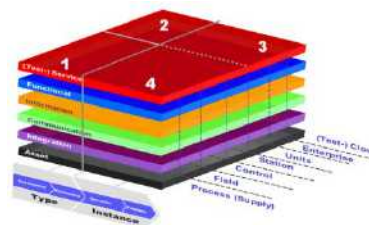




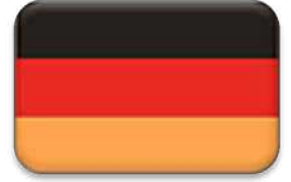
EU - IoT Industry and Environment

Security Requirements and Regulations

Markus Bartsch



China – EU – Germany



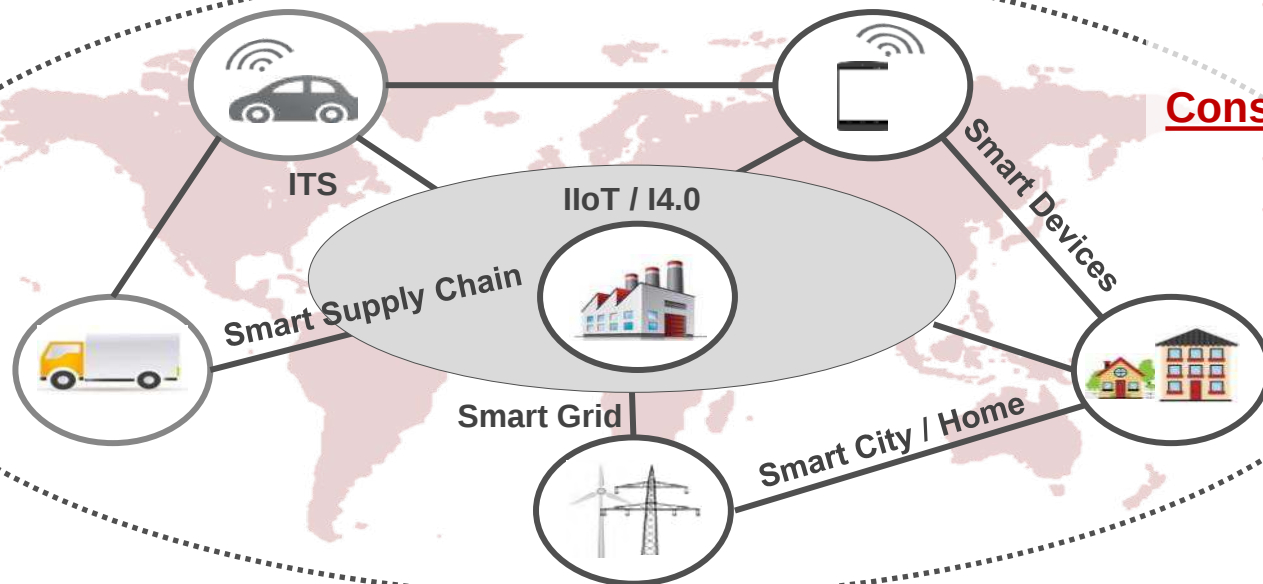
- **NIS Directive**
- **GDPR** – General Data Protection Regulation
- **CSA – Cybersecurity Act**



Smart Service World



Internet of Things



Critical Infrastructures

- NIS Directive

Consumer

- GDPR
- Cybersecurity Act

TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

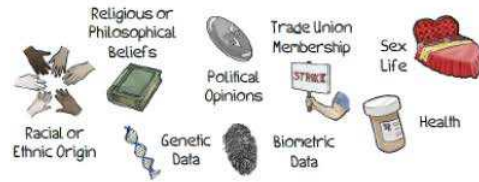
THE PLAYERS



PERSONAL DATA



SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security



Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.



Record of Data Processing Activities

Maintain a documented register of all activities involving processing of EU personal data.

Data Protection by Design

built in starting at the beginning of the design process

Data Impact Assessment

For high risk situations



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for:

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT



Consent must be freely given, specific, informed, and unambiguous.



DATA BREACH NOTIFICATION



A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



"Right not to be subject to a decision based solely on automated processing, including profiling."



Access and Rectification

Right to Erasure



Purpose Specification and Minimization



Right to Data Portability



ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.



Effective Judicial Remedies:

compensation for material and non-material harm.



INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection



Privacy Shield

Binding Corporate Rules (BCRs)



Model Contractual Clauses

GDPR - Overview



TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA



SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security



Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

Record of Data Processing Activities

Maintain a structured register of all activities involving processing of EU personal data.

Data Protection by Design

built in starting at the beginning of the design process



Data Impact Assessment

For high risk situations

LAWFUL PROCESSING

Collection and processing of personal data must be for "specific, explicit and legitimate purposes" – with consent of data subject or necessary for:

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT



Consent must be freely given, specific, informed and unambiguous

GDPR

DATA BREACH NOTIFICATION



A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects
Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency



Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."



Access and Rectification

Right to Erasure

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies

compensation for material and non-material harm



Binding Corporate Rules (BCRs)

INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection



Privacy Shield



Model Contractual Clauses

IoT → Smart Services

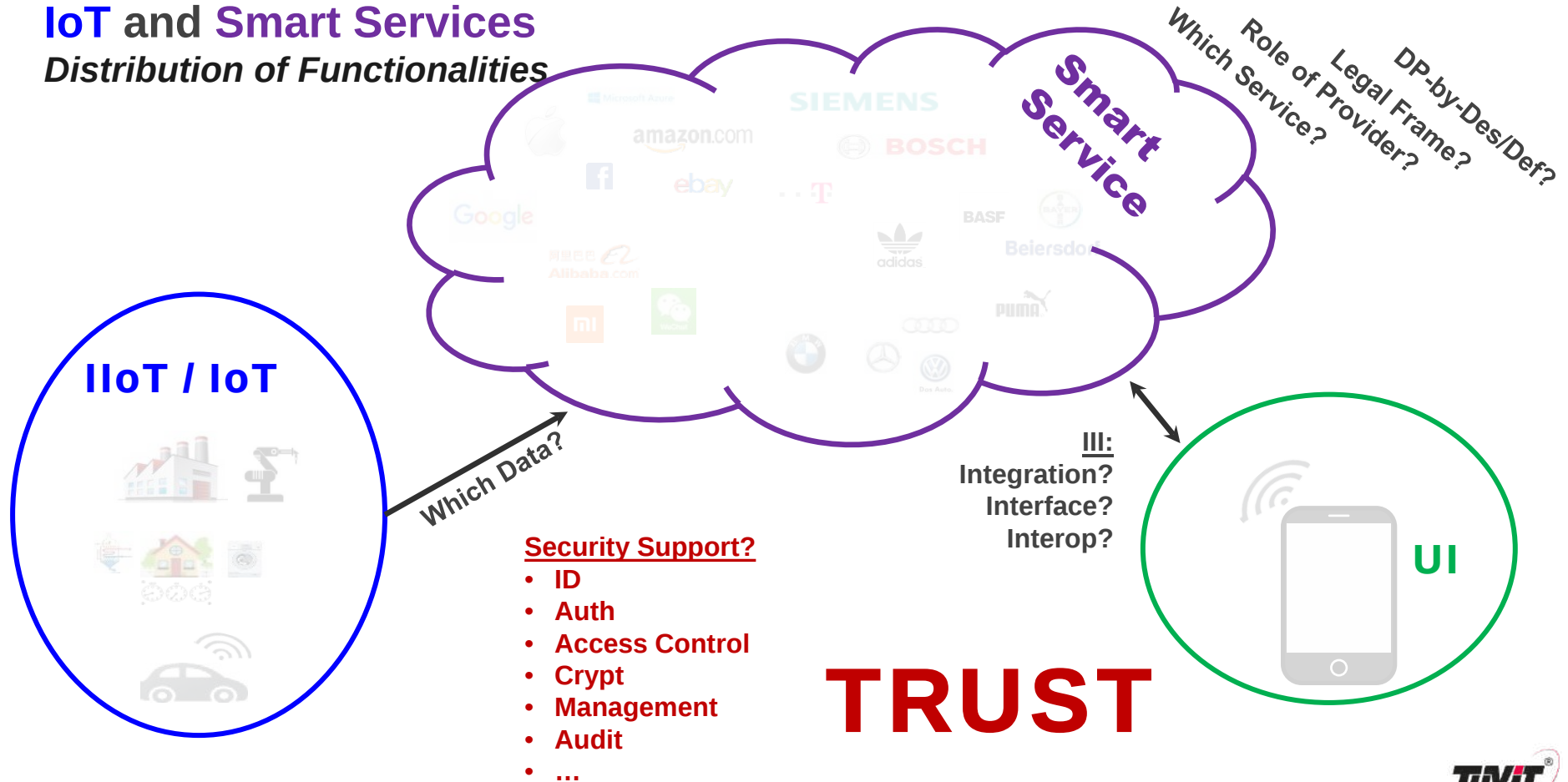


IIoT / IoT



IoT and Smart Services

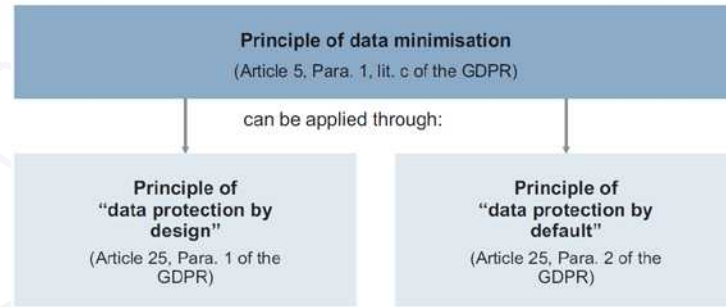
Distribution of Functionalities



Trust

- Data Protection by-Design
- Data Protection by-Default

1. Data Protection **by Design** and Data Protection **by Default** are two requirements for implementing data protection principles (e.g., data minimization) for both technical (e.g., software) and organizational aspects.



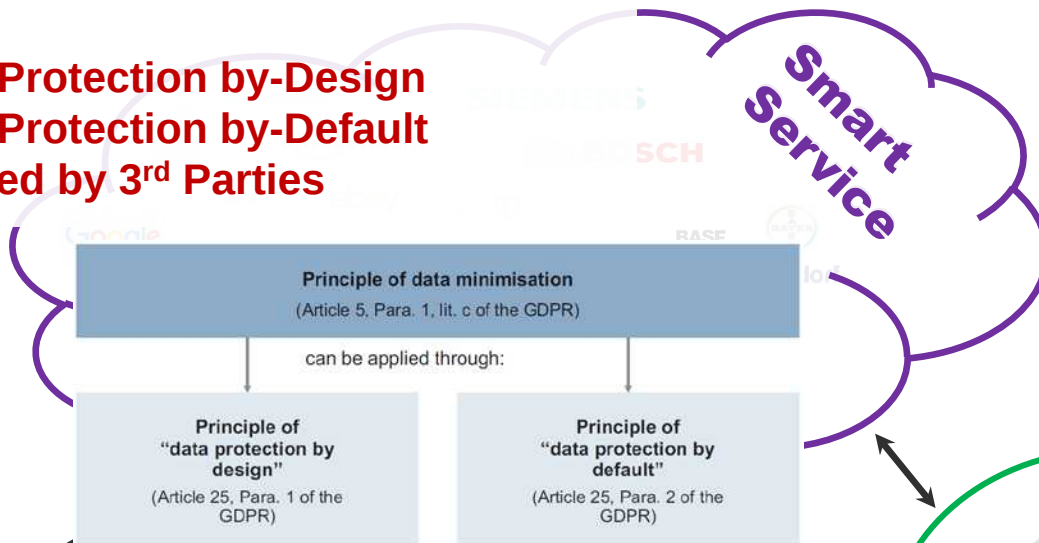
1. Data Protection **by Design** means identifying privacy risks during the development of new technologies and to consider and incorporate privacy from the outset in the overall design.
2. Data Protection **by Default** means that products or services are configured to be privacy-friendly by default
3. For the purposes of accountability considerations and decisions must be documented

DP-by-Des/Def?
Legal Frame?

Trust

GDPR

- Data Protection by-Design
 - Data Protection by-Default
- confirmed by 3rd Parties



DP-by-Des/Def?
Legal Frame?

IoT



UI



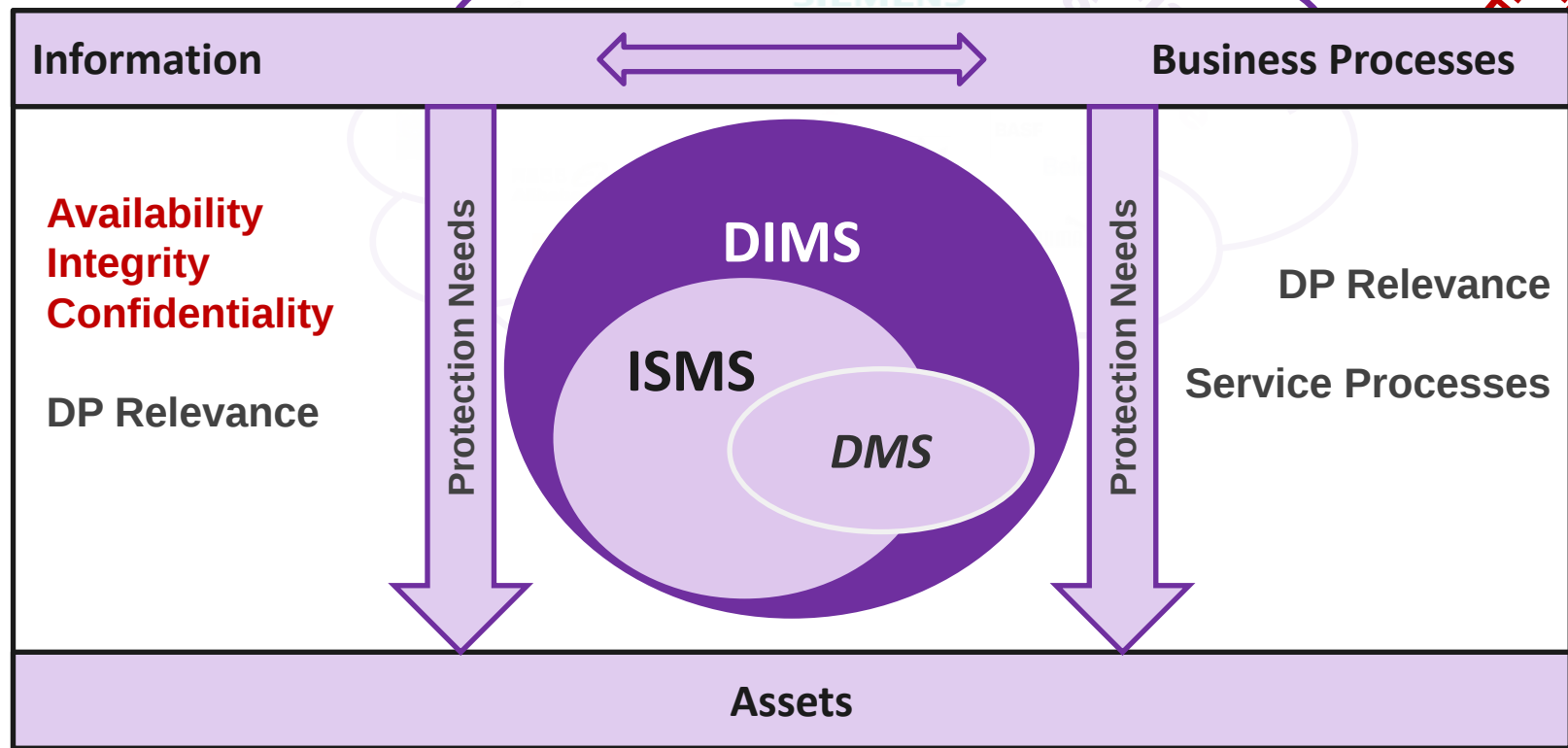
by-Design:

When Data leaves the Device (to the Smart Service)
Data Protection Regulations are fulfilled automatically

by-Default:

The "by-Design" configuration is the initial configuration

Trust → **DIMS** (confirmed by 3rd Parties)



Trust → DIMS (confirmed by 3rd Parties)



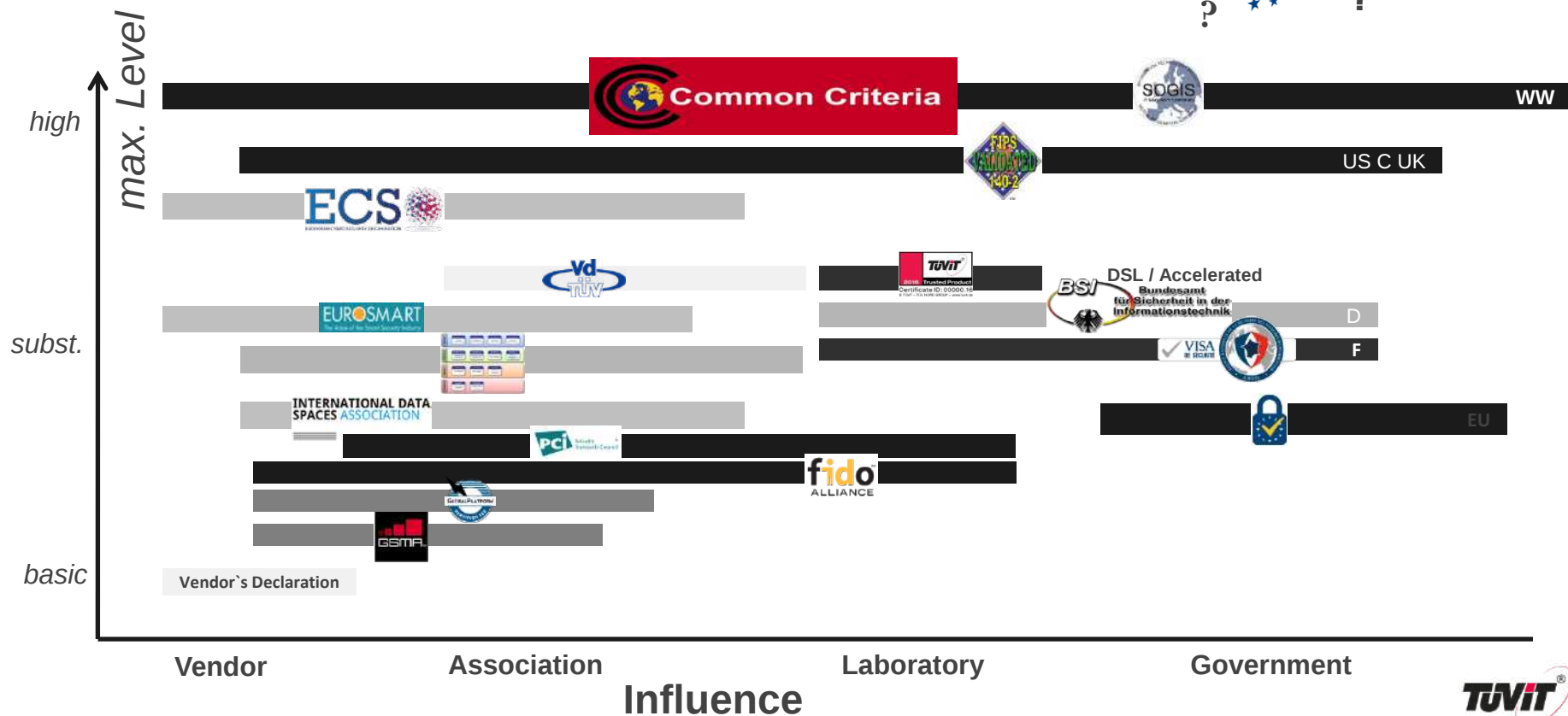
IoT and Smart Services

Device Security – not only GDPR relevant



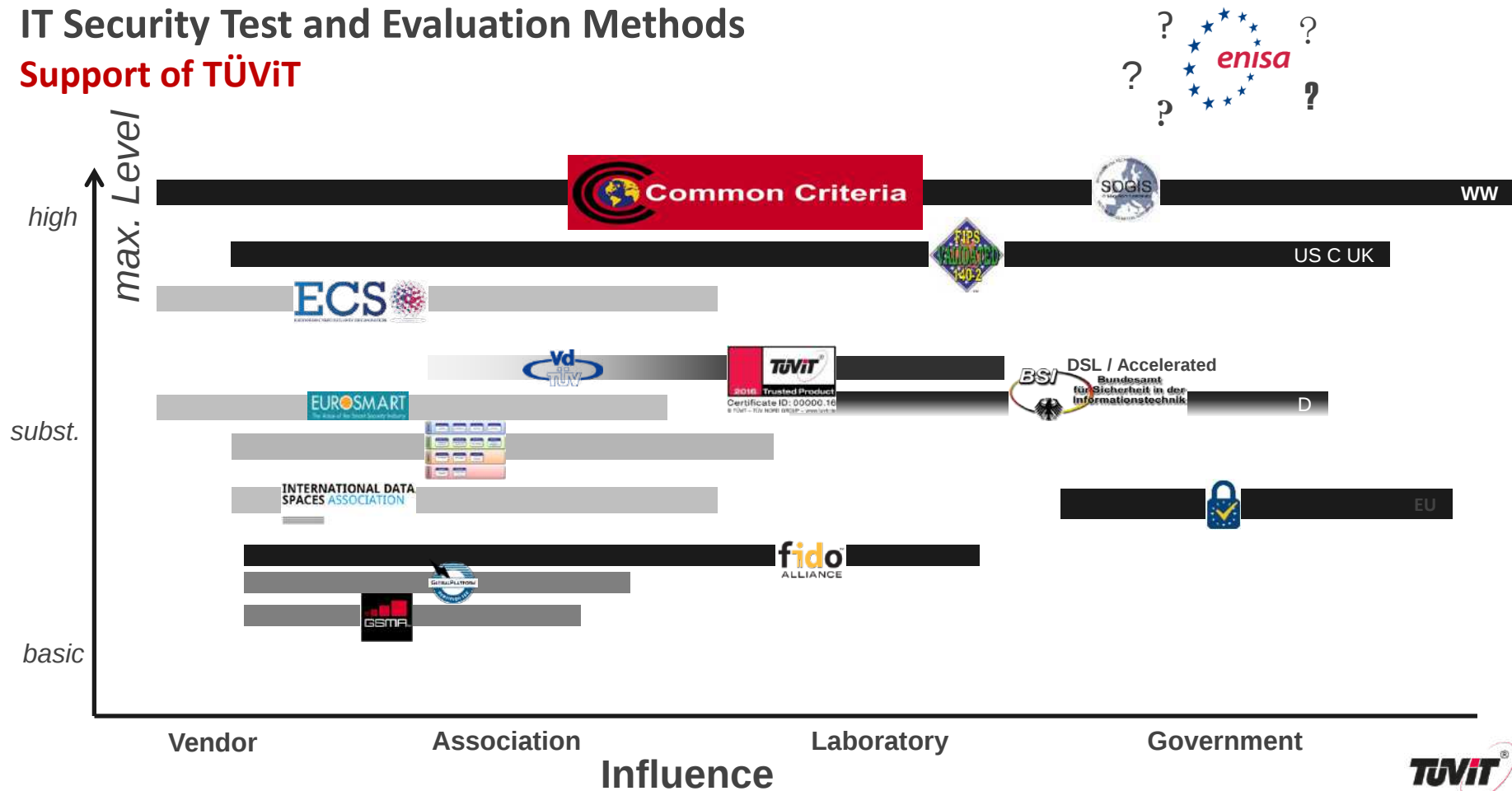
EU: IT Security Test and Evaluation Methods

"Approval Landscape" acc. to IT Components (Examples)



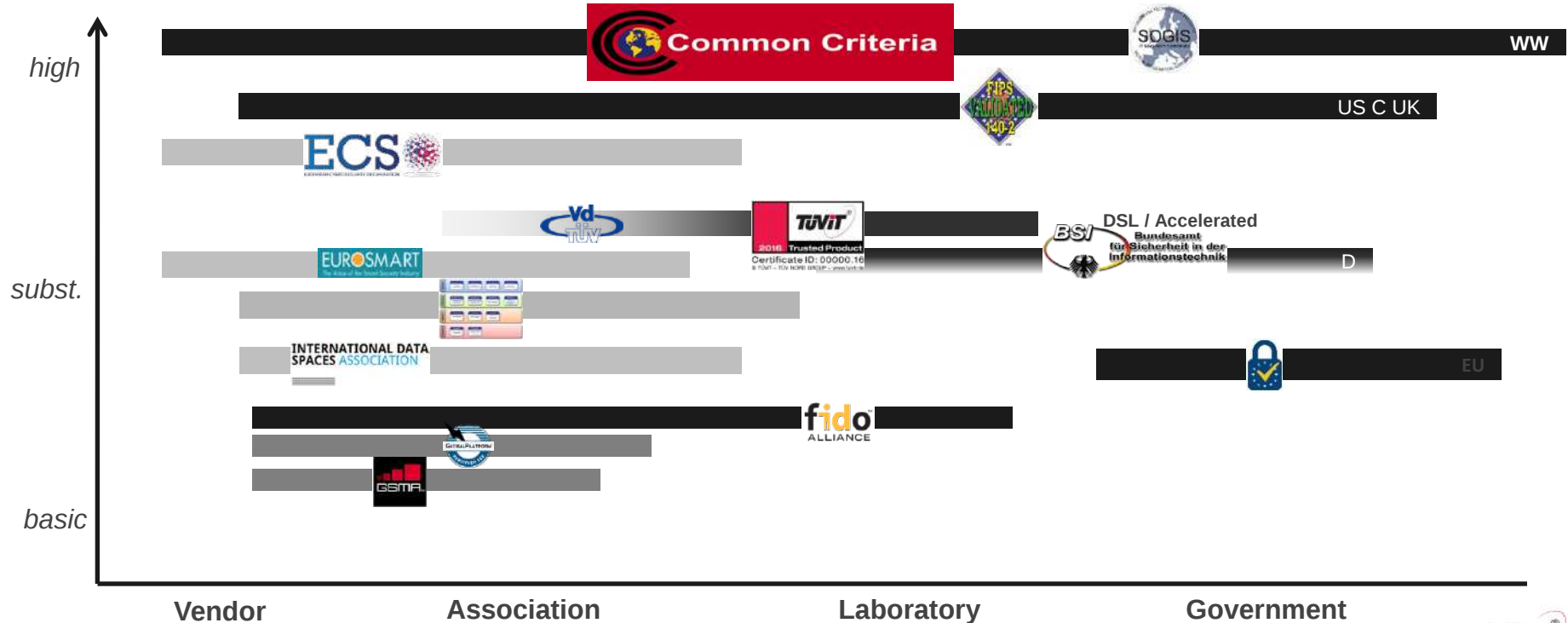
IT Security Test and Evaluation Methods

Support of TÜViT



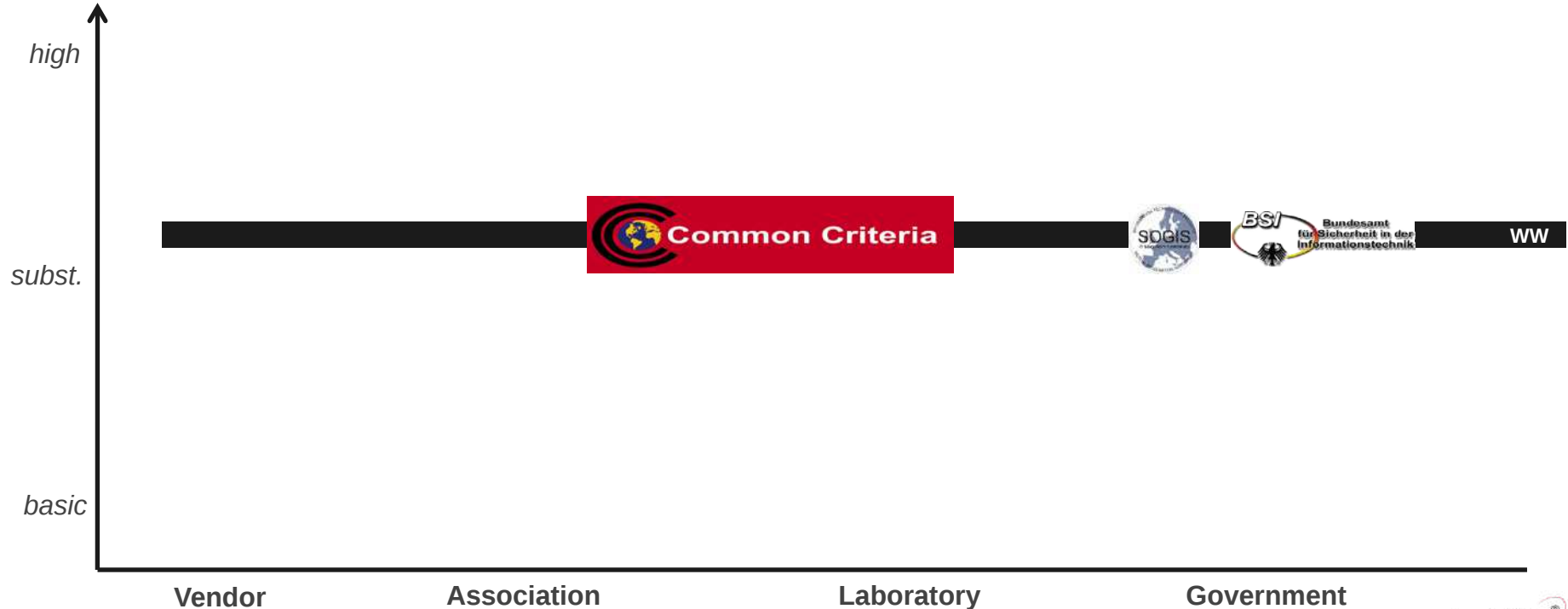
IT Security Test and Evaluation Methods

Most promising Approach (TÜViT)



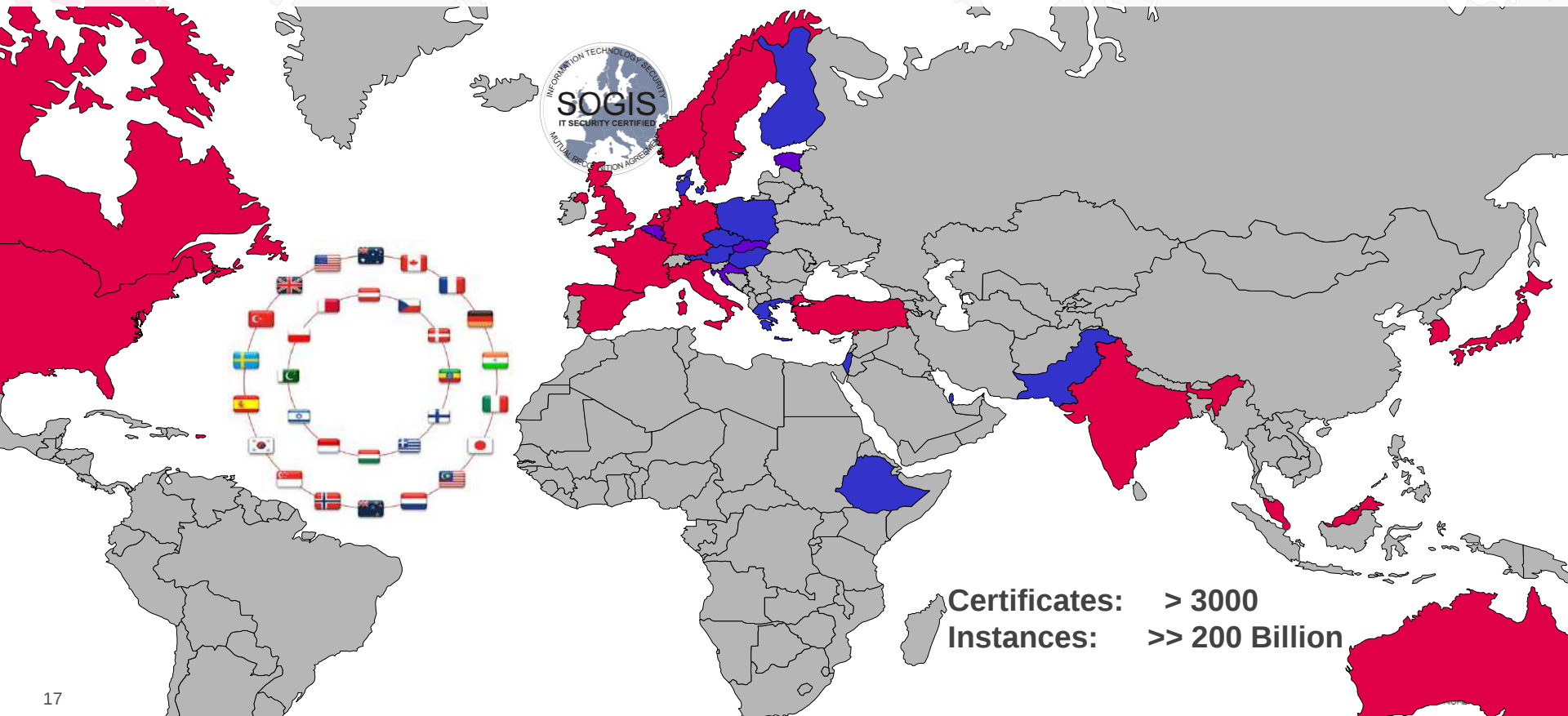
IT Security Test and Evaluation Methods

Most promising Approach (TÜViT)



Common Criteria – CCRA (~EAL2) / SOGIS

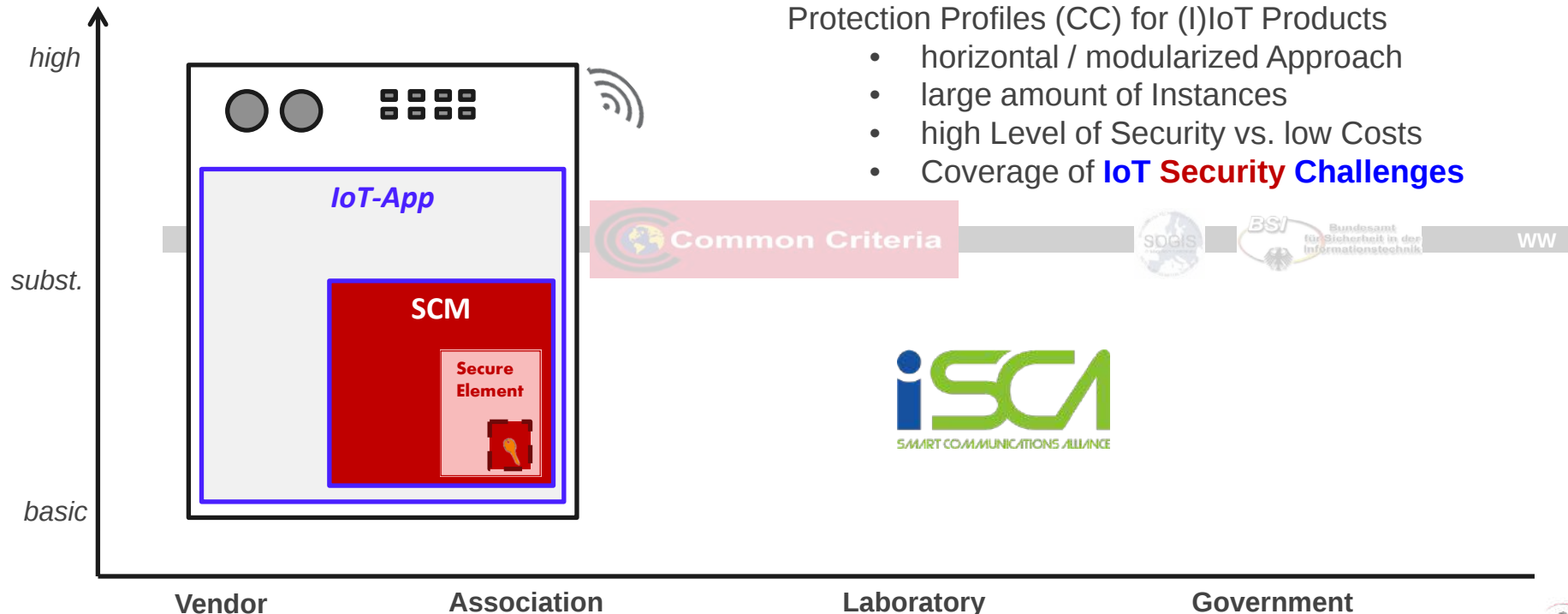
Certificate Issuing and Consuming Nations - Certificate Consuming Nations



Secure IoT PP's

Protection Profiles (CC) for (I)IoT Products

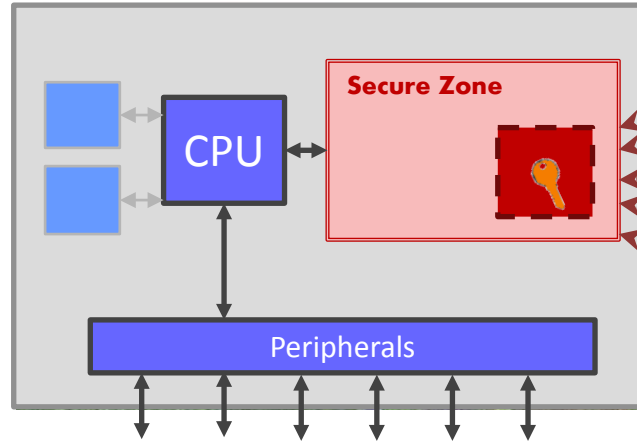
- horizontal / modularized Approach
- large amount of Instances
- high Level of Security vs. low Costs
- Coverage of **IoT Security Challenges**



Secure Elements

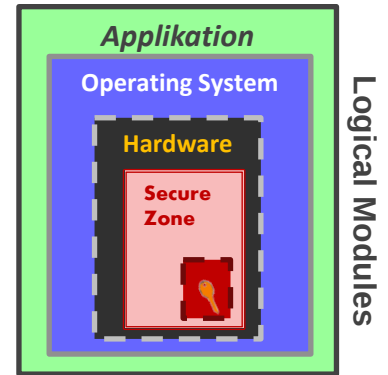


Embedded



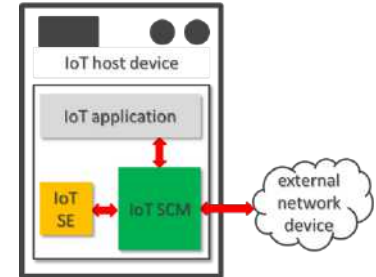
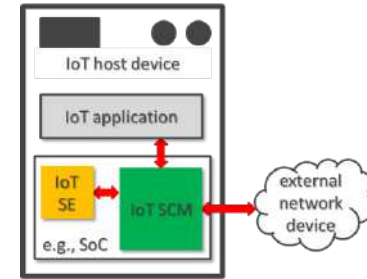
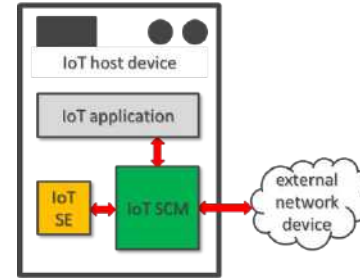
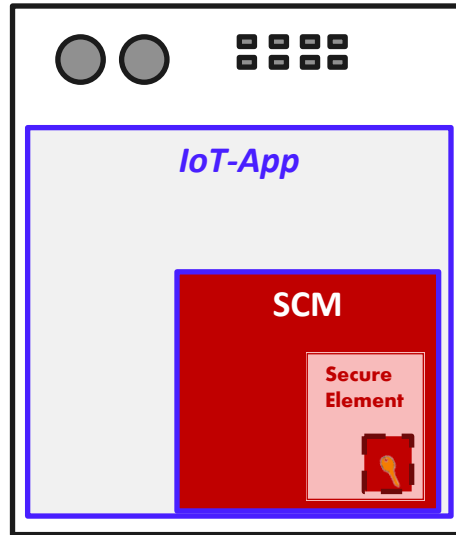
Attacks

- Electrical Stimulation
- Energy & Particle Exposure
- Inspection & Reverse Engineering
- Physical manipulation
- Electro-Magnetic Interaction / Radiation
- Electrical Measurement
- Communication



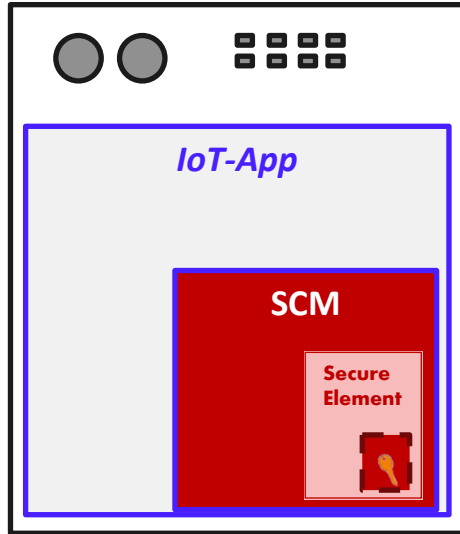
Secure IoT PP's Form Factors

IoT

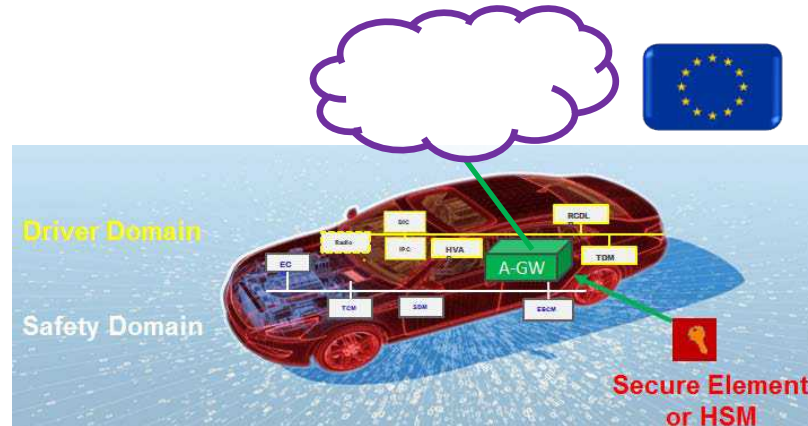
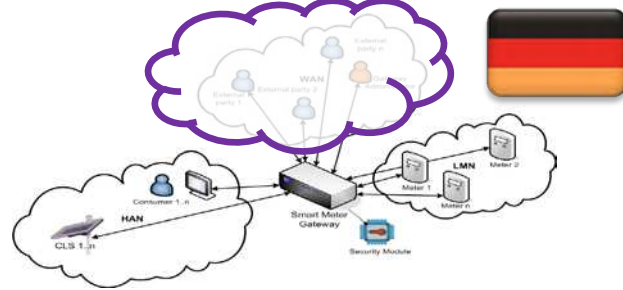


<https://youtu.be/hbYUhMabPFo>

Secure IoT PP's other Examples



German Smart Meter Gateway



EU: C-ITS

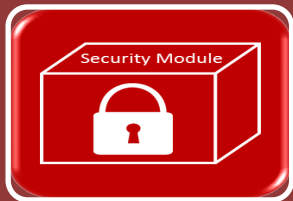
Co-operative Intelligent Transport Systems

Secure IoT - The System Approach



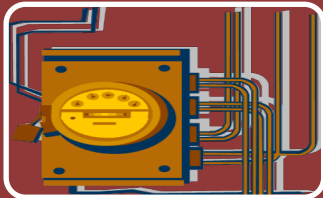
IoT SCM – Secure Communication Module

- Central communication component of the IoT / SmartHome Device
- Trusted channel/path



IoT SE – Security Element

- Implementation of cryptographic primitives
- Secure Handling of key material



IoT Cloud

- Different System Architectures → different Use Cases
- Comprising a System Architecture for many IoT SCM's

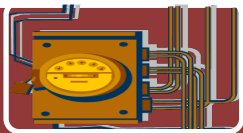
Secure IoT - The main functionality of the IoT SCM (Secure Communication Module)

EAL2+ (ALC_FLR.1)



Firewalling

- The SCM has control over all information flows
- Resistance against logical/network-based attacks



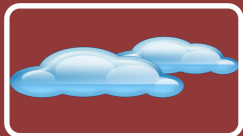
Trusted Paths

- based on cryptographic support of SE



Limitation of Information Leakage

- to protect User and IoT Cloud Provider



Update Control

- Secure Firmware updates by IoT Cloud Provider

Secure IoT - The functionality of the IoT SE (Security Element)

EAL4+ (AVA.VAN.4)



Cryptography

- Trusted Path Support
- to be used by the SCM



Storage of Key Material

- Key Access Policy
- Secure environment for storage/usage of identity-giving keys
- Resistance against Local Attacks



Random Number Generation

- For internal use
- For various purposes to be used by the SCM

Secure IoT – Next Steps

IoT



- **Evaluation & Certification**

at the German BSI



- Basis for Scheme acc. to **SOG-IS (ENISA)**



- Introduction to **European Associations**

- **Initial Evaluations**

- Basis for German IT Security Directive 2.0
*Critical Infrastructures: **IIoT Components***

- Link to **New Legislative Framework (NLF)**

New Legislative Framework (EC 765/2008)

1. Toy Safety
2. Transportable pressure equipment
3. Restriction of Hazardous Substances in Electrical and Electronic Equipment
4. Construction products
5. Pyrotechnic Articles
6. Recreational craft and personal watercraft
7. Civil Explosives
8. Simple Pressure Vessels
9. Electromagnetic Compatibility
10. Non-automatic Weighing Instruments
11. Measuring Instruments



EUROPEAN
COMMISSION

12. Lifts
13. ATEX
14. Radio Equipment
15. Low Voltage
16. Pressure Equipment
17. Marine Equipment
18. Cableway Installations
19. Personal Protective Equipment
20. Gas Appliances
21. Medical Devices
22. In Vitro Diagnostic (IVD) devices

New Legislative Framework (EC 765/2008)

IoT: Security

1. Toy Safety



2. Transportable pressure equipment



3. Restriction of Hazardous Substances in Electrical and Electronic Equipment

4. Construction products

5. Pyrotechnic Articles

6. Recreational craft and personal watercraft

7. Civil Explosives

8. Simple Pressure Vessels

9. Electromagnetic Compatibility

10. Non-automatic Weighing Instruments

11. Measuring Instruments



12. Lifts

13. ATEX

14. Radio Equipment

15. Low Voltage

16. Pressure Equipment

17. Marine Equipment

18. Cableway Installations

19. Personal Protective Equipment

20. Gas Appliances

21. Medical Devices

22. In Vitro Diagnostic (IVD) devices



IoT-App

SCM

Secure Element



IoT and Smart Services Summary



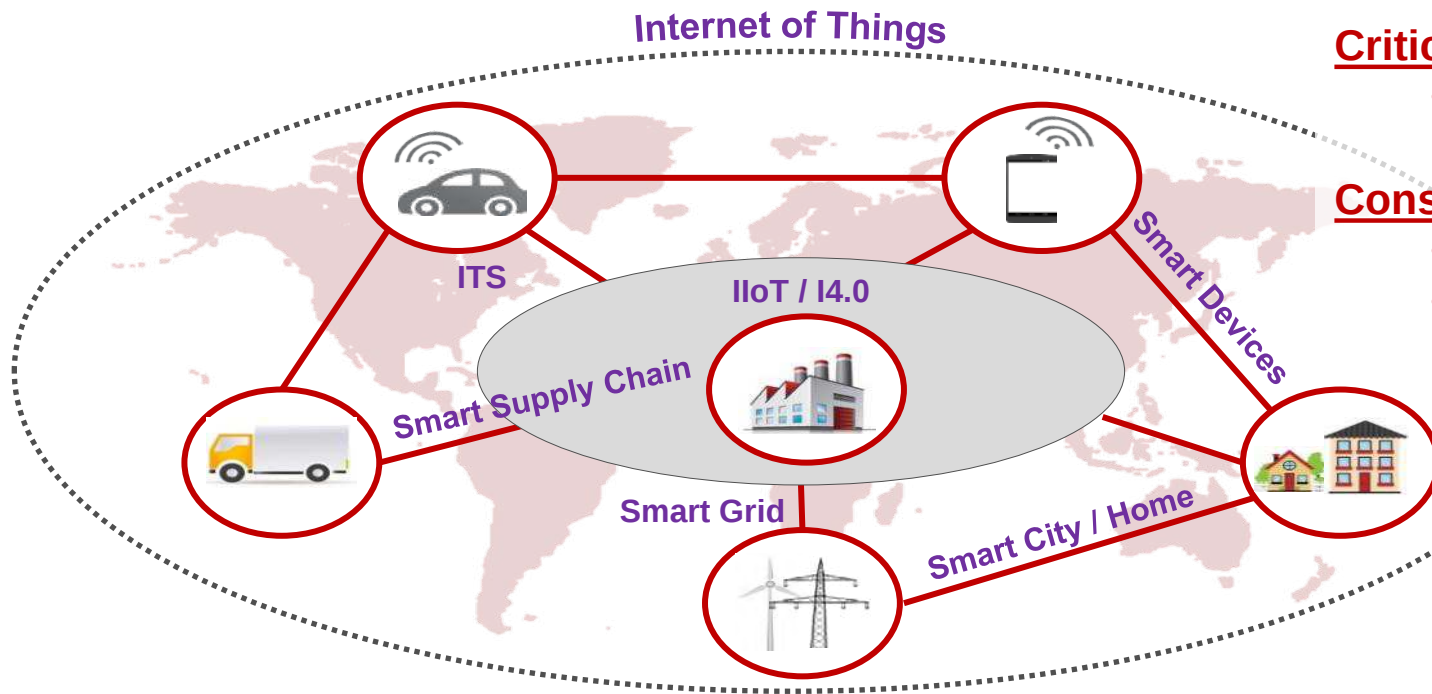
IoT

CSA: Secure IoT PPs

Basis for DP-by-Design → **GDPR**



Secured Smart Service World



Critical Infrastructures

- NIS Directive

Consumer

- GDPR
- Cybersecurity Act

Thank you very much for your attention!

TÜV Informationstechnik GmbH
Member of TÜV NORD Group

Markus Bartsch
IT Security

Langemarckstrasse 20
45141 Essen, Germany

Phone: +49 201 8999 – 616
Fax: +49 201 8999 – 666
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de

