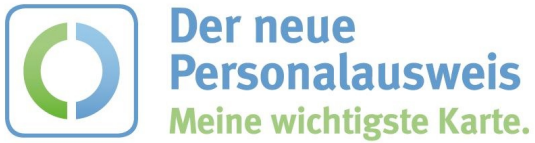
ICT Resilience in EU



Int. Workshop on Information Systems for Social Innovation (ISSI) 2013
Session: Systems Resilience
National Institute of Informatics, Tokyo, Japan
February 4, 2014

Dr. Sven Wohlgemuth

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

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

Center for Advanced Security Research Darmstadt (CASED)

www.cased.de

CASED

Secure Software Engineering		
Cryptography	Identity, Privacy, Trust	Usable Security
Cloud Security		
Mobile and Cyber-Physical 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 · 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

Agenda

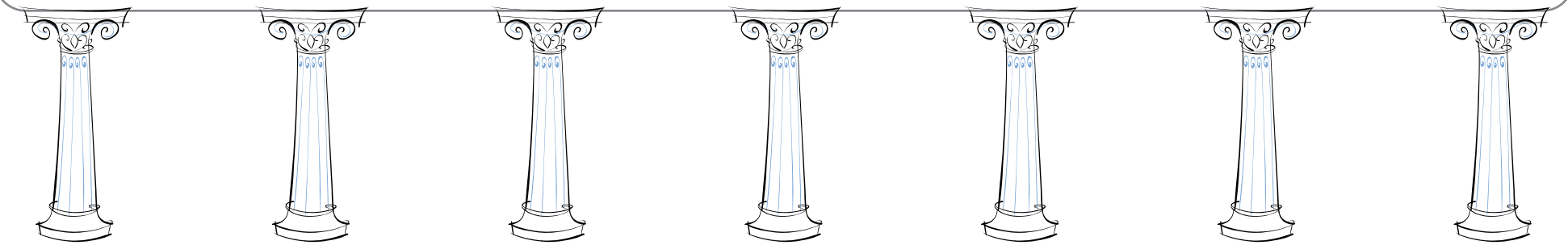
I. A Digital Agenda for Europe

II. Trustworthy Information Exchange

III. PersoApp: German national ID card

I. A Digital Agenda for Europe

Objective: ICT support to deliver sustainable economic and social benefits



I: Single digital market

II: Interoperability & standards

III: Trust & security

IV: Fast and ultra-fast internet access

V: Research and innovation

VI: Enhancing digital literarcy, skills and inclusion

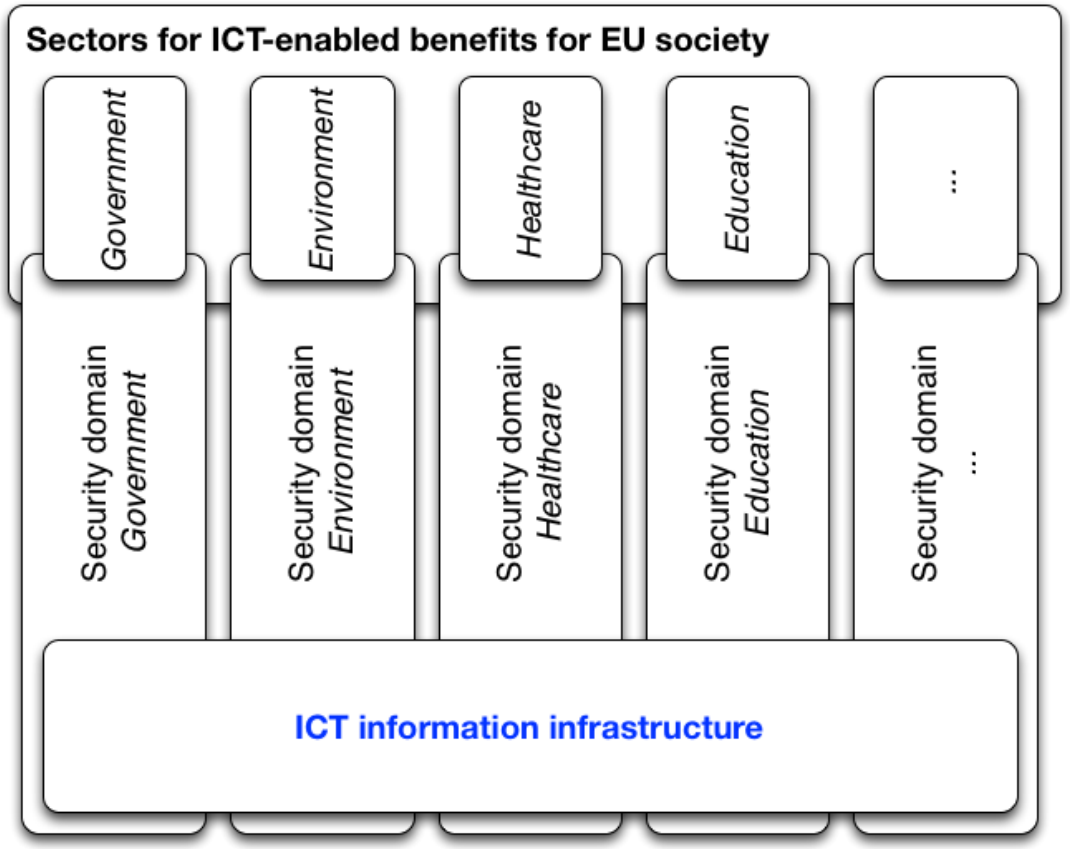
VII: ICT-enabled benefits for EU society

Expectation: Within 8 years increase European GDP by 5% & 3.8 million new jobs

Examples: e-ESTONIA The digital society (Estonia), INDUSTRIE 4.0 (Germany), EU data protection regulatory framework, Security and integrity of electronic communications networks and services (ENISA)

cf. A Digital Agenda for Europe, COM(2010) 245 final/2

ICT Supported EU Society



Threats:

Interferences due to

- Crime, Terrorism,
- Natural phenomena,
- Human errors, and
- System failures

Possible impact:

Interference propagates across sectors via dependencies, e.g. third party failures

- Common ICT information infrastructure
- Internet of Things
- Internet of Services

Security and integrity (resilience):

- Resistance against threats **(prevent and protect)** &
- Adapt sectors to deal with incidents **(respond and recover)**

cf. A Digital Agenda for Europe, COM(2010) 245 final/2, Directive 2009/140/EC as amendments to 2002/21/EC, 2002/19/EC, and 2002/20/EC

Incidents and their Impact

	Natural phenomena	Human errors	Malicious actions	System failures	Third party failure	Cause in detail
Incidents per root cause (%)	6	5	8	**76**	13	1. Hardware failure 2. Software bug … 6. Cyber attack
Average duration of recovery (hours)	**36**	26	4	9	13	
Average number of user connections	557	447	1528	2330	**2808**	1. Overload 2. Software bug … 4. Cyber attack
User hours lost	20283	11393	5858	19842	**36502**	1. Overload 2. Power cut … 6. Cyber attack

Third-party failure and non-availability of ICT have highest impact

cf. ENISA. Annual Incident Reports 2013

IT Security Situation in Germany in 2011

Risk trends

Threat	2009	2011	Forecast
DDoS attacks	↑	→	→
Unsolicited e-mails (spam)	↑	→	→
Botnets	↑	↑	↑
Identity theft	↑	↑	↑
Security vulnerabilities	–	↑	↑
Drive-By Exploits	–	↑	→
Malware	–	↑	↑

Risk potential of attack opportunities in selected applications and technologies

Technology/Applications	2009	2011	Forecast
Mobile communication	↑	↑	↑
SCADA	↑	↑	↑
DNS and BGP	↑	↑	→
Interfaces and storage media	→	↑	↑

Risk profile of innovative applications and technologies

Technology/Applications	2009	2011	Forecast
Cloud Computing	–	↑	↑
Smart Grid/Smart Meter	–	↑	↑

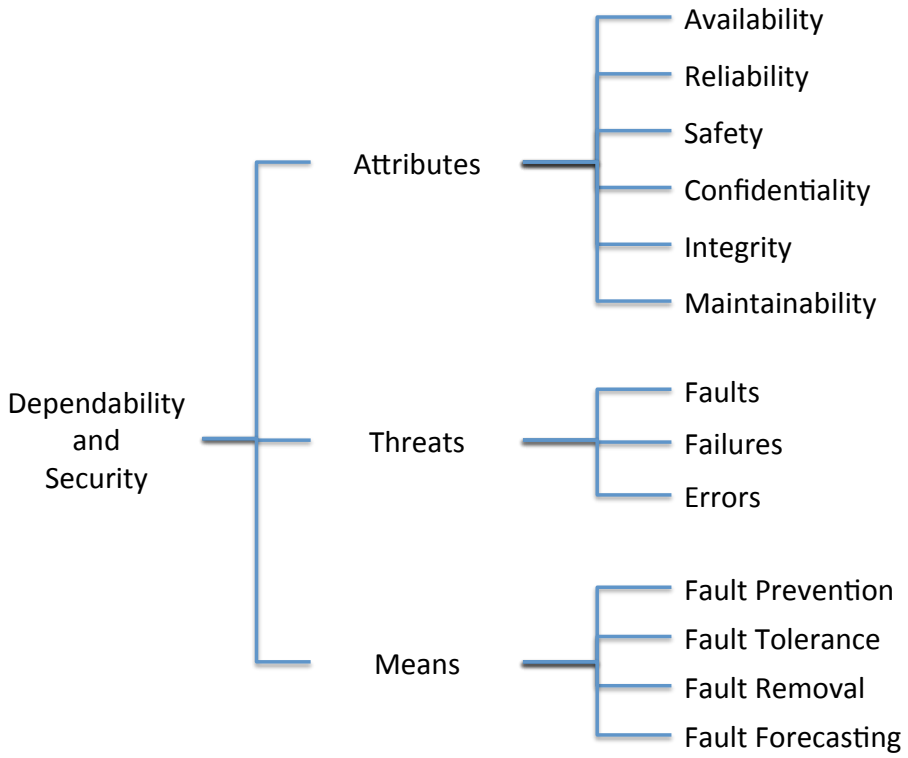
Trend:

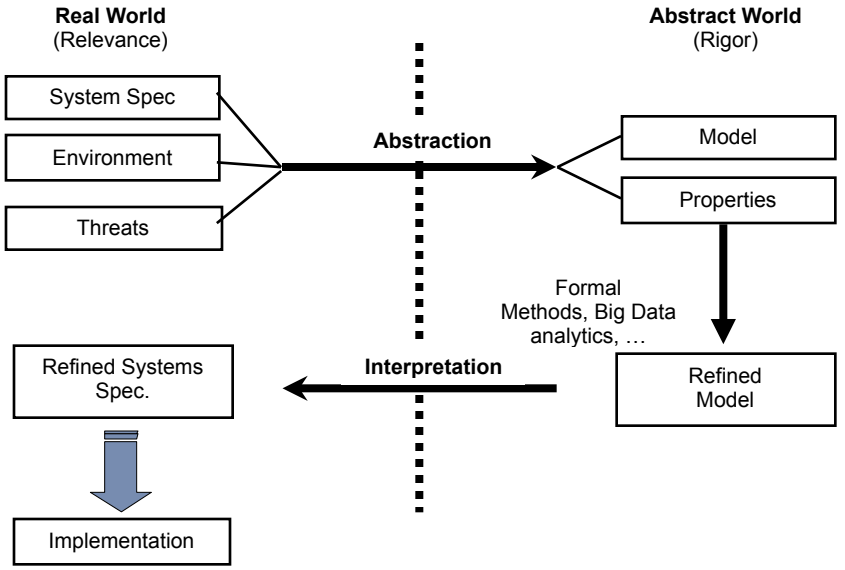
- Direct attack from attacker ➔ attack via compromised IT system
- Propagation via dependency between IT systems
- Focus: Mobile and Cyber-Physical Systems

cf. Federal Office for Information Security (BSI). The IT Security Situation in Germany in 2011.

ICT Resilience

ICT Resilience: Ability of an ICT system to provide and maintain an **acceptable level of service** in the face of various faults and challenges to normal operation (Sterbenz et al., 2010)



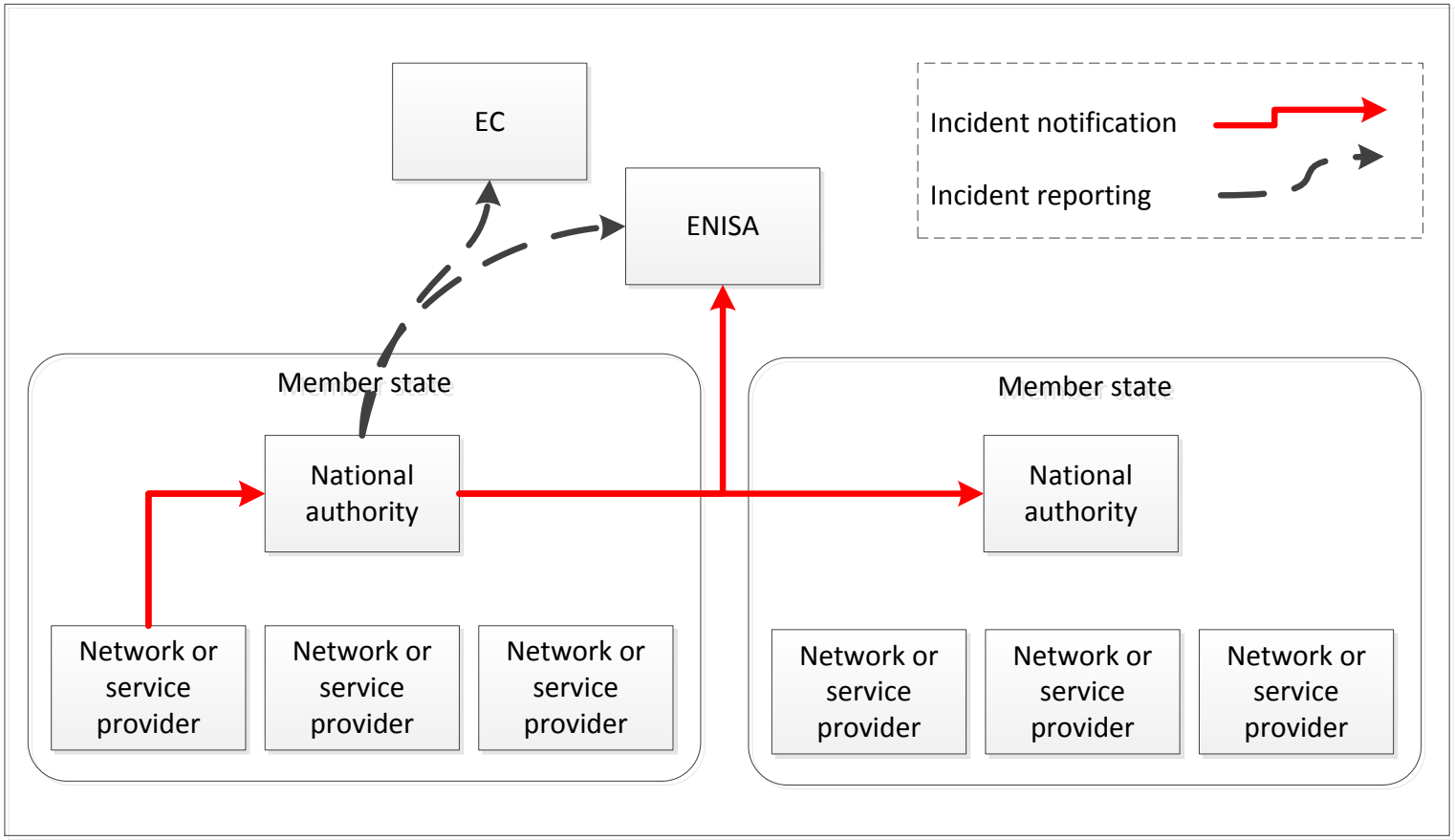


Avienžies et al., 2004

Requirements:

- Prevent and protect: Secure IT systems and information about threats
- Respond and recover: Information about incidents and system adaption in "real-time"

Support: Incident Reporting (Article 13)



Article 13 requests auditable information flow:

- Providers (public & private) should take measures and report incidents to NRA
- Audit by a qualified independent body
- Safeguarding competition and boosting consumer choice

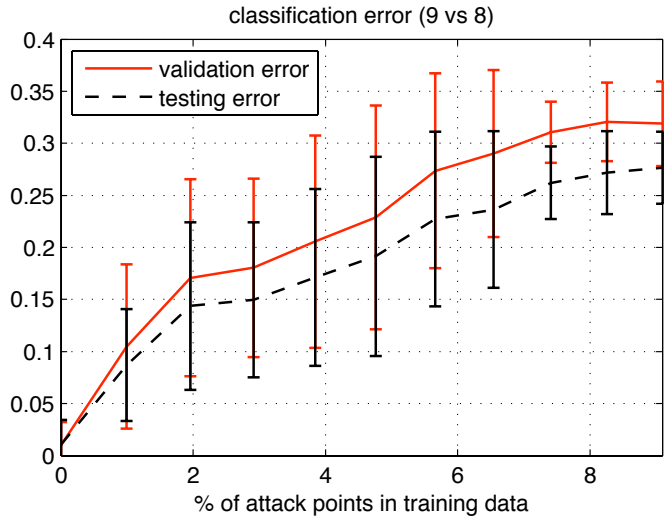
cf. Directive 2002/21/EC and Directive 2009/140/EC

Proposal for Extension: Social Network

Detection of incident for both prevent and protect & response and recover

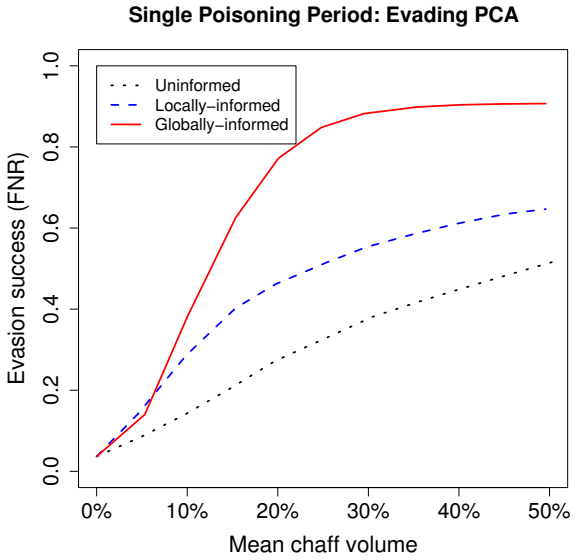
Requires authentic information according to a given threat

Supervised ML (e.g. SVM)



Biggio et al. 2012

Unsupervised ML (e.g. PCA)



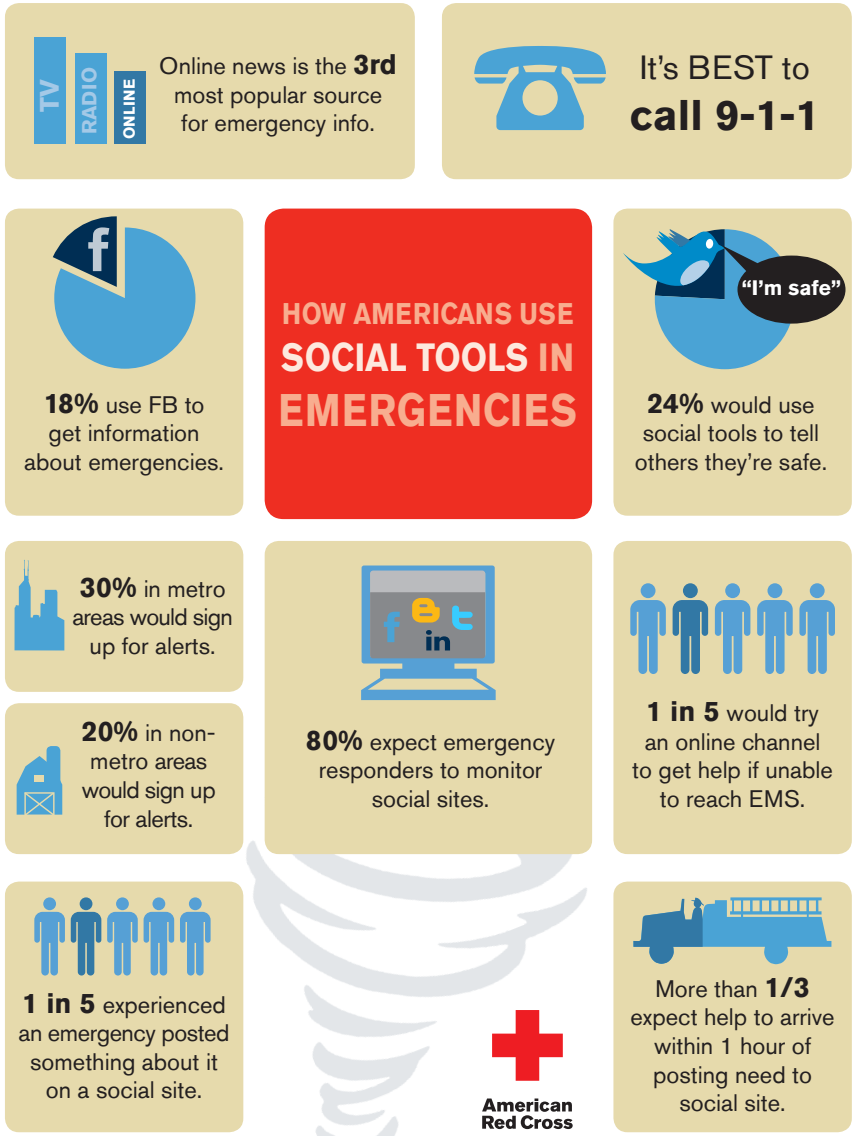
Huang et al. 2011

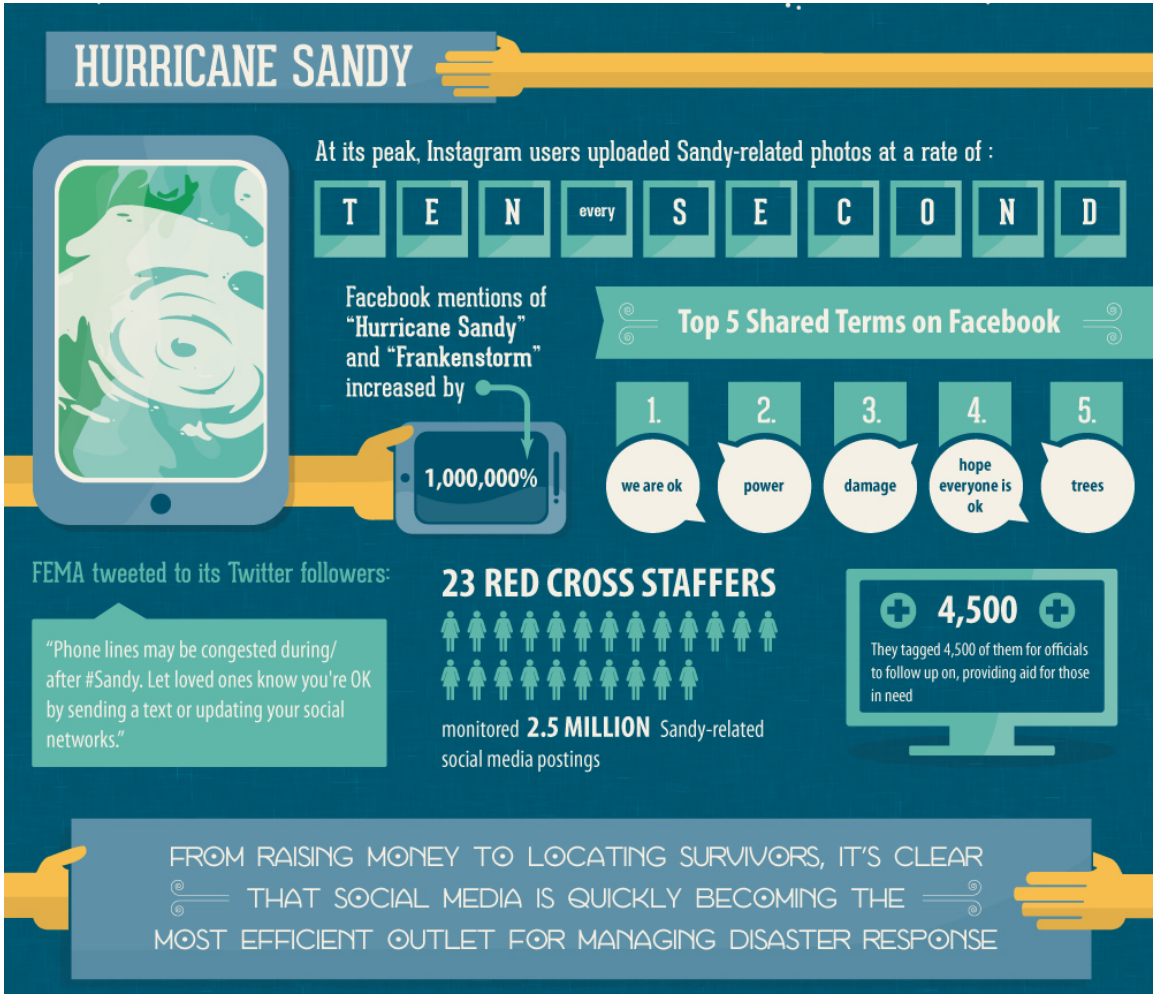
Extend set of information to improve resilience: Social Network

- Aggregation of (personal) data
- Secondary usage of (personal) data
- Disclosure of (personal) data to third parties

Security and privacy require trustworthy information sharing

Example: Information Flow with Social Networks in USA



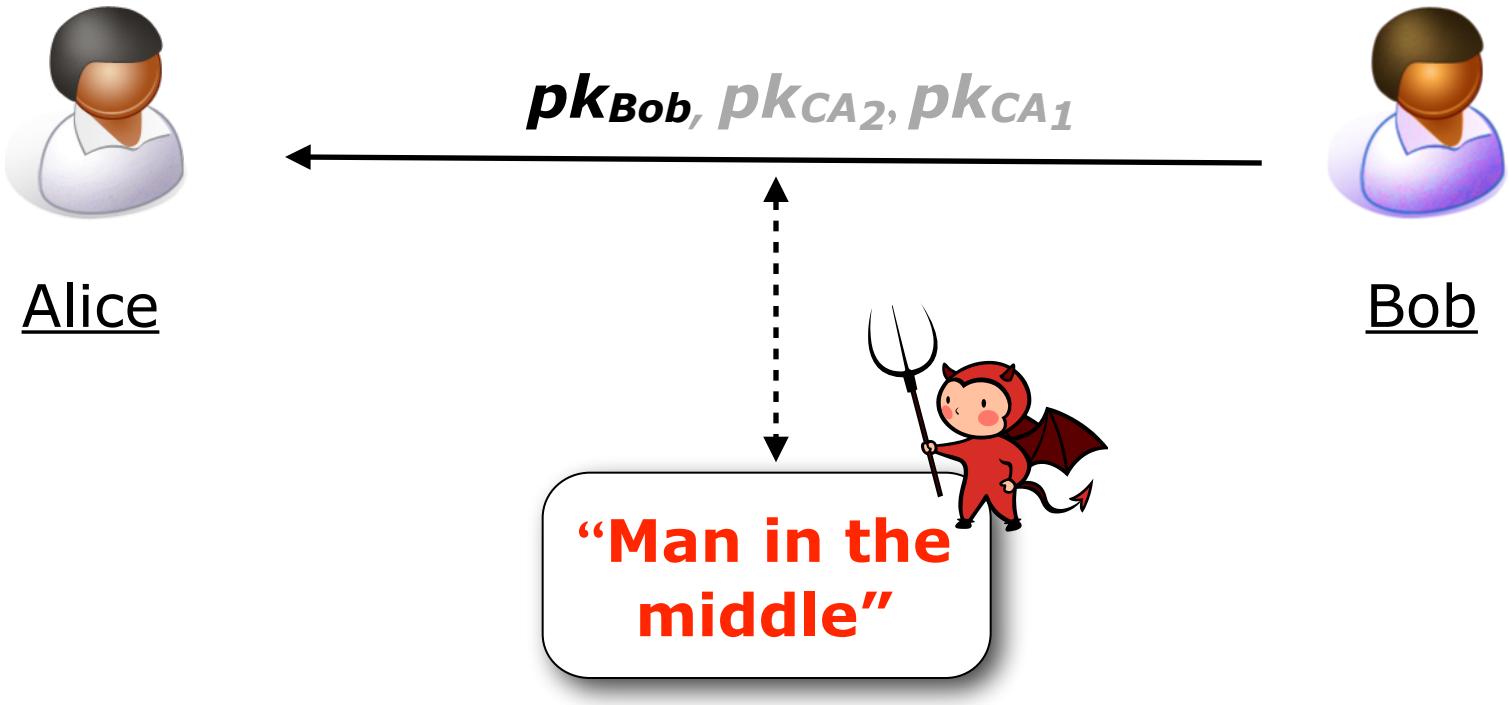


II. Trustworthy Information Exchange

Example: Public Key Exchange

Availability and integrity of pk_{Bob}

- Assumption: Authentic pre-sharing exists, e.g. via personal exchange, PKI, …

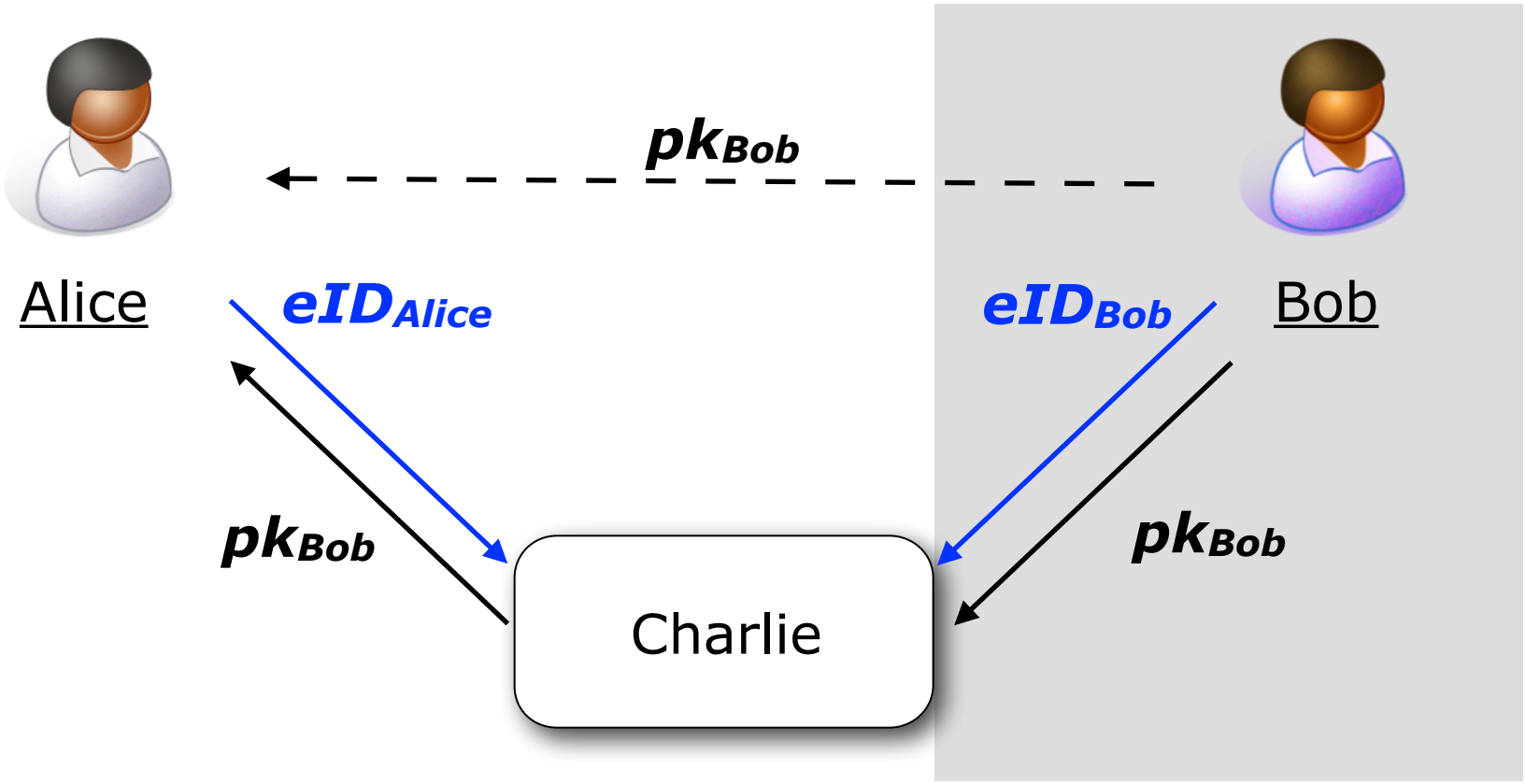


ICT-supported society:

- No global PKI for humans
- Multilateral IT Security: Accountability and unobservability are explicitly to configure
- Germany: 74% of population want to delegate responsibility to a Third Party

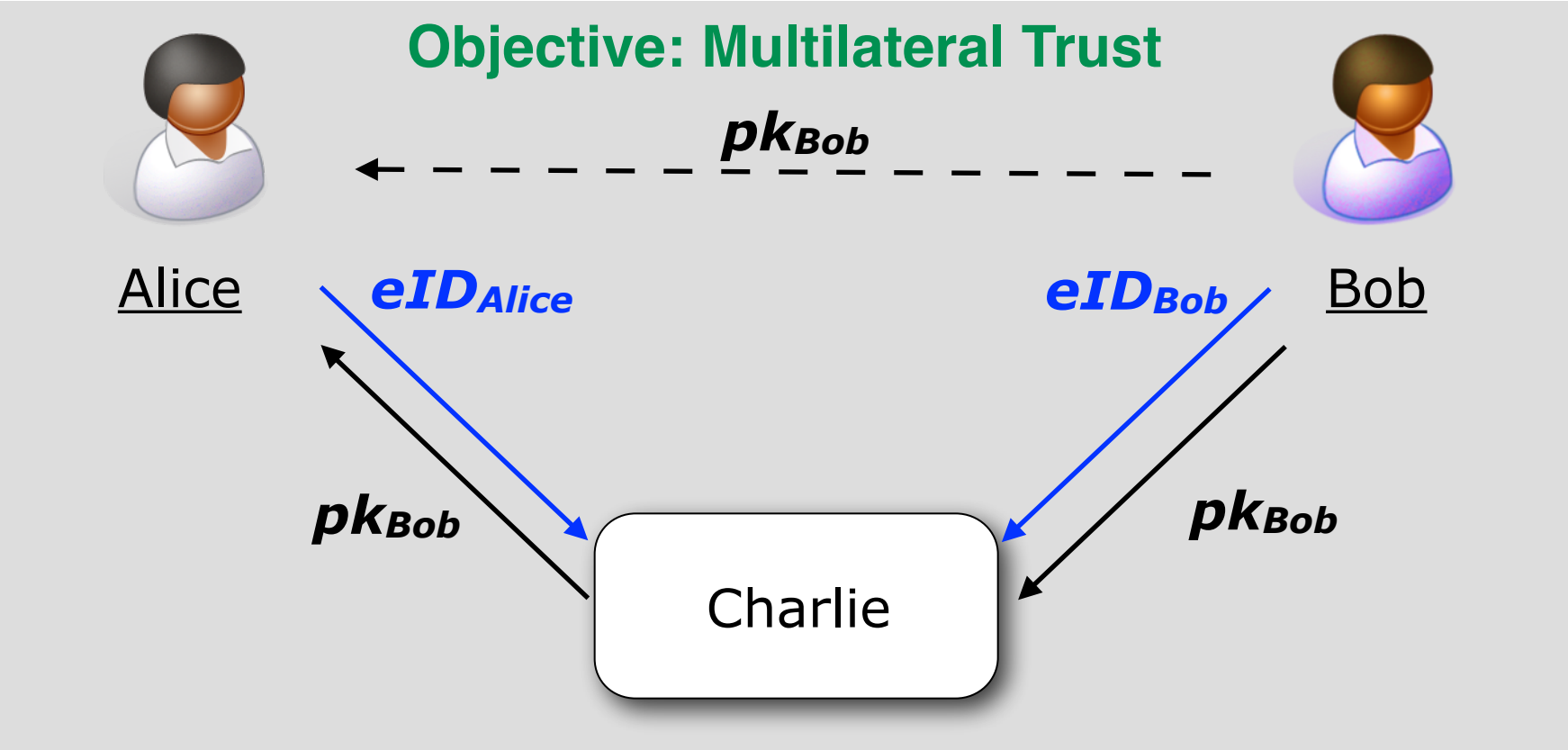
W. Diffie and M.E. Hellmann. New Directions in Cryptography, 1976; K. Rannenberg. Multilateral Security A Concept and Examples for Balanced Security, 2000; http://www.divsi.de

Trust Model



- **Availability and integrity of** pk_{Bob} via necessary "Man-in-the-Middle"
- Accountability and unobservability by access control of eID infrastructures
- **Unilateral trust: No control on usage of** pk_{Bob}

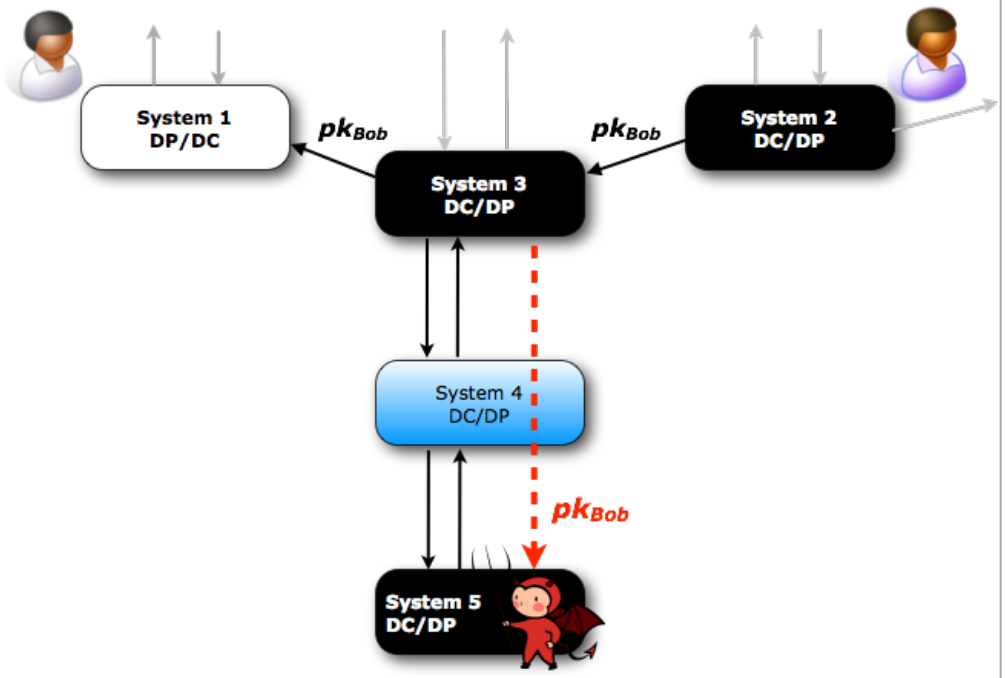
Trust Model



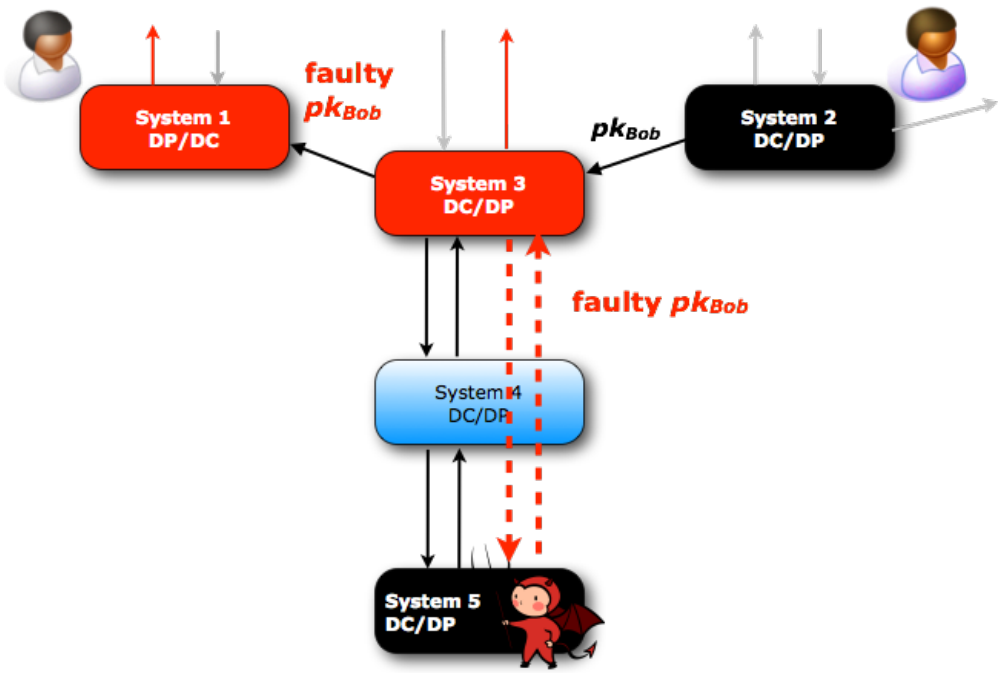
- **Availability and integrity of** pk_{Bob} via necessary "Man-in-the-Middle"
- Accountability and unobservability by access control of eID infrastructures
- **Unilateral trust: No control on usage of** pk_{Bob}

Problem: Unknown, inevitable Vulnerabilities

Adaptive IT system: "Programming at run-time" - Dependencies emerge at run-time



Case (a): Passive interference



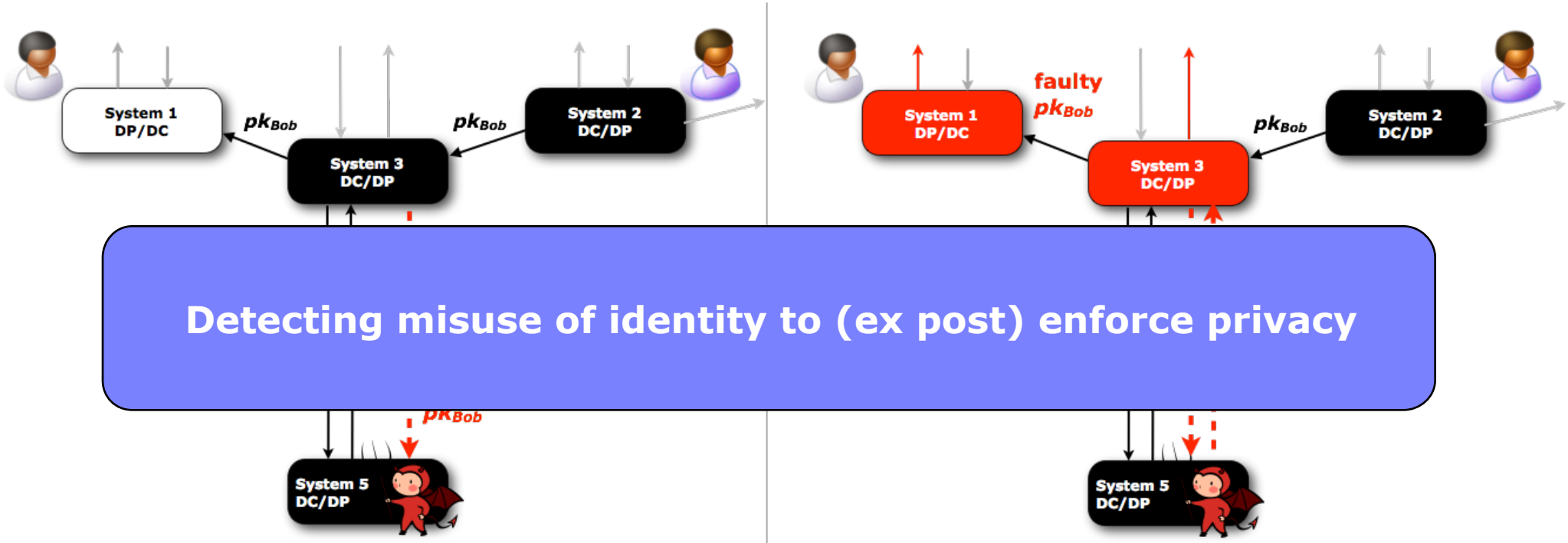
Case (b): Active interference

- Modeled dependencies imply vulnerability by undesired ones (covert channels, escalation of rights, security configuration, human errors, …)
- **Impossible to automatically detect all undesired dependencies**

C. Wang and S. Ju. The Dilemma of Covert Channels Searching, 2005.

Problem: Unknown, inevitable Vulnerabilities

Adaptive IT system: "Programming at run-time" - Dependencies emerge at run-time

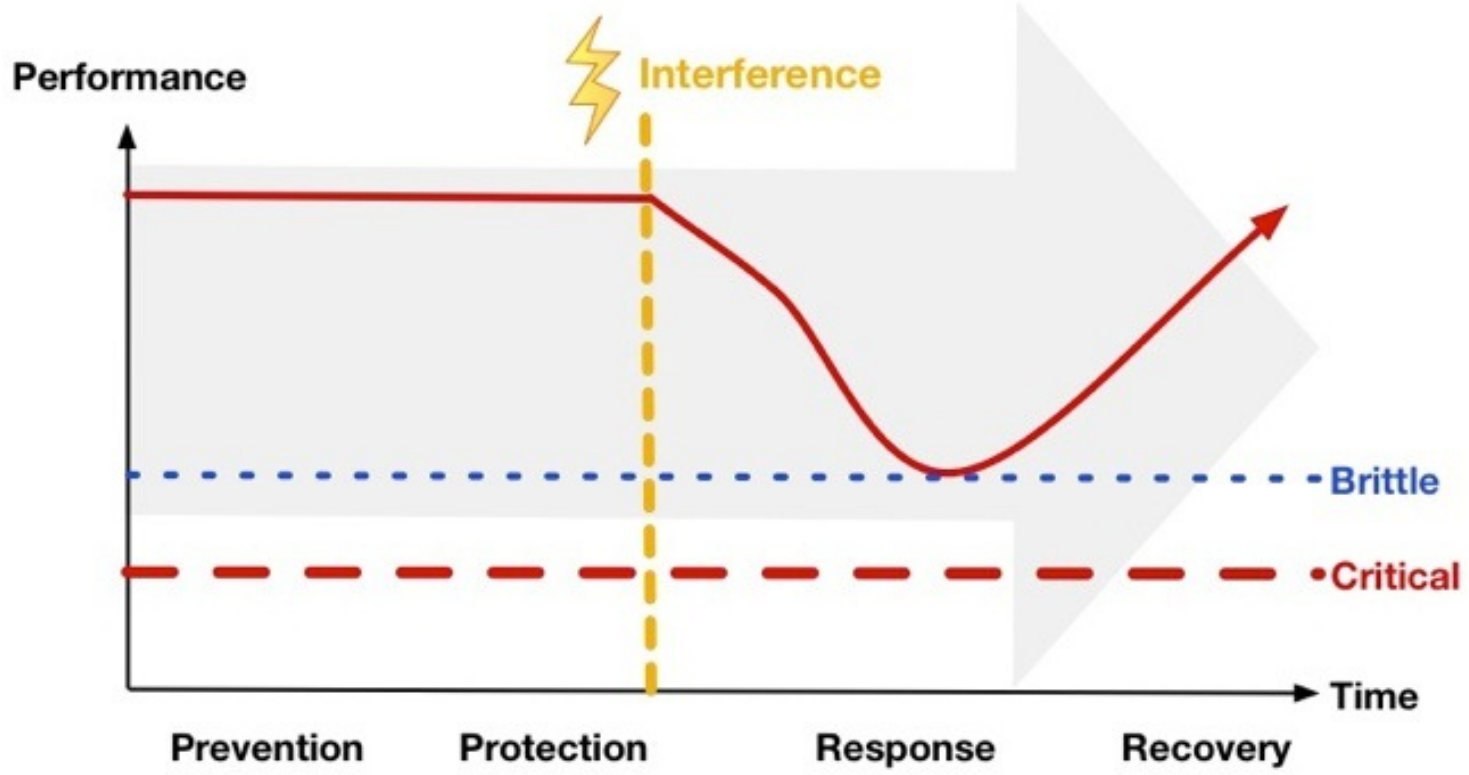


- Modeled dependencies imply vulnerability by undesired ones (covert channels, escalation of rights, security configuration, human errors, …)
- **Impossible to automatically detect all undesired dependencies**

C. Wang and S. Ju. The Dilemma of Covert Channels Searching, 2005.

ICT Resilience: Enforcing Multilateral Security

ICT Resilience: Ability of an ICT system to provide and maintain an **acceptable level of service** in the face of various faults and challenges to normal operation (Sterbenz et al., 2010)



Eigene Abbildung nach illustration following (Sheffi, 2005; Günther et al., 2007; McNanus, 2009)

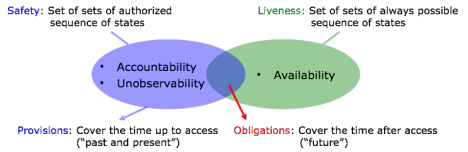
Acceptable enforcement of individual security interests for a spontaneous, trustworthy information exchange of pk_{Bob}

Approach: Control and Transparency

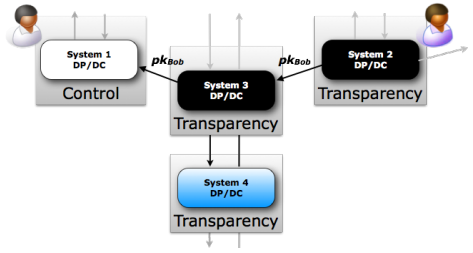
Enhanced trust infrastructure by measuring with *Privacy Control* and *Privacy Forensics*

eID client evaluates individually evidences on data usage anomalies and their origin

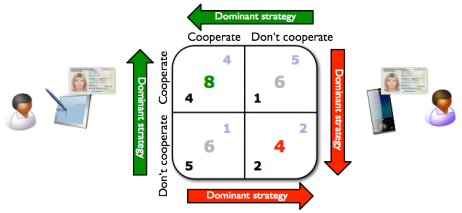
Usage Control Policy Toolbox



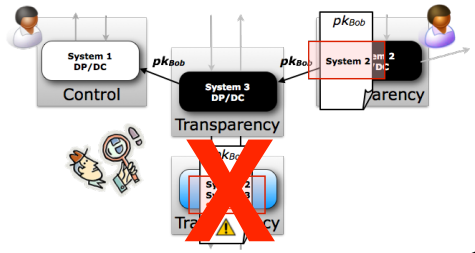
Privacy Control



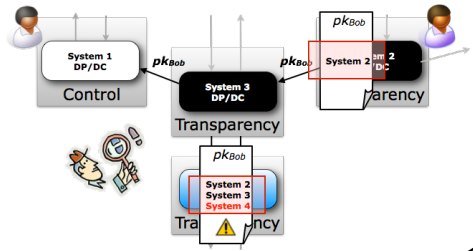
IT Risk Analysis



Optimization



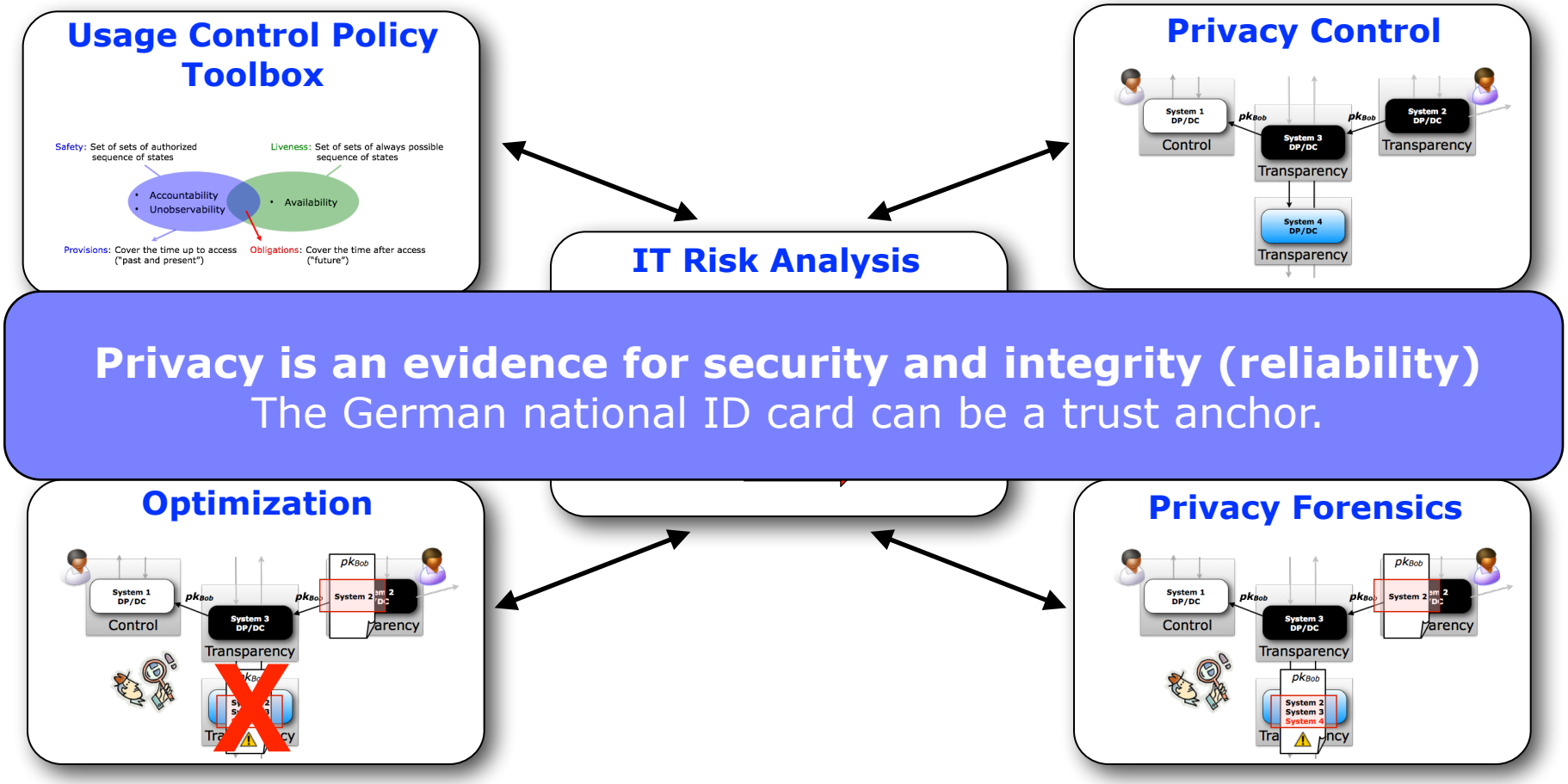
Privacy Forensics



Approach: Control and Transparency

Enhanced trust infrastructure by measuring with *Privacy Control* and *Privacy Forensics*

eID client evaluates individually evidences on data usage anomalies and their origin

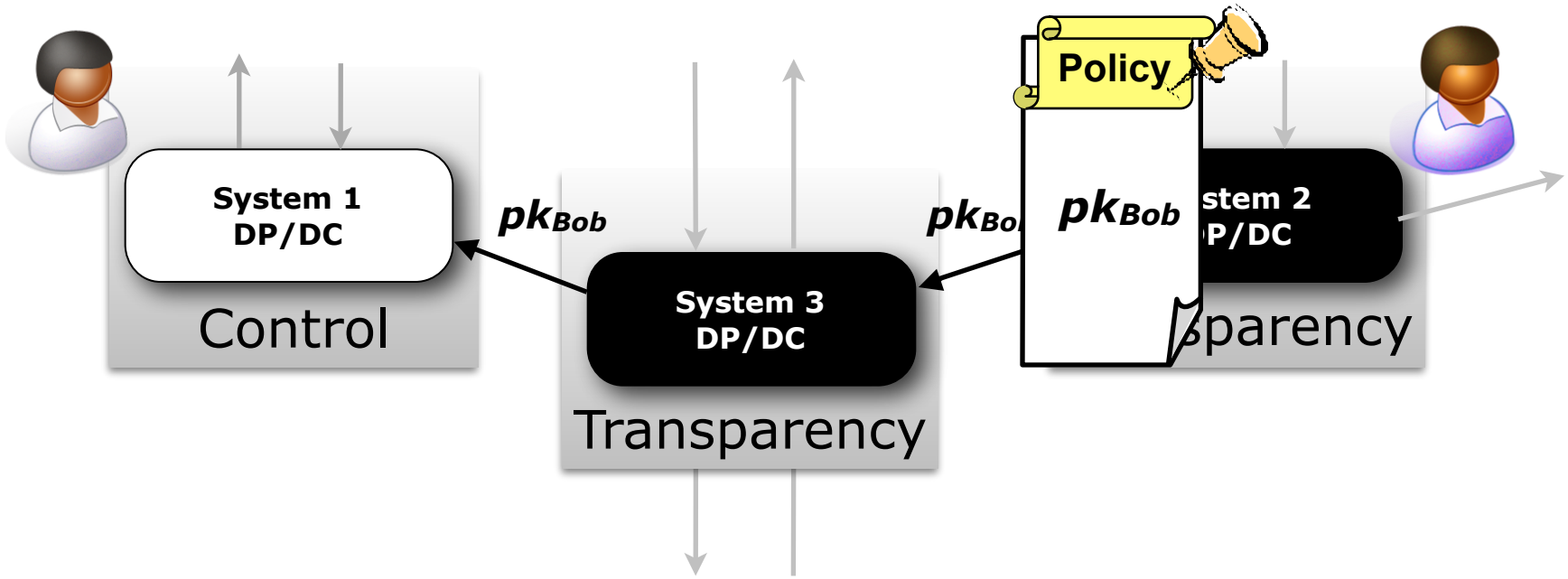


Privacy Control

Control: Individual **pseudonymized** eID based on national eID infrastructure

Specification of isolation by pseudonymized delegation of rights to third parties

In case of confidentiality breach: Information is linked to pseudonymous identity



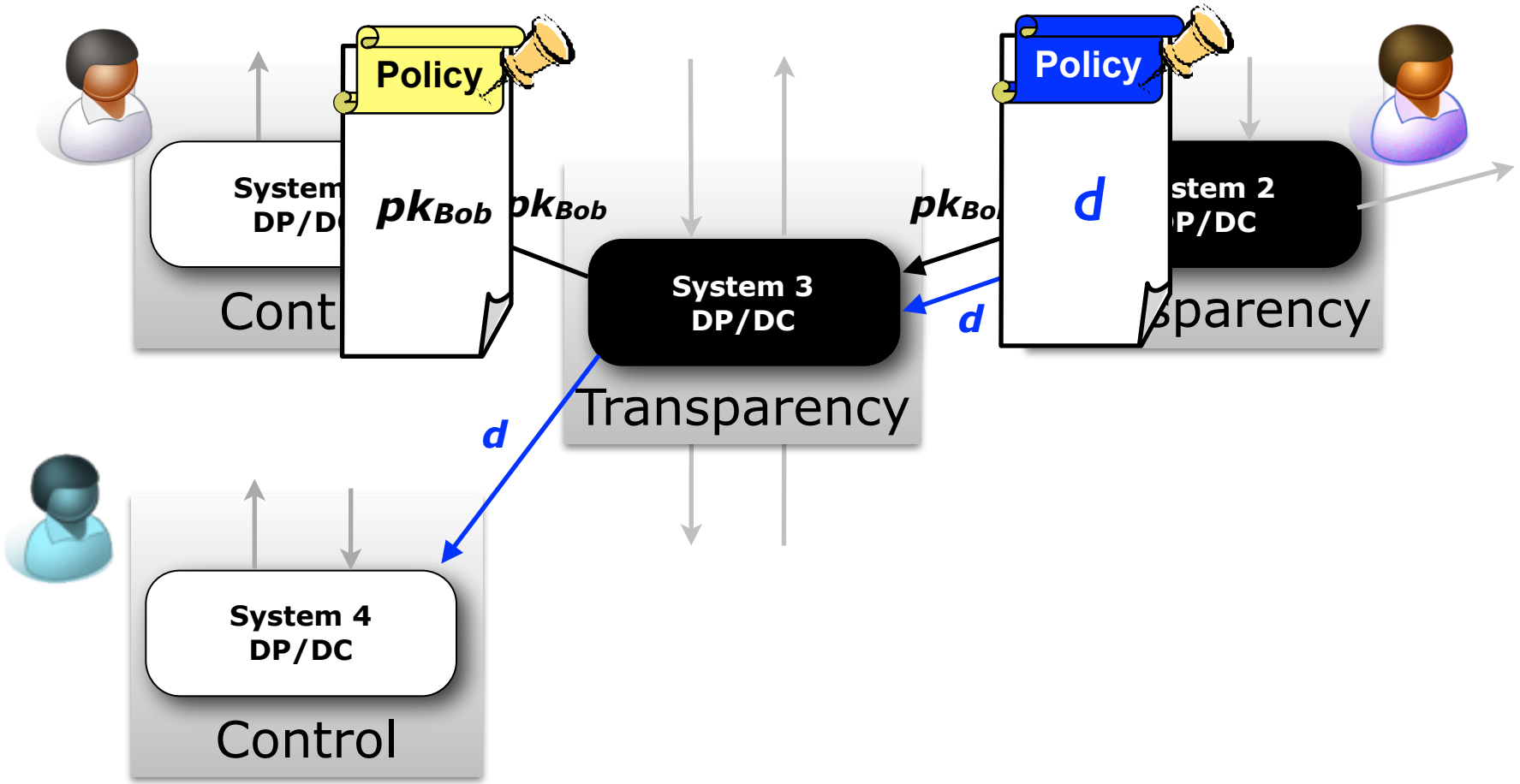
S. Wohlgemuth. Privatsphäre durch die Delegation von Rechten, 2008; N. Sonehara, I. Echizen und S. Wohlgemuth. Isolation in Cloud Computing and Privacy-Enhancing Technologies, 2011

Privacy Control

Control: Individual **pseudonymized** eID based on national eID infrastructure

Specification of isolation by pseudonymized delegation of rights to third parties

In case of confidentiality breach: Information is linked to pseudonymous identity



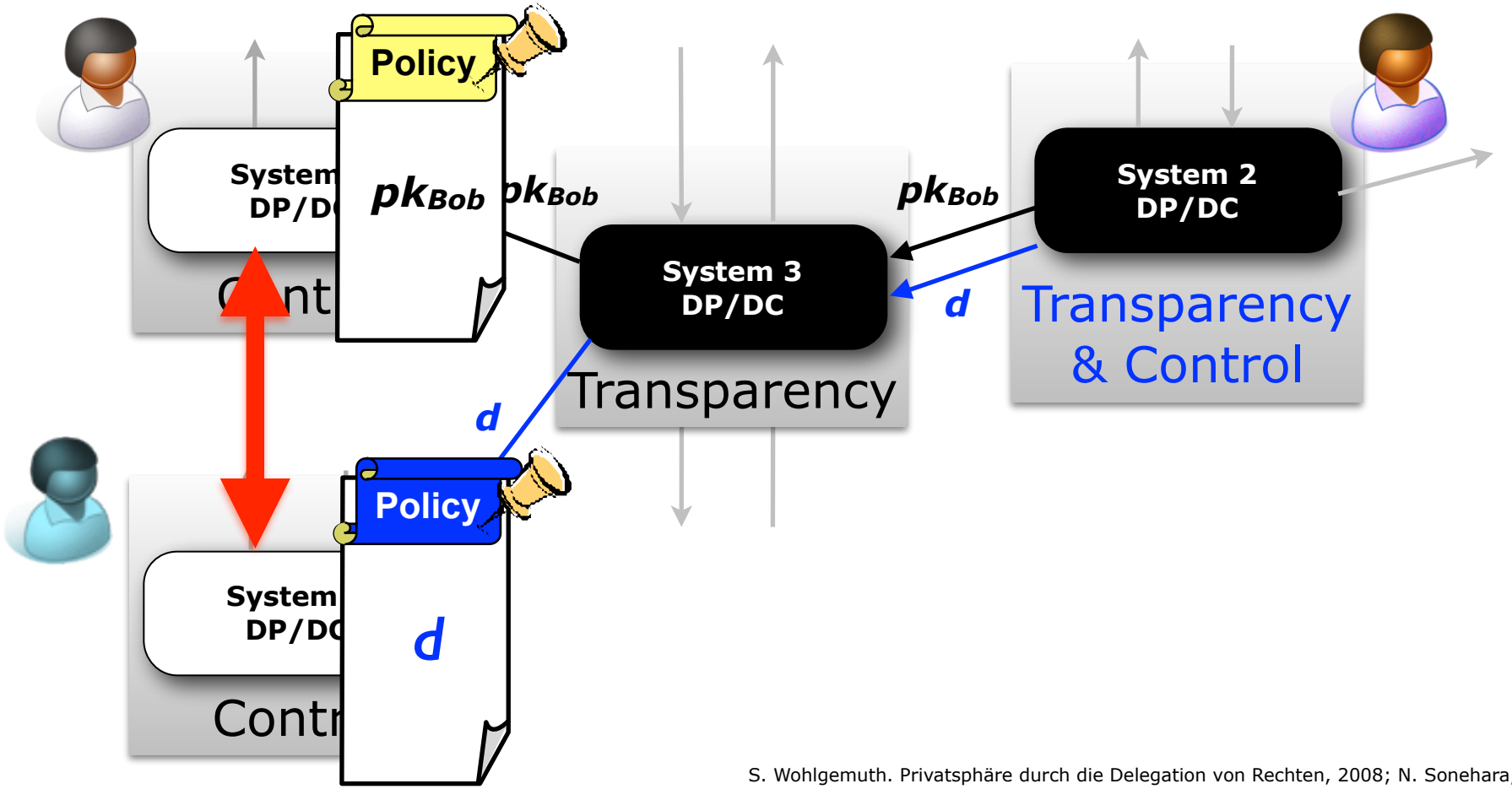
S. Wohlgemuth. Privatsphäre durch die Delegation von Rechten, 2008; N. Sonehara, I. Echizen und S. Wohlgemuth. Isolation in Cloud Computing and Privacy-Enhancing Technologies, 2011

Privacy Control

Control: Individual **pseudonymized** eID based on national eID infrastructure

Specification of isolation by pseudonymized delegation of rights to third parties

In case of confidentiality breach: Information is linked to pseudonymous identity



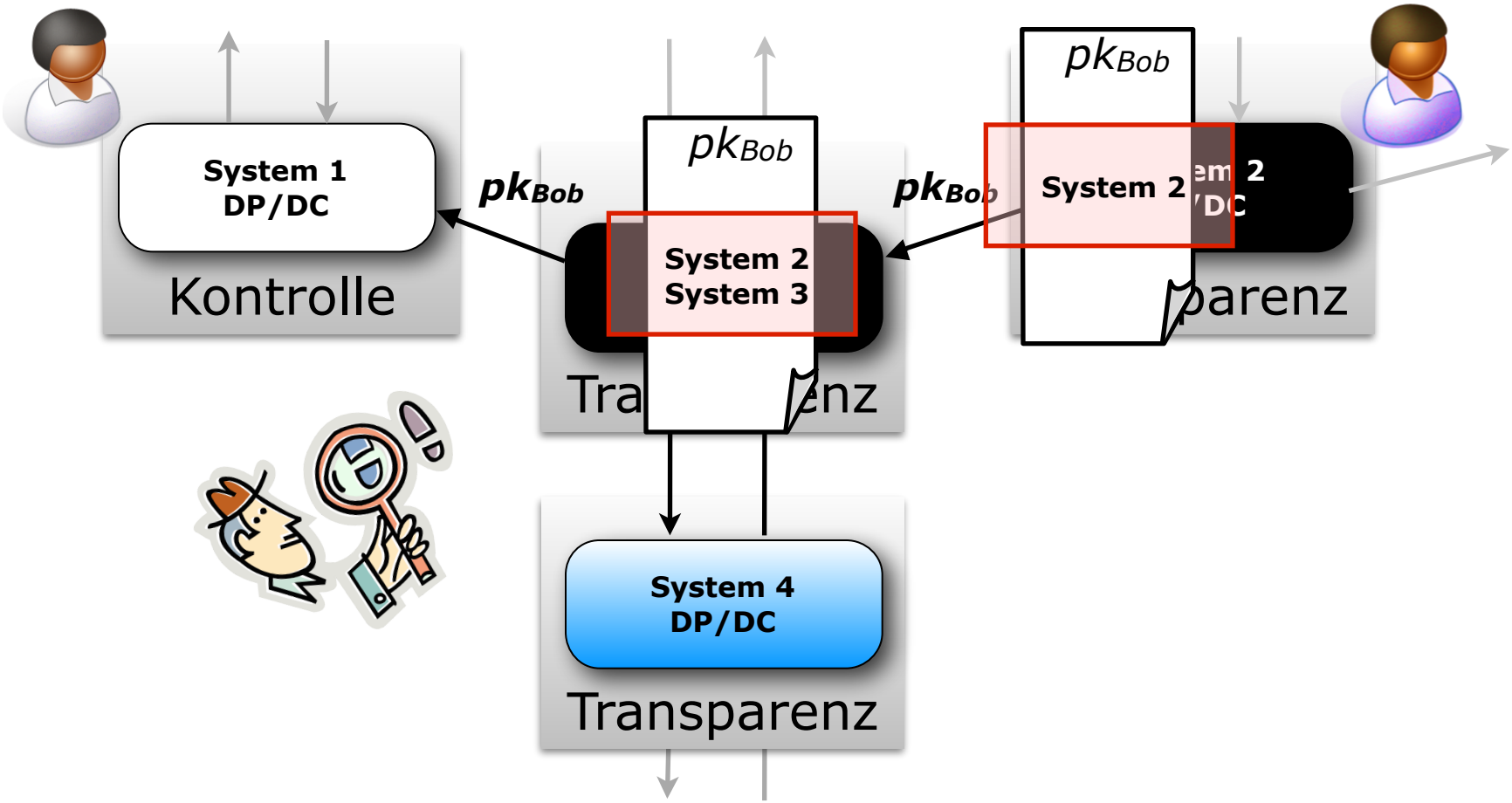
S. Wohlgemuth. Privatsphäre durch die Delegation von Rechten, 2008; N. Sonehara, I. Echizen und S. Wohlgemuth. Isolation in Cloud Computing and Privacy-Enhancing Technologies, 2011

Privacy Forensics

Control: Pseudonymous eID with eID infrastructure of national ID card

Transparency: Reconstructing usage of pk_{Bob} by data provenance

eID client enforces documenting data provenance audit trail



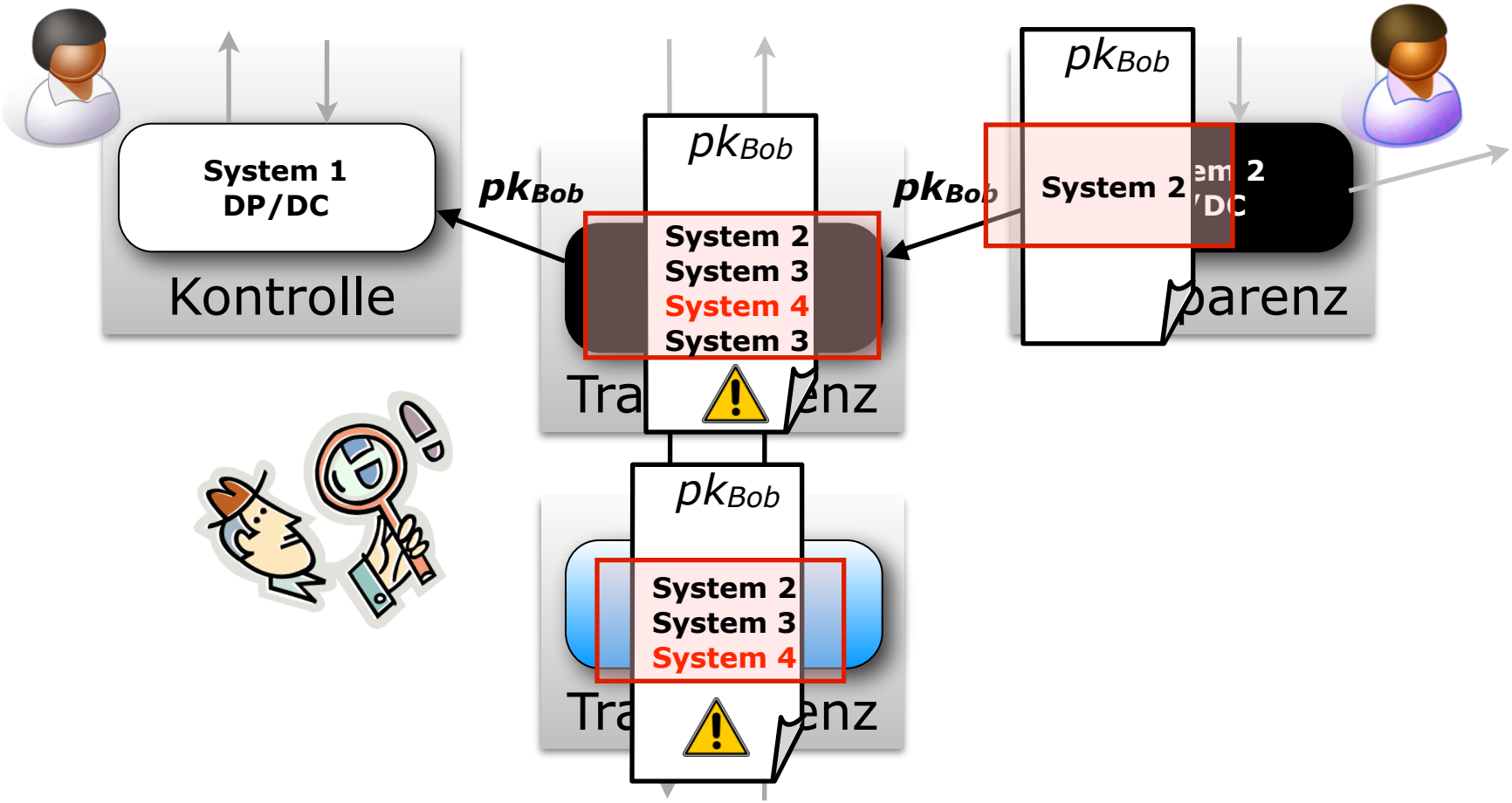
D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G.J. Sussman. Information Accountability, 2008; S. Wohlgemuth, I. Echizen, N. Sonehara und G. Müller. Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy, 2010.

Privacy Forensics

Control: Pseudonymous eID with eID infrastructure of national ID card

Transparency: Reconstructing usage of pk_{Bob} by data provenance

eID client enforces documenting data provenance audit trail



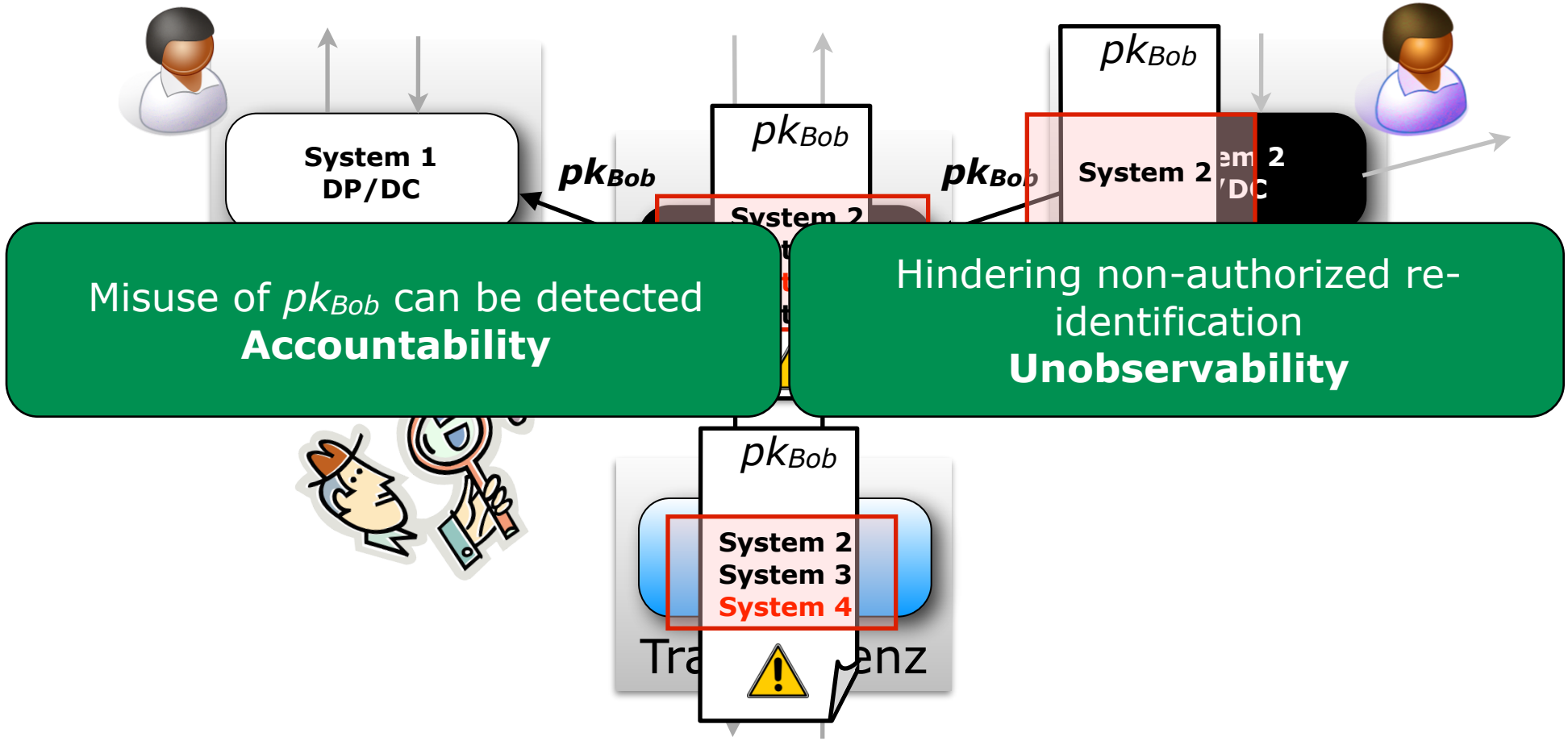
D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G.J. Sussman. Information Accountability, 2008; S. Wohlgemuth, I. Echizen, N. Sonehara und G. Müller. Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy, 2010.

Privacy Forensics

Control: Pseudonymous eID with eID infrastructure of national ID card

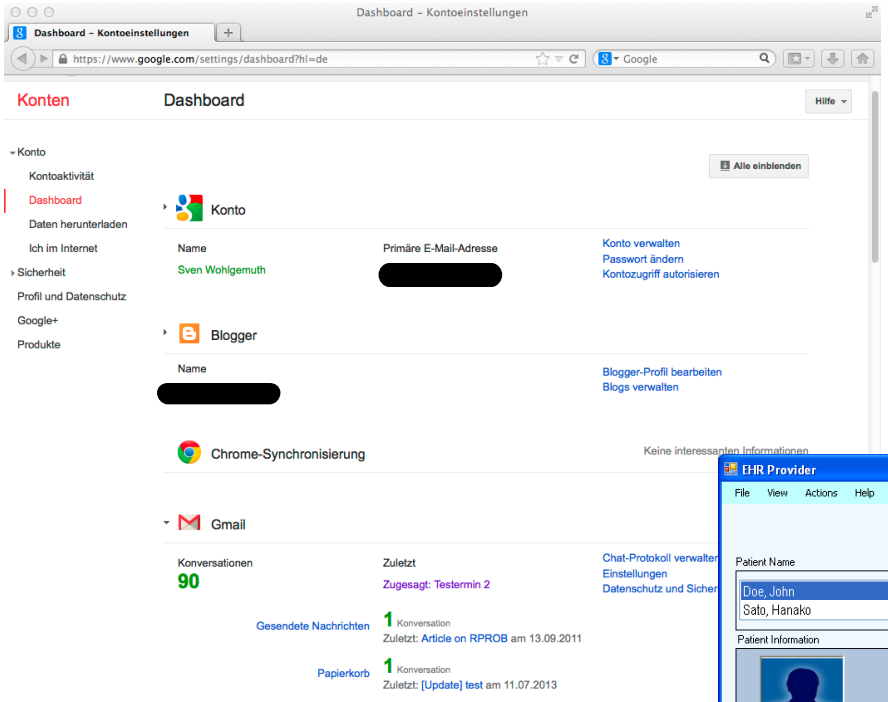
Transparency: Reconstructing usage of pk_{Bob} by data provenance

eID client enforces documenting data provenance audit trail



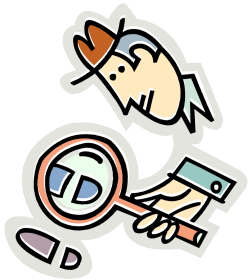
D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G.J. Sussman. Information Accountability, 2008; S. Wohlgemuth, I. Echizen, N. Sonehara und G. Müller. Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy, 2010.

Example



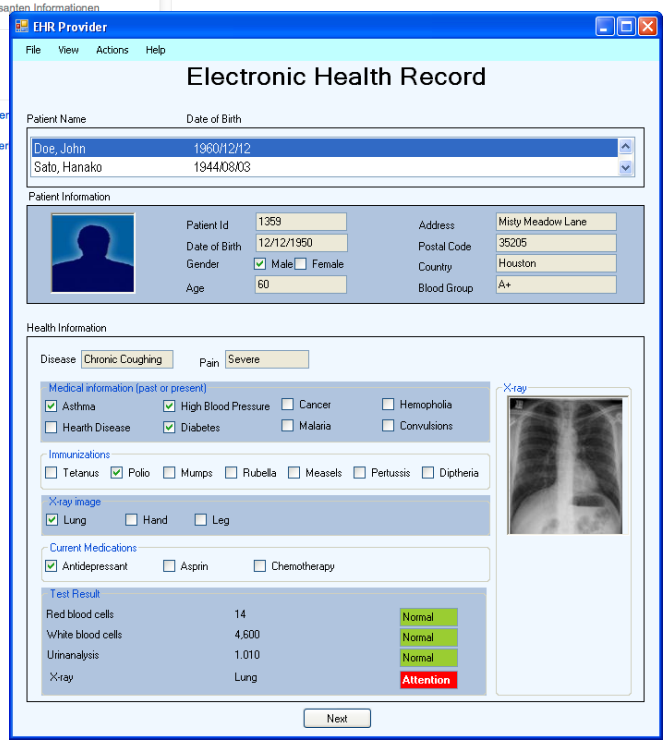
Identity Forensics

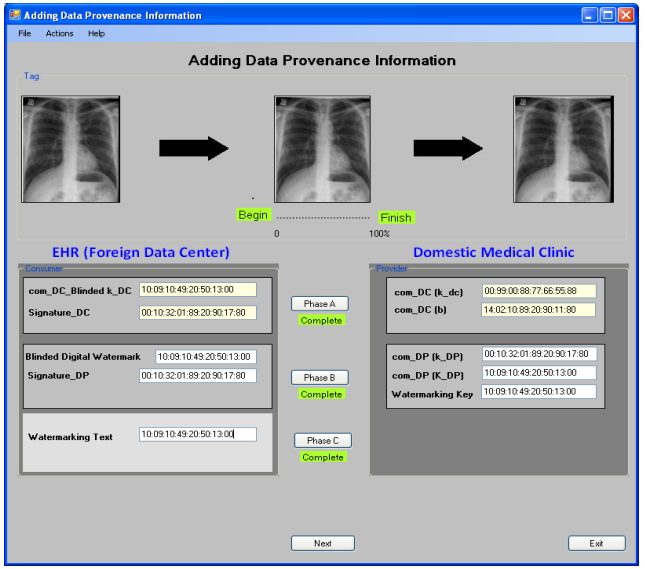
- Overview on data usage with Google ID
- Derived information are not listed
- Accountability and availability **but no** unobservability



Exemplary Privacy Forensics

- Data Provenance for images
- Accountability, availability **and** unobservability





II. PersoApp – Open Source Community

Citizen, Government, Industry, and Academia

Federal Ministry of the Interior (BMI):

- **Introduced** German national ID card with eID 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 Service GmbH:** Open source library for electronic identification
- **Fraunhofer SIT:** Guidelines for security engineering

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

Objectives of PersoApp

1. Establishment of an Open Source Community
   - **Internet Milieus in Germany**
   - **A digitalized Campus**
   - **Spontaneous information exchange**
2. Alternative to official eID client (AusweisApp)

PersoApp Major Release A1

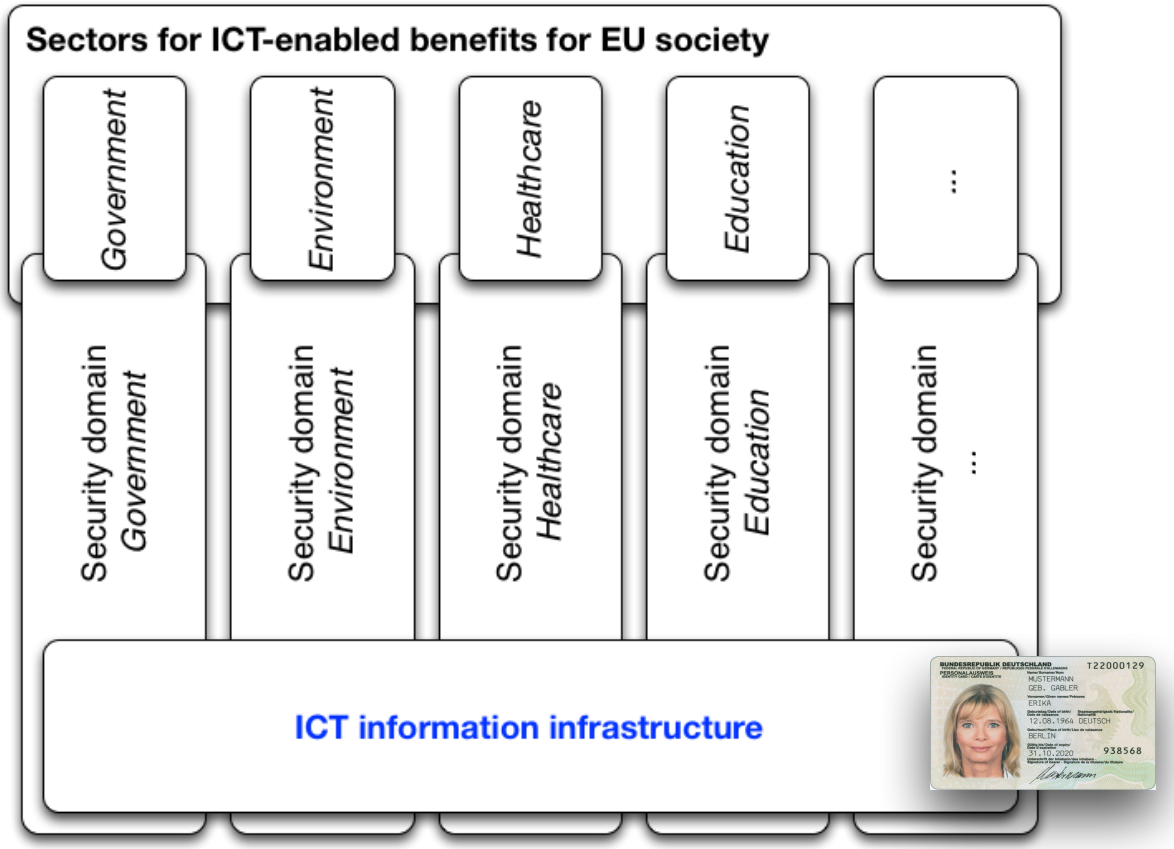
https://persoapp.googlecode.com

3. Experiments for new requirements, services, …
   - **Spontaneous information exchange**
   - **ICT Resilience: Extension of IT Security**
   - **Control and transparency**

Advisory Board

Focus:

- Consulting steering committee in requirements and interests
- 43 stakeholders from national and abroad industries, academia, data protection, and government
- Annual meeting (constitutive meeting on September 2014 at BMI)



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

Advisory Board: A Network of Networks

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

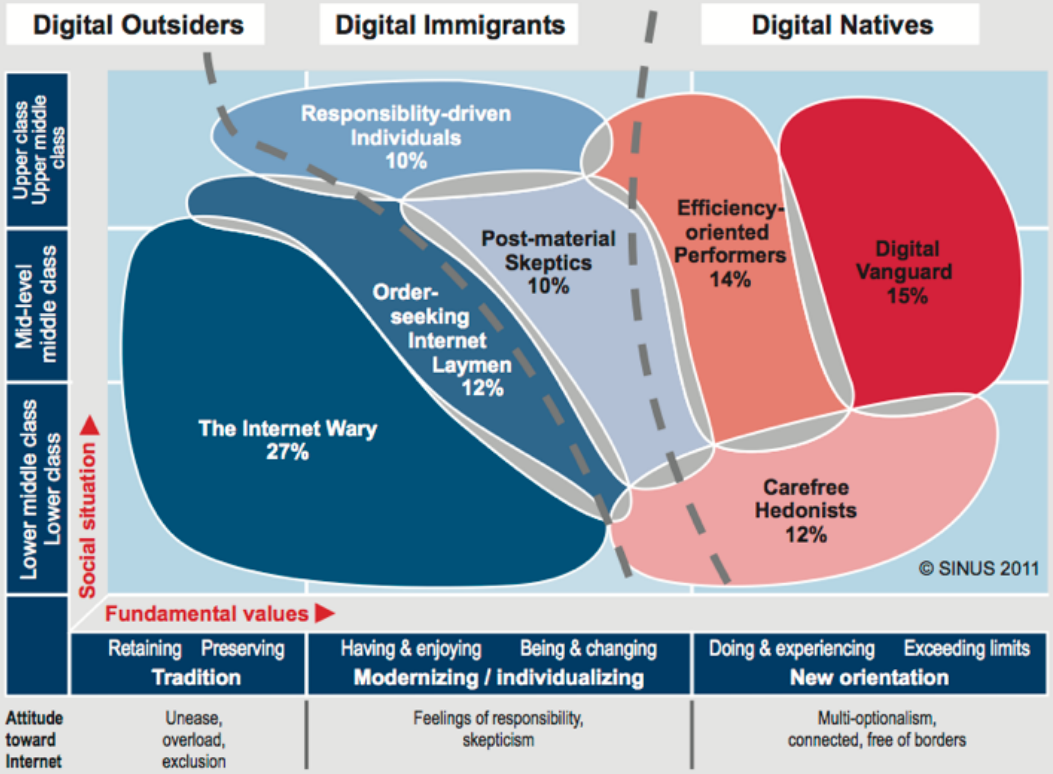
JOHANN WOLFGANG GOETHE UNIVERSITÄT FRANKFURT AM MAIN

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN · FH MÜNCHEN

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

Target Group for Initial Community Building

Internet Milieu in Germany



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

Digital Natives:

- "Always on-line" for personal benefit
- High Internet ability but less risk awareness

Digital Immigrants:

- Internet usage for communication with trusted participants
- Highly aware of security and privacy risks

Digital Outsiders:

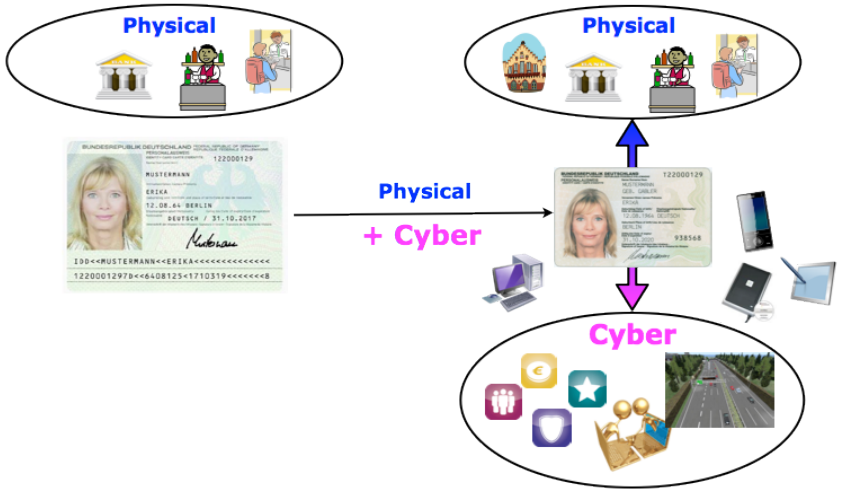
- Personal benefit of Internet usage is not clear
- Strongly uncertain for security and privacy risks

- **Digital Natives** provides orientation as disseminators
- **Digital Natives** have largest part on higher education
- **Initial community building at gymnasium and universities**

Call for Apps

eID client and extensions for

- Identity forensics
- Privacy Control
- Privacy Forensics



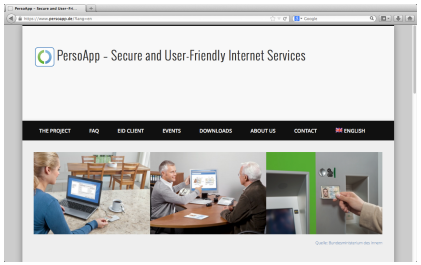
We offer

- User-centric survey
- Design of use cases in particular for mobile applications
- Open source software library for eID functionality (client) of German national ID card
- Extension by “Feature Requests”
- Guidelines for integration of security functionality in own application (Security by Design)
- Publication of results on workshop, talk, education, …

Partner are welcome!

https://www.persoapp.de

ご清聴ありがとうございました。



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

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

E-Mail Listing
- Contact: persoapp@trust.cased.de
- Project leader: persoapp-projects@trust.cased.de
- Software engineer: persoapp-devel@trust.cased.de
- Broadcast: 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
- Announcement of news and collaboration regarding PersoApp