Verband der TÜV e.V.

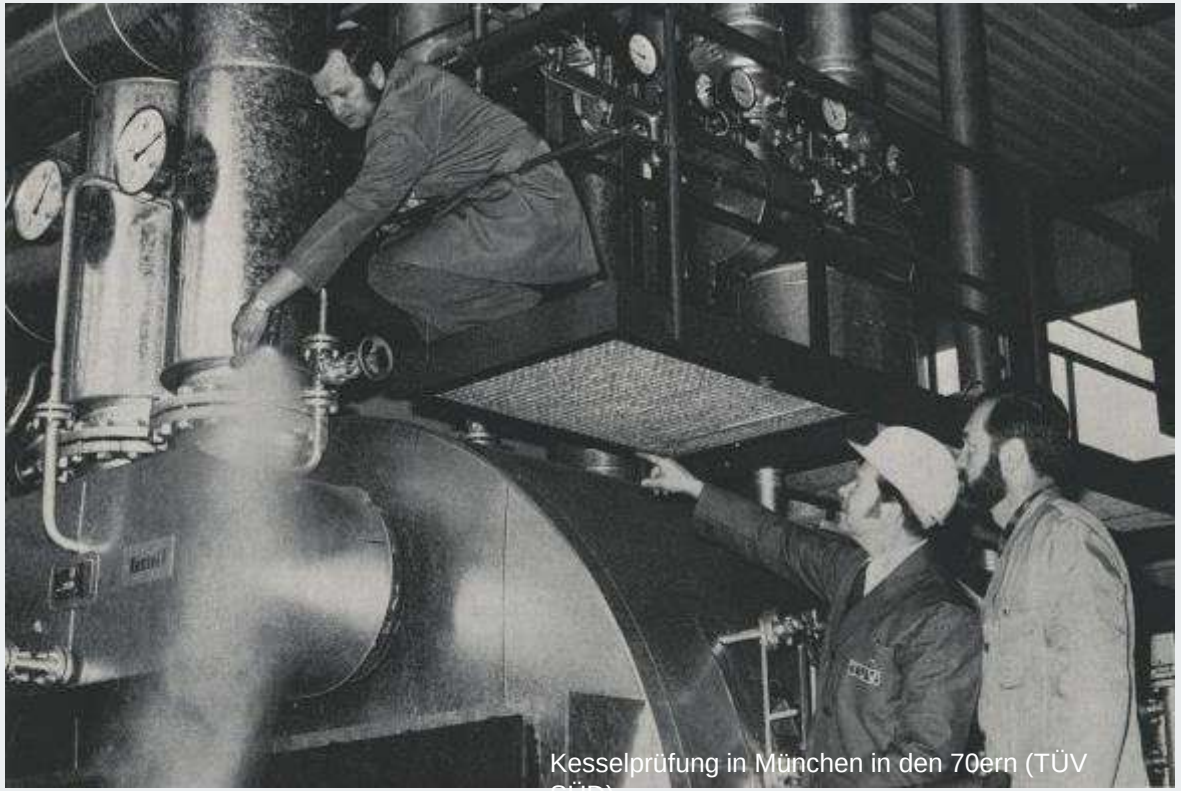
Eurolab 2019
Prüfung 4.0 am Beispiel TrustCenter

Joachim Bühler

Berlin, 9. April 2019

Wo wir herkommen

Prüfstelle in Köln-Poll in den 50ern (TÜV Rheinland)



Kesselprüfung in München in den 70ern (TÜV SÜD)

TÜV: Wo stehen wir?

Neue Wettbewerber kommen hinzu

tripadvisor DEUTSCHLAND

amazon.de Prime testen

DEUTSCHLAND TEST FOCUS MONEY BESTES FERNLEHRINSTITUT

GÜTESIEGEL TARGETING Geprüft hohe Qualität

Booking.com

BONICERT geprüfter Shop

TRUSTED SHOPS GUARANTEE

ePrivacy

yelp

kununu Volle Transparenz am Arbeitsmarkt

Google

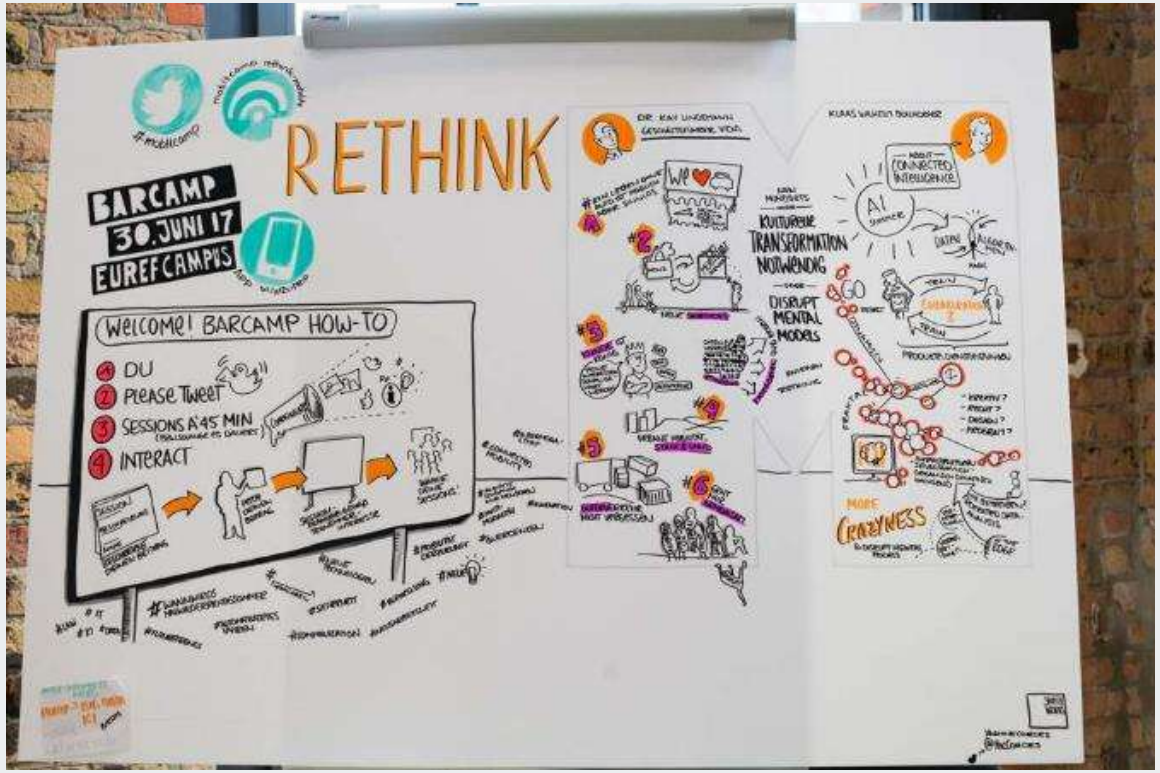
MARKTWÄCHTER

Aufgabe: Vertrauen für digitale Welt schaffen!

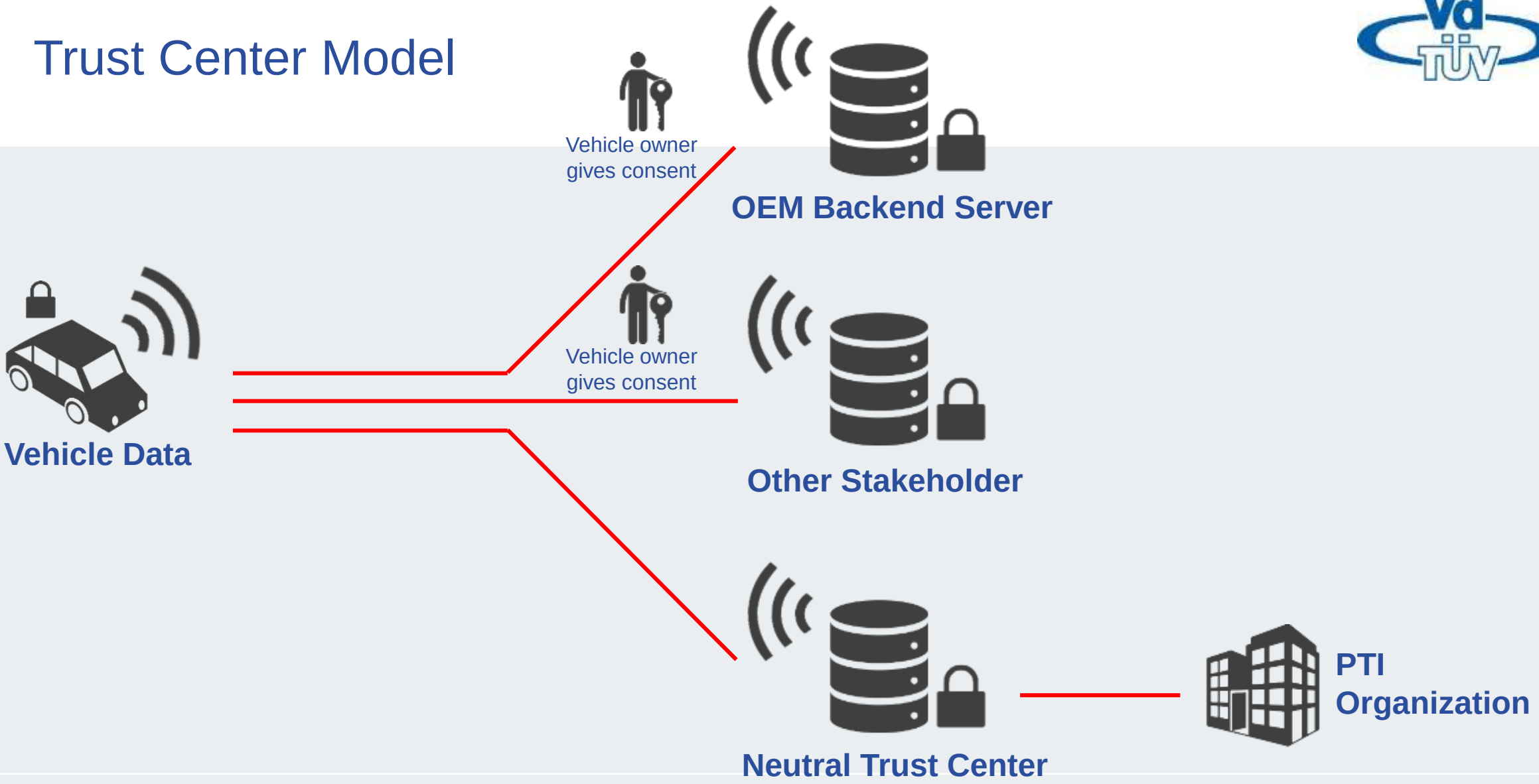
Aufgabe: Prüfgeschäft digitalisieren

- Safety um Security ergänzen
- Prüfprozess: Von der Zeitpunktprüfung zum Monitoring

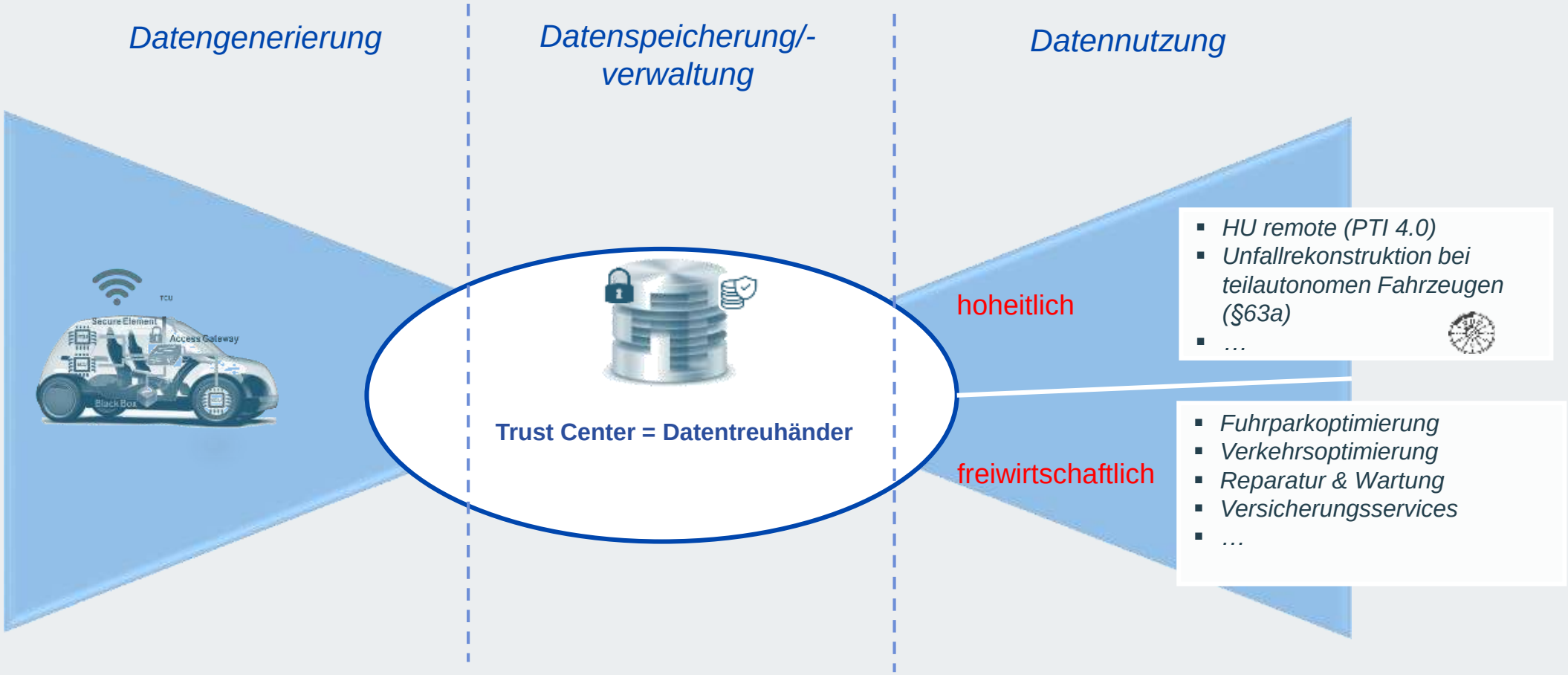
Neue Wege gehen!



Trust Center Model



Cardata over the air: hoheitliche und freiwirtschaftliche Aufgaben



Next: Branchenposition politisch umsetzen - technische Vorgaben für PTI 4.0 durch FSD entwickeln

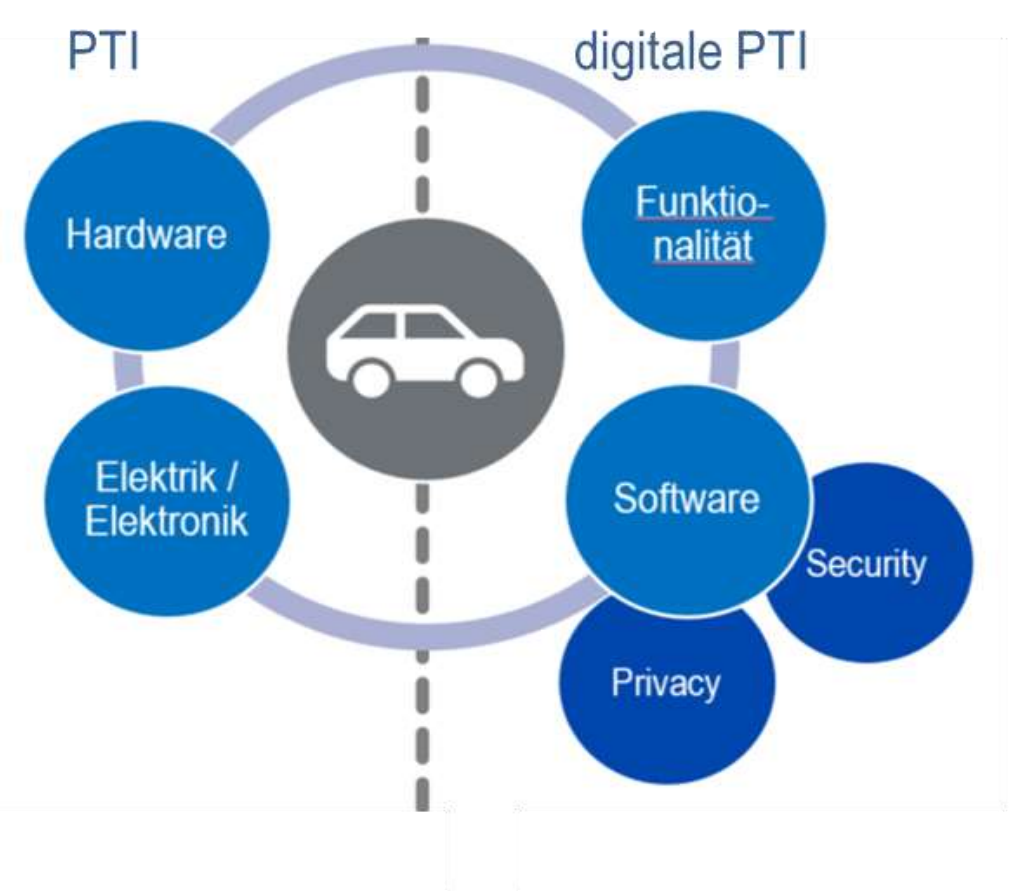
Position zum Zugang zu Fahrzeugdaten über die Remote – Fahrzeugschnittstelle (Over-the-Air)

Ein wichtiges Element des digitalen Wandels in der Mobilität ist das Wissen darüber, dass die Sicherheit und Integrität von Daten und vernetzten Systemen gewährleistet ist.
Die Prüfung von sicherheits- und umweltrelevanten Systemen erfolgt bisher über die standardisierte OBD-Schnittstelle bzw. über Messungen des Abgasstroms. Zunehmend werden Daten jedoch auch über Over-the-Air-Schnittstellen, unter anderem die Mobilfunkschnittstelle, übertragen. Der digitale Wandel bietet damit großes Potential für innovative Anwendungen in der Mobilität sowie der technischen Fahrzeuguntersuchung. Remote Services etwa für die Fahrzeugdiagnose, Unfallauswertung und Feldüberwachung sind dabei abhängig von einem verlässlichen und sicheren Zugang zu Fahrzeugdaten, unabhängig von den freiwirtschaftlichen Interessen der Fahrzeughersteller oder anderer Stakeholder.

1. Zur Wahrnehmung hoheitlicher Aufgaben durch berechtigte Stellen muss ein vollumfänglicher, diskriminierungsfreier, unentgeltlicher Zugriff[1] auf originäre Fahrzeugdaten Over-the-Air gewährleistet sein.

Die Wahrung hoheitlicher Aufgaben setzt bei vernetzten Fahrzeugen auch den uneingeschränkten Zugang zu originären Fahrzeugdaten Over-the-Air voraus. Hoheitliche Aufgaben umfassen beispielsweise den Datenspeicher nach § 63a StVG, die Fahrzeuguntersuchung gemäß Richtlinie 2014/45/EU oder Feldüberwachungsmaßnahmen im Bereich Emissionen. Prüfungen des Schutzes vor Security-Vorfällen, der Einhaltung von Datenschutz-Anforderungen, der Softwareintegrität sicherheitsrelevanter Funktionalitäten des Fahrzeugs – auch die vom Fahrzeug zur Verkehrsinfrastruktur – müssen Bestandteil der periodischen technischen Fahrzeuguntersuchung werden. Der unabhängige Zugang zu Daten und Diagnosefunktionen im Fahrzeug ist eine notwendige Grundlage für eine effiziente und unabhängige technische Fahrzeuguntersuchung im digitalen Zeitalter.

2. Der Zugang zu Fahrzeugdaten für hoheitliche Aufgaben durch berechtigte Stellen sowie deren Speicherung und Verwaltung muss über eine herstellerunabhängige Fahrzeugdatenplattform („TrustCenter"), die von einer beliehenen Stelle betrieben wird, erfolgen.



Next: Datenverarbeitung beim automatisierten Fahren §63a StVG durch Verordnung konkretisieren

GDV

Allianz

ADAC

Vd TÜV

DEKRA

Gemeinsame Positionen zur Datenverarbeitung bei Kraftfahrzeugen mit hoch- und vollautomatisiertem Fahrzeugbetrieb nach § 63a StVG

Am 21. Juni 2017 ist das Straßenverkehrsgesetz um Regelungen zum automatisierten Fahren ergänzt worden. Mit dieser Novellierung werden die Zulässigkeit und Voraussetzungen des automatisierten Fahrens, die Pflichten des Fahrzeugführers und der Schutz personenbezogener Daten geregelt. Danach müssen Fahrzeuge, die mittels hoch- oder vollautomatisierter Fahrfunktion betrieben werden, Positions- und Zeitangaben speichern, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem System erfolgt. Dies gilt auch dann, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt.

Noch nicht geregelt ist die Frage, wie die Berechtigten technisch und organisatorisch Zugriff erhalten können und an welchem Ort die Speicherung der Daten erfolgen soll. Diese Frage lässt das Gesetz unbeantwortet. Es enthält in § 63 b StVG lediglich eine Ermächtigungsgrundlage für das Bundesministerium für Verkehr und digitale Infrastruktur zur technischen Ausgestaltung des Speichermediums, zur Bestimmung des Ortes des Speichermediums sowie zur Art und Weise der Datenspeicherung.

Die Unterzeichner vertreten hierzu folgende Positionen:

1. Damit hoch- und vollautomatisiertes Fahren von der Gesellschaft breit akzeptiert wird, muss immer aufklärbar sein, wer die Verantwortung trägt (hat das System gesteuert oder der Mensch). Der Fahrer darf nur für eigenes Fehlverhalten belangt werden können. Der Gesetzgeber hat deshalb in § 63a StVG vorgesehen, dass diese Daten zur Aufklärung durch Speicherung zu Verfügung stehen müssen, um zu klären, ob das Fahrzeug zum Unfallzeitpunkt automatisiert fuhr, vom Fahrer gesteuert wurde oder sich gerade in der Übergabephase zwischen menschlichem Fahrer und Bordautomatik befand.

2. Die erforderlichen Daten müssen in der Hand eines neutralen unabhängigen Dritten (Datentreuhänder) sein, um allen Berechtigten unter den gleichen gesetzlichen Bedingungen Zugang zu den Daten zu ermöglichen. Neben einer Speicherung der Daten im Fahrzeug selbst ist deshalb zwingend eine Übertragung an einen unabhängigen Dritten erforderlich. Denn im Falle eines Fahrzeugverkaufs oder nach einer Zerstörung des Fahrzeuges durch einen Unfall ist nur über den Datentreuhänder eine Aufklärung im Interesse aller Beteiligten weiterhin möglich.

3. Die Speicherung und Übermittlung der Daten dient ausschließlich dem gesetzlichen Zweck der Nachvollziehbarkeit der Letztverantwortung (Fahrer oder System). Die Übermittlung der Daten an einen berechtigten Dritten darf nur erfolgen, soweit die gesetzliche Ermächtigung in § 63a StVG dies ausdrücklich erlaubt.

4. Verbraucher und Gesellschaft erwarten durch die Automatisierung eine deutliche Verbesserung der Sicherheit im Verkehr. Sie haben deshalb auch ein berechtigtes Interesse daran zu wissen, ob und wie häufig Fahrzeuge im automatisierten Fahrmodus an Unfällen beteiligt sind. Für den Verbraucher muss außerdem überprüfbar sein, ob die Hersteller ihr Leistungsversprechen hinsichtlich der Sicherheit ihrer Systeme erfüllen. Nur eine digitale Übermittlung der relevanten Daten

Datenverarbeitung §63a StVG

Datenverarbeitung bei Kfz mit hoch- und vollautomatisierten Betrieb

- Gem. §63a StVG müssen **Level 3 Fahrzeuge** Positions- und Zeitangaben speichern bei Wechsel der Fahrzeugsteuerung
- Erfordernis zur Klärung der Haftung bei Unfällen, Ermittlung der **Letztverantwortung**
- Digitale Übertragung der Daten zu neutralem unabhängigen Dritten (**Datentreuhänder**) und Speicherung im Fahrzeug
- Höchste Anforderungen an **Datenintegrität und Security** bei Übertragung

VdTÜV Konzept TrustCenter:
Rechtsgutachten, Aug. 18

- ✓ DSGVO – Anforderungen
  - Auftragsverarbeitungsverhältnis zwischen TrustCenter und OEM gemäß Art. 28 DSGVO
  - Datenverarbeitung gegenüber Dritten gemäß Anforderungen Art. 6 DSGVO
  - Datenspeicherung auf Anforderung des Betroffenen (TC Verantwortlicher nach Art. 4 Nr. 7)
- ✓ Wettbewerbs- und Kartellrecht
  - Unmittelbare real-time Datenzugriffe
  - Gleichberechtigter Datenzugriff
  - Keine Lock-in – Effekte
- ✓ Dateneigentum
  - Vertragliche Regelung
- ✓ Produktbeobachtungspflicht nach § 823 I BGB und ProdSg

>> Rechtskonformität bestätigt!
>>Vertrauen für sowohl Datenbetroffenen und Datennutzer!

Verband der TÜV e.V.

TÜV®

TÜV TrustCenter – Zugang zu Fahrzeugdaten sicher, neutral und standardisiert

Executive Summary

Die digitale Vernetzung der Fahrzeuge untereinander und mit der Infrastruktur ermöglichen neue Dienstleistungen, die das Potential haben, den traditionellen Mobilitätsmarkt weitreichend zu verändern. Diese Dienstleistungen basieren auf einer Vielzahl von Daten, die durch Nutzung und den Betrieb von vernetzten Fahrzeugen in einem digitalen Mobilitätsumfeld entstehen. Um einen authentischen und diskriminierungsfreien Zugang zu bestimmten Fahrzeugdaten sicherzustellen, werden cloudbasierte neutrale Datentreuhänder, TrustCenter, in Zukunft eine wichtige Rolle spielen.

Ein TrustCenter als Teil der Kommunikationsinfrastruktur für die Fahrzeugflotte ist die Komponente für die sichere, datenschutzkonforme, neutrale Speicherung von Mobilitätsdaten entlang der gesamten Wertschöpfungskette, die für verschiedene Dienstleistungszwecke verwendet werden sollen. In Zusammenarbeit mit den Fahrzeugherstellern werden bestimmte Fahrzeugdaten definiert, an den TrustCenter verschlüsselt und signiert vom Fahrzeug übertragen und von dort Dritten zur Verfügung gestellt - sofern der Fahrzeughalter einwilligt.

Beim TrustCenter steht der Fahrzeughalter im Mittelpunkt, der eine vollständige Transparenz und Datensouveränität erhält. Zukünftig können so Fahrzeugnutzer als Betroffene mit Hilfe der TrustCenter souverän entscheiden, welche Serviceanbieter einen gleichberechtigten und neutralen Zugriff auf ihre Daten erhalten sollen.

Risiken oder Bedenken, insbesondere aufgrund von lock-in – Effekten und der möglichen unberechtigten Einsicht in Datenströme werden durch die Kombination von Sicherheitsanforderungen des TrustCenters und der Zertifizierung der Datenstromwege aufgehoben. Datenschutz und Security werden so während der Erfassung, des Transports, der Speicherung und der Verarbeitung eingehalten. Diese umfassende sicherheitsrelevante Bewertung digitaler Funktionalitäten des vernetzten Fahrzeugs schafft das notwendige Vertrauen und die Akzeptanz in der Automobilbranche zwischen Fahrzeughersteller und -zulieferer sowie Aftermarkt und Bevölkerung.

Das TrustCenter ist zudem ein leistungsstarker und übertragbarer Prototyp für das Management von Daten in weiteren IoT-Industrien.

VdTÜV – Position für ein unabhängiges Mobilitätsdatenmanagement

1 *Zur Wahrnehmung hoheitlicher Aufgaben durch berechtigte Stellen muss ein vollumfänglicher, diskriminierungsfreier, unentgeltlicher Zugriff auf originäre Fahrzeugdaten Over-the-Air gewährleistet sein.*

2 *Der Zugang zu Fahrzeugdaten für hoheitliche Aufgaben durch berechtigte Stellen sowie deren Speicherung und Verwaltung muss über eine herstellerunabhängige Fahrzeugdatenplattform („TrustCenter“), die von einer beliehenen Stelle betrieben wird, erfolgen.*

3 *Der gesamte Prozess der Weitergabe von Fahrzeugdaten durch die herstellerunabhängige Fahrzeugdatenplattform ist unabhängig zu zertifizieren und mittelfristig zu standardisieren sowie in den internationalen Typgenehmigungsvorschriften von Fahrzeugen zu verankern.*

4 *Der Fahrzeugnutzer ist der Verfügungsberechtigte seiner Fahrzeugdaten. (DGSVO!)*

VdTÜV – Position für ein unabhängiges Mobilitätsdatenmanagement

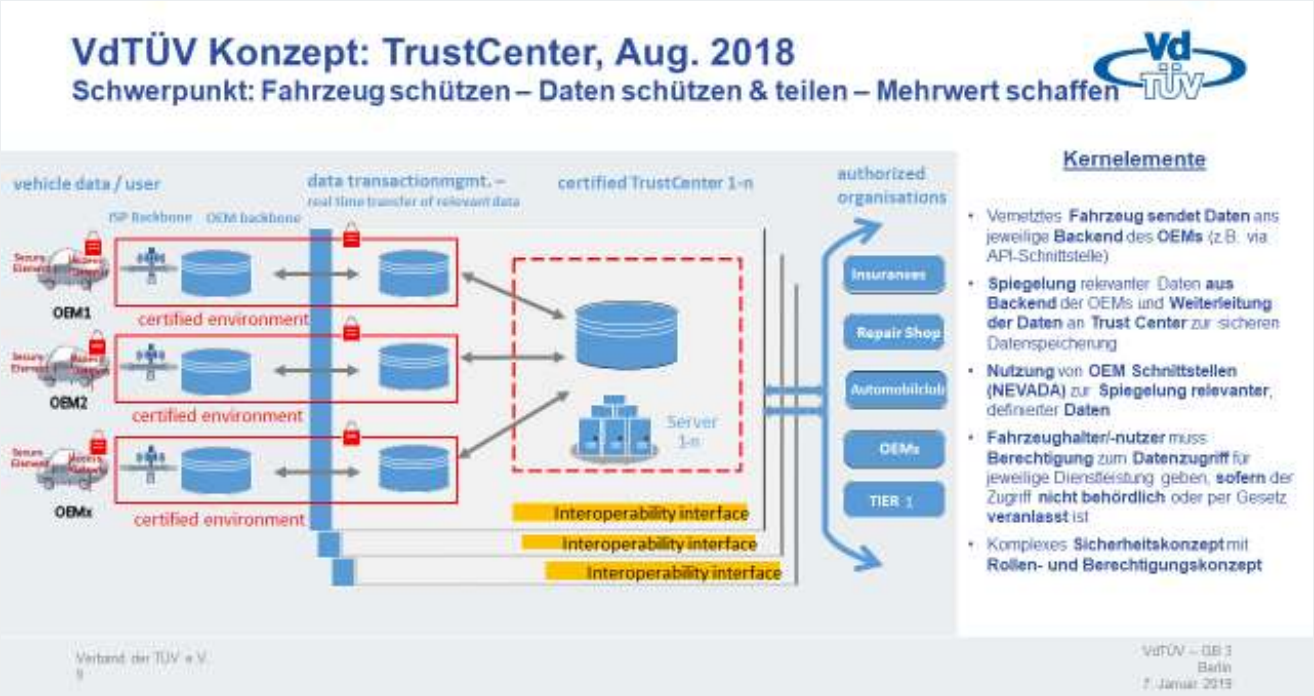
5 *Langfristig wird eine kontinuierliche Fahrzeuguntersuchung Over-the-Air als sinnvolle Ergänzung zur periodischen Fahrzeuguntersuchung angesehen.*

6 *VdTÜV drängt auf die Ausweitung des technischen Sicherheitsbegriffs bei Homologation und Überwachung. Das vernetzte Fahrzeug muss ein adäquates Automotive Security-Schutzniveau aufweisen. Hierfür müssen die regulatorischen Anforderungen erarbeitet werden.*

7 *Car2X Interactions weisen in eine vernetzte Welt: Sicherstellung der Betriebssicherheit und Zuverlässigkeit der Kommunikation zwischen Fz. und Umgebung – Regulative Anforderungen notwendig*

8 *§63a StVG Datenverarbeitung bei HAD: Daten müssen in der Hand eines neutralen unabhängigen Dritten (Datentreuhänder) sein, um allen Berechtigten unter den gleichen gesetzlichen Bedingungen Zugang zu ermöglichen.*

Next: gemeinsame TÜV-Standards erarbeiten - neue Geschäftsmodelle



- TÜV-übergreifende Sicherheitsstandards für eine Zertifizierung von Datenströmen und Cloudservices für das vernetzte Fahrzeug entwickeln – Einsetzung einer AG beim VdTÜV (Empfehlung Leitstelle Digitales)
- Prüfung des Betriebs eines gemeinsamen TrustCenters (Empfehlung Leitstelle Digitales)
- Entwicklung von TÜV-Services in der Datenveredelung durch gemeinsamen Sprint analog zu Elevator-Team (Empfehlung Leistelle Digitales)

Politik: Was getan werden sollte

Verband der TÜV e. V.

Europawahl 2019

AGENDA FÜR SICHERHEIT UND VERTRAUEN IM DIGITALEN BINNENMARKT

INDUSTRIE 4.0 UND DAS INTERNET DER DINGE

Agenda für Vertrauen und Sicherheit im digitalen Binnenmarkt

1. Industrie 4.0 und IoT: Industriestandort Europa zum Vorreiter für sichere digitale Produkte und Anlagen machen!
2. Mobilität: Sicheres vernetztes und automatisiertes Fahren - europäische Standards im Umgang mit Fahrzeugdaten setzen!
3. Künstliche Intelligenz: Vertrauen in KI-basierte Systeme und Produkte schaffen!
4. Cybersicherheit: Eine europäische digitale Sicherheitsarchitektur entwickeln!

Verband der TÜV e.V.

Danke für Ihre Aufmerksamkeit!

Dr. Joachim Bühler
T.: +49 30 760095-310
joachim.buehler@vdtuev.de

Politik: Was getan werden sollte

Agenda für Vertrauen und Sicherheit

- Wer macht was?
- Staat: BSI
- Unabhängige Dritte: TÜV etc.
- Hersteller: Software Produkthaftung

IT-Sicherheit

- Digitalcheck für Algorithmen
- Europa: Cybersecurity Act
- Produktsicherheitsbegriff um IT-Security erweitern

Digitale Sicherheitsarchitektur: Drei Säulen

Rechtsrahmen	Institutionen	Methoden
• CCA • Produktrichtlinien • BSI-Gesetz • IT-Sicherheitsgesetz • …	• BSI / ENISA • Dritte • Hersteller • Sicherheitsbehörden • Verbrauchschutz • …	• Monitoring statt Zeitpunktprüfung • TrustCenter • Datentreuhänder • Safety und Security • ….