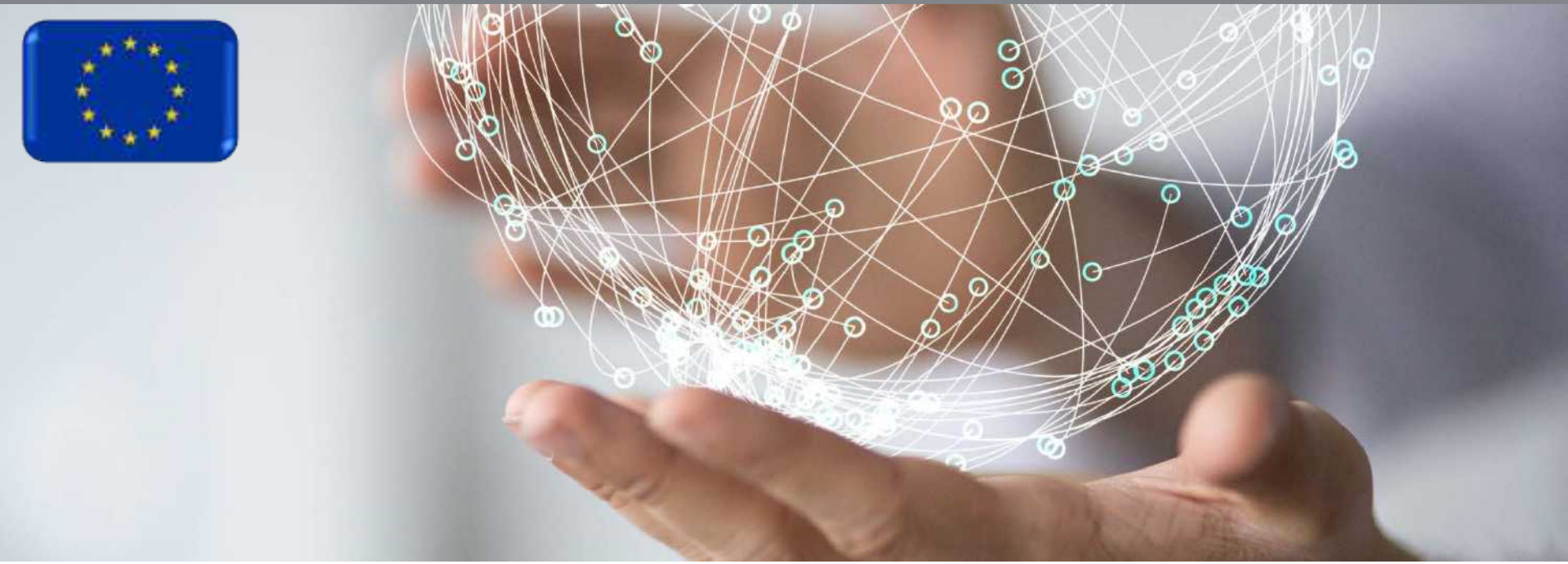
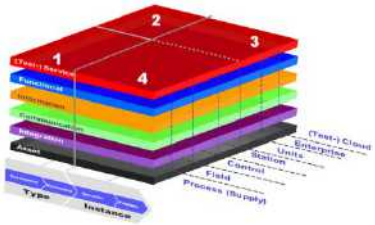


EU - IoT Industry and Environment

Security Requirements and Regulations

Markus Bartsch



TÜV NORD GROUP

China – EU – Germany

- **NIS Directive**
- **GDPR – General Data Protection Regulation**

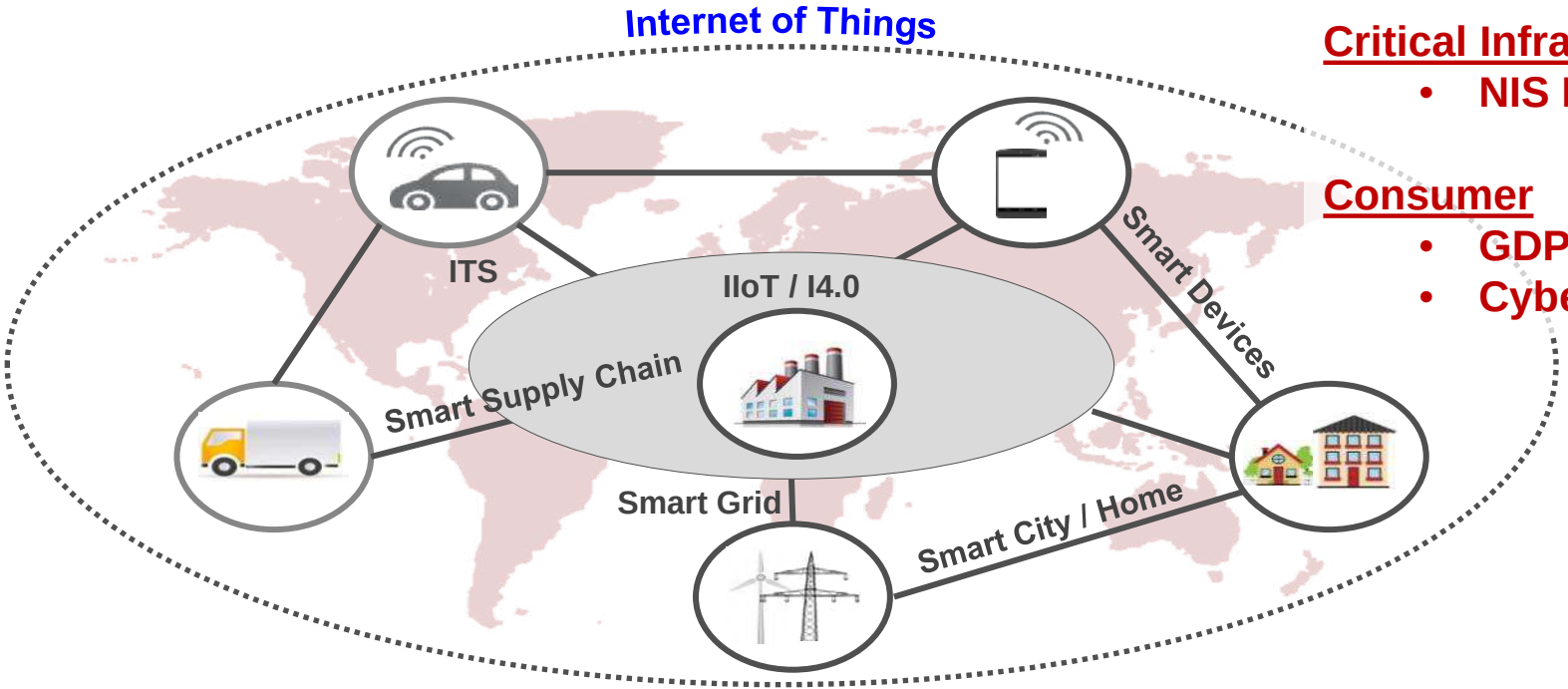
- **CSA – Cybersecurity Act**

enisa

TÜVIT
TÜV NORD GROUP

Smart Service World

EUROPEAN COMMISSION



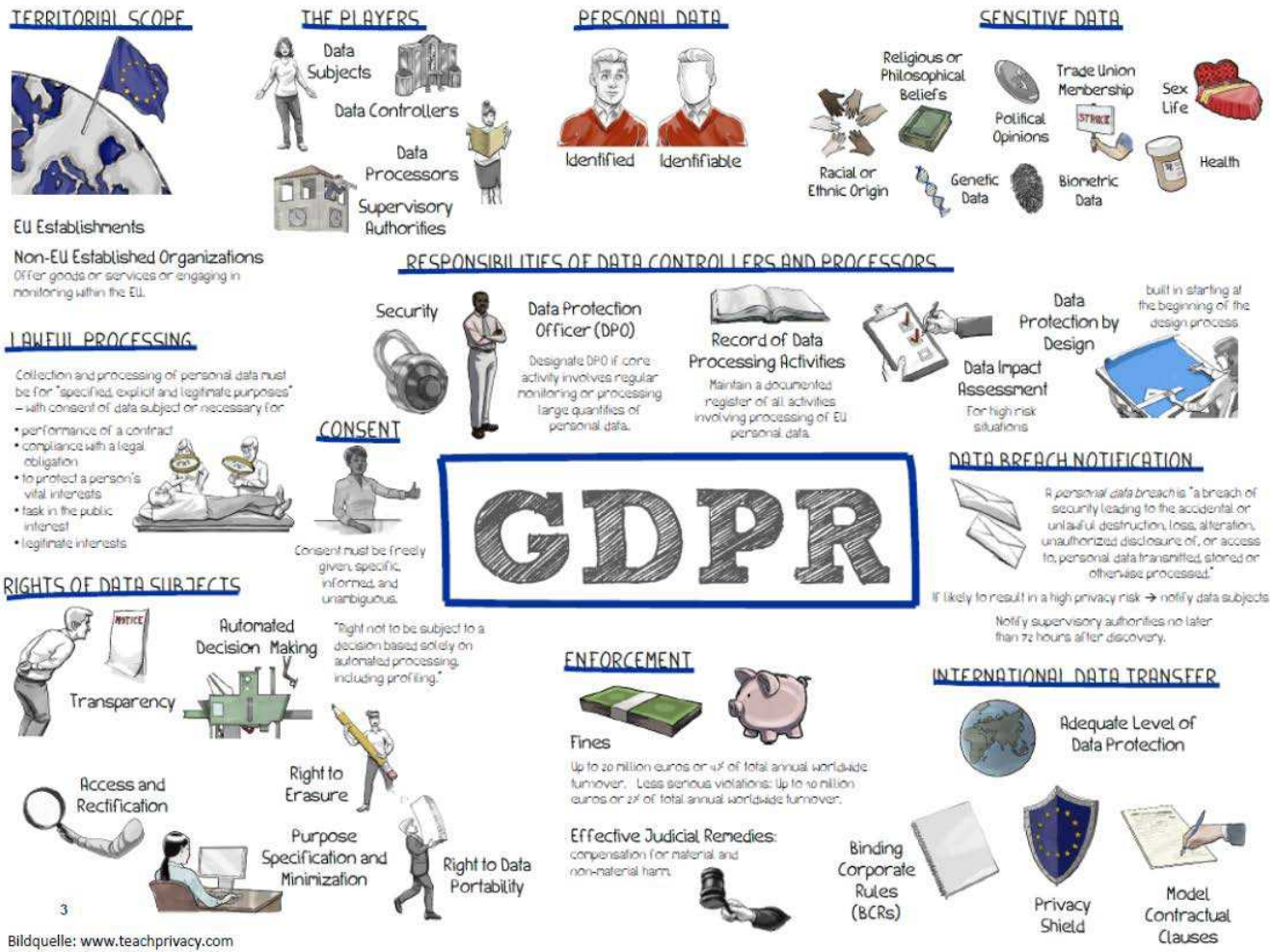
Critical Infrastructures

- NIS Directive

Consumer

- GDPR
- Cybersecurity Act

TÜVIT TÜV NORD GROUP



Bildquelle: www.teachprivacy.com

GDPR - Overview

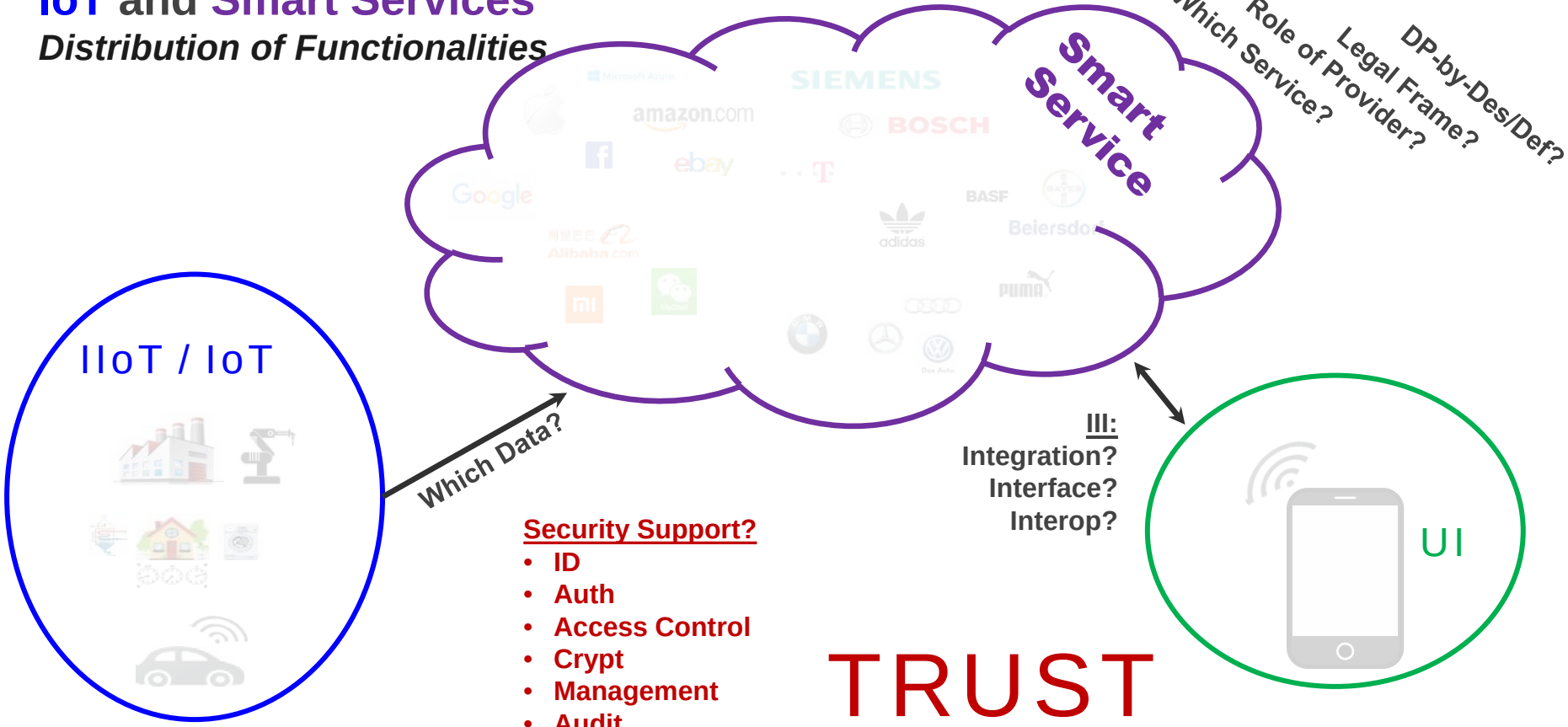
Bildquelle: www.teachprivacy.com

IoT → Smart Services

TÜVIT
TÜV NORD GROUP

IoT and Smart Services

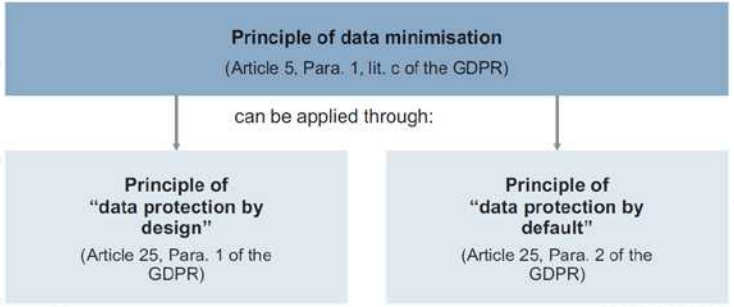
Distribution of Functionalities



Trust → Data Protection by-Design → Data Protection by-Default

DP-by-Des/Def? Legal Frame?

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

TÜVIT TÜV NORD GROUP

Trust

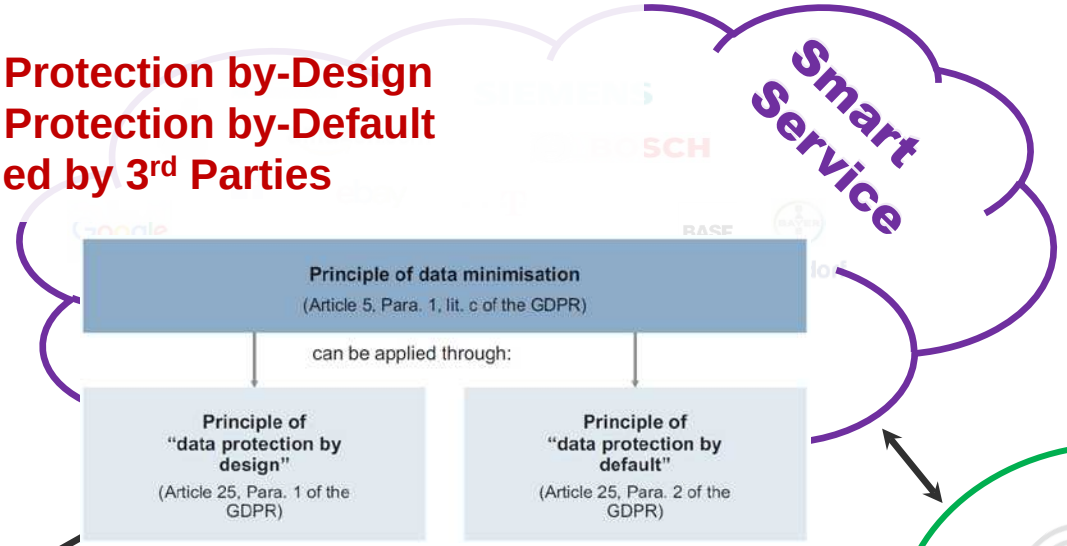
GDPR

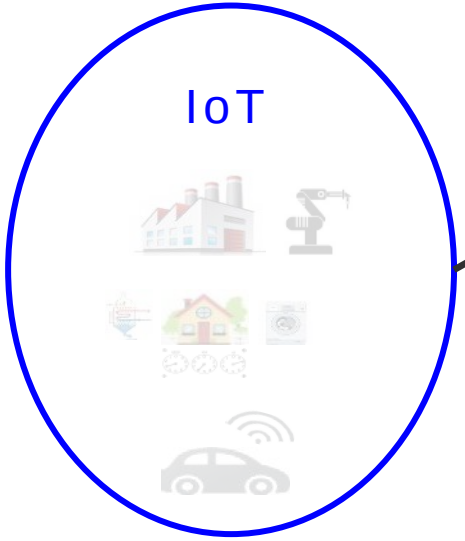
→ Data Protection by-Design

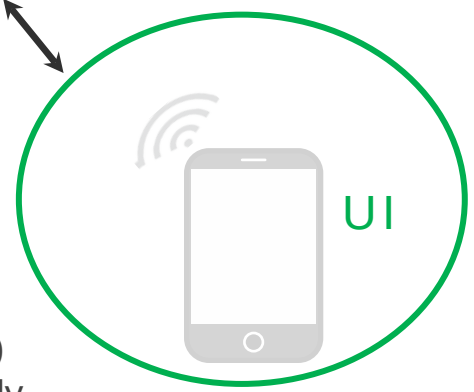
→ Data Protection by-Default

confirmed by 3rd Parties

DP-by-Des/Def? Legal Frame?







by-Design:

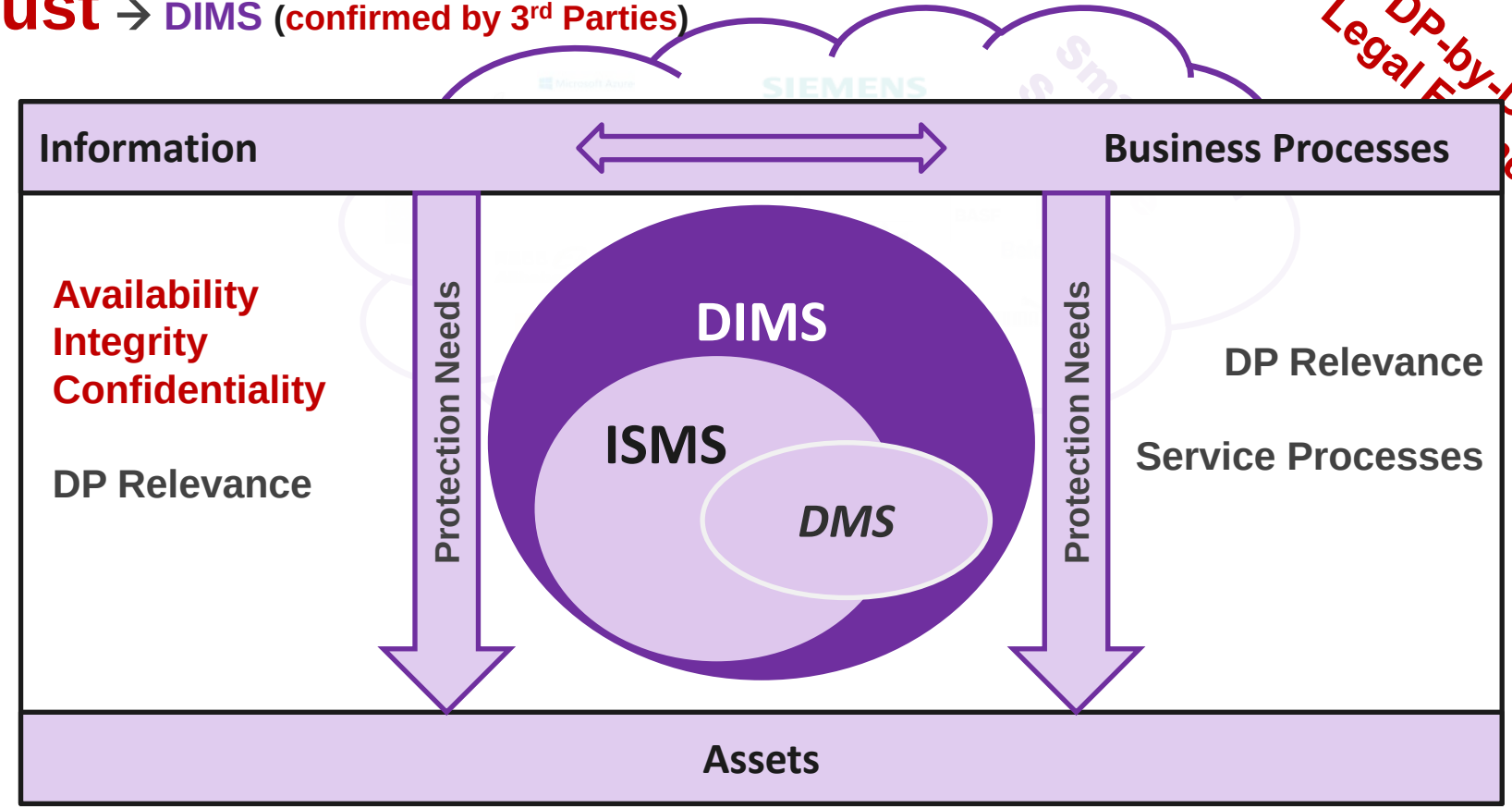
When Data leaves the Device (to the Smart Service) Data Protection Regulations are fulfilled automatically

by-Default:

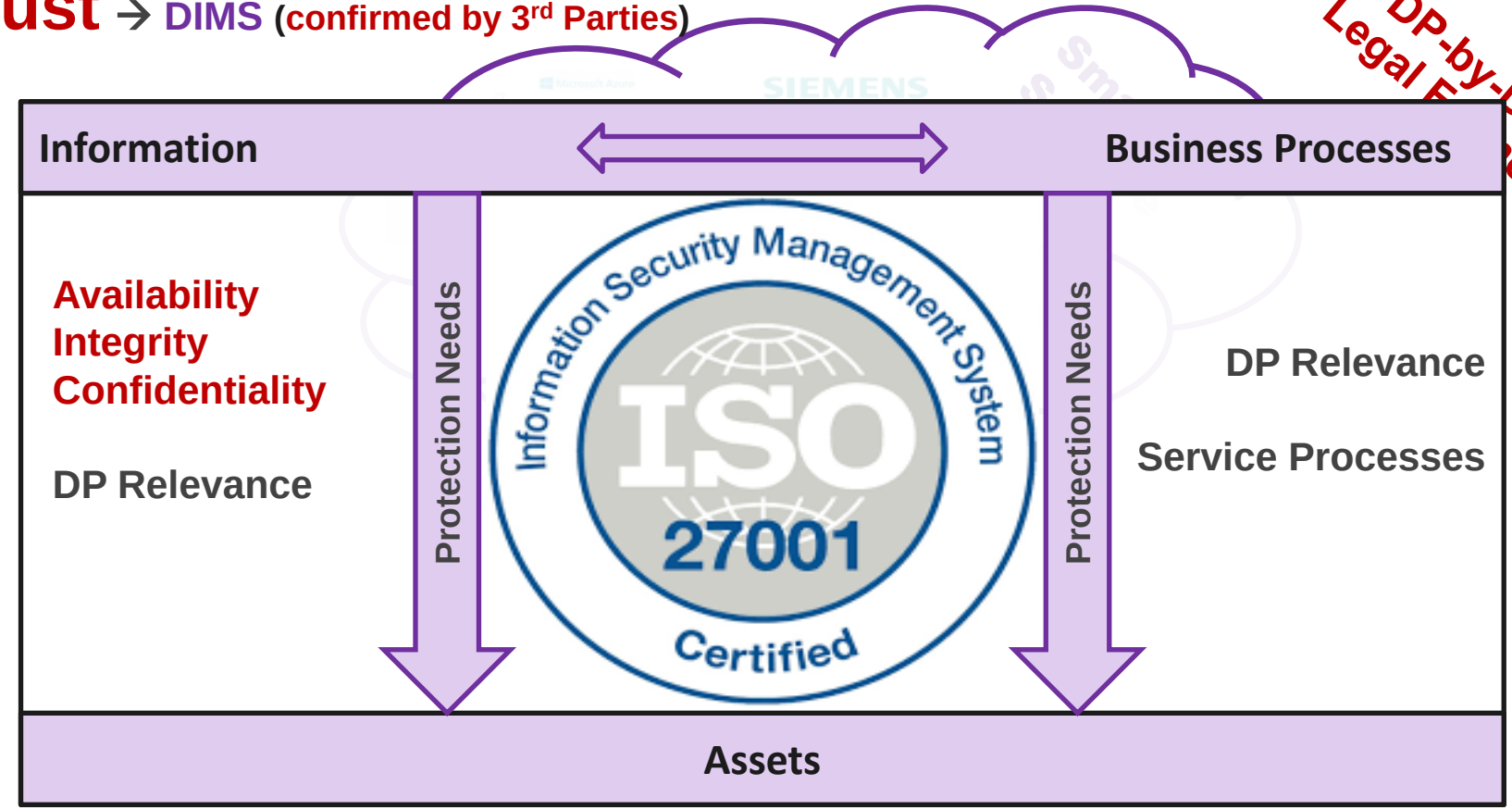
The "*by-Design*" configuration is the initial configuration

TÜVIT TÜV NORD GROUP

Trust → DIMS (confirmed by 3rd Parties)



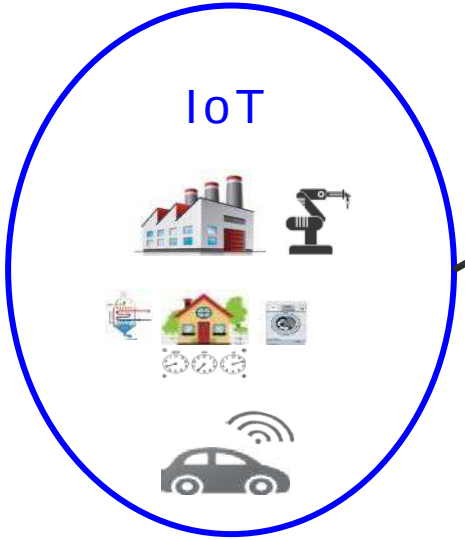
Trust → DIMS (confirmed by 3rd Parties)



IoT and Smart Services

Device Security – *not only GDPR relevant*

DP-by-Des/Def?
Legal Frame?



CSA – Cybersecurity Act

enisa

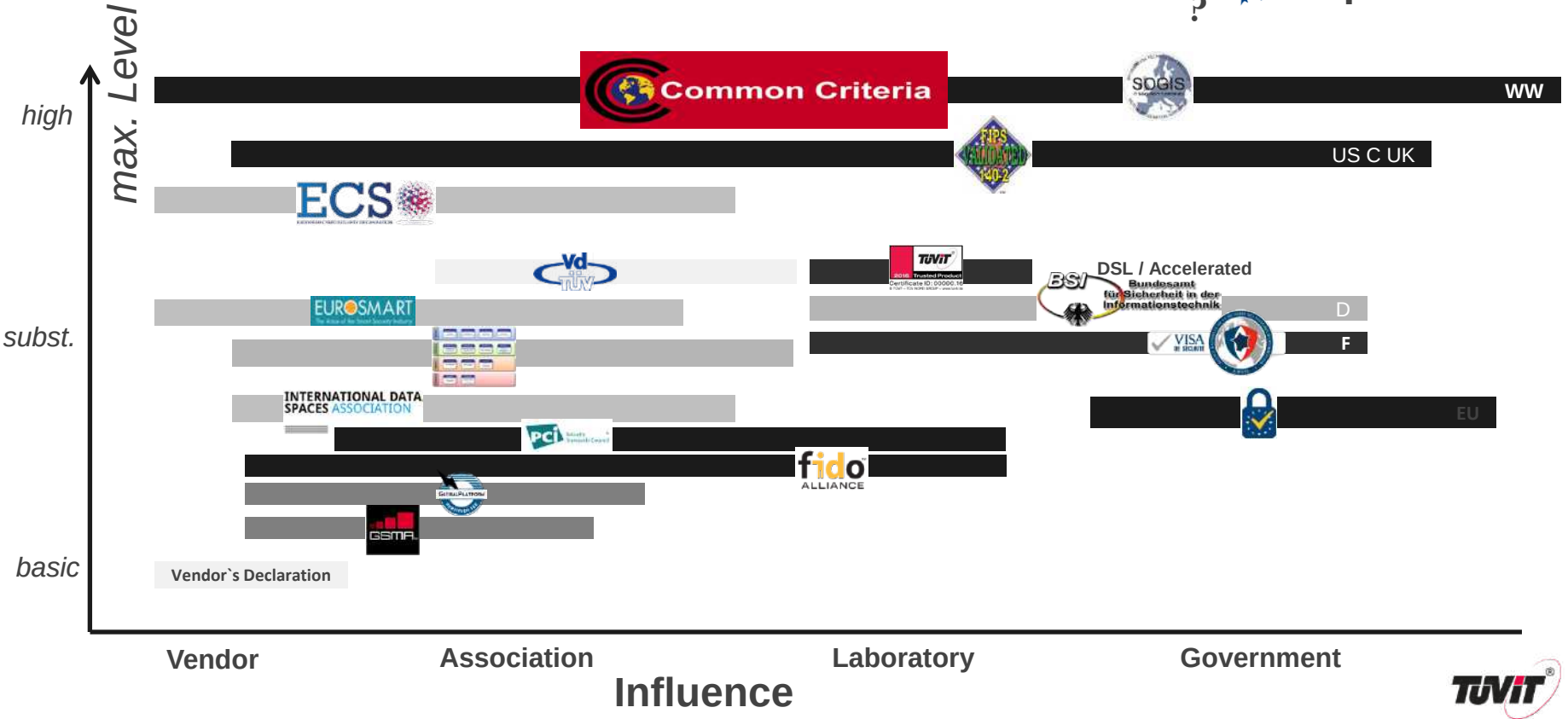
Security Support?

- ID
- Auth
- Access Control
- Crypt
- Management
- Audit
- …

TÜVIT
TÜV NORD GROUP

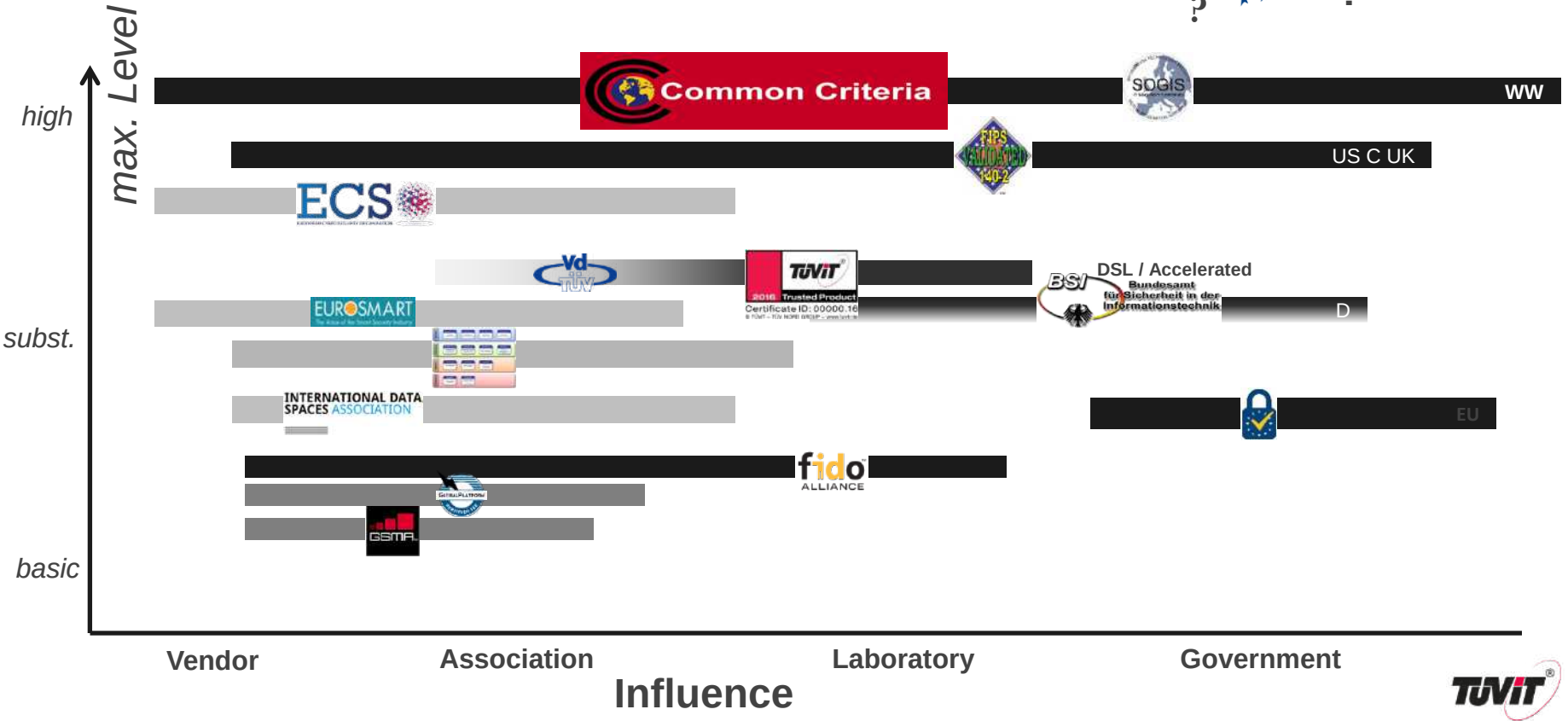
EU: IT Security Test and Evaluation Methods

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



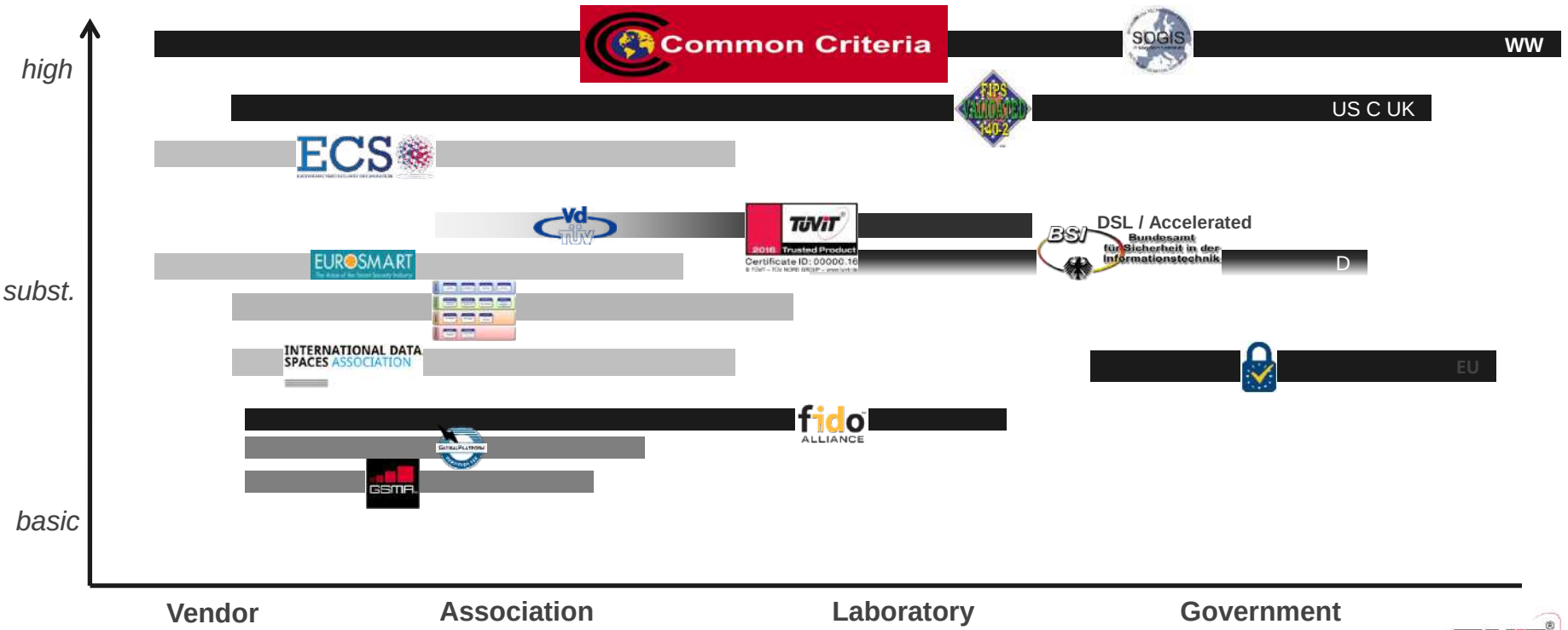
IT Security Test and Evaluation Methods

Support of TÜViT



IT Security Test and Evaluation Methods

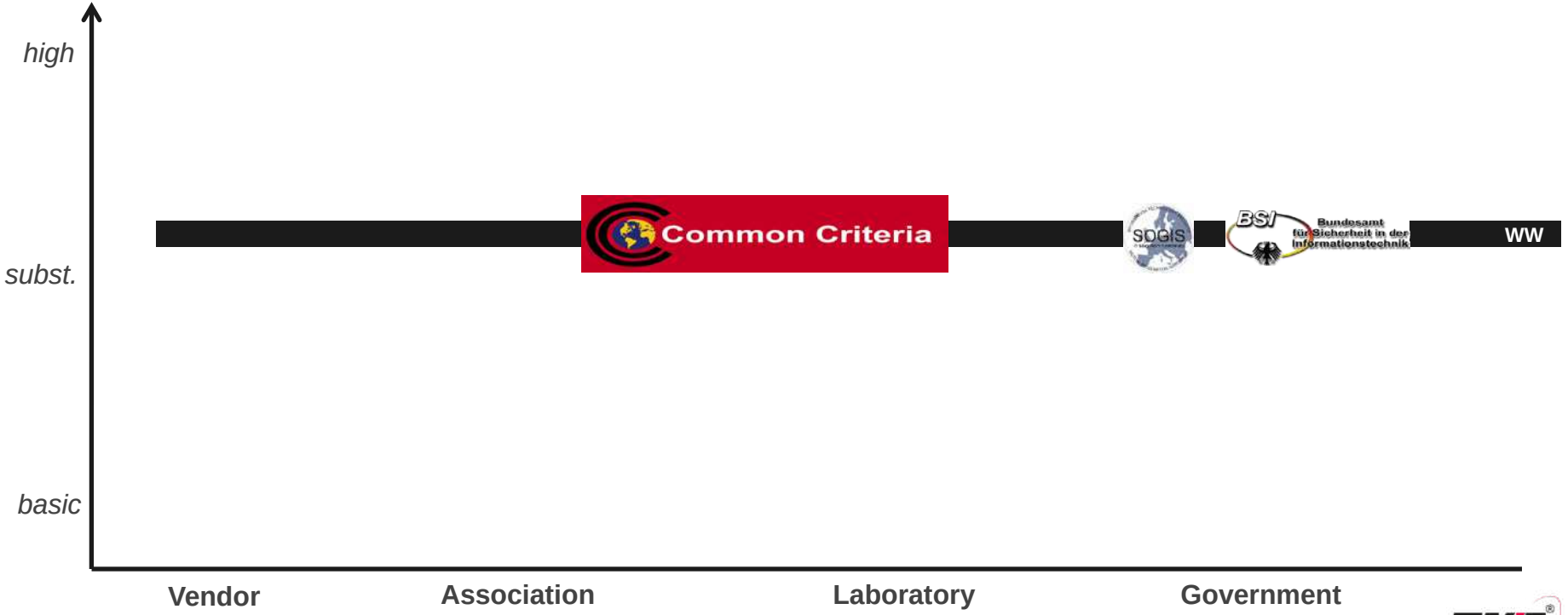
Most promising Approach (TÜViT)



TÜViT
TÜV NORD GROUP

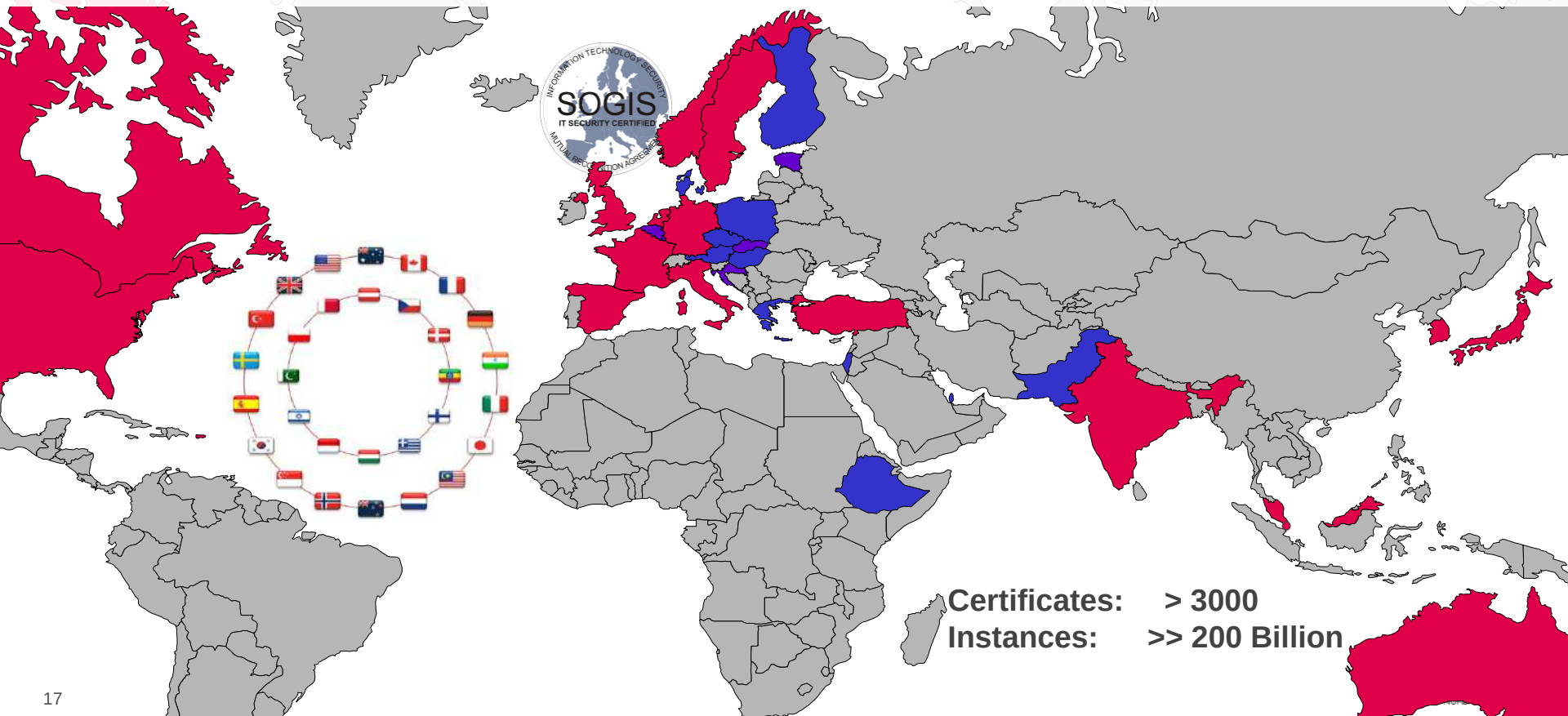
IT Security Test and Evaluation Methods

Most promising Approach (TÜViT)



Common Criteria – CCRA (~EAL2) / SOGIS

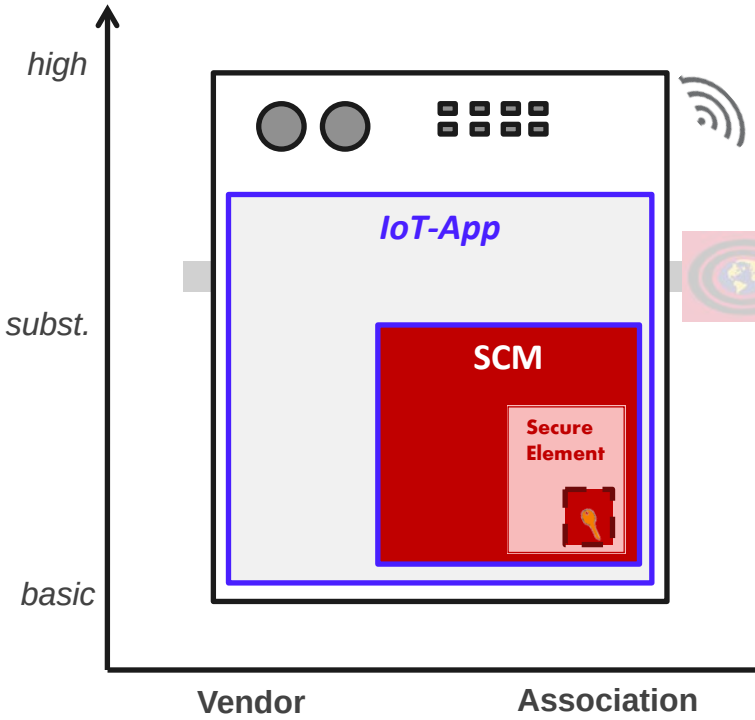
Certificate Issuing and Consuming Nations - Certificate Consuming Nations



Certificates: > 3000
Instances: >> 200 Billion

IT Security Test and Evaluation Methods

Most promising Approach (TÜViT)

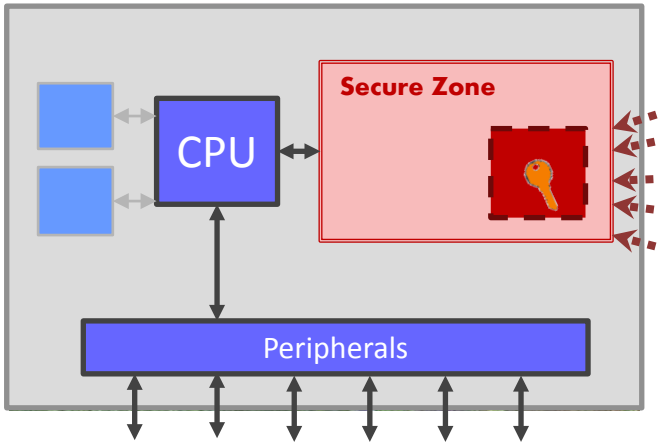


Secure IoT PP‘s

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**

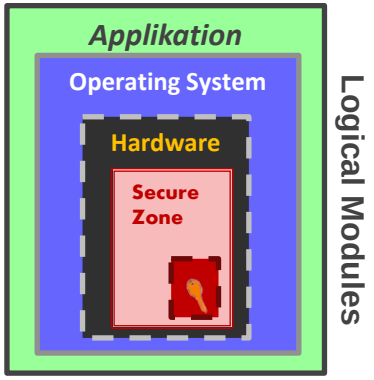
Secure Elements



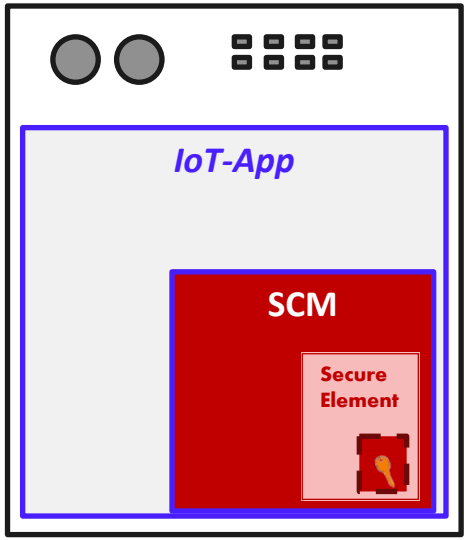
Attacks

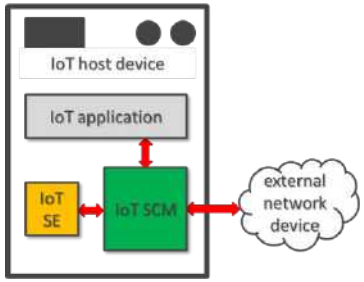
- Electrical Stimulation
- Energy & Particle Exposure
- Inspection & Reverse Engineering
- Physical manipulation
- Electro-Magnetic Interaction / Radiation
- Electrical Measurement
- Communication

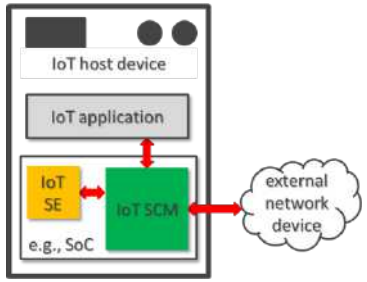
Embedded

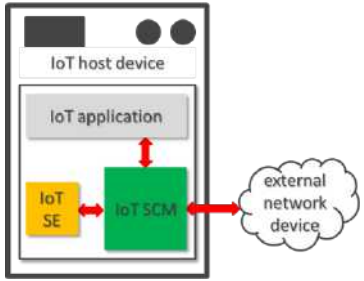


Secure IoT PP's
Form Factors



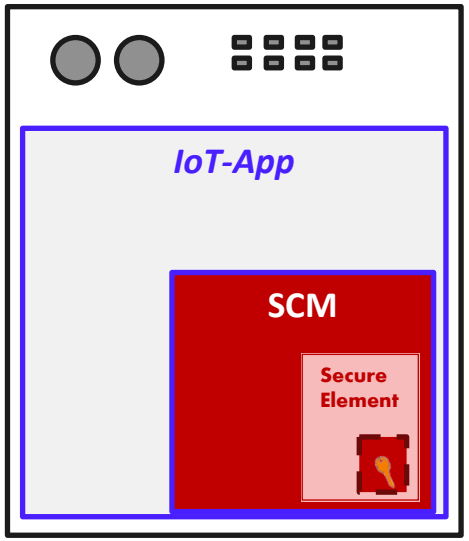




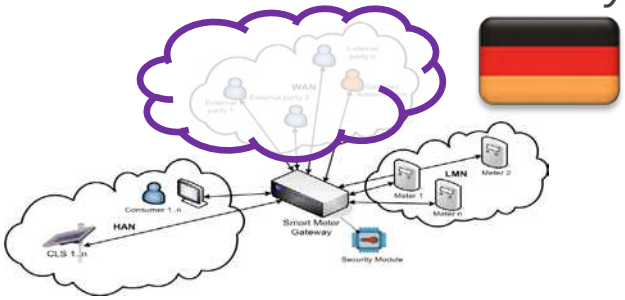


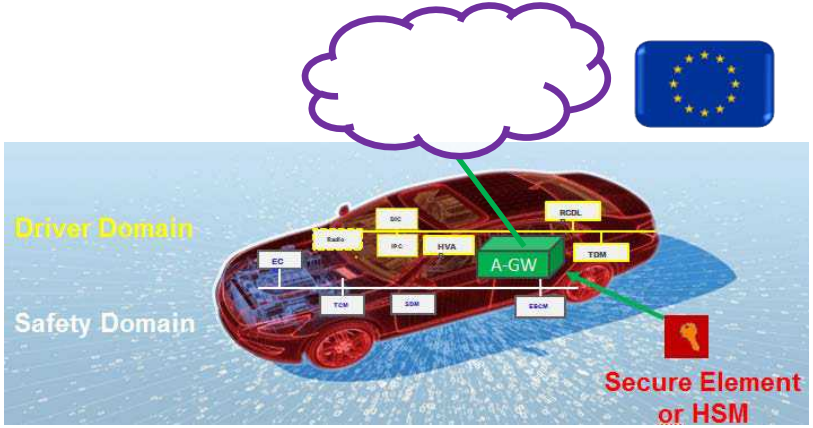
https://youtu.be/hbYUhMabPFo

Secure IoT PP's
other Examples



***German** Smart Meter Gateway*





Common Criteria

***EU**: C-ITS*

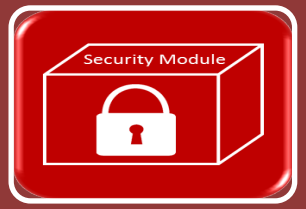
Co-operative Intelligent Transport Systems

TÜVIT TÜV NORD GROUP

Secure IoT - The System Approach

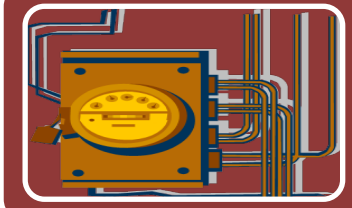
IoT SCM – Secure Communication Module

- 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

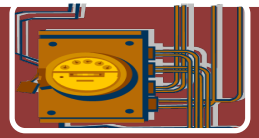
- Different System Architectures → different Use Cases
- Comprising a System Architecture for many IoT SCM's

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

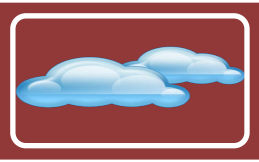


Trusted Paths

- 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

- **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
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

TÜVIT® TÜV NORD GROUP

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**

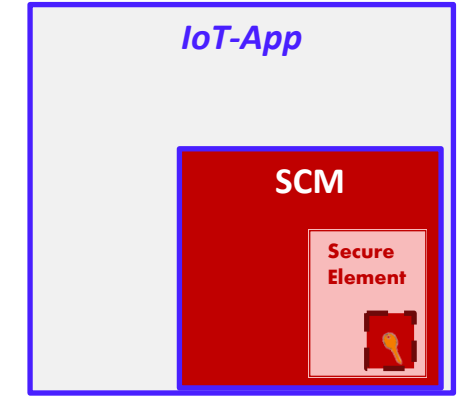
12. **Lifts**
13. ATEX
14. Radio Equipment
15. Low Voltage

16. **Pressure Equipmen**
17. **Marine Equipment**

18. **Cableway Installations**

19. **Personal Protective Equipment**
20. **Gas Appliances**

21. **Medical Devices**
22. **In Vitro Diagnostic (IVD) devices**



IoT and Smart Services
Summary

Smart Service

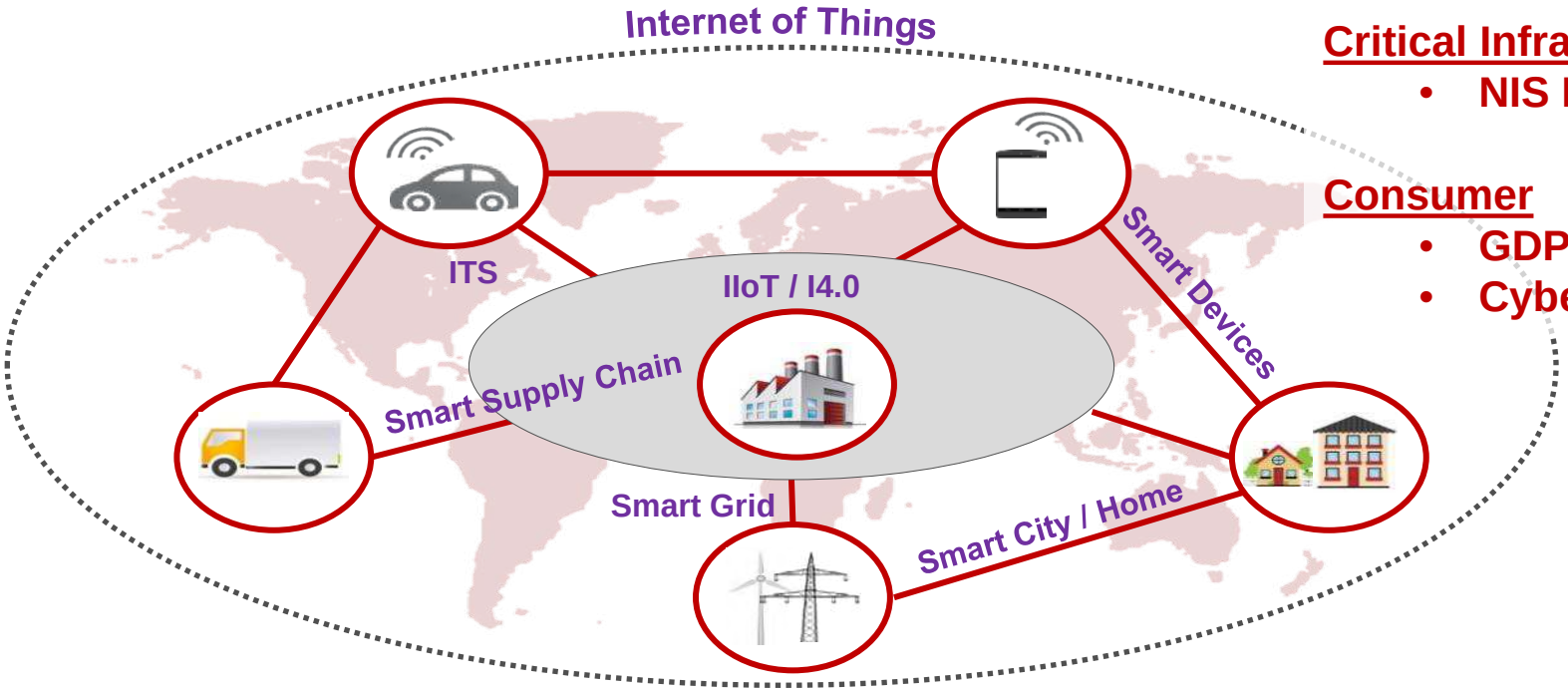
GDPR: DIMS

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