

TeleTrust-Konferenz 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 28.11.2019



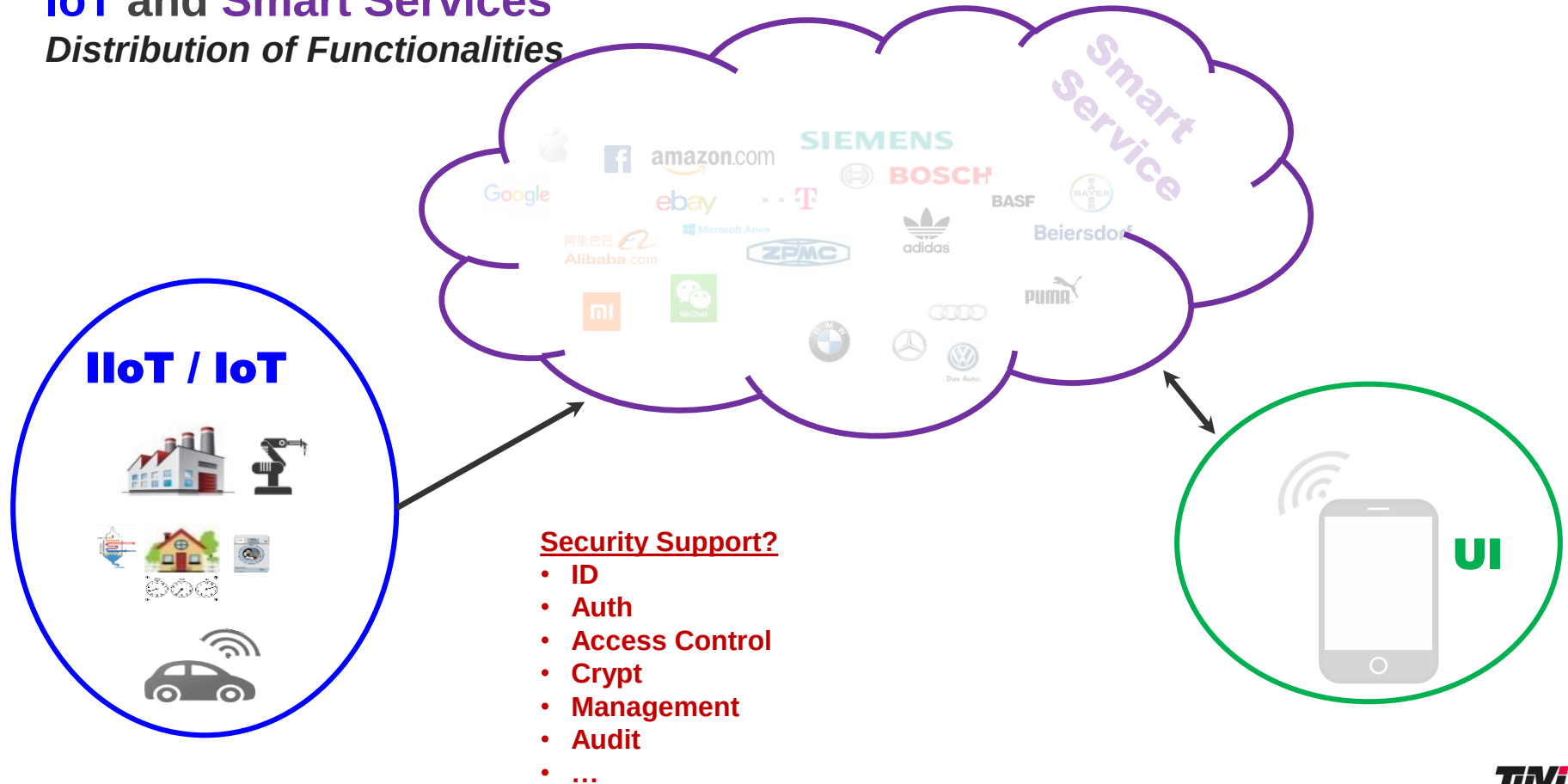
Matrěška

Modulare Prüfszenarien passend zum EU Cybersecurity Act

Markus Bartsch, TÜViT

IoT and Smart Services

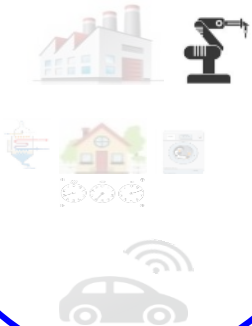
Distribution of Functionalities



IoT and Smart Services

Silk road on waterways

IIoT / IoT



Silk road on waterways

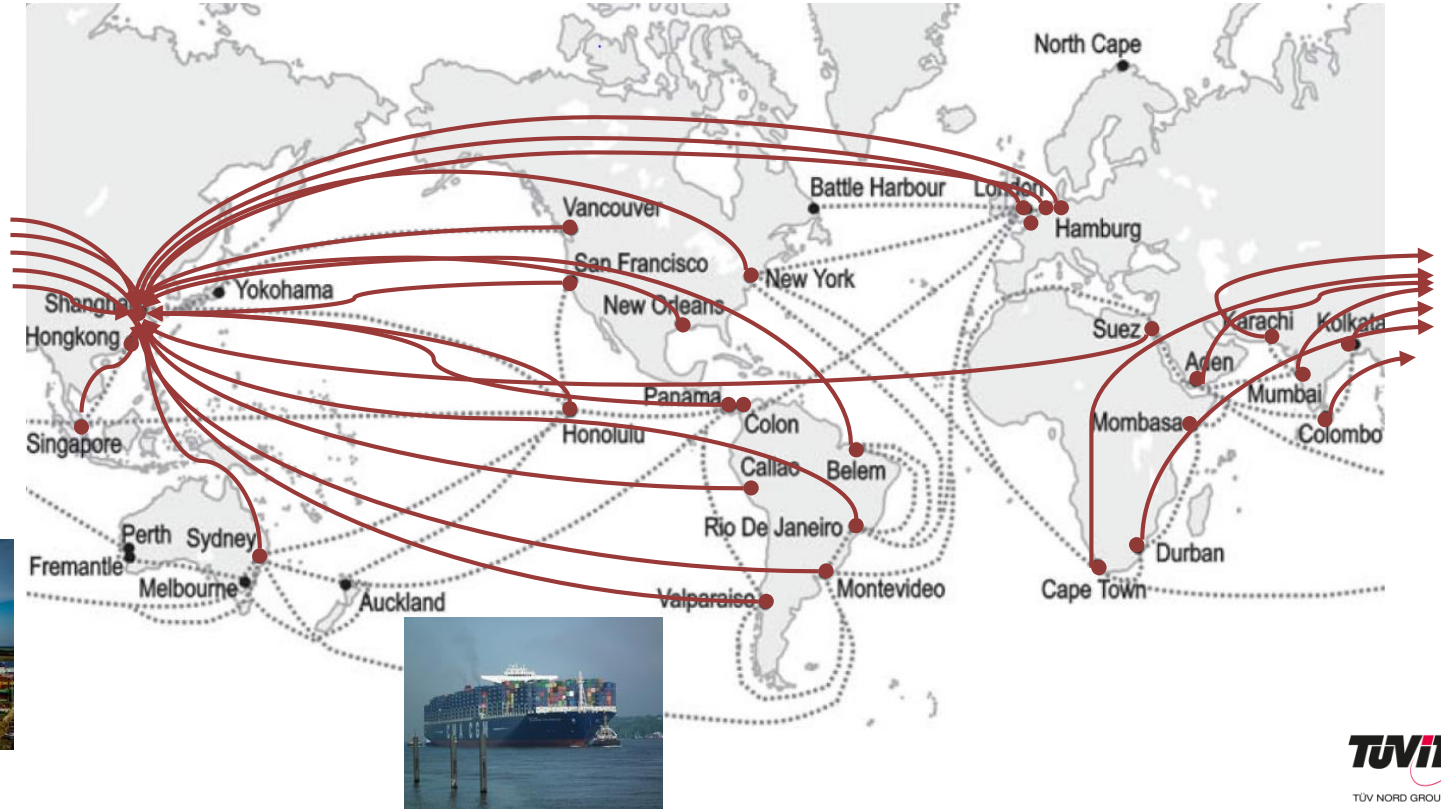


Questions answered:

- From?
- Where?
- When?
- Weight?
- What? - *roughly*

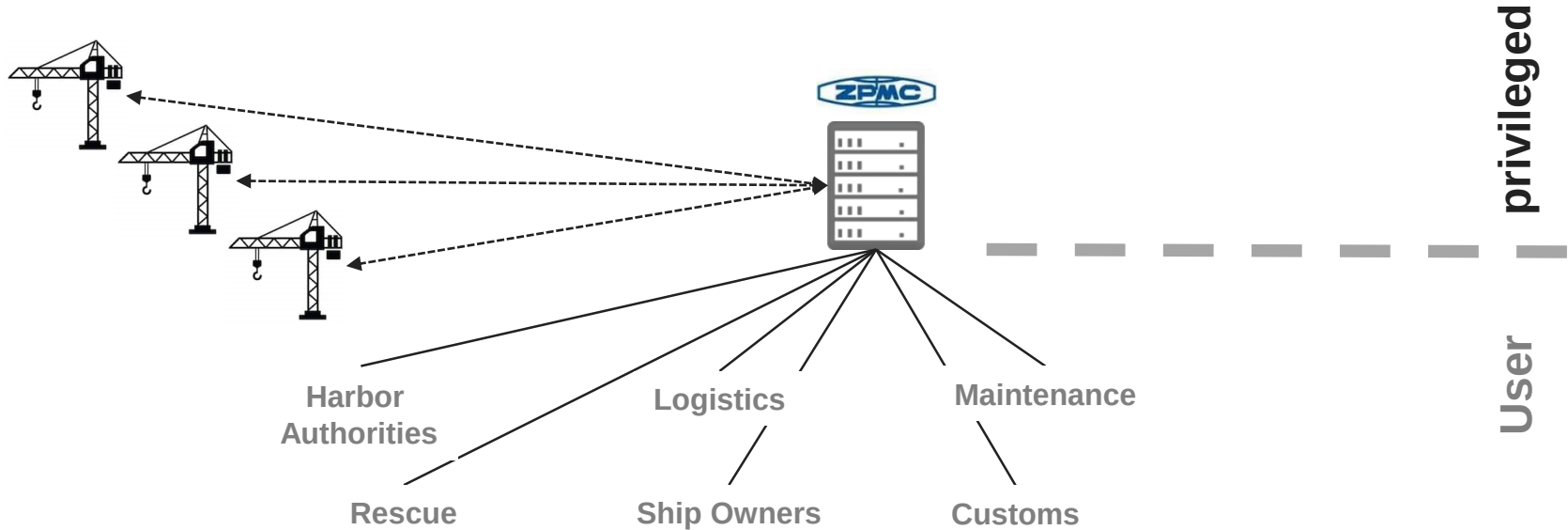
Future:

- What? – *in detail*



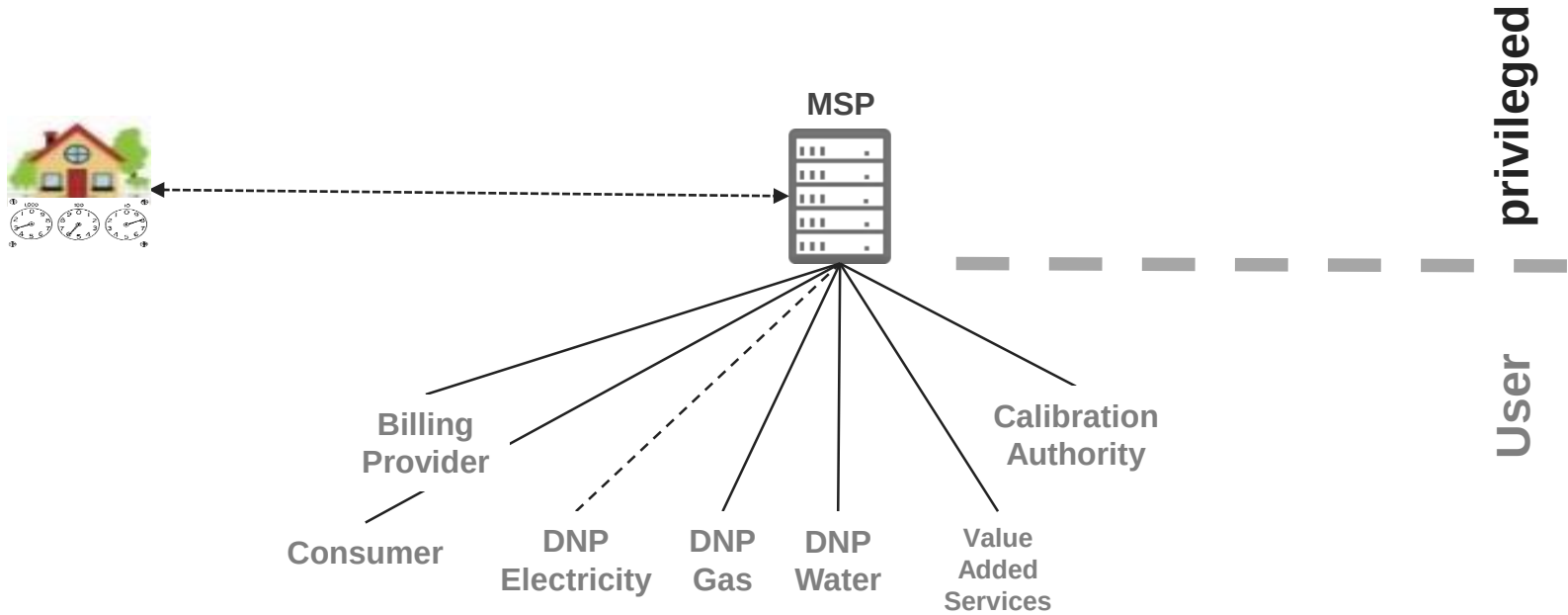
Silk road on waterways

Mission completed



IoT and Smart Energy

AMI (Advanced Metering Infrastructure)



German Metering System



MSP

Billing
Provider

Consumer

DNP
Electricity

DNP
Gas

DNP
Water

Value
Added
Services

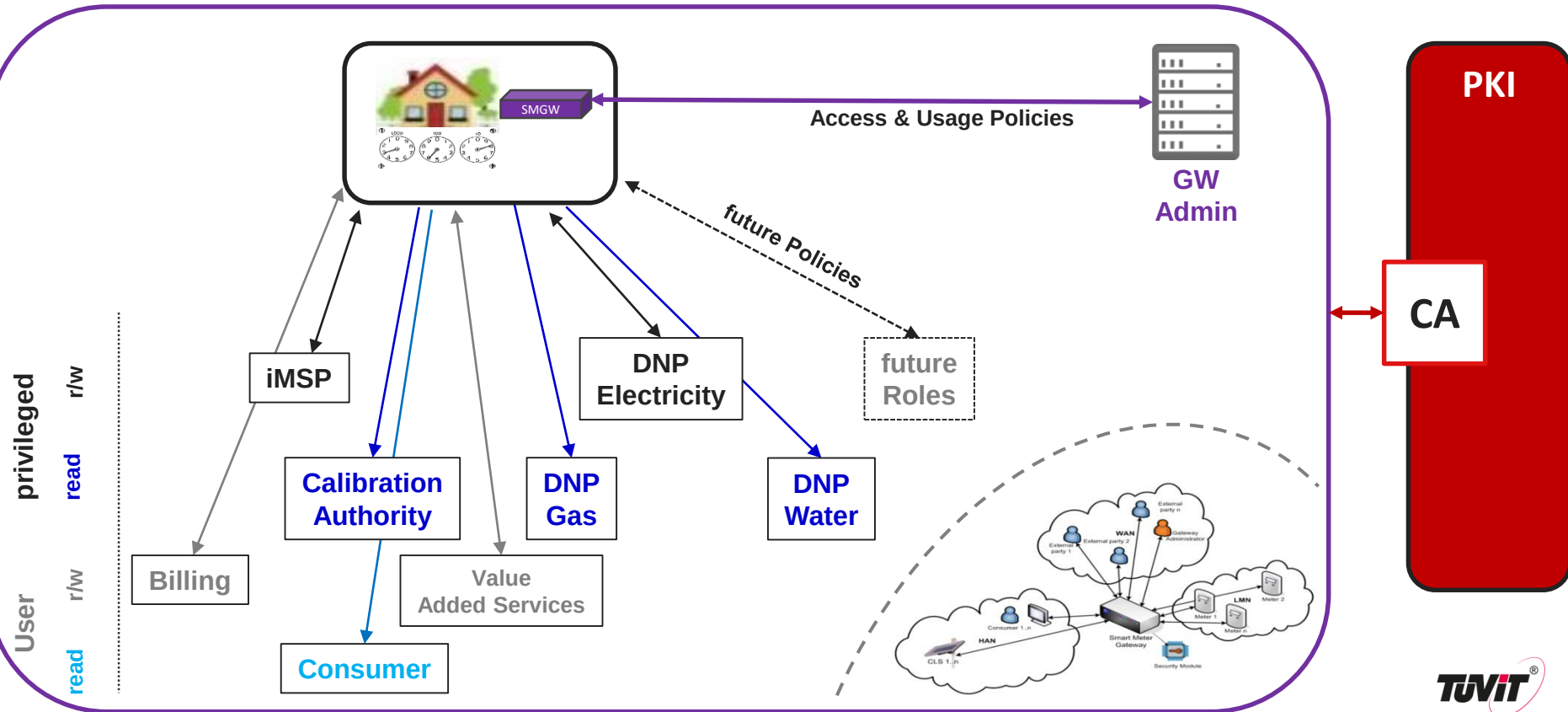
Calibration
Authority

PKI

CA

German Metering System

Usage Policies & Communication Flow based on Access Roles



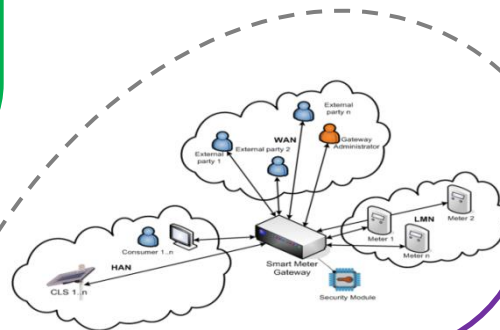
Complexity → Modularization (1)

Access Roles & Usage Policies

Secure Communication

Cryptographic Support

Secure Storage of Keys



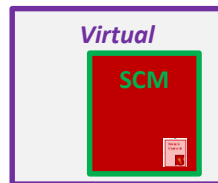
Complexity → Modularization (2)

Access Roles & Usage Policies

Secure Communication

Cryptographic Support

Secure Storage of Keys



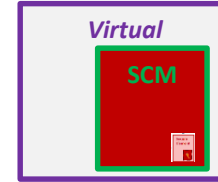
Matrěška

Virtualization

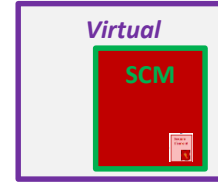
SCM - Secure Communication Module

Cryptography

Keys



Matrěška → Methodology



Common Criteria – CCRA (~EAL2) / SOGIS

Certificate Issuing and Consuming Nations - Certificate Consuming Nations



Certificates: > 3000



Common Criteria

Usage



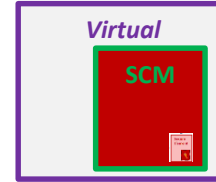
Number of Instances (last 20 years) > 100 Billion

Costs per Instance << 1 €

Duration of a
concurrent Evaluation: ~ 1 month longer than development period

CC-evaluated products are used worldwide

Usage of Common Criteria (1)



Usage of Common Criteria (2)

Matrěška Examples - based on Protection Profiles (PP) or **individual**



		German Smart Meter	Automotive		Fiscal Record	IoT	Internet Portals
			Car2X	X2Car			
	Virtual SCM	SMGW PP0073			SMAERS PP0105		DB
	SCM		VCS PP	RWU PP0106		SCA IoT SCM PP	Firewall
	Secure Element	SM-SMGW PP0077	V2X HSM PP	CSP PP0104		SCA IoT SE PP	
		S I C P PP0084					

Usage of Common Criteria (3)

System Support

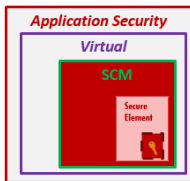


		German Smart Meter	Automotive		Fiscal Record	IoT	Internet Portals	
			Car2X	X2Car				
	Virtual SCM	SMGW PP0073			SMAERS PP0105		DB	Observation
	SCM		VCS PP	RWU PP0106		SCA IoT SCM PP	Firewall	Backend
	Secure Element	SM-SMGW PP0077	V2X HSM PP	CSP PP0104		SCA IoT SE PP		PKI
		S I C P PP0084						Production

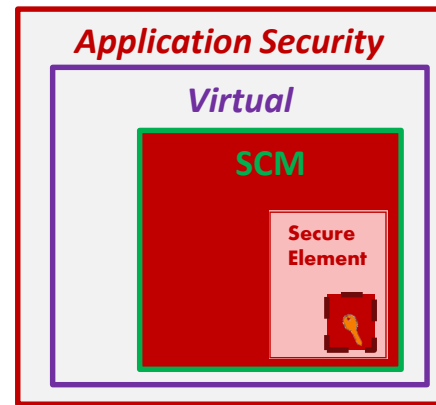
TU

Usage of Common Criteria (4)

Basis for higher Matrëška Levels (Verticals)

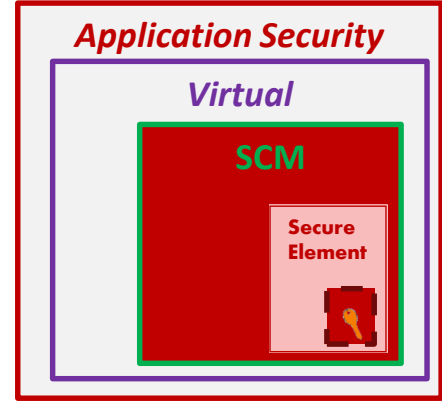
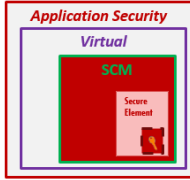


SMGW PP0073			SMAERS PP0105	
	VCS PP	RWU PP0106		SCA IoT SCM PP
SM-SMGW PP0077	V2X HSM PP	CSP PP0104		SCA IoT SE PP
		S IC P PP0084		



Layer 5: Application Security

substantial level



IoT



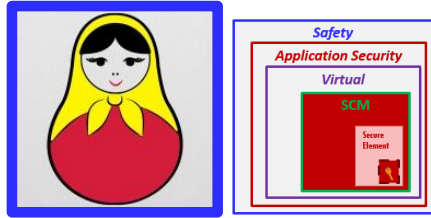
SmartHome



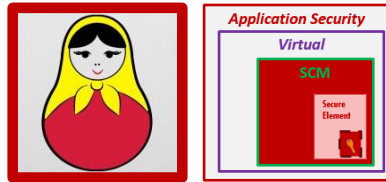
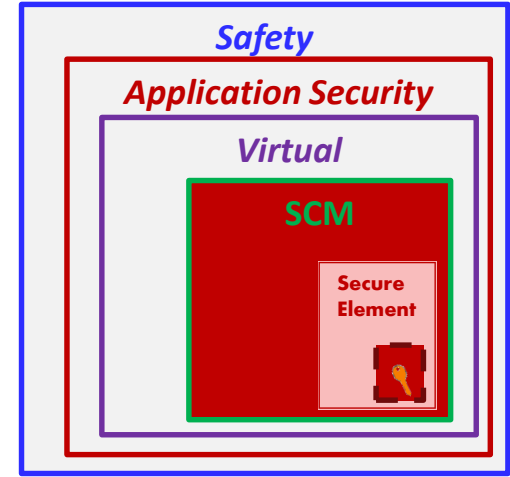
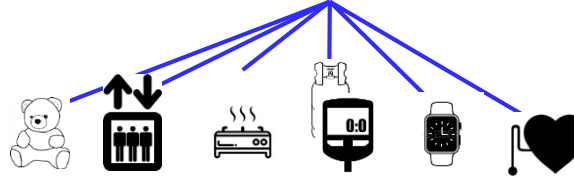
C-ITS



Layer 6: Safety



New Legislative Framework

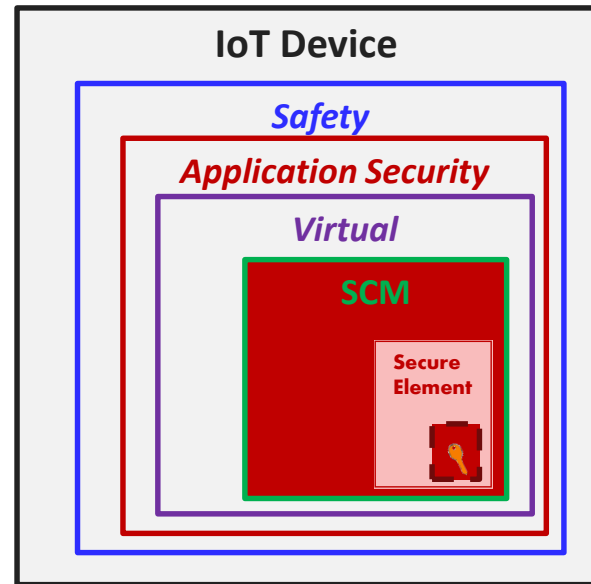
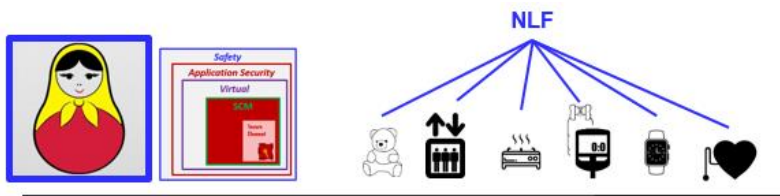
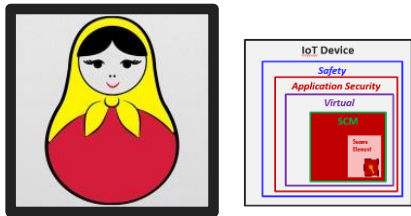


		SMGW PP0073			SMAERS PP0105	
			VCS PP	RWU PP0106		SCA IoT SCM PP
		SM-SMGW PP0077	V2X HSM pp	CSP PP0104		SCA IoT SE PP
					S IC P PP0084	

Security4Safety (S4S)

In case the **IT Security** is fulfilled in layers 1-5, safety requirements could be checked by **Continuous Monitoring**

Layer 7: Functionality (App)



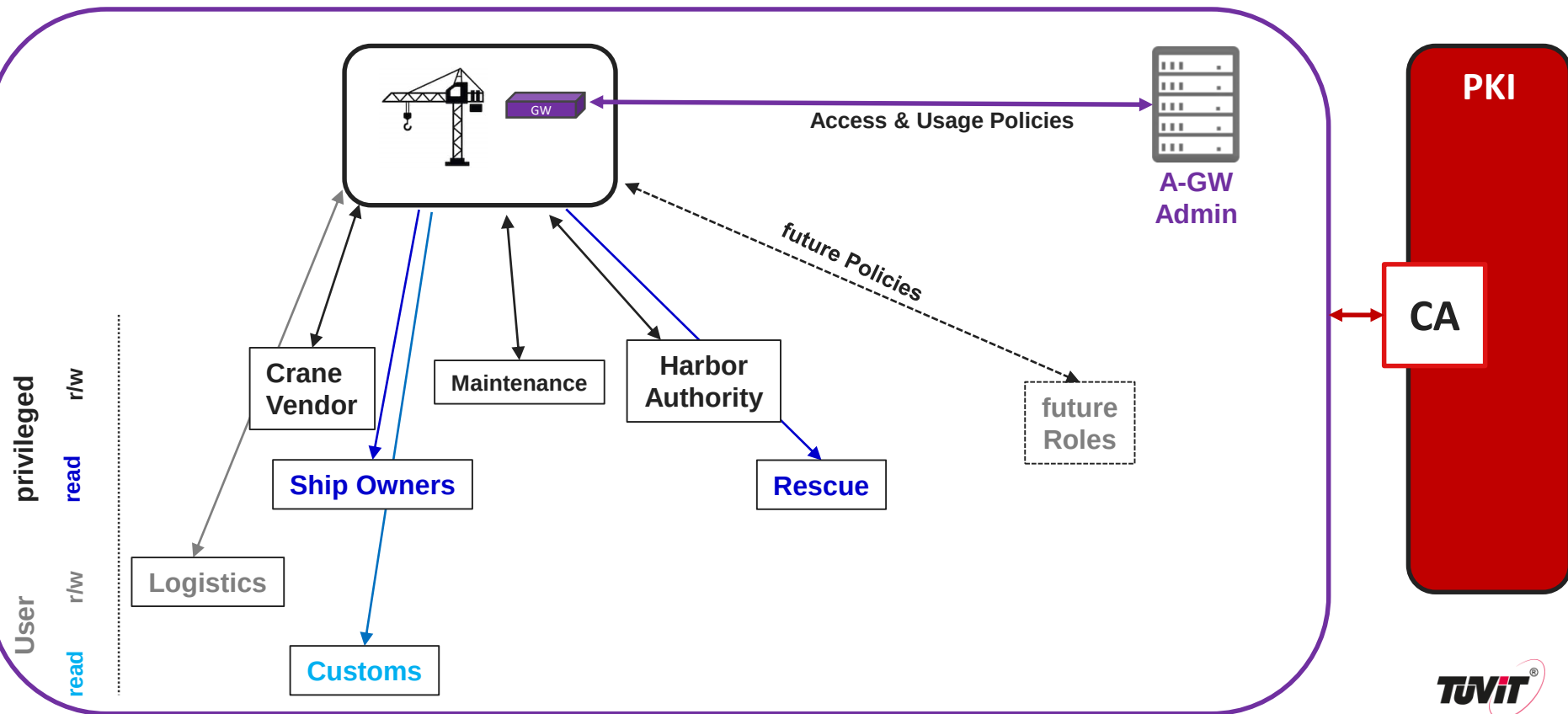
Summary



- IoT → meshed Networks → many Asset Owners
- many Asset Owners → “Kill root” (Fragment the admin / operation role) → **Complex Authorization**
- **Complex Authorization** → Modularization of **IT Security** necessary
- **Modularization of IT Security** → Use sufficient tool (**Common Criteria**)
- **Common Criteria** means re-usability → mass product
- **Mass product** → Price of evaluation relatively low
- Side effect:
 - Support for substantial **Security** on application layer
 - Basis for any **Detection** Mechanisms
 - → Basis for (automated) **Safety** Assessments (**Continuous Monitoring**)
 - Basis to protect the Digital Sovereignty

Silk road on waterways

just a Road



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

