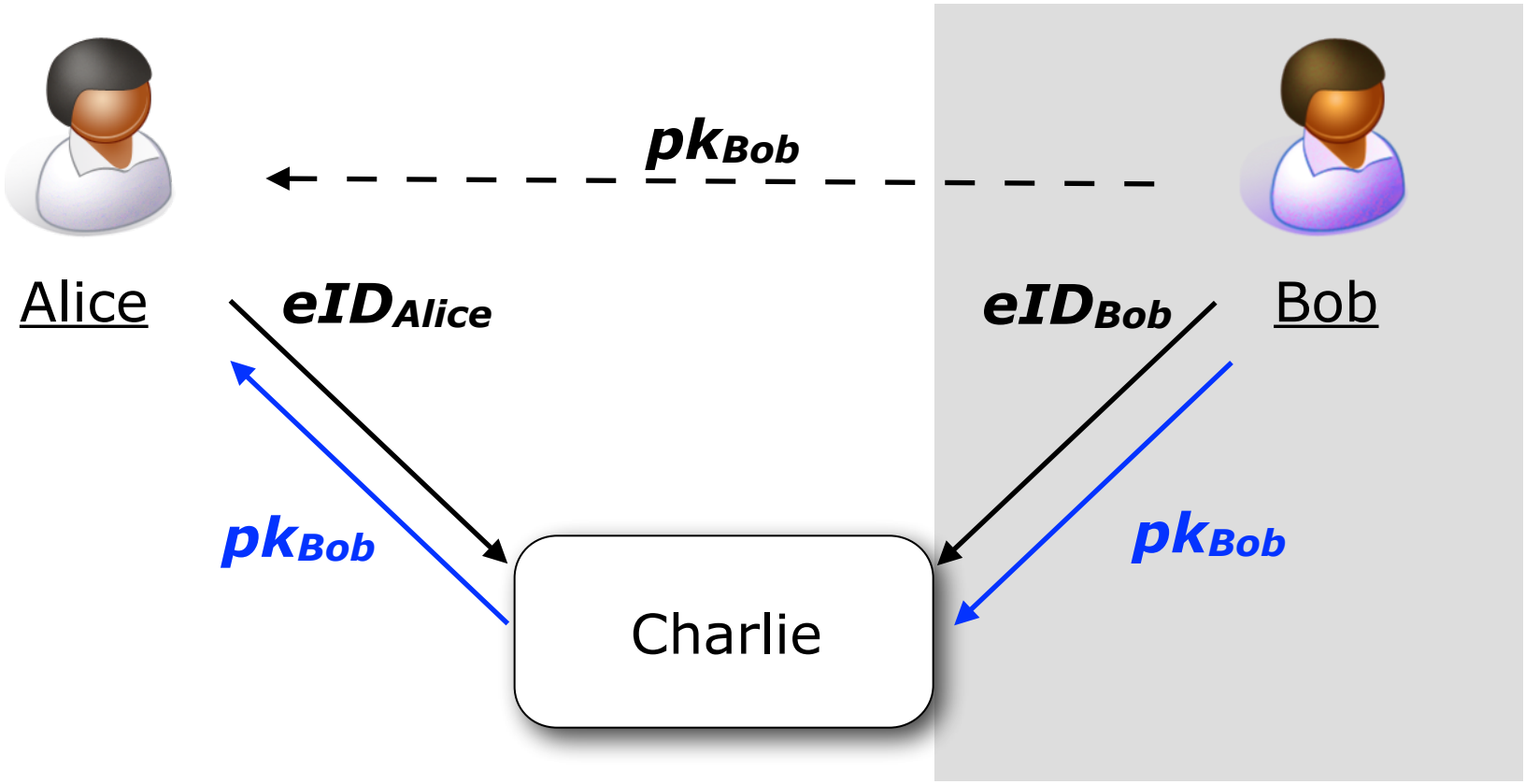
W. Diffie and M.E. Hellmann. New Directions in Cryptography, 1976; K. Rannenberg. Multilateral Security A Concept and Examples for Balanced Security, 2000; http://www.divsi.de

Individuelle Sicherheitsinteressen



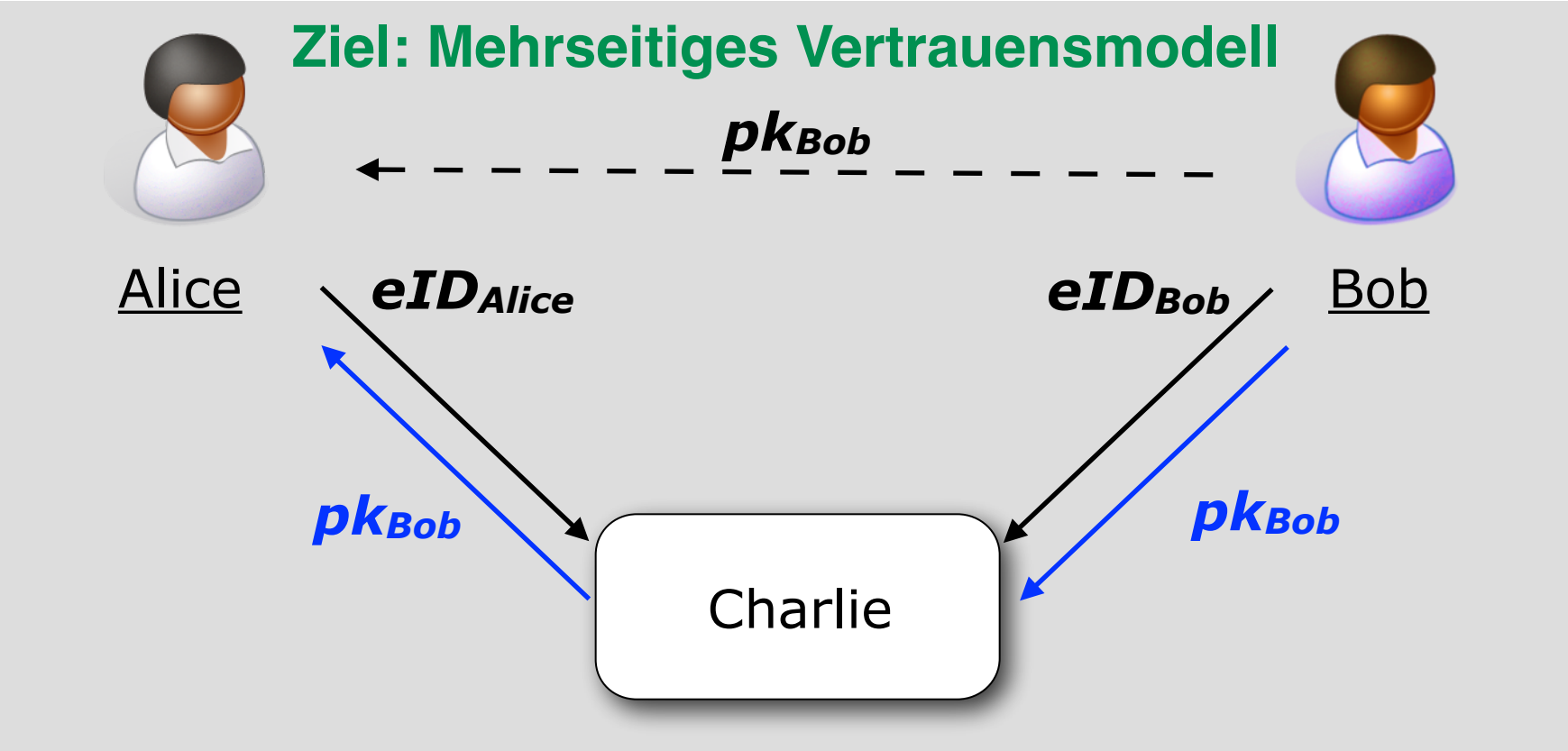
- Integrität und Verfügbarkeit von pk_{Bob} über Dritte
- Zurechenbarkeit und Unbeobachtbarkeit durch eID-Infrastrukturen

Individuelle Sicherheitsinteressen



- Integrität und Verfügbarkeit von pk_{Bob} über Dritte
- Zurechenbarkeit und Unbeobachtbarkeit durch eID-Infrastrukturen
- **Einseitiges Vertrauen: Keine Kontrolle über Nutzung von pk_{Bob}**

Individuelle Sicherheitsinteressen

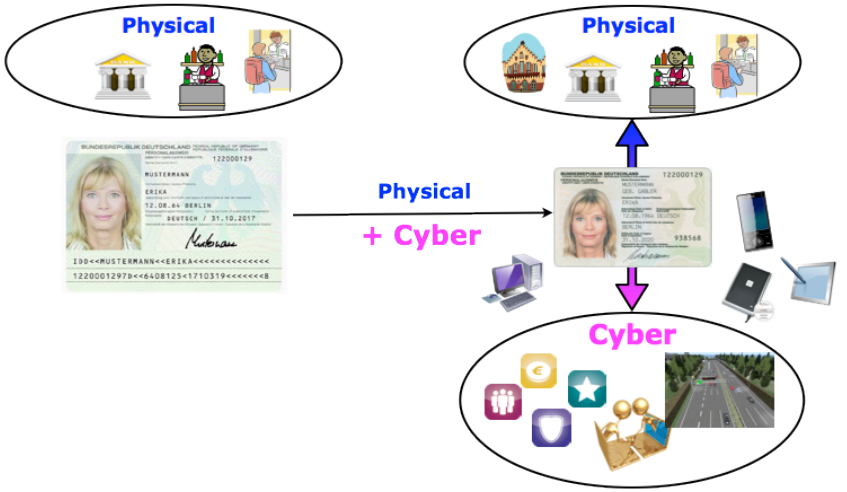


- Integrität und Verfügbarkeit von pk_{Bob} über Dritte
- Zurechenbarkeit und Unbeobachtbarkeit durch eID-Infrastrukturen
- **Einseitiges Vertrauen: Keine Kontrolle über Nutzung von pk_{Bob}**

Call for Apps

eID-Client und Erweiterungen für

- Open Source Gateway für eID-Server
- Open Source eID-Server
- Ihre Idee u.a. als Testdienst
- Kontrolle und Transparenz

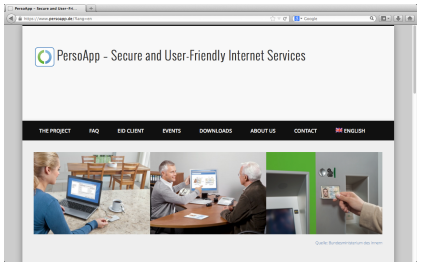


Wir bieten an

- Nutzerorientierte Anforderungsanalyse
- Entwicklung eines Use Cases insbesondere für eine mobile Anwendung
- Open-Source-Software-Bibliothek für die Online-Ausweisfunktion eines eID-Client
- Erweiterung des eID-Clients durch “Feature Requests”
- Handlungsempfehlungen für eine Integration der PersoApp-Bibliothek in Anwendungen und ihrer Prüfung
- Veröffentlichung von Ergebnissen über Workshop, Vorträge, Lehre und Internet

Nehmen Sie mit uns Kontakt auf unter https://www.persoapp.de

Beteiligen Sie sich!



Internet Portal https://www.persoapp.de
- Forum
- Pre-Release
- Demo- und Testdienst
- Dokumentation
- Veranstaltungskalender

Code Repository https://persoapp.googlecode.com/
- SVN-Repository
- Issue-Tracker

E-Mailverteiler
- Kontakt: persoapp@trust.cased.de
- Projektleiter: persoapp-projects@trust.cased.de
- Software-Entwickler: persoapp-devel@trust.cased.de
- Projektmitglieder: persoapp-broadcast@trust.cased.de
- Lenkungsausschuss: persoapp-steering@trust.cased.de
- Beirat: persoapp-advisory@trust.cased.de

Twitter über https://www.twitter.com/persoapp
- Information zu Neuigkeiten und Austausch über PersoApp