

CC within the Context of the EU Privacy Seal - EuroPriSe

TÜV Informationstechnik GmbH

The Trust Provider

- TÜViT -



Overview



- 1. Motivation**
- 2. Data Privacy**
- 3. European Privacy Seal – EuroPriSe**
- 4. CC and EuroPriSe**
- 5. Conclusion**

"Some" misuse of data ...



"56.000 data sets got stolen from PricewaterhouseCoopers and used illegally"

(Source: <http://www.heise.de/www.heise.de/newsticker/Gestohlene-PwC-Datensaetze-fuer-Missbrauch-von-Click-Buy-benutzt-Update--/meldung/>)



"SKI (Süddeutsche Klassenlotterie) lost about 17.000 data sets of customers"

(Source: http://www.computerzeitung.de/articles/datenskandal_sicherheitsexperten_fordern_meldepflicht_bei_dat_enverlusten/)

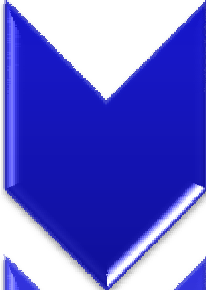


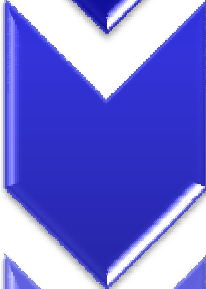
"More than 17 Mio data sets got stolen from Deutsche Telekom in 2008 and the years before"

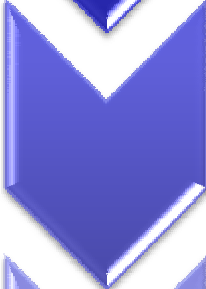
(Source: <http://www.compliancemagazin.de/markt/kommentare/>)

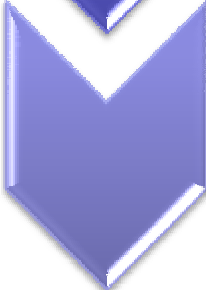
... and its general implication



- 
- Vital increase in legislation and *consumer* awareness of identity theft, electronic surveillance, data accumulation etc. demands protection of PII (Personally Identifiable Information)
 - *Consumers*: represented by citizens, business and/or public authorities

- 
- Wherever PII is collected, stored or shared about users of IT products or IT based services, privacy issues may exist

- 
- Therefore trustworthy IT products or IT based services are required by consumers

- 
- Consequently, privacy compliance becomes a major challenge of modern IT management

Overview



1. Motivation
2. **Data Privacy**
3. European Privacy Seal – EuroPriSe
4. CC and EuroPriSe
5. Conclusion

Terms and definitions



Personally Identifiable Information (PII)

- Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Personal Data (Art. 2 a Directive 95/46/EC)

- "shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

Data Privacy

- All measures which defend the individual from incorrect (illegal, unauthorized) usage of personal data / PII

Data Security

- Status in which the integrity, availability and privacy of data, programs, methods and assets is ensured

Data Protection

- All methods which help to reach the aims of data security

Scope and principles



Scope

- Data Privacy refers to
 - collection of personal data / PII
 - processing of personal data / PII
 - use of personal data / PII

Core Principles

- Personal data / PII should not be collected or processed at all, unless certain rules are adhered to:
 - Legitimacy
 - Limited use

Overview



1. Motivation
2. Data Privacy
3. **European Privacy Seal – EuroPriSe**
4. CC and EuroPriSe
5. Conclusion

Project



More information: <https://www.european-privacy-seal.eu/>

Project funding: 1,3 Mio € by EU

Duration: 06/2007 through 11/2008

Objective: Market validation for a **European Privacy Seal**

Consortium: 9 partner from 8 EU-countries



Agencia de Protección de Datos
de la Comunidad de Madrid



CNIL



ITA INSTITUT FÜR
TECHNIKFOLGEN-
ABSCHÄTZUNG



ERNST & YOUNG

BORKING CONSULTANCY

Scope



The European Privacy Seal certifies that an IT product or IT based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the pilot countries:



Austria



Spain



Germany



Sweden

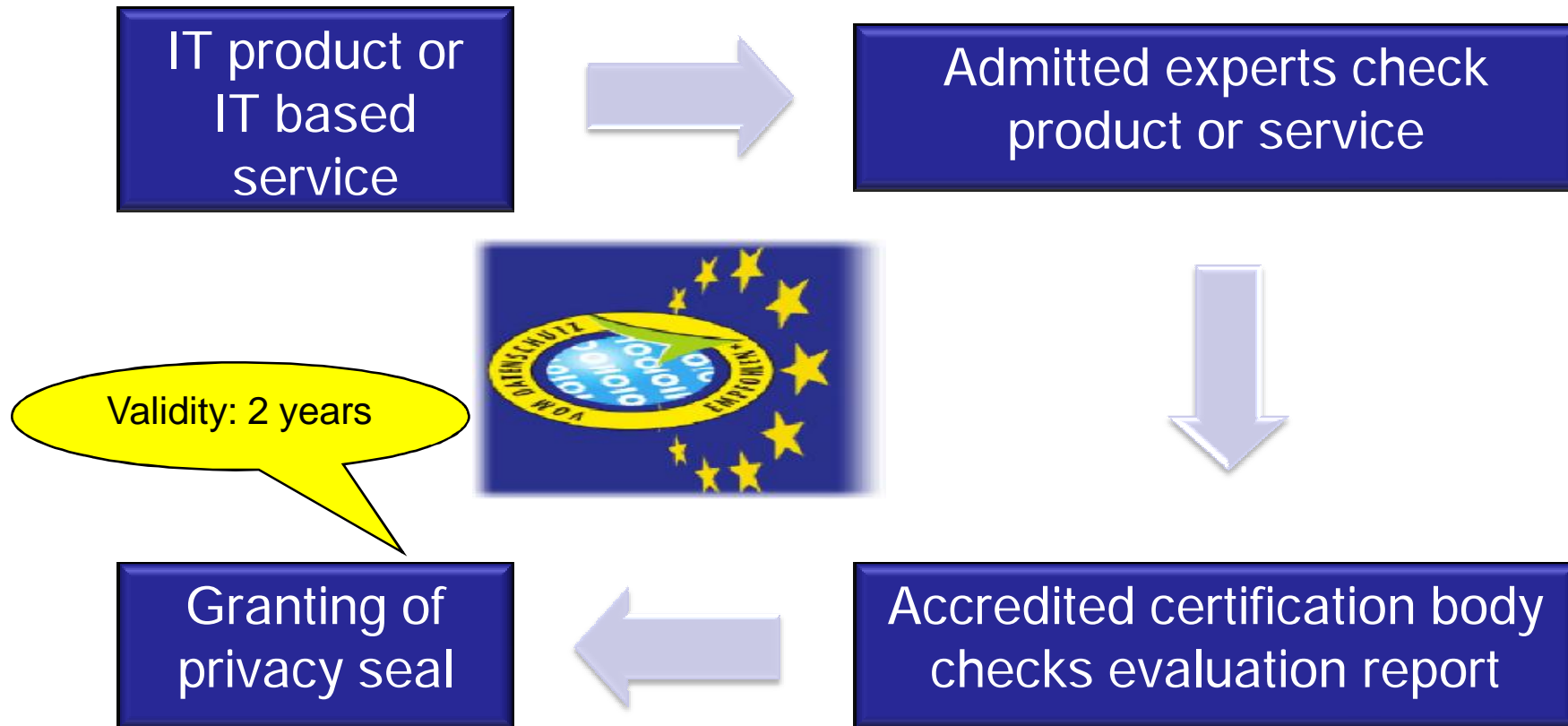


Slovak Republic



UK

Procedure



Experts & certification authorities



Expert admittance

- Proof of qualification: legal and/or technical
- Proof of reliability and independence
- Training evaluation and workshop participation

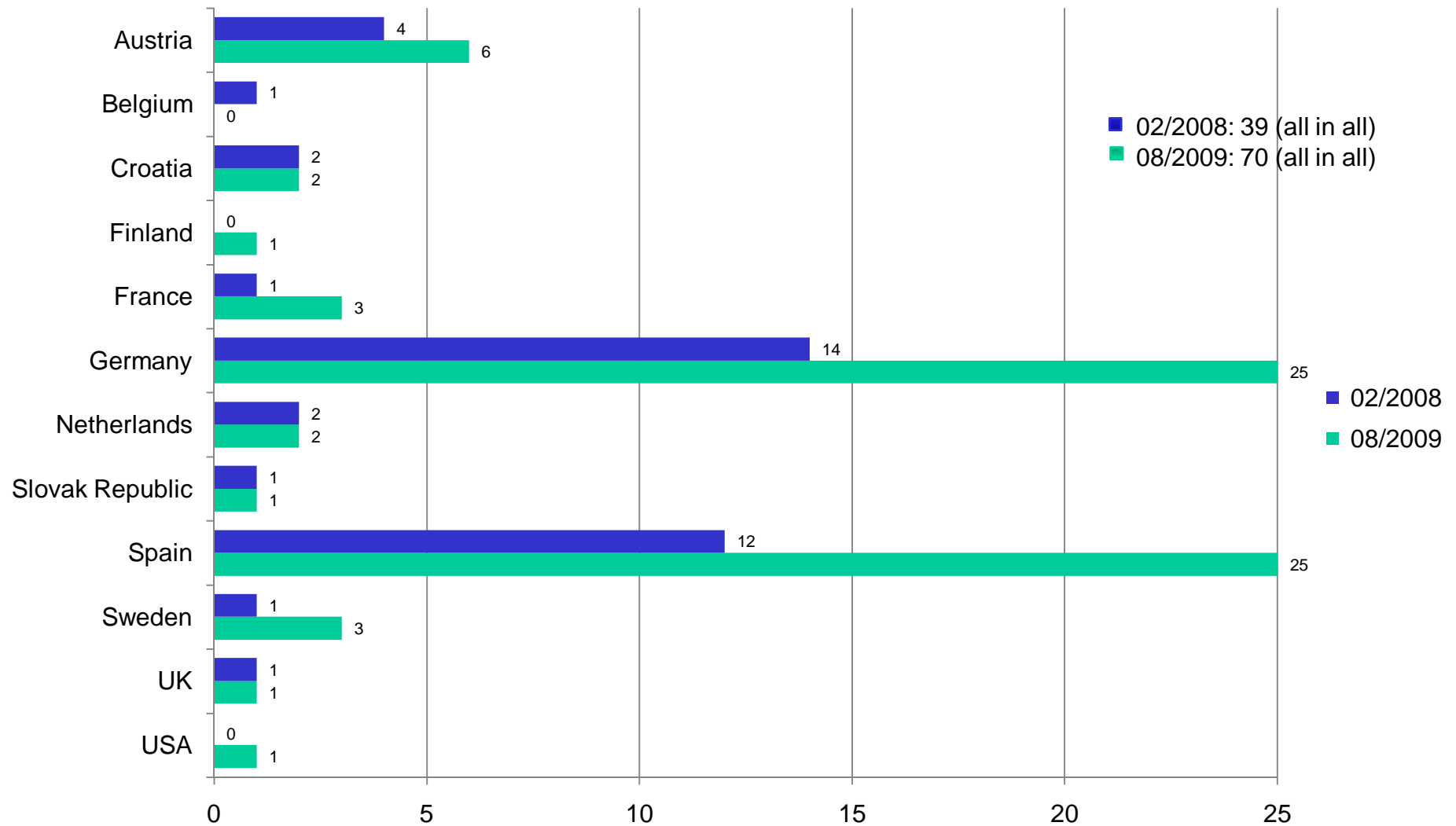
Publication of expert admittance and area of qualification

- <https://www.european-privacy-seal.eu/experts/register-experts>

EuroPriSe Board

- Accreditation of certification authorities
- Criteria maintenance
- Consistent evaluation and certification procedures

Admitted Experts

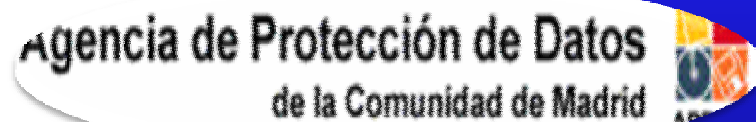


Certification authorities



ULD/ICPP Independent Centre for
Privacy Protection Schleswig-
Holstein

<http://www.datenschutzzentrum.de/>



Agencia de Protección de Datos de
la Comunidad de Madrid

<http://www.apdcm.es>

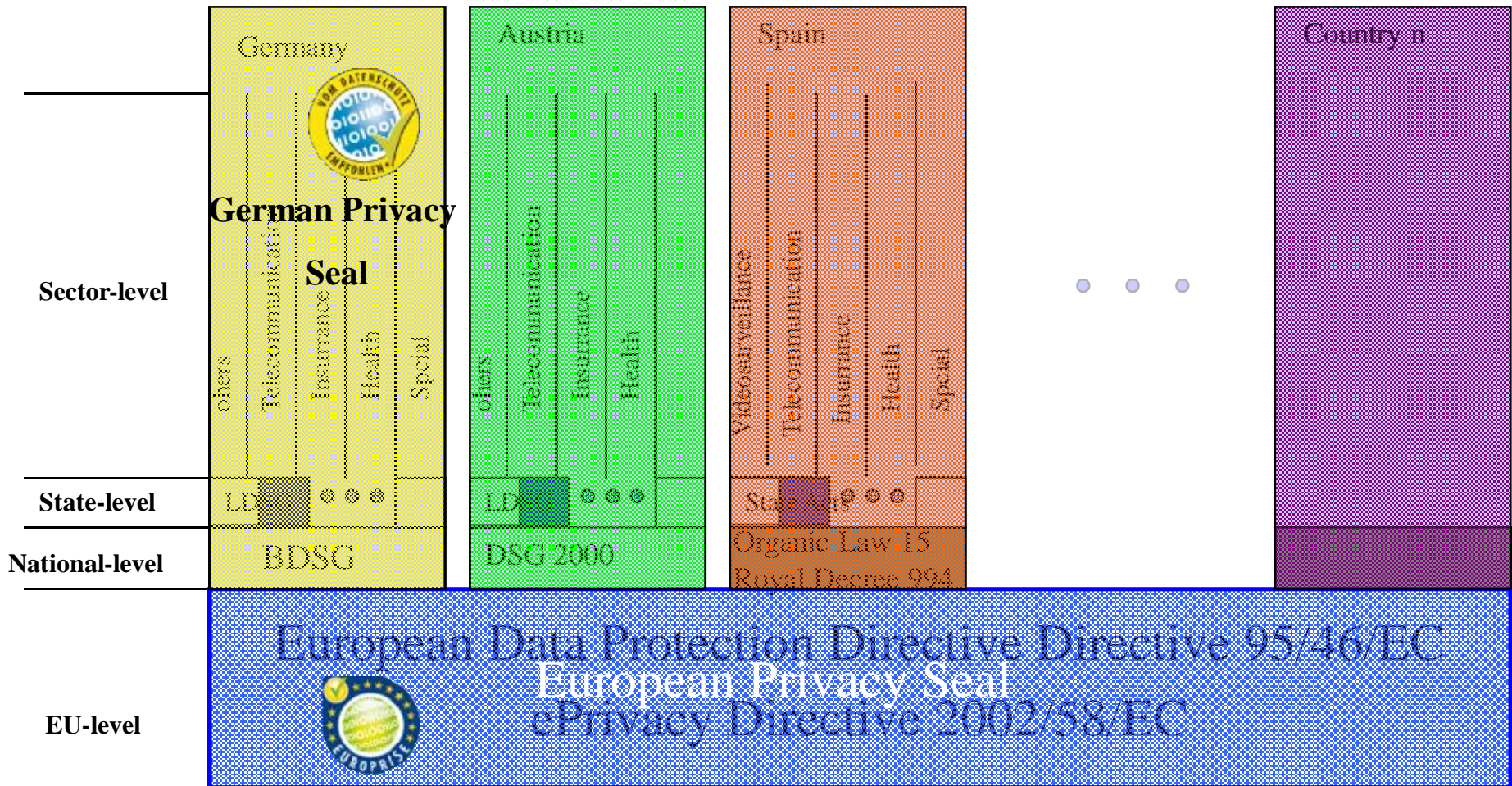
Objective

- Is the product suitable for use in a privacy compliant way, including setting, configuration, and documentation?

Criteria Sets

- **Set 1: Fundamentals issues**
e.g. purpose, avoidance, transparency of data
- **Set 2: Legitimacy of Data Processing**
e.g. legal basis or compliance w/ general data protection principles
- **Set 3: Technical/Organisational Measures**
e.g. passwords, firewalls, encryption, logs
- **Set 4: Data Subjects' Rights**
e.g. right to be informed, right of access, right of correction or erasure

Outlook: Model for national extension of EuroPriSe



Overview



1. Motivation
2. Data Privacy
3. European Privacy Seal – EuroPriSe
4. **CC and EuroPriSe**
5. Conclusion

IT security and data privacy



IT Security and Privacy are closely related

Without proper security and security policies, the privacy cannot be enforced

Technology facilitates the protection of private information

People are managing the technologies and risks

Privacy within CC



Some SFRs address privacy aspects

- e.g. audit, access control, trusted path, non-repudiation
- depending on the focus of the product, its security features might be opposed to data privacy requirements

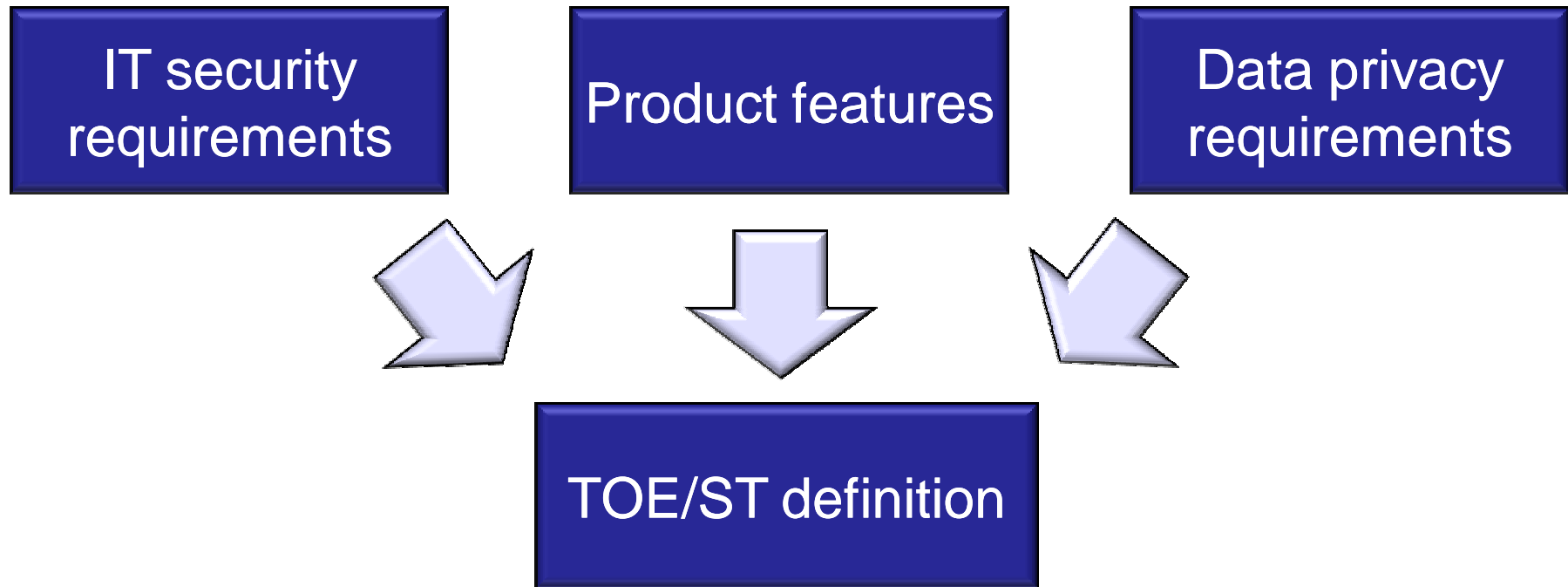
Dedicated Privacy Class FPR: Privacy

- FPR_ANO: Anonymity
- FPR_PSE: Pseudonymity
- FPR_UNL: Unlinkability
- FPR_UNO: Unobservability

German "Privacy" Protection Profiles

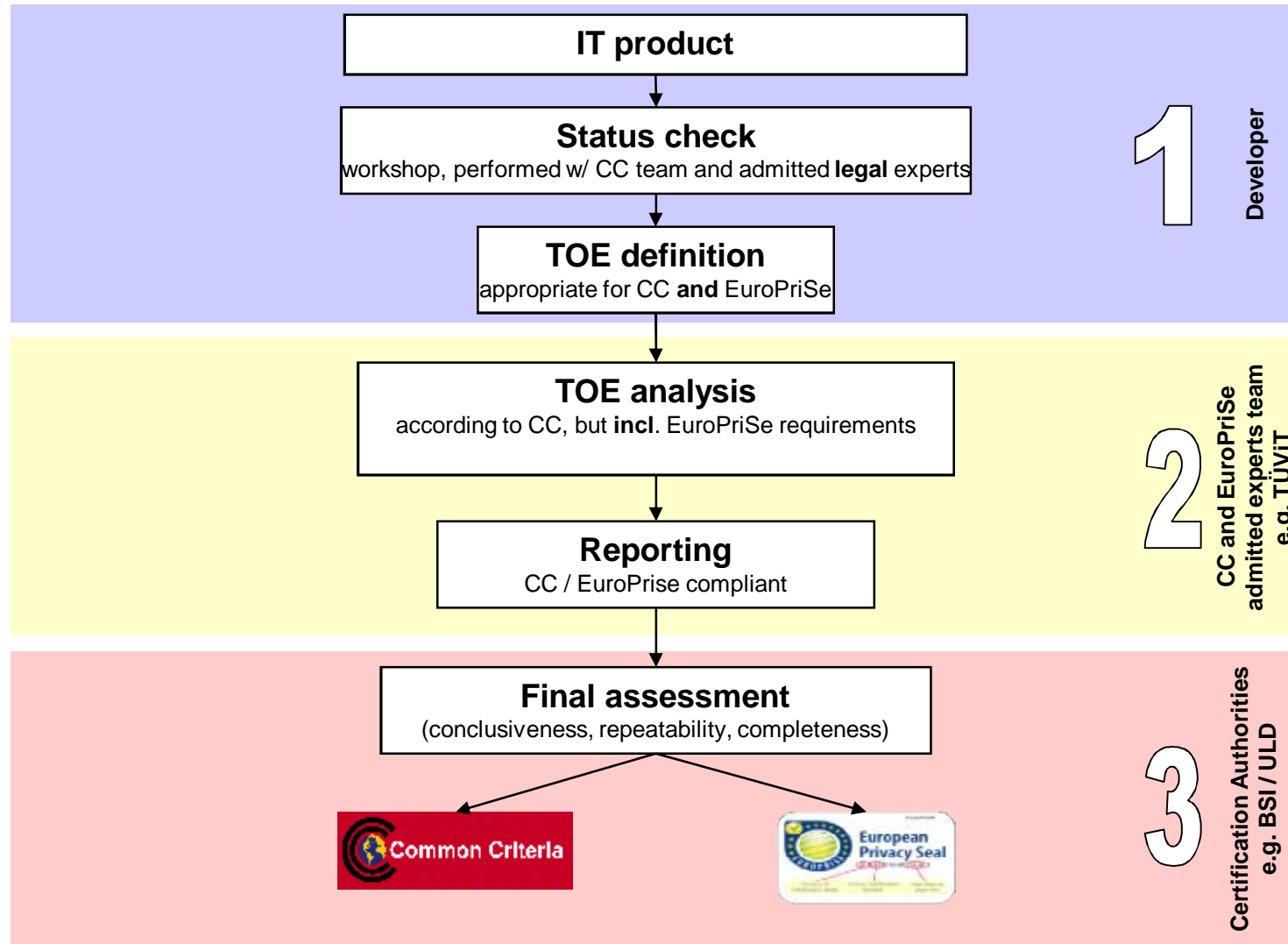
- BSI-PP-007 Discretionary Information Flow Control (SU)
- BSI-PP-008 Discretionary Information Flow Control (MU)
- BSI-PP-0023 Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0

"Combining" approach



You can't decide on one without knowing the others!

"Combining" procedure



"Mapping" the requirements (example)



EuroPriSe Criteria Catalogue

- ⊘ 3.1.5.2:
Does the product documentation provide information on risks, vulnerabilities, etc?
- ⊘ 3.1.5.3:
Does the product documentation (directed to customers, users and administrators) provide an overview of implemented security and data protection measures?

Does the company-internal product documentation (e.g., high-level-designs, specifications, etc.) contain information of implemented security and data protection measures?
- ⊘ 3.1.8 Does the documentation provide sufficient information on how to install the product properly (i.e., installation in such a way that the product's data protection mechanisms are properly configured and used)?

CC assurance class/family

- ⊘ AVA_VAN
- ⊘ AGD_OPE
incl. data protection measures
- ⊘ ASE, ADV, ALC_DVS
incl. data protection measures
- ⊘ AGD_PRE
incl. data protection measures

Overview




1. Motivation
2. Data Privacy
3. European Privacy Seal – EuroPriSe
4. CC and EuroPriSe
5. **Conclusion**

Conclusion



- 
- Vendors considering both, CC and EuroPriSe, could significantly benefit from the overlap between EuroPriSe and CC

- 
- Technical EuroPriSe requirements for an IT product can be fulfilled targeting a CC EAL2+/EAL3 evaluation

- 
- CC process needs to incl. EuroPriSe requirements on all "layers"
 - TOE and ST definition
 - Document analysis
 - Testing
 - Audit

Gracias

谢谢您 

Thank you! Grazie

Danke

Merci

谢谢您

Takk

Obrigado

Bedankt

TÜV INFORMATIONSTECHNIK GMBH

Member of TÜV NORD Group



Wolfgang Peter
Director Evaluation Body for IT Security

Langemarckstr. 20
D-45141 Essen

Phone: +49 201 8999 – 624
Fax: +49 201 8999 – 666
E-Mail: w.peter@tuvit.de
URL: www.tuvit.net