



Federal Ministry
for Digital
and Transport

IT security in the context of vehicle type approval

Table of Content

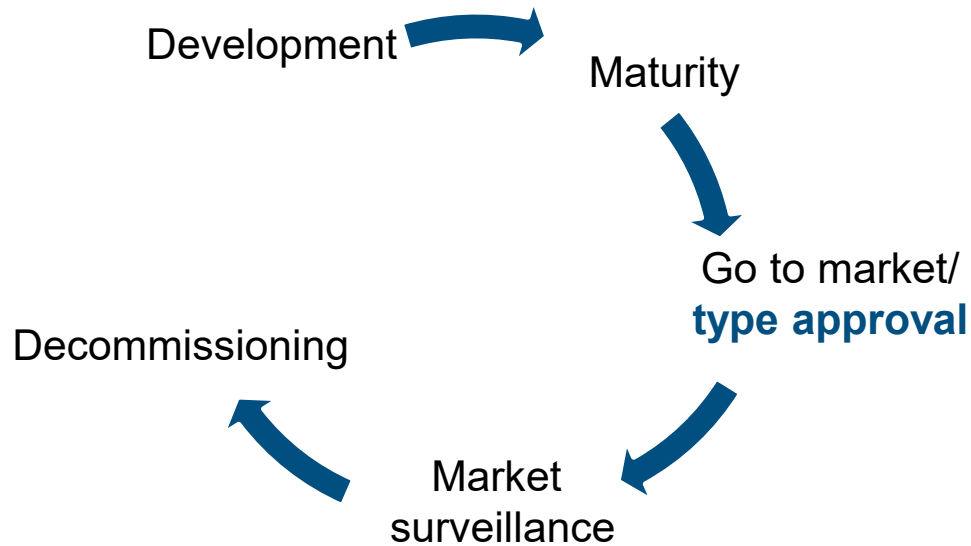
Setting our context

- Type approval of vehicles
- Special challenges of information security

UN-Regulation 155

- Integrating information security into the type approval framework
- Impact of IT security on road traffic

Life cycle of a vehicle type





Who sets the requirements for vehicle type approval?



UNECE

- 1958 Agreement
- UN Regulations
- 1998 Agreement
- United Nations Global Technical Regulations



European Union

- Regulation (EU) 2018/858
- EU framework for
- Type approval (for vehicle categories M,N,O) and market surveillance



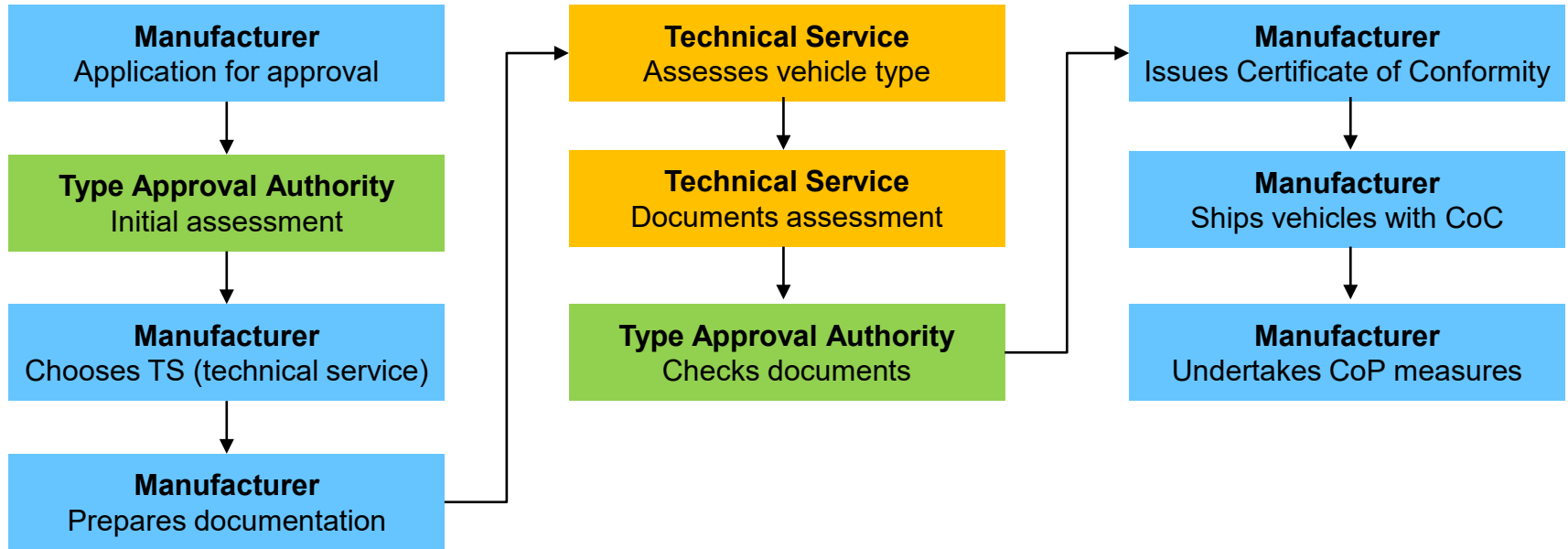
Germany

- StVZO
- German road vehicles registration and licensing regulations
- StVG
- Road traffic act

-
- Type approval is an **important instrument**, to ensure **safety in road traffic** and **protection of the environment**
 - Regulation (EU) 2018/858 is obligatory for **type approval** and **market surveillance**




Type approval process in Germany





IT security holds special challenges and threats

- IT security is a dynamic process. There is no „set it and forget it“ in IT security.
 - If data has been stolen, it can be hard to detect. The owner might never know that his data has been copied..
 - Stolen data can rarely be recovered. Once stolen, it remains stolen.
 - Security requirements vary for different types of data. Safety-relevant vehicle data with high safety standards.
- 
- Access to vehicles systems can be used to steal vehicles or manipulate them while in operation (steering, brakes, ...).
 - Stolen data can be used to profile drivers, to trace them and to use information against them. Stolen GPS data can show when the vehicle is on the road and threat actors might know when homes are empty
 - Stolen data can be used for identity theft – and vehicles will hold an increasing amount of personal data.

Integrating IT security into the vehicle type approval framework

The basis for the integration of IT security in the type approval framework is UN Regulation No. 155. This regulation was adopted by the WP.29 in 2020 and integrated into the European framework in 2021.

The regulation works on three levels to make vehicles more secure from an IT security perspective

1. OEM level: Cyber Security Management System
2. Vehicle level: Risk assessment and mitigation measures
3. Fleet level: Market surveillance

UN Regulation No. 155 – Cyber Security Management System and risk mitigation of cyber security risks

CSMS	<p>The manufacturer has to provide a cyber security management system (CSMS) to appropriately manage cyber risks throughout the operational lifetime of the vehicles.</p> <p>During development and operation of the vehicle the CSMS covers processes for threat monitoring, risk assessment and threat mitigation and direct response.</p>
Risk mitigation	<p>The IT risk assessment and mitigation measures taken during development of the vehicle are evaluated by the approval authority. Threats must be considered such as denial of service attacks via communication channels to disrupt vehicle functions. The manufacturer has to provide ample documentation of measures implemented and tests conducted.</p>
Market surveillance	<p>During the lifetime of the vehicle type the OEM is obliged to monitor the threat landscape of the vehicle fleet. The OEM report on the landscape to the federal Type Approval Authority – enabling the authority to oversee the market and require measures where appropriate.</p>

Implementation of UN Regulation No. 155 – Involved parties



Federal Motor Transport Authority

Federal type approval
authority and responsible for:

- Type approval of vehicles
- Market surveillance
- Approval of technical services for the automobile sector.



Federal Office for Information Security

Is the federal competence
centre for information security
and develops guidelines and
certification requirements.

Technical Services

Support the OEMs in technical
testing and

- Validate compliance with technical requirements
- Have to be approved for the process by the KBA.

Vehicle OEMs

Seek type approval for their
vehicles and have to:

- Apply with the KBA for type approval
- Choose a technical service
- Prove compliance with technical requirements.



Impact of IT security on road traffic

Secure information systems built the necessary basis for ...

- The safe application of automated driving functions
Only vehicles whose automated systems are secured against manipulation and misuse can be considered **safe for participation in public traffic**.
- Secure vehicle-to-vehicle communication (V2V)
Communication and data exchange in traffic need to be secure to foster the **safe application of cooperative, connected and automated mobility** and future use cases.
- Secure access to in-vehicle data
To enable vehicle data sharing concepts and resulting use cases **vehicle data needs to be trustworthy**.

Thank you for your attention

Federal Ministry for Digital and Transport
(BMDV)

Referat Öffentlichkeitsarbeit L 21
Invalidenstraße 44
D-10115 Berlin

www.bmdv.de