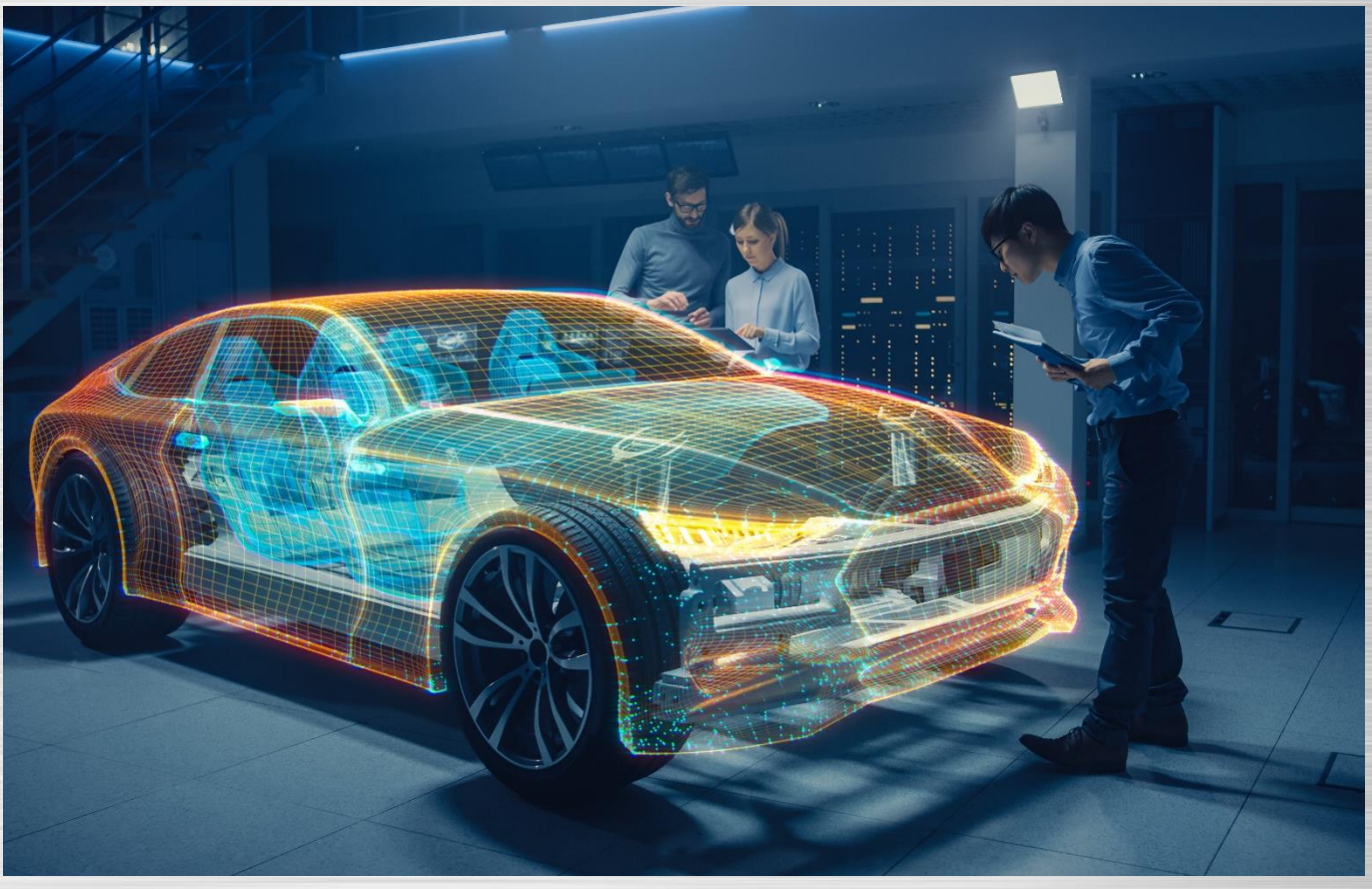

Fragenkatalog des BMWK und BMDV zum "Zugang zu Fahrzeugdaten"

Antworten Zentralverband Deutsches Kraftfahrzeuggewerbe e.V. (ZDK)

I. Datenerfassung und -speicherung

I.1 Welche Arten von Daten werden von Fahrzeugen erfasst? (Kategorisieren nach Diagnosedaten, Nutzerdaten, originären Fahrzeugdaten etc.)

Welche Daten in welcher Frequenz und Auflösung in einem konkreten Fahrzeug eines bestimmten Herstellers erfasst werden, ist Baujahr, Baureihen-, Modell- und sogar Ausstattungsabhängig. Verlässliche Informationen darüber kann daher nur der jeweilige Fahrzeughersteller liefern. Andere Marktteilnehmer können nur über eingeschränkte Beobachtung aus Sicht eines Fahrers (Anzeige des Fahrzeugs im Display oder über herstellerspezifische Apps) oder den ihnen eingeräumten Zugangsweg (Nutzung einer Diagnose-Software) begrenzte Rückschlüsse darüber ziehen, welche Daten in einem konkreten KFZ mindestens vorhanden sind.

I.2 Wie und wo werden diese Daten gespeichert?

Zu verlässlichen Informationen für ein bestimmtes Fahrzeug sei wie bei Frage I.1 auf den Hersteller verwiesen. Generell werden Daten im Fahrzeug und in den angeschlossenen Backend-Datenbanken potenziell mehrfach abgelegt. Zum Beispiel kann ein Datum „Geschwindigkeit“ aus den Sensoren an den Reifen und/oder aus GPS-Vergleichen ermittelt werden. Dieses wird dann je nach gewählter Architektur eines Herstellers weitergeleitet und gespeichert, zum Beispiel in einem Motorsteuergerät (u.a. zur Abregelung bei Maximalgeschwindigkeit), im ABS-Gerät, im TCS-Gerät und im Infotainment zur Anzeige im Display. Ein Hersteller mit stark verteilter Hardware-Architektur nutzt hierfür möglicherweise pro Anwendung (Wie ABS, TCS etc.) jeweils eine eigene Hardware. In stärker zentralisierten Architekturen wie bei Tesla können deutlich weniger Computer als Speicherorte in Betracht kommen. Nach der Weiterleitung auf das OEM-Backend hört die Duplizierung des Datums „Geschwindigkeit“ ebenfalls nicht auf. Untersuchungen (https://www.figiefa.eu/en/2018/oem-3rd-party-telematics-%E2%80%93-general-analysis.html) für die Europäische Kommission haben ergeben, dass das Datum zunächst mindestens für die interne Nutzung auf einem OEM-Backend gespeichert wird (hier mit OEM-ExVe bezeichnet). Danach wird ein Teil der Daten (möglicherweise auch die Geschwindigkeit) auf eine Datenbank kopiert, die als Aftermarket-ExVe dient. Nur vermutet werden kann aus externer Sicht, in welche weiteren Datenbanken und Anwendungen des Herstellers das Datum Geschwindigkeit noch kopiert wird.

I.3 Wie wird mit aggregierten Daten verfahren? Werden Dritten aggregierte Daten zur Verfügung gestellt?

Die Unterscheidung zwischen „Rohdaten“ und „aggregierten Daten“ ist bei genauer Betrachtung sehr schwierig und sollte daher vorsichtig verwendet werden. Um im Beispiel der Geschwindigkeit zu bleiben: Ein Radsensor an einem Rad erfasst fiktiv eine Winkelveränderung von 360 Grad an einem Rad in einer Sekunde. Die 360 Grad an Rad 1 pro Sekunde sind dann ein „Rohdatum“. Um zu einer

Geschwindigkeit an diesem Rad zu kommen, muss man als weiteres „Rohdatum“ den Reifendurchmesser kennen. Zum Beispiel 22 Zoll. Hieraus kann man eine Geschwindigkeit von 6,3 km/h bestimmen. Da gerade im Winter Reifen durchdrehen können, erfolgt wahrscheinlich auch noch eine Betrachtung der anderen Reifengeschwindigkeiten, um zu einem „aggregierten Wert“ der „über Reifen bestimmten Geschwindigkeit“ zu kommen. In Fahrzeugen mit GPS wird aus den Rohdaten „GPS-Positionen“ über eine Aggregation über der Zeit ebenfalls eine Geschwindigkeit, die „GPS-Geschwindigkeit“, berechnet. Das GPS-Signal kann ausfallen, unsicher sein, zum Beispiel im Tunnel. Die „Reifengeschwindigkeit“ kann sich bei durchdrehenden Reifen spontan oder durch Abrieb bedingter Verringerung des Reifendurchmessers kontinuierlich verändern. Was letztlich dem Fahrer als „aktuelle Geschwindigkeit“ angezeigt wird, ist potenziell dann eine komplizierte Interpolation aus beiden Werten. In dieser Hinsicht ist so etwas anscheinend Einfaches wie das Rohdatum „Geschwindigkeit“ bereits eine sehr komplexe Aggregation.

Welche Datensätze der Hersteller zur Verfügung stellt und welchen Aggregationsgrad diese Sätze besitzen, liegt im Ermessen des Herstellers selbst.

Dies zeigt sich am Beispiel des Datenpunktes “Gesundheitszustand Hochvoltbatterie”. Wegen der immensen Kosten dieses Bauteils im fünfstelligen Bereich ist eine möglichst exakte Bestimmung des Gesundheitszustands ein erheblicher Kosten- und Wettbewerbsfaktor. Aktuell konkurrieren im Markt unterschiedliche Anbieter mit unterschiedlichen Messmethoden und Algorithmen um die verlässlichste Lösung. Auch hier sollte ein Servicepartner, der den Zustand beurteilen möchte, nicht darauf verwiesen werden, dass er nur das Ergebnis des Algorithmus auf Basis der aggregierten Daten eines Konkurrenten anzeigen darf. Vielmehr sollte er Zugriff auf wesentliche Parameter der Batterie zur Bestimmung der Lebenszeit in hoher Auflösung haben, um selbst zu einer möglichst exakten Lebensdauerbestimmung zu gelangen, die er erfolgreich vermarkten kann, zum Beispiel im Rahmen von Geschäftsmodellen wie “Hochvoltbatterie as a Service”.

Zusammenfassend lässt sich sagen, dass Hersteller in unterschiedlichem Umfang Dritten auch aggregierte Daten zur Verfügung stellen, diese aber immer auch die Innovation in den betroffenen Bereichen stark einschränken, wenn nicht zusätzlich ein Zugriff auf die zugrundeliegenden Rohdaten gewährt wird, der in den meisten Fällen auch mit den heute eingesetzten Plattformen und Technologien im Auto problemlosmöglich ist.

I.4 Haben Dritte die Möglichkeit Daten im gleichen Umfang wie der Fahrzeughersteller zu erhalten? Welche Unterschiede zeichnen sich ab?

Unter Datenerhalt ist in dieser Frage anscheinend zunächst der nur lesende Zugriff auf ein Datum gemeint.

Beim Datenzugriff existieren neben dem reinen Umfang der Daten, die ein Serviceanbieter erhalten kann, auch andere kommerziell bedeutsame Kriterien wie zum Beispiel die Frequenz (Häufigkeit der

Datenübermittlung an Serviceanbieter), die Latenz (absoluter Zeitverzug: Rechtzeitigkeit um Service erbringen zu könne. Relativer Zeitverzug: Verzug im Vergleich zu potenziellen Mitbewerbern) aber auch Verfügbarkeit des Datenzugriffs (Schnittstelle innerhalb und außerhalb des Fahrzeuges).

Frequenz: Liefert ein serverbasiertes System zum Beispiel Geschwindigkeits- und Positionsdaten nur jede Minute, so ist augenscheinlich klar, dass damit keine alternative Navigationslösung entwickelt werden kann. Dies ist ein Beispiel für ein absolut (in Bezug auf einen Service) nicht erfülltes Datenzugriffskriterium.

Latenz: In der oben genannten ExVe-Studie für die Europäischen Kommission wurde ermittelt, dass ein Hersteller servicerelevante Informationen in bestimmten Situationen nur alle 48 Stunden von seinem ExVe, auf das ExVe für den Aftermarket transferiert hat. Offensichtlich kann in diesem Fall das im Wettbewerb zum Aftermarket stehende Servicekonzept des Herstellers dem Fahrer schon 48 Stunden vor einem Mitbewerber Angebote unterbreiten. Dies ist ein Beispiel für ein relativ (in Bezug auf den Mitbewerber) nicht erfülltes Qualitätskriterium.

Wenn daher die Frage wie folgt präzisiert wird: „Haben Dritte die Möglichkeit, Daten in gleichem Umfang und gleicher Qualität wie der Hersteller zu erhalten?“, dann gilt dies offensichtlich nur, wenn die exakt gleichen technischen Zugangskanäle/Systeme genutzt werden.

Die physikalische Geschwindigkeit eines Fahrzeugs beispielsweise ist eine objektiv vorhandene Eigenschaft. Die technische Messung über „Reifengeschwindigkeit“ und „GPS-Geschwindigkeit“ ist durchaus komplex. Das Datum selbst liegt im Auto in unterschiedlichen Formaten mit unterschiedlichen Frequenzen und Latenzen vor. Am OBD-Port beispielsweise kann es über den normierten eOBD-Parameter 13 als ein Byte-Wert im Bereich von 0 bis 255 km/h abgefragt werden. Höhere Geschwindigkeiten als 255 km/h, wie sie manche Sportwagen erreichen, sind hier nicht darstellbar, genauso wenig wie negative Geschwindigkeiten beim Zurückrollen oder eine höhere Auflösung wie 201,37 km/h.

Das OBD-Datum der Geschwindigkeit ist daher nicht „perfekt“, wenn jedoch an dem Zugangskanal OBD-Port per Stecker sowohl ein OEM- als auch ein IAM-Gerät den gleichen Zugriff haben, müssen beide Anbietertypen von Diagnosediensten mit der gleichen Datenzugriffsqualität arbeiten.

Innerhalb des in modernen Fahrzeugen sehr verbreiteten Betriebssystems Android Automotive hingegen wird die Geschwindigkeit als ein weiteres Datum „PERF_VEHICLE_SPEED“ gespeichert. Hier sind sowohl positive wie negative Geschwindigkeiten darstellbar, die Geschwindigkeit ist nicht auf 255km/h begrenzt und durch die Nutzung des Datentyps „float“ ist auch die Auflösung höher. Hier kann ohne Probleme eine Geschwindigkeit von z.B. 91,25 m/s (entspricht 328,5 km/h) dargestellt werden. (https://developer.android.com/reference/android/car/VehiclePropertyIds#PERF_VEHICLE_SPEED)

Zudem räumt Android den Herstellern ein, nicht diese nach bestmöglichem Aufwand bestimmte „echte Geschwindigkeit“ anzuzeigen, sondern eine davon abweichende Geschwindigkeit „PERF_VEHICLE_SPEED_DISPLAY“ (eventuell überhöht, damit eine Anzeige niemals zu wenig Geschwindigkeit anzeigt), die dem Fahrer im Display dargestellt wird.

Der Zugangskanal „Android Automotive“ erlaubt es allen Apps, die dafür entwickelt wurde, auf diese beiden Daten (aktuelle und darzustellende Geschwindigkeit) zuzugreifen.

Zusammenfassung: Dritte haben im Vergleich zum Hersteller nur die gleichen Möglichkeiten zur Entwicklung Digitaler Dienste, wenn beide Parteien die gleichen Zugangskanäle/Systeme nutzen, um in gleicher Qualität auf die potenziell vielfach im Fahrzeug und im Backend gespeicherten unterschiedlichen Daten zu einer physikalischen Fahrzeugeigenschaft zuzugreifen.

Dies erfolgt schon seit Jahren bei der gleichberechtigten Nutzung des OBD-Ports und muss daher konsequenterweise auch für die neuen Zugriffskanäle/Systeme im Auto gelten (Android Auto, Apple CarPlay, Android Automotive, ICAS-Server beim Volkswagen ID etc.), wenn diese Gleichberechtigung zur Förderung von europäischer Innovation und Wettbewerbsfähigkeit Bestand haben soll.

I.5 Unter welchen Voraussetzungen und in welchem Umfang wird aktuell Dritten ein direkter Zugriff auf im Fahrzeug verarbeitete oder gespeicherte Daten sowie auf Funktionen und Ressourcen (DFR) des Fahrzeugs gewährt? Welche konkreten Hürden und Anforderungen gibt es?

Der Begriff „direkter Zugriff“ ist in der IT eher unüblich und schwer zu definieren. Sieht man sich im Detail den Weg an, den ein Aufruf einer IT-Funktion wie „OpenDoors()“ nimmt, bevor sich im Fahrzeug die Türen entriegeln, passiert dieser Aufruf eine ganze Anzahl von weiteren Funktionen, IT-Systemen und Sicherungsschichten. Sinnvoller sind hier die Unterscheidungen zwischen Aufrufen, die zur Laufzeit immer über ein externes System wie ein OEM-Backend laufen müssen (Offboard-Zugriffe) und Aufrufen, die ohne ein externes System auskommen, weil die aufrufende Software zum Beispiel als IAM-App im Android-Automotive läuft (On-Board-Zugriffe).

On-Board-Zugriffe wie zum Beispiel über Apps sind nicht weniger sicher als Offboard-Zugriffe, weil – genau wie bei „normalen“ Smartphone-Apps – die zugreifende Software (App) zunächst dem Betreiber der Plattform (hier dem OEM) zur detaillierten Prüfung vorgelegt werden muss. Nur nach bestandener Prüfung erteilt der Hersteller die Freigabe.

Dies gilt im Übrigen für alle (!) Apps, die in einem Android-Automotive Betriebssystem laufen, völlig egal, ob diese vom OEM selbst, seinen Zulieferern oder externen Anbietern erstellt wurden. Alle Apps müssen die gleichen Designvorgaben einhalten, die gleichen Sicherheitschecks bestehen, bevor sie per App-Store für Nutzer verfügbar gemacht werden.

Bei Offboard-Zugriffen über externe Backends erfolgt eine derartige Prüfung der zugreifenden Fremdsoftware üblicherweise nicht, in diesem Sinn sind diese sogar „unsicherer“ als On-Board-Systeme.

Der bekannteste „On-Board“-Zugriff, der aktuell gewährt wird, ist der OBD-Port. Aufgrund von Sicherheitsbedenken gegenüber Fremdsoftware haben sich die Hersteller jedoch dazu entschlossen, durch Verschlüsselung und Freischaltung per Zertifikat nur für „Trusted Partner“ auch hier in die sonst übliche Prüfung der zugreifenden Systeme einzusteigen. Details sind hierzu in vertraulichen B2B-Verträgen hinterlegt.

Die „Offenheit“ anderer Zugriffskanäle wie Android Auto etc. kann wegen der Gestaltungsfreiheiten der Vertragsparteien in den B2B-Verträgen aktuell nur tendenziell beurteilt werden.

In den fahrernahen Systemen wie Apple CarPlay und Android Auto dominieren aktuell noch Infotainment-Anwendungen wie Spotify, die keine oder sehr wenig Fahrzeugdaten benötigen. Die Zahl der IAM-Anwendungen ist hier begrenzt. Im Bereich der e-Laden-Apps existieren bereits einige Anwendungen, die auch im Auto dargestellt werden können.

In den fahrzeugnahen Systemen wie Android Automotive oder den ICAS-Servern sind noch weniger Anwendungen bekannt, auch wenn zum Beispiel unabhängige Diagnoseanbieter die Möglichkeiten des ICAS-Servers nutzen könnten, um eine leistungsfähige on-Board-Echtzeit-Diagnose zu entwickeln, die als Konkurrent zu den neuen On-Board-Diagnosesystemen der Hersteller alternative Diagnosen und Reparaturen anbieten könnte.

Im Bereich der Offboard-Systeme über OEM-Backends sind die Art und der Standardisierungsgrad der angebotenen Funktionen und Datenpunkte noch unzureichend, um nachhaltig Dienstanbieter anzuziehen. Ein Ausweis hierfür sind die finanziellen Probleme, in die internationale Anbieter wie WeJo und Otonomo geraten sind oder die Unternehmenszahlen Deutscher Datenmarktplatzanbieter wie High-Mobility oder Caruso, wie sie zum Beispiel bei Northdata einsehbar sind.

Es scheint so zu sein, dass OEMs versuchen, da ertragsreiche Service- und Ersatzteilgeschäft unter Nutzung der neuen Technologien exklusiv für sich zu nutzen, indem sie als Ergebnis von Echtzeitdiagnosen dem Fahrer Service und Wartungsangebote direkt ins Display einspielen. Andere Anbieter werden hier nur zugelassen, wenn sie ein Komplementärportfolio wie Entertainment anbieten. Die etablierte Konkurrenz wie IAM-Diagnose wird auf die überholte OBD-Technik oder die im Gegensatz zu On-Board-Lösungen nicht wettbewerbsfähige Offboard-ExVe-Alternative verwiesen.

I.6 Welche Datenübertragungstechnologien werden genutzt und welche Standards bzw. Schnittstellen existieren für die Datenübertragung vom Fahrzeug in das OEM-Backend sowie für den Datenaustausch zwischen Fahrzeugen verschiedener Hersteller und Modelle?

Dies ist grundsätzlich eine Frage an die Hersteller.
Ein Datenaustausch zwischen Fahrzeugen verschiedener Hersteller findet aktuell nicht statt. Es existieren jedoch Bestrebungen von Initiativen wie Covesa mit dem VSS-Standard, alternative Standards zu den API und Daten-Standards von Google zu entwickeln.
Im Kleinen versuchen Anbieter wie Caruso oder High Mobility auch, hier eine Vereinheitlichung zu ermöglichen. Diese nachträgliche Offboard-Vereinheitlichung ist aber von Natur aus in den Möglichkeiten deutlich begrenzter als eine On-Board Vorabstandardisierung wie die von Googles Android Automotive.
Anwendungen von Service-Anbietern, die On-Board auf Android Automotive laufen, können sich darauf verlassen, dass das Google-API ihnen einen einheitlichen Satz von Daten und Funktionen in definierter Qualität zur Verfügung stellt, egal, auf welchem Fahrzeug dieses System läuft. Aus dem gleichen

Grund interessieren sich auch App-Entwickler von Smartphone-Apps bei Google nur für die Android-Version, aber nicht für Hersteller oder Modell des Smartphones.
Ein Offboard-Anbieter wie Caruso oder High Mobility kann aber Daten und Funktionen nur in Umfang und Qualität auf den kleinsten gemeinsamen Nenner aller beteiligten Fahrzeuge vereinheitlichen.
Für die Betreiber der Marktplätze wie für die Anbieter von Services ist auf dieser Basis keine Entwicklung von Geschäftsmodelle möglich.
Mit den wenigen Daten und Funktionen, die es in jedem Kfz von jedem Hersteller gemeinsam in der Mindestqualität (also geringster Frequenz und höchster Latenz) gibt, lässt sich kaum ein softwaretechnisch leistungsfähiges Konkurrenzprodukt zu On-Board-Lösungen wie Android Automotive bauen. Verzichtet man darauf und adressiert nur softwaretechnisch leistungsfähige Modelle weniger Hersteller, dann zerfällt die Kundengruppe in zu kleine Segmente, als dass sich die Service-Entwicklung lohnt.
Ein Smartphone-Entwickler für Android kann heute über eine Milliarde potenzieller Kunden erreichen, es wird kaum jemanden geben, der einen ähnlichen Aufwand nur die Besitzer der aktuellen Premium-Modelle von zwei deutschen Herstellern betreibt.

I.7 Mit welchen Technologien und sonstigen Verfahren oder Anforderungen werden Fahrzeugdaten geschützt, auf die Dritten ein direkter Zugriff gewährt wird? In welcher Hinsicht unterscheiden sich diese Technologien, Verfahren und Anforderungen vom direkten Zugriff der OEM auf Fahrzeugdaten?

Die vom OEM realisierten Schutzkonzepte sind individuell und in weiten Teilen vertraulich. Aus Sicht des IAM ist es nur wichtig, festzustellen, dass der IAM nur eine konsequente Gleichbehandlung an jedem Zugriffskanal fordert, den auch ein OEM im Zuge des Anbietens von Aftermarketdienstleistungen nutzt. Hier folgt der IAM auch genau den gleichen Sicherheitsvorschriften und -prozessen, die der OEM für die eigenen Anwendungen oder die Anwendungen seiner Zulieferer aufgestellt hat.
Der ZDK fordert daher kein neues Zugriffssystem nur für den IAM und auch keine eigenen Sicherheitsvorschriften, keine eigenen Entwicklungs- oder Betriebsprozesse.

I.8 Wie wird aktuell sichergestellt, dass Fahrzeugdaten nur für legitime Zwecke verwendet werden? Welche Maßnahmen werden ergriffen, um die Privatsphäre bzw. den Datenschutz der Fahrzeugnutzer zu gewährleisten?

Herstellerseitig wird für den Zugriffskanal ExVe versucht, Daten pro Use Case vorab zu clustern. Der Serviceanbieter wird dann im Vertrag dazu verpflichtet, die Nutzung auf diesen Use Case zu begrenzen.

Teilweise existieren auch Anforderungen, dass ein Anbieter schon eine vorherige Tätigkeit in diesem Bereich nachweisen muss.

Dieser Ansatz greift aus Sicht des ZDK aus mehreren Gründen zu kurz.

1. Er ist im Sinne des Datenschutzes des Nutzers rechtlich überflüssig. Die DSGVO regelt ohnehin schon, dass Daten im Sinne der Datensparsamkeit nur für den vom Nutzer akzeptierten Use Case genutzt werden dürfen. Diese Zustimmung erteilt jeder Smartphone Nutzer nach dem Installieren einer App beim Ansehen und Akzeptieren der AGB. Eine zusätzliche Verpflichtung von Seiten des Herstellers ist aus Sicht der Kunden entbehrlich.
2. Er ist wettbewerbsrechtlich bedenklich. Diese Vorabclusterung in Use Cases dient vermutlich eher dazu, aus Sicht der Hersteller unerwünschte Serviceangebote in Konkurrenz zu seinen eigenen Lösungen zu erschweren. Mindestens für gesetzlich mandatierte Konkurrenz nach GVO und Typgenehmigung erscheint dieses Vorgehen bedenklich.
3. Er begrenzt Innovation. Wenn Anbieter innovative Ideen haben, auf deren Basis sie aus vorhandenen Funktionen und Daten einen Dienst erbringen können, sollte der Zugriff nicht auf die wenigen Daten und Funktionen eingeschränkt werden, von denen der Hersteller ausgeht, sie würden für einen bestimmten Use Case ausreichen.

Ein fiktives Beispiel: Voraussage eines Termins zum Reifenwechsel.
Ein Hersteller meint, dafür würden die Werte „Letzter Reifenwechsel“, „Typ des Reifens“ und „aktueller Kilometerstand“ ausreichen.
Ein innovativer Reifenanbieter A möchte aber gerne noch die aktuellen Beschleunigungen, Geschwindigkeiten erfahren (Beanspruchung des Reifens) um die Abnutzung präziser zu nutzen.
Der innovativere Anbieter B hätte benötige zusätzlich die GPS-Positionen, um aus Kenntnis der Straßen (Wo wird hart gefahren?) zusätzliche Genauigkeit der Vorhersage abzuleiten.
Der innovativste Anbieter C wählt einen ganz anderen Weg. Er möchte den Zugriff auf die Reifengeschwindigkeit und die GPS-Geschwindigkeit separat. Da die Reifengeschwindigkeit den Raddurchmesser als konstant annimmt, wird sich die Reifengeschwindigkeit stetig gegenüber der GPS-Geschwindigkeit erhöhen, wenn sich der Reifen abnutzt und der Durchmesser sinkt. Das Rad muss dann deutlich schneller drehen, um die GPS-Geschwindigkeit zu erreichen.

Fazit: Das Vorgeben von Daten pro Use Case erhöht weder den Datenschutz des Nutzers noch fördert es die dringend nötige Innovation im europäischen Automotive-Sektor. Daher wird auch von Anbietern wie Google keine solche Kategorisierung vorgegeben. Allen App-Entwicklern und Services stehen die gleichen Funktionen und Daten der Plattform zur Verfügung.

II. Anforderungen an eine potenzielle EU-Sektor-Regulierung (SSL)

II.1 Welchen Anwendungsbereich sollte eine mögliche SSL haben? Wo besteht ein Regelungsbedarf bzw. existiert eine Regelungslücke?

Eine SSL sollte die GVO und Typgenehmigung ergänzen und so an den technischen Fortschritt und die damit notwendigen Prozesse, Geschäftsmodelle und den Umgang mit neuen Bedrohungen anpassen. Dem Sinn nach definiert die GVO die Bereiche im Automotive Sektor, in dem Wettbewerb gewünscht ist (Services, Ersatzteile). Die Typgenehmigung definierte die dafür notwendigen Prozesse, Informationen und Systeme sowie Geschäftsmodelle nach dem Stand der Technik von 2018. Charakteristisch für die damalige Zeit war das Fahrzeug als „offenes System“, ein geringer Digitalisierungsgrad mit einem geringen Überwachungsgrad, ein relativ langsamer technischer Wandel und ein erheblicher „Graubereich“.

Im Bereich der Werkstatt und Diagnoseservices reichte als Zugriffssystem der OBD-Port. Die Bereitstellung von Informationen zur Reparatur oder zur Entwicklung von Diagnosegeräten erfolgte unidirektional vom Hersteller als Einmallieferung oder als Abo auf Webseiten.

Deshalb war auch das Geschäftsmodell sehr einfach. Zu – immer weiter steigenden – FRAND-Preisen konnte ein Anbieter Anleitungen erwerben und damit Diagnose- und Werkstattdienste anbieten.

Einfache Ersatzteile wie Ölfilter wurden „reverse Engineered“, bei komplexeren Teilen erhielt der gewählte Zulieferer im Rahmen eines B2B-Agreements vom OEM das Recht, das gleiche Produkt unter eigenem Label auch als Aftermarketteil anzubieten. Eine einmalige oder gar kontinuierliche Prüfung von entwickelten Aftermarketlösungen vom Ersatzteil bis zur Diagnoselösung fand kaum statt.

Mit dem technischen Fortschritt in den letzten Jahren hat sich die Situation dramatisch verändert.

1. Es entstehen neue Zugriffssysteme wie Android Automotive, ICAS etc.
2. Es kommen neue Bedrohungsrisiken durch Cyberattacken hinzu.
3. Parallel kann durch die technischen Möglichkeiten wie elektronische Zertifikate jedes Ersatzteil und jedes zugreifende System authentifiziert und autorisiert werden. Das Fahrzeug und alle angeschlossenen Serviceanbieter werden so zum total überwachten digitalen oder digitalisierten Ökosystems unter Kontrolle des Herstellers.
4. Die Änderungszyklen der Software von OEM, Zulieferern und Anbietern werden immer kürzer. Trotzdem muss zu jeder Zeit das Gesamtsystem sicher funktionieren. Die Zusammenarbeit über die gesamte Lebensdauer eines KFZ wird daher deutlich intensiver. De Facto gibt es dann keine Dritte mehr, da freie – genau wie vom OEM ausgewählte – Anbieter stets entlang eines einheitlichen Vertrags-, Prozess- und Sicherheitsvorgehens arbeiten müssen.

5. Ultimativ müssen sich dann auch die Geschäftsmodelle anpassen, möglicherweise im Sinne eines kontinuierlichen Umsatzsplits zwischen Herstellern und Serviceanbieter statt der umsatzunabhängigen Einmalzahlungen.

Die SSL muss definieren, für welche Bereiche innerhalb des Autos (Apps, Ersatzteile) und außerhalb (Reparatur etc.) Wettbewerb mit einem einklagbaren Recht auf Teilnahme gelten soll und wo ein Hersteller ausschließlich seine Lieferanten nach B2B-Gesichtspunkten wählen darf.

II.2 Welchen Anwendungsumfang sollte eine mögliche SSL haben? Welche Zugänge zu DFR werden konkret benötigt und von wem?

Wie in den vorherigen Antworten dargestellt, sollte jedem Zugriff nach den gleichen Standards auf die gleichen Systeme gewährt werden, die ein Hersteller im Rahmen dieser Services nutzt. Hierfür muss die SLL den rechtssicheren Rahmen darstellen.

Wichtig ist, dass die SSL nicht festschreiben sollte, dass ein neues System, ein neuer Prozess oder eine neue Sicherheitsrichtlinie nur für „Dritte“ entwickelt oder genutzt wird. Es werden lediglich die vorhandenen Systeme genutzt.

II.3 Welche dieser zusätzlichen Daten könnten sicherheitskritisch sein und warum? Wie kann sichergestellt werden, dass nur zugriffsberichtigten Dritten der Zugang zu DFR gewährt wird?

Jede Software, die Zugriff auf jedwede Systeme, die ein Hersteller nutzt, erhält, kann grundsätzlich vom Hersteller vorab geprüft und freigegeben werden. Es sei denn, dieser hält eine solche Prüfung aufgrund der sonstigen Sicherheitselemente in seinem Fahrzeug für entbehrlich.

Wie streng die Prüfvorgaben sind, hängt offensichtlich von der Kritikalität eines Systems ab, wie „nah“ am Fahrzeug es angesiedelt ist. Eine Entertainment-App in der weitgehend abgeschotteten Sandbox Apple CarPlay wird weniger Prüfaufwand erfordern als die Freigabe einer unabhängigen Diagnoseapp im ICAS-Server.

Es darf jedoch nicht er Zustand entstehen, dass ein System wie ein ICAS-Server generell als „Sicherheitskritisch“ eingestuft wird, um damit jeden Zugriff durch „Dritte“ zu verbieten. Denn moderne Fahrzeuge sind hochgradig vernetzt. Ein Jeep beispielsweise wurde durch das Infotainment-System gehacked, aktuell wurden gerade viele Nutzerdaten vom Volkswagen-Backend gestohlen. Es gibt daher kein System, was per se „Sicherheitsunkritisch“ wäre. Grundsätzlich sind alle Systeme „sicherheitskritisch“. Diese gilt sowohl für Anwendungen und Services des OEMs wie denen des IAM.

Des Weiteren ist es auch nicht so, dass „Dritte“ generell weniger kompetent oder vertrauenswürdig sind als ausgewählte Zulieferer. OEMs entwickeln On-Board-Diagnosen auch nicht selbst, sondern

durch Zulieferer. Wenn jetzt fiktiv ein Zulieferer A diese Software für den ICAS-Server im Auftrag des OEM selbst entwickelt hat, sollte seine womöglich in der gleichen Abteilung entwickelte Version für den Aftermarket nicht weniger leistungsfähig oder vertrauenswürdig sein. Zumal sie vor einer Freigabe wie jede andere App nach den exakt gleichen Prozessen und Sicherheitsvorgaben vom OEM erneut getestet werden würde.

II.4 Können Sie konkrete Use-Cases benennen, für die ein direkter Zugriff auf Fahrzeugdaten, Funktionen oder Ressourcen für erforderlich erachtet wird? Falls möglich, wie müsste ein alternativer Zugang zu Fahrzeugdaten ausgestaltet sein, um die genannten Use-Cases unter gleichen Wettbewerbsbedingungen zu ermöglichen?

Wie oben beschrieben: Nur gleicher Zugriff auf die gleichen Systeme nach gleichen Prozessen sichert Innovation im Europäischen Automotive Sektor und damit dessen Wettbewerbsfähigkeit gegenüber der Konkurrenz aus den USA und Asien.

II.5 In welchen Use-Cases wird auch ein schreibender Zugriff auf Fahrzeugdaten für notwendig erachtet? Wenn ja, in Bezug auf welche Daten? Welche Daten davon sind sicherheits- bzw. typgenehmigungsrelevant?

Im Allgemeinen zahlt ein Kunde immer nur für Services an seinem Auto, die etwas „verändern“. Jeder Ölwechsel wird in einem digitalen Wartungsheft eingetragen. Jedes neue komplexere Ersatzteil muss angelernt, also im Fahrzeug registriert werden. Jede neue App, selbst wenn es sich nur um Spotify handeln sollte, wird „schreibend“ in einem Kfz-Computer abgelegt und verändert „schreibend“ die Anzeige in Displays. Grundsätzlich verändern die Dienstleistungen der Serviceanbieter (egal, ob Inspektion, App oder Ersatzteiltausch) das Fahrzeug immer.

Es gibt nur wenige Dienste, die sich nur durch lesenden Zugriff auf Daten bereitstellen lassen. Strenggenommen ist aber auch ein lesender Zugriff ein verändernder Zugriff und damit potenziell sicherheitskritisch. Denn ein verbreitetes Werkzeug von Cyberkriminellen ist die Denial of Service Attack, in der ein System „nur lesend“ zu viele Anfragen erhält. Da diese Anfragen die Prozessor- und Buslast erhöhen und die Servicebereitschaft bis zum Erliegen bringen können, ist offensichtlich auch ein „Nur-Lese-Zugriff“ nicht immer unkritisch.

Der Unterschied zwischen lesendem und schreibendem Zugriff ist genauso unscharf wie der zwischen sicherheitskritischen und unkritischen Systemen.

Es ist deshalb anzunehmen, dass jedes System und jeder Zugriff darauf sicherheitskritisch ist und gemäß dem Sicherheitskonzept des OEMs abzuwickeln ist, das einheitlich (!) für jede Software von jedem Anbieter anzuwenden ist, die auf diesem Zugriffsystem laufen soll.

Zur Typgenehmigungsrelevanz von Daten:

Genau wie jedes System auf seine Sicherheit zu prüfen ist, muss für jeder Dienst, jede App, jedes Ersatzteil von Seiten des Herstellers geprüft werden, ob potenziell durch die Nutzung typgenehmigungsrelevante Eigenschaften geändert werden könnten. Wenn ja, sind die entsprechenden Genehmigungen einzuholen.

Dies kann aber erneut in der Regel nur auf Basis des gesamten Services beurteilt werden und nicht anhand des Zugriffs auf bestimmte Daten und Funktionen. Eine Verschlechterung des CO2-Ausstoßes wird beispielsweise ja nicht durch einen „schreibenden Zugriff“ auf den Parameter „CO2-Emission“ ausgelöst, sondern dieser kann sich als Reaktion auf eine Vielzahl möglicher Änderung verändern.

II.6 Wie hoch wäre der Aufwand für die Bereitstellung dieser zusätzlichen Daten?

Der ZDK fordert keine Bereitstellung zusätzlicher Daten, die der OEM nicht ohnehin erhebt. Der ZDK fordert auch keine Entwicklung dezidierter Systeme nur für den IAM. Die einzige Forderung ist die konsequente Nutzung aller vorhandenen (!) technischen Möglichkeiten zur Entwicklung von innovativen Diensten nach den vorhandenen (!) Prozessen und den vorhandenen (!) Sicherheitsvorgaben.

Damit ist kein zusätzlicher Investitionsaufwand der OEMs in Fahrzeugsysteme oder Backendsysteme nötig.

Lediglich sollten die vorhandenen Prozesse auf Seiten der OEMs für die Registrierung von Lieferanten/Dienstanbietern, für die Prüfung von Services und Produkten stärker automatisiert werden, um mit der potenziell größeren Menge an Anbietern umzugehen.

Diese Automatisierung würde sich im Übrigen aber auch schon für die bestehende Lieferantenstruktur lohnen, da hierdurch die Prozessreife und die Cybersicherheit generell steigen.

II.7 Welche Standards oder Schnittstellen sollte die SSL definieren (z.B. Mindestdatensatz, Formate etc.)? Wie könnte die Definition ausgestaltet werden?

Grundsätzlich basiert ein digitales Ökosystem immer auf einem einheitlichen Standard. Vor diesem Hintergrund ist es hochgradig sinnvoll, Standardisierungen, wie sie auch die Automotive Welt erfolgreich umgesetzt hat (s. z.B. AUTOSAR) auch für eine SSL als Gegenpart zur Dominanz von Google zu entwickeln.

Vielversprechende Ansätze hierzu hat das W3C zusammen mit Genivi/Covesa im Standard VSS und VISS geleistet.

Zwei zeitliche Aspekte erfordern hier jedoch besondere Beachtung:

1. Der Standard sollte von Institutionen wie Covesa oder CEN kontinuierlich weiterentwickelt werden, um mit der technischen Konkurrenz aus China und den USA mithalten zu können. Hier sind deutlich häufigere Updates nötig, als sie beispielsweise bei eOBD erfolgen mussten.
2. Wichtiger als die Verabschiedung eines Standards, der trotz der Vorarbeiten noch finalisiert, abgestimmt und realisiert werden muss, ist die unverzügliche Öffnung aller vorhandenen technologischen Systeme nach gleichen Prozessen und Sicherheitsstandards, wie in der SSL gefordert. Zusätzlich sollte mindestens ein von Anbieter oder Hersteller wählbares Default-Geschäftsmodell angeboten werden müssen, das in seinen Parametern vom Gesetzgeber reguliert wird. Wenn beiden Parteien bewusst ist, wie man in der „Coopetition“ gemeinsam kommerziell erfolgreich ist, dann wird sich auch die grundsätzlich kommerziell lohnende Standardisierung beschleunigen.

Lässt man das Geschäftsmodell offen, wird aus Skepsis eben nicht am Standard gearbeitet, weil beide Parteien nicht wissen, was man ultimativ von der Nutzung kommerziell erwarten kann.

II.8 Welche Rahmenbedingungen sollten für den Zugang gelten? Welche bestehenden Konzepte des Datenzugangs könnten auch im Rahmen der SSL relevant sein? Wie können bestehende Konzepte mit einer SSL verbunden werden?

Jedes bestehende oder neue System, was vom Hersteller oder seinem Lieferantennetzwerk zur Bereitstellung von Diensten genutzt wird, für die die SSL/GVO Wettbewerb fordert, muss nach den gleichen Regeln und Prozessen auch von Konkurrenzanbietern nutzbar sein.

II.9 Gibt es weitere wichtige Punkte, die eine SSL regeln sollte?

Der neben oder sogar vor der Technik wichtigste Punkt ist das wählbare Geschäftsmodell. Beispielsweise kann eine Umsatzbeteiligung je nach Servicekategorie vorgeschrieben sein. Anbieter und Hersteller sind völlig frei, andere Modelle mit anderen Parametern zu vereinbaren. Trotzdem sollte für die Partner das Recht bestehen, sich auf dieses vorgeschriebene Modell zurückzuziehen. Der andere Partner hätte in Bezug auf dieses Modell einen Kontrahierungszwang. Dieses Vorgehen ist nicht neu, sondern findet sich in ähnlicher Form in der EU-Roamingregelung, wo neben Prinzipien „Roam like at home“ auch feste Oberwerte pro Service vorgeschrieben sind. Verwandte Konzepte finden sich auch in der EU-Regelung zu AFIR, wenn es um Ladestrompreise für Spontankunden geht.

III. Verhältnis zu anderen Regulierungen

III.1 Der Data Act stellt die Grundlage für eine mögliche SSL dar. An welchen Stellen gibt es Ergänzungsbedarf? An welcher Stelle sollte es vom Data Act abweichende Regelungen geben? An welcher Stelle sollte an gesetzgeberischen Entscheidungen des Data Act festgehalten werden? An welcher Stelle könnten sich potenzielle Kollisionen oder Widersprüche ergeben?

Die SSL muss eher eine Anpassung der GVO/Typgenehmigung an den technischen Fortschritt darstellen als eine Detaillierung des Data Act. Der Data Act hat einen Fokus auf Datenzugriff, digitale und digitalisierte Serviceerbringung im Verbund aus Hersteller (dem Plattformanbieter der Plattform Kfz) und Diensteanbieter erfordert deutlich mehr, um neben Cybersicherheit auch Aspekte wie Funktionszugriff, Typgenehmigungsrelevanz, Verantwortung/Garantie etc. erfolgreich abbilden zu können.

III.2 Sehen Sie weitere mögliche Synergien oder Widersprüche zu bestehender Regulierung oder Regulierungsvorhaben (z.B. Anh. X der Typgenehmigungs-Verordnung)?

Die enge Verwandtschaft zur Typgenehmigung wurde bereits erläutert. Zusätzlich hat eine SSL wegen des starken Fokus auf den IT-Fortschritt auch eine enge Verwandtschaft zur Plattformregulierung der EU in Digital Service Act und Digital Markets Act. Sie ist in dieser Hinsicht die Anwendung der Plattformgesetzgebung auf die „Plattform Auto“. Als wichtige Forderungen hieraus seien zu nennen:

1. Gleichberechtigung vor den Kunden: Gemäß den genannten Vorschriften dürfen auf Plattformen wie zum Beispiel Google Serviceangebote wie Google-Maps des Plattformanbieters nicht prominenter vor den Kunden platziert werden als Alternativen wie Waze. Analoges würde im Fahrzeug zum Beispiel für Wartungsapps oder Charging-Apps gelten, die Kunden bei identifizierten Problemen im Fahrzeug oder Ladebedarf entweder zu den Angeboten des OEMs oder zu Alternativen leiten würden.

2. Gleichberechtigung im Zugriff auf die Plattform: In DSA/DMA ist definiert, dass ein Hersteller seinen Anwendungen, die in Konkurrenz zu Alternativen stehen (wie eben Google Maps auf Android-Smartphones oder Microsoft Edge auf Windows-Systemen), keinen exklusiven Zugriff auf bestimmte Daten und Funktionen der untergelagerten Systeme einräumen darf, um hierdurch seine Angebote gegenüber den Alternativen aufzuwerten. Das gleiche Prinzip muss die SSL fordern. Jedes Zugriffssystem ist allen Anbietern in gleichem Umfang in Bezug auf Daten- und Funktionszugriff zu öffnen.

Zentralverband Deutsches Kraftfahrzeuggewerbe (ZDK)

Der ZDK in Bonn, Berlin und Brüssel vertritt die berufsständischen Interessen von 39.370 Autohäusern; Karosserie- und Kfz-Meisterbetrieben mit 470.000 Beschäftigten. Im Jahr 2023 erzielten die im ZDK organisierten Betriebe einen Umsatz von rund 211,4 Milliarden Euro mit dem Verkauf neuer und gebrauchter Fahrzeuge sowie mit Wartung, Reparatur und Service. Bei der Ausbildung ist der ZDK mit über 95.500 Auszubildende im Handwerk führend.