VDA Verband der Automobilindustrie

Position

ADAXO: Automotive Data Access – Extended and Open

VDA-Konzept für den Zugriff auf fahrzeug-generierte Daten

Inhalt

I Zusammenfassung

1. Innovationen durch Daten – Data Value Chain: von der Generierung der Daten bis zum Serviceangebot für den Kunden

Die im VDA vertretenen Unternehmen bieten schon jetzt umfassende Datenangebote für kundenorientierte Use Cases und vielfältige technische Zugriffsmöglichkeiten auf Daten. Dieses proaktive Angebot wird kontinuierlich weiter ausgebaut.

Das Engagement der Automobilindustrie zur Förderung von Innovation und datengetriebenen Geschäftsmodellen spiegelt sich durch die Investitionen im Bereich von mehreren Milliarden Euro wider, die für zukunftsweisende Betriebssysteme, Elektrik-/Elektronikarchitekturen und Vernetzung getätigt werden.

Diese Investitionen stellen die fundamentale Basis für alle Geschäftsmodelle dar, die auf Fahrzeugdaten beruhen.

2. Ein gemeinsamer Markt für Daten – für unsere Kunden, die Mobilität und die Umwelt

Die im VDA zusammenarbeitenden Unternehmen glauben an den Mehrwert, der durch die Nutzung und den Austausch von Daten erzeugt werden kann.

Gemeinsam fördern wir diesen Mehrwert durch den proaktiven weiteren Ausbau des Datenangebots und durch sichere technische Zugriffsmöglichkeiten, um unseren Kunden Mehrwert durch relevante datenbasierte Services zu bieten und um die Mobilität unserer Kunden und der Gesellschaft zu verbessern – umweltverträglich, klimaschonend und sicher. Die Souveränität über die Daten liegt im Rahmen der geltenden Gesetze beim Kunden.

Die Basis dafür ist ein stabiles und verlässliches regulatorisches Rahmenwerk, das allen Beteiligten ein „Level Playing Field“ und den Freiraum zur Entwicklung des noch jungen Datenmarktes bietet.

Mit unserem Engagement ermöglichen wir innovative Geschäftsmodelle für alle Beteiligten. Es ist das Verständnis aller im VDA vertretenen Unternehmen, dass eine etwaige Regulierung des Datenmarktes für alle Beteiligten faire Spielregeln enthält.

Datenverfügbarkeit und Zugriffsmöglichkeiten sind nicht ausschließlich auf das Fahrzeug zu beziehen, sondern ebenfalls auf die fahrzeugrelevanten Daten bei Serviceanbietern, Versicherungen, Finanzierungsunternehmen und in anderen nachgelagerten Bereichen im automobilen Umfeld. Nur so ist die Entwicklung neuer Services, im Interesse der Kunden, möglich.

3. Ein wachsendes Datenangebot – als Motor datenbasierter Geschäftsmodelle

Nur ein umfassendes Datenangebot, das von allen Fahrzeugherstellern über alle Modelle hinweg unterstützt wird, ermöglicht es Serviceanbietern und Dienstleistern, erfolgreich neue Geschäftsmodelle auszurollen.

Entsprechend unterstützen die Unternehmen des VDA die Erarbeitung eines Basisdatensatzes. Dieser Datensatz soll unter Einhaltung der gesetzlichen Voraussetzungen für alle Fahrzeuge bereitgestellt werden können. Bedingung ist, dass diese technisch dazu in der Lage sind.

Dieser Datensatz ist als gemeinsamer Startpunkt zu verstehen. Er wird kontinuierlich auf Basis von kundenorientierten Use Cases erweitert. Treiber für die Erweiterung werden die Use Cases sein, bei denen der größte Kundennutzen und damit die größte Nachfrage ersichtlich wird und für die schnell und weitreichend Daten zur Verfügung gestellt werden können. Entscheidungen über den Ausbau der Use Cases werden über die Verbände im partnerschaftlichen Dialog getroffen.

Die beteiligten Unternehmen sagen zu, Transparenz über ihr gesamtes, via Extended Vehicle (ExVe)[1] online verfügbares Datenangebot zu schaffen. Die Beschreibung dieser Daten erfolgt durch geeignete semantische Auszeichnung der Daten, um Interoperabilität zu gewährleisten.

4. ADAXO: Automotive Data Access – Extended and Open: Vertraulichkeit als Erfolgsfaktor

Der VDA vertritt Unternehmen, deren Erfolg auf Innovationen basiert und die entsprechend den Schutz von geistigem Eigentum und Innovationen unterstützen. Die für datenbasierte Geschäftsmodelle notwendige Vertraulichkeit wird durch das ADAXO-Konzept, das die Weiterentwicklung des bisherigen VDA-Konzeptes darstellt, zugesichert. Durch das ADAXO-Konzept entsteht zudem die Möglichkeit, den Datenersterhebern gegenüber weder die Identität der zugreifenden Unternehmen noch ihr Geschäftsmodell offenzulegen. Das Konzept der ADAXO-Neutralität kann auch in Datenräumen umgesetzt werden und stellt für uns den logischen nächsten Schritt in der neutralen Datenbereitstellung dar. Schlussendlich verbleibt die vollständige Souveränität über die Daten beim Fahrzeugkunden.

Das Datenangebot von ADAXO beinhaltet unter anderem den oben erwähnten initialen Datensatz, der über den beschriebenen Use-Case-Ansatz erarbeitet und kontinuierlich weiter ausgebaut wird.

[1] Konzept Extended Vehicle: Hersteller leiten die Daten über ein OEM-Backend aus.

5. FRAND – als gemeinsame Spielregel für partnerschaftliche Zusammenarbeit im Sinne unserer Kunden

Fair, Reasonable and Non-Discriminatory (FRAND) sind die gemeinsamen Spielregeln für alle Beteiligten am Datenmarkt. Die VDA-Verbandsunternehmen bieten den FRAND-Zugriff für Daten und Funktionen den Unternehmen an, die sich ebenso dem FRAND-Prinzip gegenüber verpflichten.

Seitens der OEM werden alle Daten und Funktionen angeboten, die sie auch zur Erbringung ihrer eigenen Services nutzen. Der diskriminierungsfreie Zugang zu den Daten erfolgt entweder maskiert (z. B. Neutraler Server) oder direkt über den OEM, jeweils auf der Basis von B2C- und B2B-Verträgen.

Diese Verträge werden unternehmensindividuell ausgestaltet. Aus Sicht der im VDA vertretenen Unternehmen können standardisierte Vertragskomponenten angestrebt werden, soweit das kartellrechtlich zulässig ist. Ein fairer Datenaustausch basiert auch auf einer transparenten Preisgestaltung, die nicht prohibitiv wirkt.

6. Berechtigungsmanagement – Mehrwert im Interesse unserer Kunden erzeugen

Im Sinne der geltenden Gesetze werden Daten nur zweckgebunden, somit Use-Case-basiert, übermittelt.

- Aus Kundenperspektive und aus datenschutzrechtlicher Sicht sollte das Berechtigungsmanagement zentral, konsistent und einfach zu bedienen sein und somit beim Hersteller (beim OEM) als zentralem Ansprechpartner der Datenerhebung liegen.

- Die Datensouveränität liegt beim Kunden. Der Kunde entscheidet im Rahmen der geltenden Gesetze darüber, welche Daten welchen Empfängern übermittelt werden. Die Hersteller sollen den Kundenwünschen entsprechen.

- Der kommerzielle Datenfluss wird nicht durch die OEMs überwacht, es sei denn, es wird durch legale, vertragliche oder sicherheitsrelevante Zwecke notwendig.

- Vertraulichkeitsklauseln stellen sicher, dass keine Analysen zu Kundendaten erfolgen und damit Reverse Engineering ausgeschlossen ist. Die Berechtigung für Dienste von Dritten kann verschlüsselt werden, sodass dadurch keine Geschäftsmodelle von Dritten bei OEMs bekannt werden.

Die Hersteller können Daten OEM-betriebenen und nicht OEM-betriebenen Datenmarktplätzen zugänglich machen, die die entsprechende Voraussetzung hierfür erfüllen. Die Einhaltung der gesetzlichen Anforderungen wird durch die Datenersterheber über ein Ende-zu-Ende-Berechtigungsmanagement sichergestellt.

7. Technischer Zugriff – kundenfokussiert und effizient Daten bereitstellen

Schon jetzt bieten die im VDA vertretenen Unternehmen verschiedene technische Zugriffsmöglichkeiten an, um im Rahmen gesetzlicher Vorgaben kundenorientiert Fahrzeugdaten zur Verfügung zu stellen. Alle Unternehmen unterstützen das ADAXO-Konzept, über das nach FRAND-Prinzip Daten bezogen werden können, z. B. der gemeinsam entwickelte Basisdatensatz. Daneben bieten die Hersteller eigene Online-Portale an, über die Unternehmen, abgesichert durch B2B- und B2C-Verträge, auch direkt Daten beziehen können. Mit dem Mobility Data Space (vormals Datenraum Mobilität) kommt ein weiterer Marktplatz dazu, der insbesondere die Möglichkeit bietet, mit hoher Transparenz über das Datenangebot und über standardisierte Konnektoren schnell und effizient Daten aus verschiedensten Datenquellen zu beziehen. Eine Vielzahl der VDA-Mitglieder unterstützen bereits diesen Ansatz und fördern den weiteren Ausbau.

8. Zugriff auf Daten durch Dritte – Sicherheit im Vordergrund

Schon jetzt wird die Möglichkeit geboten, im Rahmen der technischen Voraussetzungen und der gesetzlichen Anforderungen Dritte direkt auf Fahrzeugdaten und Funktionen zugreifen zu lassen.

Im Rahmen der Weiterentwicklung werden verschiedene Fahrzeughersteller unter Beachtung von regulatorischen Anforderungen (z. B. UNECE R155 Cybersecurity), Zertifizierungsaspekten sowie den Anforderungen an Softwareupdate-Managementsysteme (UNECE R156) die Möglichkeit bieten, im Fahrzeug Software von Drittanbietern zu installieren. Dafür sollten mit den Verbänden Richtlinien entwickelt werden, um die Installation von Third-Party-Software in Fahrzeugen abzusichern.

Grundlegend bleibt jedoch, dass die Freigabe der Software und das Management von Fahrzeugressourcen (z. B. Bandbreiten für Datenübertragungen im Fahrzeug) nur durch das für die Zertifizierung des Fahrzeugs verantwortliche Unternehmen erfolgen können. Die Sicherheit aller Verkehrsteilnehmer steht bei jeglicher Betrachtung etwaiger Möglichkeiten für alle Unternehmen stets im Vordergrund.

II Einordnung und Kontext

II.1. Europäische und nationale Datenstrategien als Innovationsförderung

Mit der Europäischen Strategie für Daten (EU-Datenstrategie)[2] hat die EU-Kommission 2020 ihre Vision für eine Datenökonomie in Europa veröffentlicht. Die EU wird in Richtung eines gemeinsamen Marktes für Daten mit Datenflüssen zwischen den Mitgliedsstaaten und Sektoren auf der Basis europäischer Werte und Normen und unter der Prämisse fairer, praktischer und klarer Regeln arbeiten. Zielstellung ist die Mehrung der Wertschöpfung in Europa, sowohl für Bürger als auch die industriellen Stakeholder. Insbesondere soll sichergestellt werden, dass es zu einem fairen Datenaustausch zwischen allen Beteiligten kommt, um dem Ansatz eines „Level Playing Field“ gerecht zu werden. Eine Bevorzugung einzelner Interessengruppen, Branchen oder Unternehmensgrößen soll damit ausgeschlossen werden.

Vor dem Hintergrund dieser EU-Strategie – und auch nationaler Datenstrategien – gibt es seitens der EU-Kommission konsekutive Regulierungen und aktuelle Regulierungsvorhaben. Exemplarisch sollen hier genannt werden:

1. Seit November 2020 liegt ein Entwurf für einen **Data Governance Act** (DGA) vor, durch den die Europäische Datenökonomie gestärkt werden soll. Hierfür soll der Datenaustausch zwischen Unternehmen, Privatpersonen und dem öffentlichen Sektor vereinfacht und Vertrauen in den Datentransfer geschaffen werden.

2. Der **Data Act** (DA) hat den erweiterten Zugang und die Nutzung von Daten sowohl öffentlicher als auch privater Akteure zum Ziel. Er soll die Fairness im Datenmarkt zwischen den einzelnen beteiligten Stakeholdern sicherstellen. Hierzu adressiert der DA explizit den Datenaustausch von Business-to-Business(B2B)-Daten und Business-to-Government(B2G)-Daten.

3. Der **Digital Markets Act** (DMA) der eine Reihe eng definierter Kriterien für die Einstufung von großen Online-Plattformen als Gatekeeper vorsieht, soll die Marktmacht auf den Datenmärkten ausbalancieren.

4. Der **Digital Services Act** (DSA), soll die Expansion kleinerer Plattformen sowie KMU und Start-ups auf dem Datenmarkt erleichtern. Er soll einen sichereren digitalen Raum schaffen, in dem die Grundrechte der Nutzer geschützt sind und gleiche Wettbewerbsbedingungen für Unternehmen gelten.

5. Der **Implementation Act High Value Datasets** soll das sozioökonomische Potenzial von Daten freisetzen.

Alle genannten Regulierungsvorhaben haben eines gemein: Sie stärken den Kunden und seine Rechte auf Datenhoheit und stoßen die Innovation Richtung Datenmarkt auf europäischer Ebene an.

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

Nicht nur auf europäischer Ebene, sondern auch auf nationaler Ebene werden von EU-Mitgliedsstaaten Strategien entwickelt, um den Übergang zur Digitalisierung zu ermöglichen. Die deutsche Bundesregierung hat beispielsweise eine **„Datenstrategie der Bundesregierung“**[3] ausgearbeitet. Diese beschreibt die Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum: Grundsätzliches Ziel dieser Strategie ist es, eine Datenkultur zu schaffen, die

- die Wahrung grundlegender Werte, Rechte und Freiheiten der Gesellschaft gewährleistet und
- gleichzeitig die Bereitstellung von Daten maßgeblich steigert und somit Innovationen fördert[4].

Basis für die Umsetzung der Datenstrategie sind der nachhaltige Ausbau von leistungsfähigen und sicheren Dateninfrastrukturen und die Schaffung von sektoralen Datenräumen – unter anderem in den Bereichen Industrie, Umwelt und Mobilität.

Andere EU-Mitglieder verfolgen mit ihren jeweiligen nationalen Datenstrategien vergleichbare Ziele.

II.2. Regulatorisches Rahmenwerk als Level Playing Field

Die Gesetzesinitiativen der EU sollen im Binnenmarkt gleiche Wettbewerbsbedingungen für Unternehmen in Bezug auf den Datenaustausch gewährleisten. Die Basis dafür ist ein stabiles und verlässliches regulatorisches Rahmenwerk, das allen Beteiligten ein „Level Playing Field“ und den Freiraum zur Entwicklung der noch jungen Datenmärkte bietet.

Es ist das Verständnis aller im VDA vertretenen Unternehmen, dass eine etwaige Regulierung des Datenmarktes für alle Beteiligten faire Spielregeln enthalten muss. Diese Regeln zu Datenverfügbarkeit und Zugriffsmöglichkeiten sind nicht ausschließlich auf das Fahrzeug zu beziehen, sondern ebenfalls auf die fahrzeugbezogenen Daten bei Serviceanbietern, Versicherungen, Finanzierungsunternehmen und anderen nachgelagerten Bereichen im automobilen Umfeld.

Damit das Datenangebot in Europa auch sektorübergreifend strategisch sinnvoll ausgebaut werden kann, wird ein Forum aller Beteiligten notwendig, in dem Positionen ausgetauscht und Interessenausgleiche verhandelt werden können. Hier könnten in gemeinschaftlicher Anstrengung Lösungen für aktuell noch unklare oder beschränkende Voraussetzungen innerhalb der geplanten Regulierungen diskutiert und erarbeitet werden.

Der VDA als deutscher Zusammenschluss der Automobilindustrie ist bereit, die Datenkultur im europäischen Binnenmarkt maßgeblich zu fördern und voranzutreiben.

[3] Datenstrategie der Bundesregierung, Kabinettsfassung vom 27. Januar 2021.
[4] Datenstrategien: Was passiert in Deutschland und der EU? › BASECAMP.

II.3. Regulierungsdichte aus Sicht der Automobilindustrie

Die einleitenden Ausführungen zeigen die Regulierungsdichte und die damit verbundene Anforderungskomplexität, die direkt – auch negativen – Einfluss auf die Innovationsfähigkeit der Automobilbranche haben. Bislang sind kaum Synergien oder Querverbindungen zwischen den Regulierungsvorhaben ersichtlich. Daneben haben einzelne Generaldirektionen der EU-Kommission bereits Studien in Auftrag gegeben, die die Anforderungen in Bezug auf den Zugriff auf Fahrzeugdaten beschreiben und sehr detaillierte Lösungsoptionen vorschlagen (s. Anhang V.1). Eine bessere Verzahnung der Vorhaben der verschiedenen Generaldirektionen ist wünschenswert.

Zudem übersieht die parallele und in weiten Teilen entkoppelte Vorgehensweise im Rahmen der europäischen Gesetzesinitiativen die bereits bestehenden und praxiserprobten Konzepte und Initiativen der OEMs hinsichtlich Ausleitung von Fahrzeugdaten im Rahmen von „Access to in-vehicle-data“.

Aus Sicht des VDA sind keine weiteren spezifischen Regulierungen zum Thema Daten notwendig. Diese erzeugen zusätzliche Komplexität in der technischen Umsetzung und der Ausgestaltung datengetriebener Geschäftsmodelle. Beides hemmt Innovationsaktivitäten – nicht nur in der Automobilbranche, sondern auch aufseiten der Anbieter von datenbasierten Diensten und Services.

Es müssen vielmehr sektorübergreifende Regulierungen harmonisiert werden. Nur so sind Innovationen im Rahmen der Digitalisierung und branchenübergreifender Austausch von Daten für die Schaffung neuer Geschäftsmodelle möglich.

II.4. Unterstützung datengetriebener Geschäftsmodelle und Innovationen

Der VDA und seine Mitglieder unterstützen die Datengenerierung und das Teilen von Daten proaktiv mit Innovationen entlang der Wertschöpfungskette: von der Datenerzeugung bis hin zur Schaffung der Voraussetzungen für funktionierende hersteller- und branchenübergreifende Datenmärkte. Hier werden seit Jahren hohe Investitionsvolumina eingesetzt, um nachhaltige Wettbewerbsmodelle zu entwickeln und zu etablieren, die erfolgreich mit internationalen Wettbewerbern konkurrieren können und auf großes Interesse aus den Märkten treffen.

Darüber hinaus befürworten und unterstützen der VDA und seine Mitglieder seit Langem die sichere Anbindung an Datenräume des öffentlichen Sektors zum harmonisierten und branchenübergreifenden Datenaustausch.

II.5. Sicherer Zugang zu Fahrzeugdaten

Ein Fokusthema der diversen Datenstrategien ist der Schutz vor cyberkriminellen Machenschaften. Dies gilt sowohl für die Strategien der Politik als auch der Industrie. Vor dem Hintergrund der Digitalisierung in der Automobilbranche wachsen die Bedrohung durch potenzielle Angriffe auf technische Schnittstellen im Fahrzeug und die Gefahr von unberechtigtem Zugriff auf sensible Fahrzeugfunktionen. Nicht nur das Bereitstellen von Schnittstellen zum Datenaustausch mit Dritten erzwingt zusätzlichen Sicherungsaufwand, sondern auch der Schutz bei bidirektionalen Verbindungen durch beispielsweise Schreibzugriffe von Dritten bzw. Softwareinstallationen von Drittanbietern im Fahrzeug. Jegliche gewünschte Nutzung der Schnittstellen erfordert es, damit einhergehende Risiken zu minimieren.

Die Absicherung sämtlicher Schnittstellen im Fahrzeug, die eine Verbindung zur Außenwelt haben, erfolgt maßgeblich durch die Fahrzeughersteller, da diese die nötigen Eingriffe in die Fahrzeugarchitektur sicher und effizient bewerkstelligen können. Dabei ist insbesondere auch zu berücksichtigen, dass die Anforderungen an die Absicherungen angesichts rasanter Digitalisierung immer komplexere Lösungen erforderlich machen.

Vor diesem Hintergrund haben die Fahrzeughersteller bereits vor Jahren das Extended-Vehicle-Konzept (ExVe) für den sicheren Zugang zu Fahrzeugdaten entwickelt. ExVe beschäftigt sich mit dem Austausch von Daten zwischen dem Fahrzeug und dem Server der Fahrzeughersteller über die Mobilfunk-Schnittstelle. Die ExVe-Web-Schnittstelle ist bei allen modernen Fahrzeugen verfügbar und stellt so die gesicherte Kommunikation zwischen dem Fahrzeug und dem Server des Fahrzeugherstellers[5] sicher. Dritte können – auf der Basis entsprechender B2B-Vereinbarungen – über eine gemäß ISO 20078 genormte Schnittstelle auf die Fahrzeugdaten zugreifen. Ein Eingriff in die Fahrzeugarchitektur durch die ISO-zertifizierte[6] und standardisierte Schnittstelle ist ausgeschlossen.

Der Einsatz von ExVe erfolgt seit Jahren zuverlässig und hat sich auf breiter Front bewährt. Bereits heute sind Millionen von Fahrzeugen in Europa auf diese Weise mit Servern von Fahrzeugherstellern verbunden und machen Daten für Dritte verfügbar. Wesentliche Stärke des Konzepts ist dabei die Offenheit hinsichtlich Art und Menge der übertragbaren Daten, was Fahrzeugnutzern, Serviceprovidern und Herstellern eine große Vielfalt innovativer Anwendungsmöglichkeiten eröffnet – unter gleichzeitiger Einhaltung der gesetzlichen Vorschriften (EU-DSGVO).

Mit dem ADAXO-Konzept, das auf dem ExVe-Konzept als integralem Bestandteil basiert, legt der VDA nun ein zeitgemäßes und zukunftssicheres Modell für den Austausch von fahrzeuggenerierten Daten zwischen allen Stakeholdern wie auch Anforderungen an bidirektionale Verbindungen und Drittsoftware im Fahrzeug vor. Dieses Konzept wird in den folgenden Kapiteln des vorliegenden Dokuments vertiefend vorgestellt.

[5] Andere Schnittstellen, beispielsweise die Schnittstelle zwischen Handy und Fahrzeug oder die Vehicle-to-Vehicle-Kommunikation (V2V), sind vom Konzept nicht beeinflusst. Ebenso bleibt der Zugriff auf Fahrzeugdaten für Reparatur- und Wartungsmaßnahmen über die im Fahrzeug verbaute Diagnoseschnittstelle OBD-2 weiterhin erhalten.
[6] ISO 20077/20078/20080.

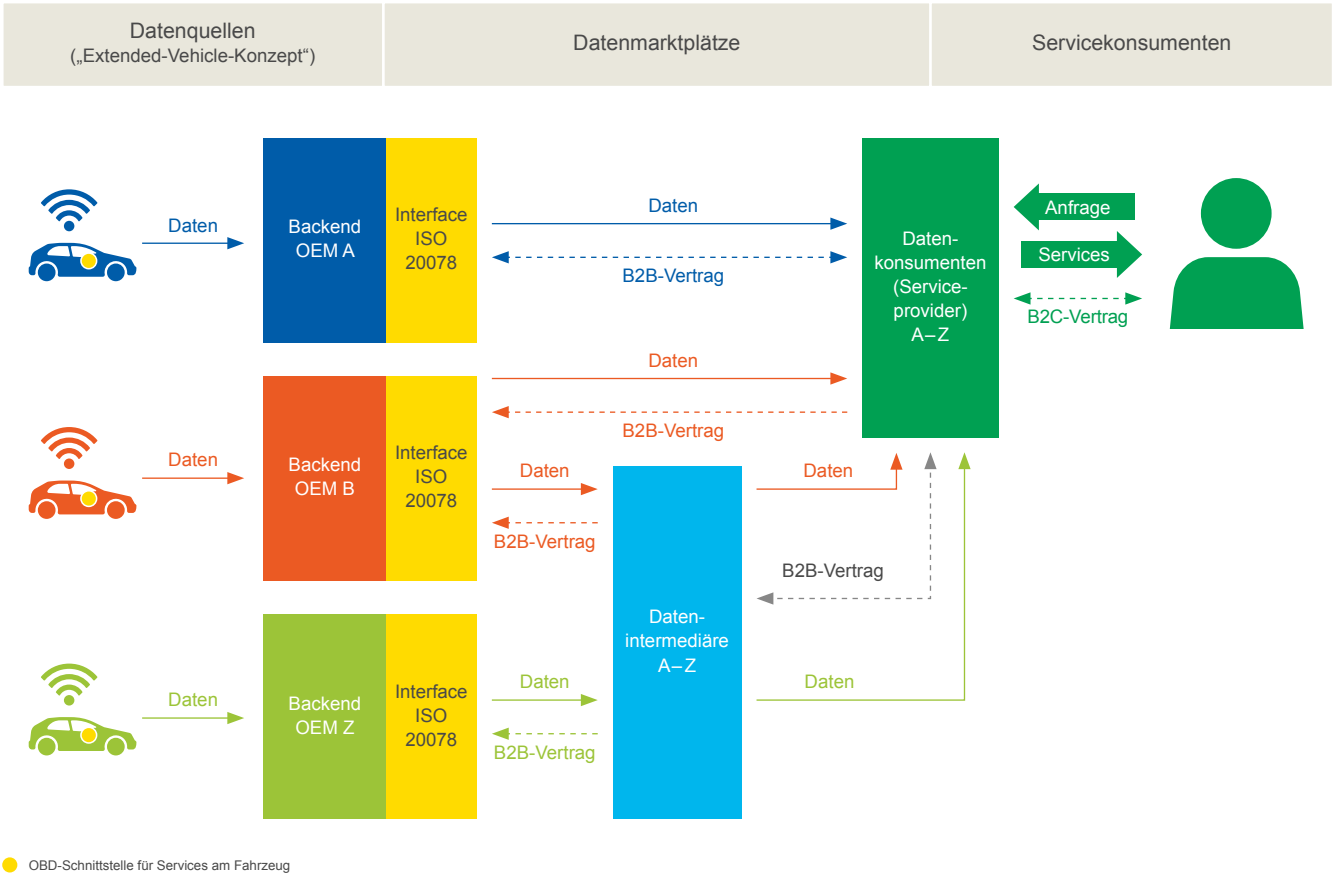
III ADAXO-Konzept – technische Vertiefung

ADAXO beschreibt Prinzipien des freien, nicht diskriminierenden Zugangs zu Daten und Funktionen des entsprechenden Berechtigungsmanagements unter dem Aspekt der Cybersecurity. ADAXO schafft damit die Grundlagen, auf denen Plattformen zum Datenaustausch entstehen können, ohne selbst eine solche zu sein.

III.1. Datenfluss und Vertragsbeziehungen im ADAXO-Konzept

Ein wesentlicher Eckpfeiler der europäischen Digital- und Datenstrategien ist es, die Nutzung und den Austausch von Daten zu vereinfachen, um auf dieser Basis neue Geschäftsmodelle entstehen zu lassen. Zudem eröffnet es Drittanbietern die Möglichkeit, bidirektionale Verbindungen ins Fahrzeug zu etablieren sowie Software in das Fahrzeug zu integrieren. Die deutsche Automobilindustrie begrüßt dies und forciert den Datenaustausch mit Dritten, um dem Potenzial, das in Services auf Basis fahrzeuggenerierter Daten liegt, Rechnung zu tragen.

Datenfluss und Vertragsbeziehungen in ADAXO



Die im VDA vertretenen Unternehmen bieten schon jetzt umfassende Datenangebote für kundenorientierte Anwendungsfälle und vielfältige Lösungen für den Austausch von Daten an. Das Einbringen von Drittsoftware in das Fahrzeug soll – unter der Berücksichtigung von regulatorischen Anforderungen – stärker ausgebaut werden. Zudem sollen weitere Zugriffe, wie beispielsweise schreibende Zugriffe von Dritten auf Fahrzeugsysteme gemäß Anforderungen an die Cybersicherheit, vermehrt möglich sein. Dieses proaktive Angebot wird kontinuierlich weiter ausgebaut.

Die Bereitstellung der Daten erfolgt über das Extended-Vehicle-Konzept, das durch eine Mobilfunk-Schnittstelle im Fahrzeug die Daten auf das OEM-Backend ausleitet. Der Zugriff auf die Daten erfolgt über eine gemäß ISO 20077/20078/20080 standardisierte Schnittstelle.

Austausch und Nutzung der Daten sind abhängig vom jeweiligen Use Case bzw. Angebot und erfolgt ggf. über angebundene Datenmarktplätze. Der Austausch der Daten kann entweder auf der Basis eines B2B-Vertrags zwischen OEM und Datenkonsument erfolgen oder wahlweise kann auch ein Intermediär (z. B. Neutrale Server, unternehmenseigene Plattformen) zwischengeschaltet werden. Hieraus ergeben sich ggf. die für verschiedene Geschäftsmodelle erforderliche „Entkopplung“ der Geschäftsbeziehung zwischen Datenquellen und Datenkonsumenten sowie Vereinfachungen im Management der Beziehungen zwischen OEM und Intermediär bzw. Intermediär und Datenkonsument.

Die Datenintermediäre bündeln Daten und stellen diese Dritten (Datenkonsumenten) zur Verfügung, um auf dieser Basis ein Produkt oder einen Service für Kunden entwickeln und anbieten zu können. Daneben besteht die Möglichkeit, dass der OEM direkt mit dem Datenkonsumenten eine Vereinbarung schließt. Grundlage für den Austausch sind jeweils B2B-Verträge, je nachdem, welche Art der Bereitstellung der Daten gewählt wird (siehe Grafik „Datenfluss und Vertragsbeziehungen in ADAXO“).

Ziel dieses Ansatzes ist, dem Endkunden den bestmöglichen Service anzubieten und ihn selbst aus verschiedenen Angeboten bzw. Anbietern wählen zu lassen.

III.2. Datenzugriff nach FRAND-Prinzipien

Eine der Grundprämissen von ADAXO ist ein fairer, angemessener und diskriminierungsfreier Datenzugang für Dritte. Zwar ist der Zugang zu Daten nicht kostenlos, da unterschiedliche Kostentreiber wie z. B. die Bereitstellung/Entwicklung von Datenzugriffen oder der Betrieb existieren, jedoch muss die Preisfindung immer fair erfolgen. Insbesondere durch die frei zugängliche Bereitstellung der Daten über unterschiedliche Marktplätze, Intermediäre und Datenräume wird der Preis durch das Zusammenspiel von Angebot und Nachfrage bestimmt. Daher haben die Datenmarktplätze nicht nur die Funktion des technischen Datenaustausches, sondern auch die einer natürlichen Regulierung des marktüblichen Preises im Sinne einer fairen Preisgestaltung. Eine Nichtbereitstellung an einzelne Interessenten, d. h. deren bewusste Benachteiligung, ist nicht zulässig.

Zukünftige Regulierungsvorhaben sollten darauf abzielen, Datenmärkte zu initiieren. Nur durch funktionierende Datenmärkte kann eine Preisgestaltung gemäß des FRAND-Prinzips sichergestellt werden.

III.3. Berechtigungs- und Consentmanagement in ADAXO

Ein Berechtigungsgeber in ADAXO kann üblicherweise der Fahrzeugeigentümer, Fahrzeughalter und/oder der Fahrzeugnutzer sein. Je nach Datenpunkt kann der Berechtigungsgeber variieren.

Ein wesentlicher – weil für innovative Geschäftsmodelle besonders wertvoller – Teil der aus dem Fahrzeug ausgeleiteten Daten besitzt Personenbezug. Diese Daten unterliegen grundsätzlich den Regelungen der DSGVO. Ihre Nutzung kann nur auf der Basis eines im Kontext der beabsichtigten Datennutzung gegebenen Einverständnisses durch den Berechtigungsgeber erfolgen.

Hieraus ergibt sich zwingend die Notwendigkeit, ein leistungsfähiges und DSGVO-konformes Berechtigungsmanagement zu etablieren. Das ADAXO-Konzept wird diesem Anspruch in vollem Umfang gerecht:
Im Sinne der geltenden Gesetze werden Daten nur zweckgebunden, somit Use-Case-basiert, übermittelt.

- Aus Kundenperspektive und aus datenschutzrechtlicher Sicht sollte das Berechtigungsmanagement zentral, konsistent und einfach zu bedienen sein und somit beim Hersteller (beim OEM) als zentralem Ansprechpartner der Datenerhebung liegen.

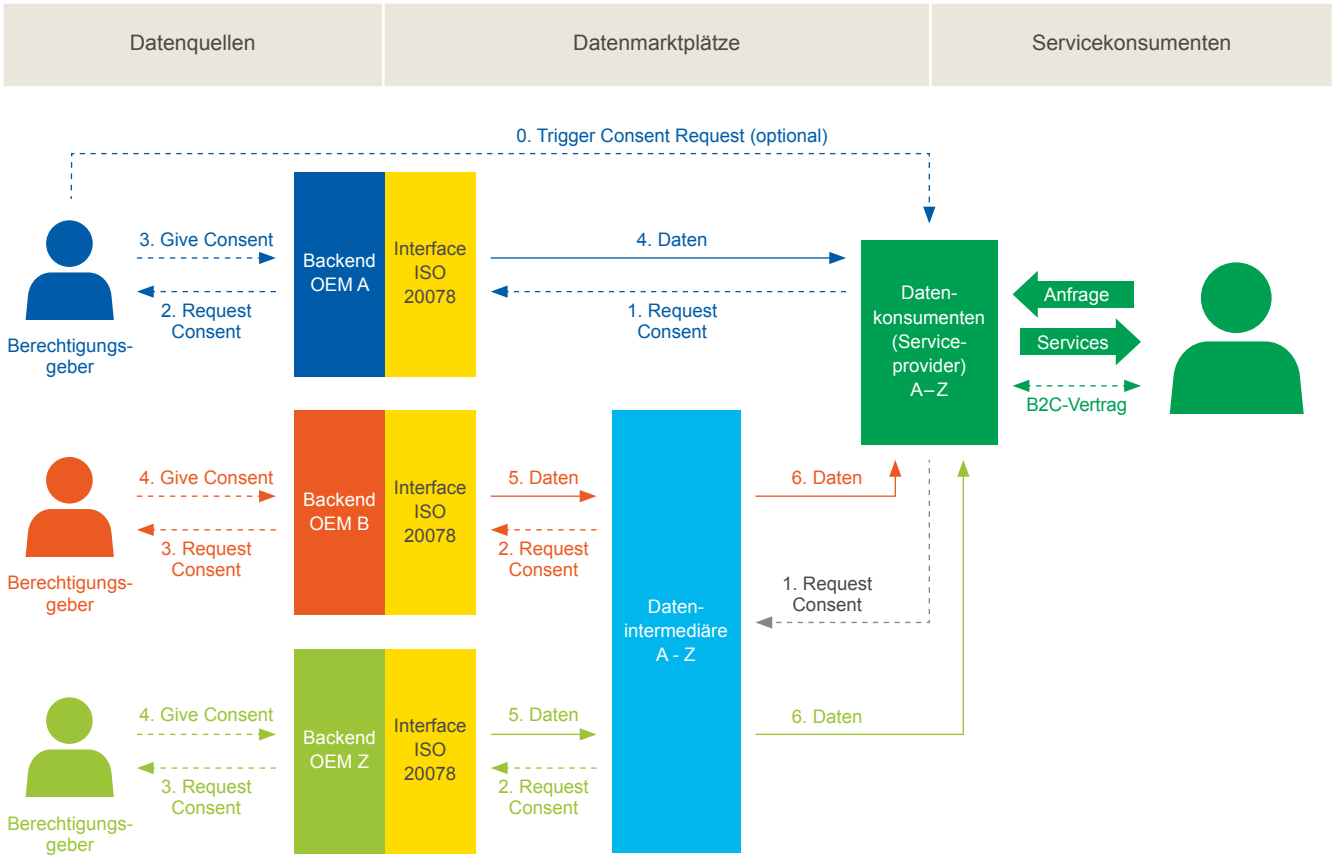
- Die Datensouveränität liegt beim Kunden. Der Kunde entscheidet im Rahmen der geltenden Gesetze darüber, welche Daten welchen Empfängern übermittelt werden. Die Hersteller sollen den Kundenwünschen entsprechen.

- Der kommerzielle Datenfluss wird nicht durch die OEMs überwacht, es sei denn, es wird durch legale, vertragliche oder sicherheitsrelevante Zwecke notwendig.

- Vertraulichkeitsklauseln stellen sicher, dass keine Analysen zu Kundendaten erfolgen und damit Reverse Engineering ausgeschlossen ist. Die Berechtigung für Dienste von Dritten kann verschlüsselt werden, sodass keine Geschäftsmodelle von Dritten bei OEMs dadurch bekannt werden.

Die Hersteller können Daten OEM-betriebenen und nicht OEM-betriebenen Datenmarktplätzen zugänglich machen, die die entsprechende Voraussetzung hierfür erfüllen. Die Einhaltung der gesetzlichen Anforderungen wird durch die Datenersterheber über ein Ende-zu-Ende-Berechtigungsmanagement sichergestellt.

Berechtigungs- und Consentmanagement in ADAXO



Wie bereits dargestellt, fließen im ADAXO-Konzept die Daten zunächst über eine Mobilfunk-Schnittstelle vom Fahrzeug zum Backend-System des Fahrzeugherstellers. Die Voraussetzung hierfür ist, dass der Inhaber der Rechte an den Daten hierzu sein Einverständnis erklärt. Regelmäßig ist dies der Berechtigungsgeber des Fahrzeugs[7]. Das Management des Einverständnisses erfolgt, indem dieser zunächst (einmalig) online einen sog. Owner Account beim Fahrzeughersteller anlegt. Danach kann er diesen Account nutzen, um gemäß DSGVO über seine Daten zu verfügen. So kann er seine Daten für eine bestimmte Nutzung zur Verwendung durch Dritte freigeben, die Zustimmung widerrufen, eine Kopie der Daten anfordern etc.

Der Owner Account eröffnet aber auch dem Fahrzeughersteller die Möglichkeit, sich direkt an den Berechtigungsgeber zu wenden, um dessen Zustimmung zur Weitergabe seiner Daten für bestimmte Nutzungen durch Dritte einzuholen, sofern er hierzu von einem solchen Dritten aufgefordert wird: Ein Serviceanbieter wendet sich also an den OEM mit der Bitte, bestimmte

[7] Falls der Besitzer das Fahrzeug verleiht oder personenbezogene Daten von Mitfahrern erhoben werden, wird davon ausgegangen, dass der Besitzer mündlich das Einverständnis dieser Personen einholt.

Daten bestimmter Kunden für eine definierte Nutzung freizugeben. Der OEM leitet diese Anfrage an den Besitzer des Owner Account weiter. Sofern er der Nutzung zustimmt, kann der OEM die entsprechenden Daten an den anfragenden Datenkonsumenten weiterleiten.

Sofern der Datenfluss über einen Datenintermediär erfolgt, ist der Intermediär selbstverständlich ebenfalls in das Berechtigungsmanagement einzubinden: In diesem Fall wendet sich der Datenkonsument an den Intermediär, mit der Bitte, bestimmte Daten von angeschlossenen Datenquellen bereitzustellen. Der Intermediär muss diese Anfragen dann zunächst an die jeweiligen OEMs weiterleiten. Diese wenden sich dann mit der Anfrage – wiederum unter Nutzung des Owner Account – an den Berechtigungsgeber. Sofern dieser sein Einverständnis gibt, kann der OEM die entsprechenden Daten an den Intermediär weiterleiten, der sie dann dem Datenkonsumenten übergibt.

Ein besonderer Fall für das Berechtigungsmanagement ist die Situation, in der ein Berechtigungsgeber selbst einen bestimmten Service nutzen möchte, für dessen Bereitstellung auf seine personenbezogenen Daten zugegriffen werden muss. In diesem Fall löst also der Berechtigungsgeber den beschriebenen Consent-Prozess aus und erteilt über seinen Owner Account beim OEM sein Einverständnis für die Weitergabe seiner Daten.

III.4. Cybersecurity

Cybersecurity sichert das Fahrzeug gegen unberechtigte Zugriffe Dritter ab. Unautorisierte Zugriffe auf die Fahrzeugsysteme ermöglichen den Akteuren, Informationen zu empfangen und/oder an Fahrzeuge außerhalb des Fahrzeugs selbst zu senden und auch mit mehreren Fahrzeugen gleichzeitig eine Schnittstelle zu bilden, ohne physischen Zugang zum Fahrzeug zu benötigen. Um solchen Angriffen entgegenwirken zu können, sind logische und physische Isolierungstechniken notwendig. Dies ist wichtig, denn die beste Methode, zu verhindern, dass ein Angreifer aus der Ferne die Kontrolle über ein Fahrzeug übernimmt oder dessen Leistung manipuliert, besteht darin, sicherzustellen, dass es keine Möglichkeiten bzw. Verbindungen gibt, über die unberechtigte Externe auf Fahrzeugkomponenten zugreifen und Befehle an sie senden können. Im Rahmen der Weiterentwicklung werden verschiedene Fahrzeughersteller unter Beachtung von regulatorischen Anforderungen, Zertifizierungsaspekten sowie den Anforderungen an Softwareupdate-Managementsysteme die Möglichkeit bieten, im Fahrzeug Software von Drittanbietern zu installieren. Aus Gründen der Cybersecurity und zum Schutz vor Manipulation der Software im Fahrzeug werden die geforderten internationalen Standards umgesetzt. So greift beispielsweise die UNECE R155 (Cybersecurity Management System, CSMS) ab Juli 2022 bei der Typzulassung von neuen Fahrzeugtypen. Verabschiedet wurde im Sommer 2020 ebenfalls die UNECE R156, die den Aufbau und Betrieb eines zertifizierten Softwareupdate-Managementsystems (SUMS) regelt. Diese UNECE-Regularien stellen u. a. die notwendigen Cybersecurity-Aktivitäten vor, während und nach der Produktentwicklung sicher und werden beim ADAXO-Konzept stets berücksichtigt.

III.5. Voraussetzungen für Konnektivität

Aufgrund der Verkopplung mit einer Vielzahl von Funktionen besteht seitens der Datengeber grundsätzlich das Interesse, möglichst langzeitig eine bestehende Basiskonnektivität von Fahrzeugen aufrechtzuerhalten.

Deshalb bleibt die Basiskonnektivität des Fahrzeugs aufrechterhalten, solange einerseits die technischen Voraussetzungen gegeben sind und andererseits der Berechtigungsgeber die Basiskonnektivität gebucht hat. Potenzielle technische Einflussfaktoren, die zu einem Ende der Basiskonnektivität führen können und typischerweise außerhalb des Gestaltungsraumes von Datengeber und -nehmer (Datenkonsument) liegen, sind beispielsweise die Abschaltung älterer Mobilfunknetze (2G-Netz, 3G-Netz), in älteren Systemen nicht mehr schließbare Sicherheitslücken (non-fixable Security Incidents) oder grundsätzlich das Lebensende der eingesetzten Technologie.

III.6. Freier Zugang zu Fahrzeugressourcen

III.6.1. Diskriminierungsfreier Zugang zu Fahrzeugressourcen

Seitens der OEM werden alle Daten und Funktionen angeboten, die sie auch zur Erbringung ihrer eigenen Services nutzen. Der diskriminierungsfreie Zugang zu den Daten erfolgt entweder über Intermediäre (ggf. maskiert, z. B. per Neutralen Server) oder direkt über den OEM, jeweils auf der Basis von B2C- und B2B-Verträgen.

Im Gegensatz zum rein lesenden Zugriff auf im Backend abgelegte Fahrzeugdaten (d. h. ohne Rückwirkung auf das Fahrzeug selbst) bestehen bei einer schreibenden (bzw. lesenden und schreibenden) Verbindung zum Fahrzeug, wie dies etwa für die Remote-Diagnose erforderlich ist, zusätzliche Risiken für die Integrität der Fahrzeugsysteme und deren Betriebssicherheit. Daher werden im Falle der Remote-Diagnose alle diagnoserelevanten Daten und Funktionen durch den Fahrzeughersteller über eine Abstraktionsschicht zur Verfügung gestellt, um besonders riskante Operationen und Betriebszustände ausschließen zu können. Hierbei gilt der Grundsatz, dass berechtigte Dritte zum gleichen Zeitpunkt und im gleichen Umfang Zugang zu solchen Remote-Diagnose-Diensten erhalten, die von Vertragshändlern und -werkstätten und Serviceprovidern des jeweiligen Herstellers genutzt werden können.

Eine Remote-Diagnose kann zu jedem Zeitpunkt immer nur von einer einzigen Partei durchgeführt werden, um eine gegenseitige Beeinflussung auszuschließen.

Die ISO 20080 (Remote Diagnostic Support) ist entsprechend dieser Position zu erweitern.

Da Remote-Diagnosen und Reparaturen durch schreibenden Zugriff regelmäßig auch die Abschaltung von Schutzvorrichtungen (z. B. Einklemmschutz Fenster) und Veränderungen von Stellgliedern (z. B. Ausfahren der Anhängerkupplung) umfassen, muss eine Sachkenntnis des Nutzers und Verpflichtung zum ordnungsgemäßen Gebrauch durch den Serviceprovider sichergestellt sein.

Interaktion mit dem Servicekonsumenten über HMI findet über verfügbare technische Lösungen statt und die Information wird im HMI des Fahrzeugs gespiegelt. Die bereits verfügbaren technischen Lösungen können diese Anforderungen erfüllen.

III.6.2. Überwachung und Durchsetzung

Sollten zur Überwachung und Durchsetzung Untersuchungsmechanismen erforderlich sein, wird dies unterstützt. Das kann auch über ein „strukturiertes Forum“ der Betroffenen und ggf. auch unter Beteiligung der EU-Kommission erfolgen, siehe Empfehlung in Kapitel IV.2.

III.6.3. Verhinderung unerlaubter Geschäftsüberwachung

Der kommerzielle Datenfluss wird nicht durch die OEMs überwacht, es sei denn, es wird durch legale, vertragliche oder sicherheitsrelevante Zwecke notwendig. Vertraulichkeitsklauseln stellen sicher, dass keine Analysen zu Kundendaten erfolgen und damit Reverse Engineering von Serviceangeboten ausgeschlossen ist.

Use Case lesender Datenzugang:

- Siehe Kapitel III.2 zum präzisierten Authorization-Workflow als Erweiterung zur ISO 20078.
- Der Berechtigungsgeber (Vertragspartner des OEM für die Telematikumfänge) muss eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.
- Via eines Datenintermediär (z. B. Neutraler Server) sind die Serviceprovider und die Kunden der Serviceprovider maskierbar. Dadurch ist die „Non-Disclosure“ im oben genannten Sinne gegeben.

Use Case Remote Diagnostic Support (RDS):

- Remote Diagnostic Support (RDS) bezeichnet lesende und schreibende „Online“-Zugriffe auf die Fahrzeugsysteme über das OEM-Backend zu Telediagnose- und Wartungszwecken, also Zugriffe, die eine unmittelbare Rückwirkung auf das Fahrzeugbordnetz und seine Komponenten inkl. Aktoren haben können.
- Die im Folgenden beschriebene Position ist nicht auf Telediagnose- und Wartungszwecke beschränkt, sondern lässt sich auf alle Use Cases des „Remote Online Access (ROA)“ übertragen (z. B. auch Nutzung von Remote-Services wie z. B. Remote Door Unlock).

- Ein Datenintermediär (z. B. Neutraler Server) agiert als technischer Dienstleister für den Serviceprovider, der einen B2B-Rahmenvertrag für RDS mit den jeweiligen OEM gemäß Rahmenbedingungen abschließt.

- Die Haftung verbleibt beim Serviceprovider, der Abschluss eines RDS-Vertrags zwischen Serviceprovider und OEM erfolgt gemäß B2B-Rahmenvertrag.

- Das Handling der Authentifikation und Autorisierung der Kunden (individuell ausführende Serviceeinheit) des Serviceproviders erfolgt durch den Datenintermediär (z. B. Neutraler Server).

- Der Berechtigungsgeber muss eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

- Der Serviceprovider muss aufgrund des geregelten Haftungsübergangs eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

- Über einen identifizierbaren Datenintermediär (z. B. Neutraler Server) und identifizierbaren Serviceprovider sind die Kunden des Serviceproviders (individuell ausführende Serviceeinheit) maskierbar. Dadurch ist die „Non-Disclosure“ für die individuell ausführende Serviceeinheit im oben genannten Sinne gegeben.

III.6.4. Zugangsauthentifikation

Eine Differenzierung zwischen lesendem Datenzugriff auf das OEM-Backend (ohne Rückwirkung auf Fahrzeugsysteme) und schreibendem Zugriff, z. B. Remote Diagnostic Support (RDS), auf das Fahrzeug via OEM-Backend ist notwendig, da bei einem Direktzugriff auf das Fahrzeug ein geregelter Haftungsübergang vom OEM auf den Serviceprovider gewährleistet sein muss.

- Lesender Datenzugang:

  – Siehe Kapitel III.2 zum präzisierten Authorization-Workflow als Erweiterung zur ISO 20078).

  – Der Berechtigungsgeber (Vertragspartner des OEM für die Telematikumfänge) muss eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

  – Via Datenintermediär (z. B. Neutraler Server) können die Serviceprovider und die Kunden der Serviceprovider maskiert werden. Dadurch ist die „Non-Disclosure“, wie in Kapitel III.6.3 beschrieben, gegeben.

- Schreibender Datenzugang (z. B. Remote Diagnostic Support, RDS):

  – Remote Diagnostic Support (RDS), ISO 20080, bezeichnet lesende und schreibende „Online“-Zugriffe auf die Fahrzeugsysteme über das OEM-Backend zu Telediagnose- und Wartungszwecken, also Zugriffe, die eine unmittelbare Rückwirkung auf das Fahrzeugbordnetz und seine Komponenten inkl. Aktoren haben können.

  – Die im Folgenden beschriebene Position ist nicht auf Telediagnose- und Wartungszwecke beschränkt, sondern lässt sich auf alle Use Cases des „Remote Online Access (ROA)“ übertragen (z. B. auch Nutzung von Remote-Services wie Remote Door Unlock).

  – Ein Datenintermediär, z. B. Neutraler Server, kann als technischer Dienstleister für den Serviceprovider agieren, durch Abschluss eines Standard-Rahmenvertrags für RDS mit jedem OEM gemäß Rahmenbedingungen.

  – Die Haftung verbleibt beim Serviceprovider, der Abschluss eines RDS-Vertrags zwischen Serviceprovider und OEM erfolgt gemäß Standard-Rahmenvertrag.

  – Im Falle der Nutzung eines Datenintermediärs (z. B. Neutraler Server) erfolgt das Handling der Authentifikation und Autorisierung der Servicekonsumenten (individuell ausführende Serviceeinheit) des Serviceproviders durch den Intermediär.

  – Der Berechtigungsgeber muss eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

  – Der Serviceprovider muss aufgrund eines geregelten Haftungsübergangs eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

  – Über einen Datenintermediär (z. B. Neutraler Server) und identifizierbaren Serviceprovider sind die Kunden des Serviceproviders (individuell ausführende Serviceeinheit) maskierbar. Dadurch ist die „Non-Disclosure“, wie in Kapitel III.6.3 beschrieben, gegeben.

III.6.5. Haftung

Eine Differenzierung zwischen lesendem Datenzugriff auf das OEM-Backend (ohne Rückwirkung auf Fahrzeugsysteme) und Remote Diagnostic Support (RDS) auf das Fahrzeug via OEM-Backend ist notwendig, da bei einem Direktzugriff auf das Fahrzeug ein geregelter Haftungsübergang vom OEM auf den Serviceprovider gewährleistet sein muss. Die Haftung bei RDS verbleibt beim Serviceprovider, der Abschluss eines RDS-Vertrags zwischen Serviceprovider und OEM erfolgt gemäß Standard-Rahmenvertrag. Der Serviceprovider muss bei RDS aufgrund eines geregelten Haftungsübergangs eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden.

III.6.6. Identifikation des Endkunden

Endkunden können sowohl der Berechtigungsgeber wie auch der Servicekonsument sein.

Bei lesendem Zugriff können via Datenintermediär (z. B. Neutraler Server) die Servicekonsumenten der Serviceprovider maskiert werden.

Bei RDS jedoch muss der Serviceprovider aufgrund eines geregelten Haftungsübergangs eindeutig für den OEM identifizierbar sein und kann deswegen nicht maskiert werden. Allerdings können durch den Datenintermediär (z. B. Neutraler Server) die Servicekonsumenten des identifizierbaren Serviceprovider (individuell ausführende Serviceeinheit) maskiert werden.

Für beide oben stehenden Anwendungsfälle kann der Berechtigungsgeber aufgrund des erforderlichen Telematikvertrags für die Basiskonnektivität nicht maskiert werden.

III.7. Darstellung unterschiedlicher Datenarchitekturen im Fahrzeug

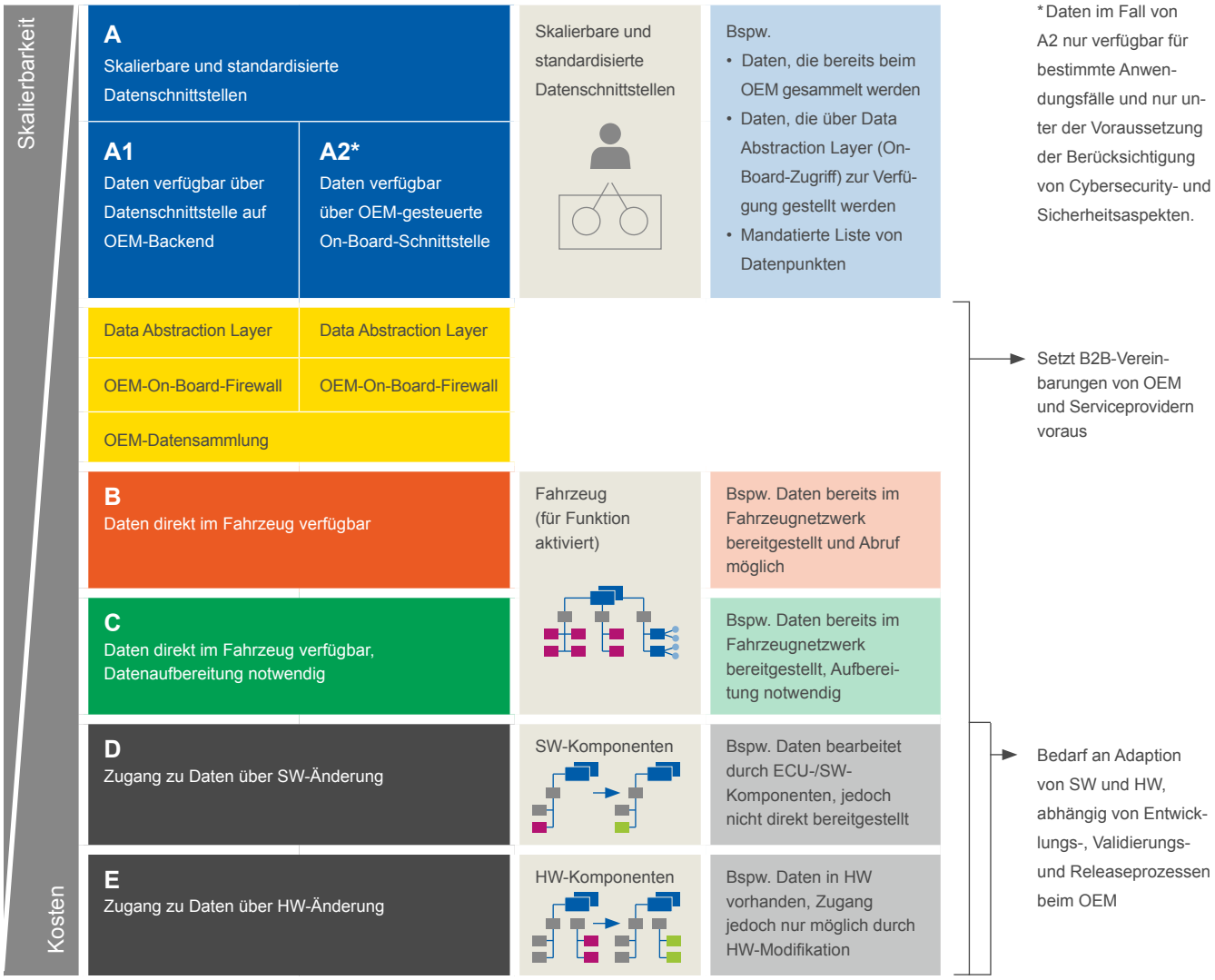
Die Datenarchitektur im Fahrzeug unterscheidet grundsätzlich einen öffentlichen (A) und privaten Bereich (B – E), vergleichbar mit einem Internet, in dem öffentliche Informationen zugänglich sind, und dem Intranet, das beispielsweise durch Security-Maßnahmen geschützt ist.

Der Bereich A umfasst Daten, die über skalierbare und standardisierte Schnittstellen authentisierten Dritten zur Verfügung gestellt werden. Der Datensatz in A wird dabei kontinuierlich erweitert.

Hierbei unterscheiden wir zwischen einem ExVe-Interface, das am Backend des OEM zur Verfügung steht (A1), und einem On-Board-Interface, das nur für bestimmte Use Cases Daten zur Verfügung stellen kann (A2).

Für die Bereitstellung von Daten bestimmen die Anforderungen der Cybersecurity, in welchem Maß und zu welchem Zweck Daten zur Verfügung gestellt werden können. Aufgrund höherer Risiken bei einem On-Board-Zugriff, wird der mögliche Umfang der verfügbaren Daten bei A2 geringer als bei A1 sein.

Unterschiedliche Datenarchitekturen im Fahrzeug



Detaillierung der Fälle B und C: (B) Es gibt Datenumfänge, die direkt als On-Board-Ressource verfügbar sind und verfügbar gemacht und auf Ebene A hochgehoben werden können. (C) Auf Basis dieser Daten können auch mittels Vorverarbeitung weitere Daten verfügbar gemacht werden. Jedoch werden hierfür zusätzliche Ressourcen benötigt.

Daten, die B und C zugeordnet werden können und in A verfügbar gemacht werden sollen, erfordern ein zusätzliches B2B-Agreement zwischen OEM und Drittpartei, d. h., sie sind nur mit Zustimmung des OEM oder auf Basis einer gesetzlichen Grundlage möglich. Auf Basis einer solchen Vereinbarung und seiner technischen Möglichkeiten wird der OEM zusätzliche Daten aus dem Fahrzeug der dritten Partei über die Schnittstelle bereitstellen (Fall B) bzw. nimmt zuvor eine On-Board-Vorverarbeitung vor (Fall C). Die Drittpartei muss die Spezifikation für eine solche Vorverarbeitung in Form von Anforderungen oder einem Pseudocode bereitstellen, der OEM übernimmt die Integration. Bei der Spezifikation sind Datensparsamkeit, adäquate Schnittstellenbreite (Anzahl der Datenpunkte) und Latenz sowie ereignisbasierte Aktualität und Verarbeitungsfrequenz zu berücksichtigen.

Detaillierung der Fälle D und E: Darüber hinaus gibt es Daten, auf die noch kein Zugriff möglich ist (D und E). Im Fall von D ist eine Erhebung der Daten nur mit einer Änderung einer Softwarekomponente möglich. Beispielsweise wird ein Datum bereits von einer ECU berechnet, jedoch noch nicht versendet. Im Fall von E ist die Erhebung nur mit einer Änderung einer Hardwarekomponente möglichh, beispielsweise wenn die ECU nicht an die Abstraktionsschicht technisch angebunden ist oder Sensorik nicht verbaut ist.

Die Use Cases, die den Fällen D und E zugeordnet werden können, erfordern daher ein zusätzliches B2B-Agreement zwischen OEM und Drittpartei, d. h., sie sind nur mit Zustimmung des OEM oder auf Basis einer gesetzlichen Grundlage möglich.

Je tiefer die Erhebung neuer Daten in die Datenarchitektur eingreift, desto komplexer (Kosten und Zeit) ist die Umsetzung.

Die Entwicklung von Software für Fahrzeugsysteme und damit auch für Software zur Datenbereitstellung unterliegt klaren Vorgaben, wie z. B. Lastenheften, herstellerspezifischen Standards und Designvorgaben sowie industrieweiten Security- und Functional-Safety-Vorgaben und regulatorischen Rahmenbedingungen. Zudem werden Ressourcenbedarfe (z. B. RAM und CPU) individuell vereinbart.

Durch den Fahrzeughersteller definierte und selbst verwendete Validierungs- und Freigabeprozesse sind einzuhalten, da z. B. Safety- und Security-Anforderungen nur bei Betrachtung des Gesamtsystems beherrschbar sind (siehe insb. Variantenvielfalt, mögliche Testapplikation und Absicherungsprozesse).

Aus diesen Gründen sind eine von diesen Prozessen entkoppelte Entwicklung und Integration von Software nicht darstellbar.

Grundsätzlich hat der Fahrzeughersteller die Verantwortung für die Integration, funktionale Sicherheit und Security, das Konfigurations- und Ressourcenmanagement. Eine mögliche Integration von Drittpartei-Software ist nach heutigem Stand nur unter der zusätzlichen Prämisse der Offenlegung des Quellcodes realisierbar.

Alle Daten werden vor der Bereitstellung an Dritte abstrahiert. Ziel dieser Abstraktion ist es, die rein technischen Fahrzeugsignale nutzbar zu machen und sie möglichst unabhängig von Hersteller und Fahrzeuggeneration zu beschreiben (beispielsweise Vehicle Signal Specification, VSS). Der Zugriff auf die bereitgestellten Daten erfolgt immer oberhalb dieser Abstraktionsschicht. Dabei kann der Abstraktionsgrad je Generation der E/E-Architektur variieren. Der aktuell hohe Integrationsaufwand für eine sichere Datenbereitstellung kann in zukünftigen E/E-Architekturen durch den Einsatz von Virtualisierungs- und Software-Isolationstechnologien gegebenenfalls reduziert werden.

Das ADAXO-Konzept ermöglicht auch die Darstellung neuer Inhalte, ggf. unter Zuhilfenahme von HW- oder SW-Änderungen im Fahrzeug. Durch das ADAXO-Konzept werden die im Fahrzeug umgesetzten Anforderungen an die funktionale Sicherheit (z. B. ASIL-Konformität von Fahrzeugfunktionen) unterstützt.

Im Gegensatz zum rein lesenden Zugriff auf an Schnittstellen verfügbare Fahrzeugdaten (d. h. ohne Rückwirkung auf das Fahrzeug selbst) bestehen bei Nutzung von Funktionen zusätzliche Risiken für die Integrität der Fahrzeugsysteme und die Betriebssicherheit. Im Falle der Remote-Diagnose (bzw. bei einem schreibenden Zugriff über On-Board-APIs) werden alle diagnoserelevanten Daten und Funktionen durch den Fahrzeughersteller über eine Abstraktionsschicht zur Verfügung gestellt, um besonders riskante Operationen und Betriebszustände ausschließen zu können. Hierbei gilt der Grundsatz, dass berechtigte Dritte zum gleichen Zeitpunkt, im gleichen Umfang und zum vereinbarten Zweck Zugang zu solchen Remote-Diagnosediensten und schreibenden On-Board-APIs erhalten, die von Vertragshändlern und -werkstätten sowie Serviceprovidern des jeweiligen Herstellers genutzt werden können.

Hinweis: Der detaillierte Ablauf des Use Case Remote-Diagnose ist in Anlage V.2 zu finden.

Das Fahrzeug muss für Schreibzugriffe ausreichend gesichert sein, z. B. gegen Wegrollen oder Einklemmen von Personen im Fenster. Dieser gesicherte Zustand muss im Fahrzeug über die HMI bestätigt werden (wenn Fahrzeug nicht verschlossen) bzw. über eine App durch eine verantwortliche Person (wenn Fahrzeug verschlossen). Eine entsprechende Gesetzgebung wird empfohlen.

III.7.1. Installation und Ausführung von On-Board-Software

Im Zuge der Einführung neuer Architekturen werden z. B. Hypervisor-Technologien zur Verfügung stehen, die eine Hardwareabstraktion insoweit ermöglichen, als eine Vorverarbeitung von Informationen zukünftig auch durch Dritte möglich sein wird.

Die Nutzung von On-Board-Ressourcen birgt zusätzliche Risiken für die Integrität der Fahrzeugsysteme und die Betriebssicherheit. Die Sicherheit aller Verkehrsteilnehmer und am Reparaturprozess Beteiligter steht bei jeglicher Betrachtung etwaiger Möglichkeiten für alle Unternehmen stets im Vordergrund.

Durch den Fahrzeughersteller definierte und selbst verwendete Validierungs- und Freigabeprozesse sind einzuhalten, da z. B. Safety- und Security-Anforderungen nur bei Betrachtung des Gesamtsystems beherrschbar sind (siehe insb. Variantenvielfalt, mögliche Testapplikation und Absicherungsprozesse).

Die Entwicklung von Software für Fahrzeugsysteme und damit auch von Software zur Datenbereitstellung unterliegt klaren Vorgaben, wie z. B. Lastenheften, herstellerspezifischen Standards und Designvorgaben sowie industrieweiten Security- und Functional-Safety-Vorgaben und regulatorischen Rahmenbedingungen. Zudem werden Ressourcenbedarfe (z. B. RAM und CPU) individuell vereinbart.

Aus diesen Gründen sind eine von diesen Prozessen entkoppelte Entwicklung und Integration von Software nicht darstellbar.

Grundsätzlich hat der Fahrzeughersteller die Verantwortung für die Integration, funktionale Sicherheit und Security sowie das Konfigurations- und Ressourcenmanagement. Eine mögliche Integration von Drittpartei-Software ist nach heutigem Stand nur unter der zusätzlichen Prämisse der Offenlegung des Quellcodes realisierbar.

Grundlegend bleibt jedoch, dass die Freigabe der Software und das Management von Fahrzeugressourcen (z. B. Bandbreiten für Datenübertragungen im Fahrzeug) nur durch das für die Zertifizierung des Fahrzeugs verantwortliche Unternehmen erfolgen können. Dies muss auch unter Beachtung von regulatorischen Anforderungen (z. B. UNECE R155 Cybersecurity), Zertifizierungsaspekten sowie den Anforderungen an Softwareupdate-Managementsysteme (UNECE R156) erfolgen, wenn im Fahrzeug Software von Drittanbietern installiert wird.

Dafür sollten mit den Verbänden Richtlinien entwickelt werden, um die Installation von Third-Party-Software in Fahrzeugen abzusichern. Das in Kapitel IV.2 genannte „strukturierte Forum“ kann hierfür eine Grundlage bilden.

III.7.2. Interaktion mit dem Fahrer mittels HMI (Human Machine Interface)

Bei einem Zugriff auf das HMI (u. a. Bildschirm und Bedienelemente) müssen folgende Rahmenbedingungen sichergestellt werden:

- gesetzliche Vorgaben, Vorgaben zur Driver Distraction analog NHTSA, ethische/moralische Vorgaben;
- HMI-Gestaltungsvorgaben, z. B. Schriftgrößen, Layout, Fahrerzentrierung, Animationen;
- Architektur-, Ressourcen- und Security-Vorgaben.

Je nach eingesetzter Technologie (OEM-spezifische Lösung oder Projected Mode) wird diese Governance-Rolle durch den Fahrzeughersteller oder den Plattformverantwortlichen (z. B. Apple für CarPlay) wahrgenommen. Zudem unterscheiden sich die Technologien bezüglich Funktionalität, Skalierbarkeit, Implementierungskosten und -dauer.

Bestimmte Anzeigen/Signale dürfen aufgrund funktionaler Sicherheit nicht unmittelbar oder ggf. gar nicht erfolgen (beispielsweise Videostreaming bei der Fahrt).

Kriterien für die Bewertung:

- Skalierbarkeit für OEM: Aufwand für den OEM, Drittanbieterlösungen zu prüfen und freizugeben, muss beherrschbar sein.

- Skalierbarkeit für Drittpartei: Möglichst geringe Anpassungen je OEM nötig bzw. Lösung ist für alle Marken einheitlich nutzbar.

- Erfüllung Anforderungen Dritter: funktionale Anforderungen, z. B. Wartungsanwendungen, Interaktion mit dem Kunden.

- kurzfristige Realisierbarkeit: Technologie ist bereits im Markt verfügbar bzw. kann kurzfristig eingeführt werden.

Bewertung der Technologien

	Projected Mode	Benachrichtigungen	Native App auf Headunit (OEM-App-Store)
Beschreibung	Verfügbarkeit Projected Mode in allen Fahrzeugen / OEM-übergreifend	Öffnung ConnectedDrive Messaging Service für Dritte	Entwicklung von Android-Apps durch dritte Partei, Aufnahme in OEM-App-Store
Funktionalität	Eigene Anwendungen auf Basis der erlaubten Templates	Info-Nachrichten mit Nachrichteninhalt (Text) und Absender (navigierbare Adresse und Telefonnummer)	Eigene Anwendungen (Android-App)
Technologiebereitsteller und „Governance“	Apple/Google	OEM	OEM
Markenübergreifendes Ökosystem / Skalierbarkeit Sicht dritte Partei	+++	++	+
Aufwand OEM / Skalierbarkeit Sicht OEM	+++	++	–––
Erfüllung Anforderungen Dritter	0	+	+++
Kurzfristige Realisierbarkeit	++	++	–––
Verbesserungspotenzial	Erweiterung der zugelassenen Funktionen	Integration in CarData-API, ggf. Rückkanal	

1. Projected Modes
   a. bieten eine gute Skalierbarkeit für OEM und Drittpartei: Im Fall des Projected Mode muss die Drittpartei nur einmal entwickeln, OEM-Adaptionen sind nicht notwendig. Die Prüfung/Qualifizierung übernimmt der Plattformanbieter (z. B. Google oder Apple), der dies im Gegensatz zu den OEMs als Kerngeschäft betreibt.
   b. sind für Endkundeninteraktion nutzbar, nicht jedoch für umfassende Business Cases (z. B. Remote Diagnose).
   c. sind sofort verfügbar.
   d. müssen aber über die derzeit verfügbaren Domänen Messaging, Infotainment und Navigation erweitert werden, d. h., die funktionalen Anforderungen der Drittanbieter werden noch nicht erfüllt. Gemeinsame Ansprache von z. B. Apple/Google zwecks Ausbaus der Funktionalitäten von Projected Modes empfohlen. Die Nutzung der Projected Modes im Markt wächst stark (insbesondere in den USA), sodass von einer Ausweitung der verfügbaren Domänen auszugehen ist.

2. Message Center
   a. bieten eine gute Skalierbarkeit für OEM und Drittpartei.
   b. sind für Endkundeninteraktion eingeschränkt nutzbar: Textnachricht mit teilweise aktiven Inhalten (z. B. Geolokation, Telefonnummer), bieten einen Rückkanal für Bestätigung o. ä..
   c. sind sofort verfügbar.
   d. erfüllen somit die funktionalen Anforderungen der Drittanbieter in Bezug auf eine größere Vielfalt von Use Cases, sind aber in Bezug auf Interaktionsmöglichkeiten beschränkt.
   e. standardisierte Formate sind auszuarbeiten.

3. OEM-Native-Apps (OEM-App-Store)
   a. bieten sehr beschränkte Skalierbarkeit über OEMs und Drittparteien.
   b. bieten umfangreiche Endkundeninteraktion.
   c. sind teilweise verfügbar.
   d. erfüllen somit die funktionalen Anforderungen der Drittanbieter vollständig.

Auf Basis der evaluierten Kriterien wäre ein OEM-seitiges Angebot und eine Nutzung seitens der Drittanbieter von Technologie 1 und 2 zu empfehlen (siehe Abbildung „Bewertung der Technologien“). Darüber hinaus müssen Angebote von Drittparteien als solche erkennbar sein.
Die Lösungsalternative 3 erfüllt nach heutigem Stand die Kriterien nicht, da diese umfangreiche Entwicklungs-, Validierungs- und Freigabeprozesse (pro App und OEM) erfordert und folglich nicht skaliert.

Nach heutigem Stand sind bereits verschiedene Technologien verfügbar, die einen HMI-Zugriff für Drittparteien ermöglichen. Davon sind jedoch nur zwei Technologien skalierbar für OEMs und Drittparteien einsetzbar. Diese sind mit Off-Board- und On-Board-APIs kombinierbar, wie in Kapitel III.7.1 beschrieben wird.

III.8. Zugang per On-Board-Diagnose(OBD)-Schnittstelle

Alle Daten und Funktionen, die den Herstellerwerkstätten über die OBD-Schnittstelle zur Verfügung stehen, werden auch Drittanbietern diskriminierungsfrei zur Verfügung gestellt. Details über den Zugang werden im Rahmen der EU-Typgenehmigung VO 2018/858 Anhang X Ziffer 2.9 geregelt. Sollten Fahrzeughersteller im Rahmen der Umsetzung der UNECE-Regulierung R155 und R156 (Cybersecurity und SUMS) Maßnahmen, z. B. Einführung einer Zertifikatsdiagnose, getroffen haben, werden diese unabhängigen Marktteilnehmern, gegen Prüfung/Erlangung der entsprechenden Zertifikate, ebenfalls diskriminierungsfrei zur Verfügung gestellt.

Für Reparatur- und Fehlerdiagnose bleibt der OBD-Zugang erhalten. Die OBD-Schnittstelle wird entsprechend neuen Anforderungen und gemäß dem Stand der Technik angepasst. Daten werden grundsätzlich wie in Kapitel III.7 beschrieben verfügbar gemacht.

IV Progressive Handlungsempfehlung eines ganzheitlichen Konzepts für den Automobilsektor

Mit dem ADAXO-Konzept wird ein sicherer, wettbewerbsfreundlicher und innovationstreibender Zugang zu Fahrzeugdaten ermöglicht.

Abschließend sind hier die Ziele und Handlungsempfehlungen zusammengefasst.

IV.1. Prämissen und Hauptziele

Die zwei elementaren Ziele von ADAXO lauten:

- **„Wir befähigen die Kundinnen und Kunden durch fahrzeug- und mobilitätsbezogene Daten, Mehrwert für sich und die Gesellschaft zu erzeugen."**
  Die Entscheidung über die Nutzung der persönlichen fahrzeug- und mobilitätsbezogenen Daten liegt direkt bei den Kundinnen und Kunden (Berechtigten). Sie allein entscheiden, wo der Mehrwert durch das Teilen ihrer Daten entstehen soll, um ihre persönliche Mobilität wie auch die Mobilität aller nachhaltiger, sicherer und komfortabler zu machen.
  Die im VDA vertretenen Unternehmen haben Kundinnen und Kunden in den Mittelpunkt ihres Konzepts gestellt und versetzen sie in die Lage, Mehrwert aus ihren Daten zu generieren.
  Die Handlungsempfehlungen dienen dazu, im fairen Zusammenspiel mit weiteren Marktteilnehmern die Voraussetzungen dafür umzusetzen.

- **„Wir unterstützen die Zielrichtung der Europäischen Datenstrategie, Innovationen und zukunftsorientierte Geschäftsmodelle zu fördern."**
  Fahrzeug- und mobilitätsbezogene Daten sind ein entscheidender Hebel, um Innovationen und Geschäftsmodelle zu fördern, die Europa wettbewerbsfähig für die Zukunft aufstellen. Dies können neue Geschäftsmodelle sein, beispielsweise von Start-ups, die aus der Zusammenführung verschiedenster, auch explizit sektorübergreifender Datenquellen entstehen. Aber auch etablierte Geschäftsmodelle, z. B. im unabhängigen Wartungs- und Reparaturbereich, können durch Datennutzung ihre Wertschöpfung und Services verbessern.
  All dies trägt dazu bei, dass der europäische Wirtschaftsraum global wettbewerbsfähiger und resilienter wird. Die im VDA vertretenen Unternehmen fühlen sich verpflichtet, auch in der Datenökonomie ihren Beitrag zur Zukunftsfähigkeit Europas zu leisten. Europäische Werte und Grundsätze, die in der Europäischen Datenstrategie formuliert sind, liegen der Umsetzung dabei selbstverständlich zugrunde.

Folgende Rahmenbedingungen müssen erfüllt sein:

- **Safety first**
  Ein Automobil ist kein Smartphone. Der Zugriff auf Fahrzeugdaten darf nur unter kompromissloser Beachtung der Sicherheit des Fahrzeugs und seiner Insassen erfolgen. Keine Innovation und auch kein neues Geschäftsmodell rechtfertigt die Gefährdung der Fahrzeugnutzerinnen und -nutzer oder die unsachgemäße Verwendung ihrer persönlichen Daten. Den Rahmen dafür bildet die durchgängige Beachtung der geltenden Regularien zu Cybersecurity, Datenschutz und dem Softwareupdate-Management.

- **Fairness**
  Es ist das gemeinsame Verständnis der im VDA vertretenen Unternehmen, dass der Mehrwert aus Daten nur auf der Basis von für alle Beteiligten funktionierenden Geschäftsmodellen geschaffen werden kann. Nur wenn alle Marktteilnehmer Daten bereitstellen, können die gemeinsamen Ziele erreicht werden.

IV.2. Handlungsempfehlung zur Realisierung einer Datenökonomie innerhalb der Automobilindustrie

Die innerhalb des VDA vertretenen Unternehmen unterstützen mittels des gemeinsamen ADAXO-Konzeptes die Ziele der Europäischen Union und somit auch explizit die Ziele der EU-Datenstrategie zur Stärkung der Datenökonomie Europas sowie das festgelegte Ziel der Generierung eines „Digital Single Market“[8]. Die hierfür notwendigen technischen Rahmenbedingungen und Implementierungen – siehe Kapitel III – ermöglichen, unter Sicherstellung der FRAND-Bedingungen und mittels des Extended-Vehicle-Konzepts, eine weitergehende Förderung der Datennutzung und des Datenaustausches für datensuchende Dritte. Fernerhin kann die systemische Integrität der Fahrzeuge und entsprechend die imminente Sicherheit aller Verkehrsteilnehmer gemäß essenziellen sicherheitstechnischen Aspekten (u. a. Cybersecurity) sichergestellt werden und somit ein relevanter Beitrag in Richtung „Vision Zero“[9] geleistet werden.

Kernelemente sind entsprechend ebenfalls die weitergehende Partizipation der Marktteilnehmer an neuen Innovationen und Geschäftsmodellen wie auch ein anzustrebender harmonisierter Ansatz innerhalb der Europäischen Union. Vor diesem Hintergrund wird empfohlen, die konsistente Anschlussfähigkeit an horizontale Regulierungen (u. a. Data Act und Data Governance Act) sicherzustellen.

Vor diesem Hintergrund gibt die deutsche Automobilindustrie folgende Handlungsempfehlungen:

(1) Datensouveränität: Der Zugang zu Daten erfolgt unter Wahrung der Datensouveränität der Kundinnen und Kunden und unter Sicherstellung der Cybersecurity auf Basis des Extended-Vehicle-Konzepts und unter FRAND-Bedingungen.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
[9] https://op.europa.eu/en/publication-detail/-/publication/d7ee4b58-4bc5-11ea-8aa5-01aa75ed71a1

(2) Berechtigungsmanagement: Die Entscheidungshoheit über die Verwendung der Daten liegt beim Kunden selbst – die transparente und für den Kunden zentrale Verwaltung des Berechtigungsmanagements beim OEM setzt diese Maßnahme folgerichtig auch im Kontext der Cybersecurity und der übergreifenden Verantwortung der OEM für die Sicherheit der Kunden um.

(3) Schutz von Geschäftsmodellen Dritter: Es wird sowohl technisch als auch vertraglich sichergestellt, dass eine kommerzielle Nachverfolgung von Daten respektive der Anwendungsfälle („Use Case") Dritter ausgeschlossen werden kann. Entsprechend wird via Verwendung des Extended-Vehicle-Interfaces für Drittparteien – individuelle Serviceprovider, Marktplätze im Sinne von Intermediären – sichergestellt, dass ein Monitoring von Use Cases ausgeschlossen werden kann. Vor dem Hintergrund bestimmter rechtlicher, vertraglicher und / oder Sicherheitsgründe sowie für die Optimierung des Datentransfers und des Berechtigungsmanagements ist ein Monitoring in dedizierten Umfängen notwendig.

(4) Transparenz über verfügbare Daten: Die Transparenz über die verfügbaren Daten (Kategorie A)[10] des individuellen OEM soll über einen einsehbaren Datenkatalog je OEM gewährleistet werden. Der Katalog wird über das Extended-Vehicle-Konzept, respektive ein entsprechendes Webinterface in einem elektronischen Format zur Verfügung gestellt. Im Rahmen technischer Erweiterungen und neuer Fahrzeuggenerationen können sukzessive weitere Daten in diesen Katalog mit aufgenommen werden. Es besteht zudem die Möglichkeit, dass auf Basis individueller B2B-Verträge weitere Daten in die Kategorie A aufgenommen werden.

(5) Einheitliches Rahmenwerk: Erarbeitung eines einheitlichen Rahmenwerks zur Beschreibung von Fahrzeugdaten, mit dem Ziel der Schaffung erweiterter Transparenz und des Verständnisses von Datennutzern. Entsprechend soll eine gemeinsame Terminologie, im Sinne einer Metadatenbeschreibung, über die OEMs hinweg erarbeitet werden.

(6) Datensatz für Mehrwertdienste: Es besteht Konsens, dass ein grundlegender, initialer und herstellerübergreifender Datensatz für herstellerübergreifende Mehrwertdienste zu erarbeiten ist. Es wird ein nicht statischer Datensatz angestrebt, der sich über die Zeit hinweg entwickeln und anpassen wird.

(7) Vorgehensweise: Prämisse eines übergreifenden Datensatzes und damit auch der essenziellen, konstanten Weiterentwicklung dessen ist eine grundlegende Use-Case- und damit mehrwertbasierte Logik, die mittels eines „strukturierten Forums" etabliert werden sollte. Hierbei ist essenziell, dass sowohl die etwaigen Drittparteien, die die Daten der OEM nutzen wollen, als auch die Datenbereitsteller die konkreten Datenbedarfe in Ableitung relevanter Use Cases betrachten, priorisieren und unter der Prämisse der allgemeinen Wirtschaftlichkeit abschließend bewerten. Ferner ist als Grundhypothese hervorzuheben, dass die derzeitige Datenbasis sich über die neuen Fahrzeuggenerationen grundlegend und konstant erweitern und weiterhin entwickeln wird.

Das „strukturierte Forum" sollte grundlegend unter Einbezug der relevanten Datennutzer und der individuellen OEM durchgeführt werden. Fernerhin wird angeregt, dass die EU-Kommission eine tragende Rolle, beispielsweise in der Funktion eines Organisators und Moderators, einnimmt und somit die essenzielle Neutralität des Forums gewahrt wird.

Die deutsche Automobilindustrie ist davon überzeugt, dass das ADAXO-Konzept einen substanziellen Beitrag zur Umsetzung der europäischen Datenstrategie liefert. Die Umsetzung werden wir aktiv vorantreiben und fordern alle interessierten Parteien zur Mitgestaltung auf.

[10] Siehe Kapitel III.7

V Anlagen

V.1. Studie EU-Kommission: TRL Remedy Measures und erste Evaluierung

Die von der Europäischen Kommission beauftragte Studie umfasst die nachfolgenden Handlungsempfehlungen, die aus Sicht der Studie notwendig sind, um einen funktionierenden Datenmarkt zu etablieren.

1. Availability of data and functions catalogue
   Für die effiziente Entwicklung unabhängiger fahrzeugdatenbasierter Dienste dritter Parteien ist insbesondere die Transparenz über die herstellerübergreifende Verfügbarkeit von Daten erforderlich.

2. Standardisation of data and functions
   Eine Standardisierung der Daten und Funktionen für Services (schreibend/lesend) hat das Ziel, die rein technischen Fahrzeugsignale effizienter nutzbar zu machen und sie möglichst unabhängig von Hersteller und Fahrzeuggeneration zu beschreiben (beispielsweise Vehicle Signal Specification, VSS).

3. Minimum functions and minimum dataset(s)
   Für die Entwicklung unabhängiger fahrzeugdatenbasierter Dienste dritter Parteien ist insbesondere eine herstellerübergreifende Verfügbarkeit von Daten und Funktionen erforderlich. Hierdurch soll eine Initialbefähigung von Multi-Brand-Services dritter Parteien ermöglicht werden mit dem Ziel, ein Ökosystem zu etablieren, das auf Basis von Angebot und Nachfrage weiterwächst.

4. Standard contract terms for B2B contracts
   Für die effiziente Entwicklung unabhängiger fahrzeugdatenbasierter Dienste dritter Parteien sind insbesondere einheitliche Vertragsbestandteile begrüßenswert, soweit kartellrechtlich zulässig.

5. Maximum fees for data/function access
   Die Forderung eines Maximalpreises kann die Bereitstellung neuer Geschäftsmodelle absichern. Diese Forderung kann sich aber auch prohibitiv auf das Datenangebot auswirken.

6. Preventing inappropriate business intelligence by resource provider
   Die Forderung einer Verhinderung der Analyse der Datenzugriffe dient der Absicherung von in Entwicklung befindlichen neuen Geschäftsmodellen Dritter.
   Eine Differenzierung zwischen lesendem Datenzugriff auf das OEM-Backend (ohne Rückwirkung auf Fahrzeugsysteme) und Remote Diagnostic Support (RDS) auf das Fahrzeug via OEM-Backend ist notwendig, da bei einem Direktzugriff auf das Fahrzeug ein geregelter Haftungsübergang vom OEM auf den Serviceprovider gewährleistet sein muss.

7. Preserving unencrypted OBD access
   Alle Daten und Funktionen, die den Herstellerwerkstätten über die OBD-Schnittstelle zur Verfügung stehen, werden auch Drittanbietern diskriminierungsfrei zur Verfügung gestellt. Details über den Zugang werden im Rahmen der EU-Typgenehmigung VO 2018/858 Anhang X Ziffer 2.9 geregelt.

8. OEM connectivity contract without bundled services

Eine Datenübertragung des Fahrzeugs ist an ein Serviceangebot des OEM gekoppelt, und damit auch die Datenübertragung für Drittparteien. Mit einer Basiskonnektivität soll dem Endkunden ein gleichberechtigtes Angebot an Servicediensten von Dritten ermöglicht werden.

9. Maximum response times for OEMs

Daten und Funktionen sollten in gleicher Qualität (Latenz und Trigger) allen Marktbeteiligten (OEMs und Dritte) zur Verfügung stehen. Für den Prozess des Bereitstellens neuer Daten und Funktionen sollten marktübliche Antwortzeiten, die Kunden bei der Nutzung von digitalen Endprodukten und den darauf aufbauenden Diensten gewohnt sind, angestrebt werden.

10. Access to remotely available data and functions based on fair, reasonable and non-discriminatory (FRAND) principles

Im Gegensatz zu einem rein lesenden Zugriff auf im Backend abgelegte Fahrzeugdaten (d. h. ohne Rückwirkung auf das Fahrzeug selbst) bestehen bei einer schreibenden Verbindung zum Fahrzeug und zu dessen Daten und Ressourcen – sog. Remote-Diagnose und Wartungsfunktionen – zusätzliche Risiken für die Integrität der Fahrzeugsysteme und die Betriebssicherheit. Für einen Zugriff berechtigter Dritter gilt der Grundsatz, dass diese zum gleichen Zeitpunkt und im gleichen Umfang Zugang zu solchen Remote-Diagnose-Diensten und -Funktionen erhalten, die von Vertragshändlern und -werkstätten und Serviceprovidern des jeweiligen Herstellers genutzt werden können.

11. Reporting information to Commission to monitor compliance with FRAND principles

Hierzu wird regelmäßig durch die Hersteller, durch Serviceprovider oder durch Neutrale Server an die EU-Kommission berichtet.

12. Separation of duties

Zugriffsgenehmiger und Datenhalter sind nicht in einer Rolle zusammengefasst. Nicht der Datenhalter genehmigt den Zugriff auf die Daten, sondern der Kunde. Hierbei ist eine Differenzierung zwischen lesendem Datenzugriff auf das OEM-Backend (ohne Rückwirkung auf Fahrzeugsysteme) und Remote Diagnostic Support (RDS) auf das Fahrzeug via OEM-Backend notwendig. Im Prozess ist zwischen OEM, Telematikkunde (Vertragspartner des OEM für die Telematikumfänge) sowie Serviceprovidern zu unterscheiden.

13. On-board application platform

Ermöglicht im Rahmen der technischen Gegebenheiten den Zugriff auf Daten, Funktionen und Ressourcen im Fahrzeug sowie die Schnittstellen zum Kunden. Hierzu müssen im Fahrzeug zusätzliche Schnittstelle bereitgestellt werden. Dies bedeutet, dass der Zugriff bis auf Ebenen, die sicherheits- und fahrzeugzulassungsrelevant sind, erfolgt.
Die Entwicklung von Software für Fahrzeugsysteme und damit auch von Software zur Datenbereitstellung unterliegt klaren Vorgaben, wie z. B. Lastenheften, herstellerspezifischen Standards und Designvorgaben sowie industrieweiten Security- und Functional-Safety-Vorgaben und regulatorischen Rahmenbedingungen. Grundsätzlich hat der Fahrzeughersteller die Verantwortung für die Integration, funktionale Sicherheit und Security sowie das Konfigurations- und Ressourcenmanagement. Deshalb muss der OEM jederzeit eine Rückwirkungsfreiheit von Datenerhebung und Datennutzung sicherstellen. Dies ist nur durch eine kontrollierte Nutzung der Datenerhebung und Funktionen möglich. Hierzu müssen kontrollierte Nutzungsbereiche mit dem Fahrzeughersteller definiert werden.

14. Specific consent management and identity validation procedures for ExVe

Die Grundlage einer Datenerhebung und -nutzung ist die explizite Zustimmung des Kunden für einen bestimmten Zweck. Hierzu ist insbesondere bei der Identity Validation eine Differenzierung zwischen lesendem Datenzugriff auf das OEM-Backend (ohne Rückwirkung auf Fahrzeugsysteme) und Remote Diagnostic Support (RDS) auf das Fahrzeug via OEM-Backend notwendig, da bei einem Direktzugriff auf das Fahrzeug ein geregelter Haftungsübergang vom OEM auf den Serviceprovider gewährleistet sein muss.

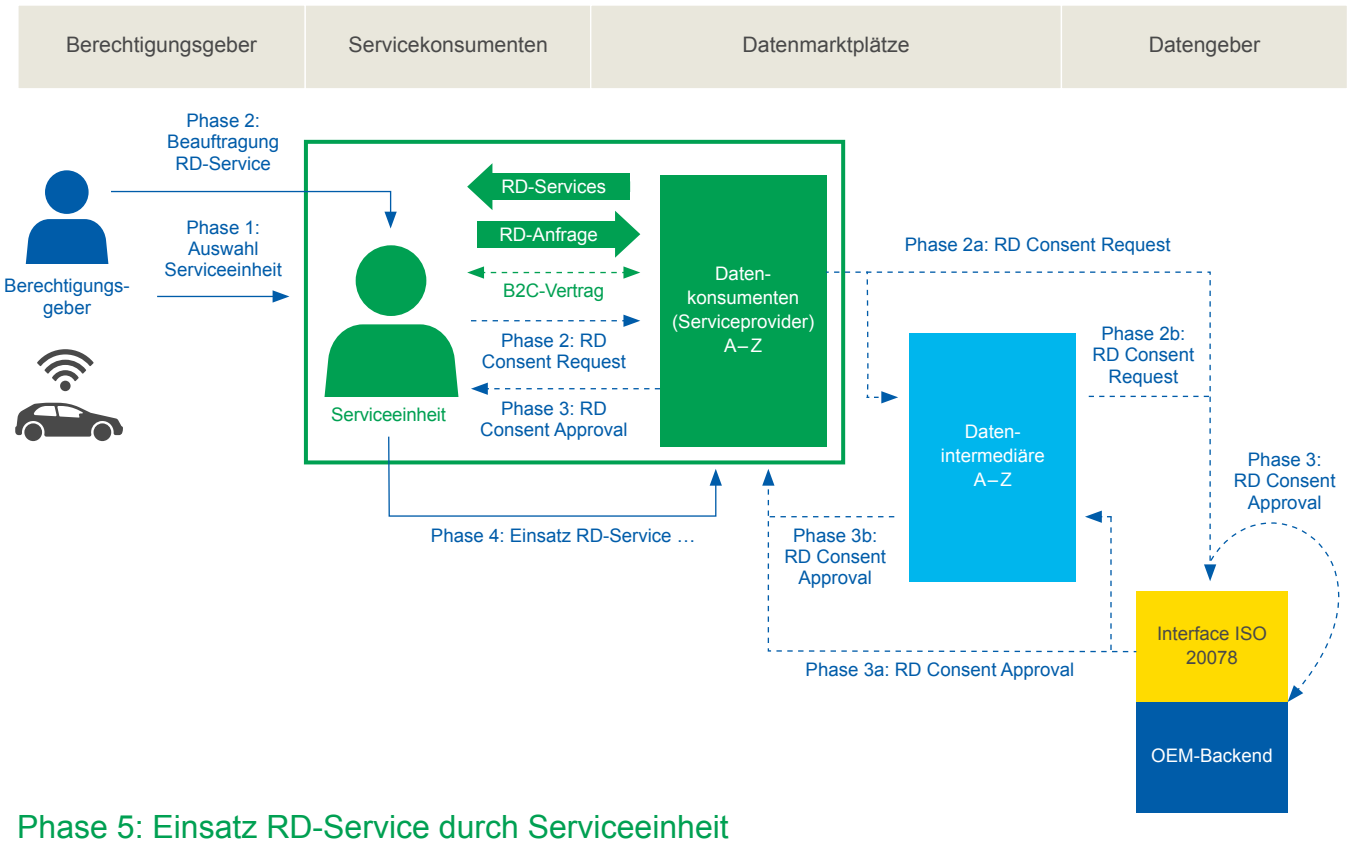
V.2. Detaillierung Abläufe Remote-Diagnose

Remote-Diagnose (RD) – Customer Journey

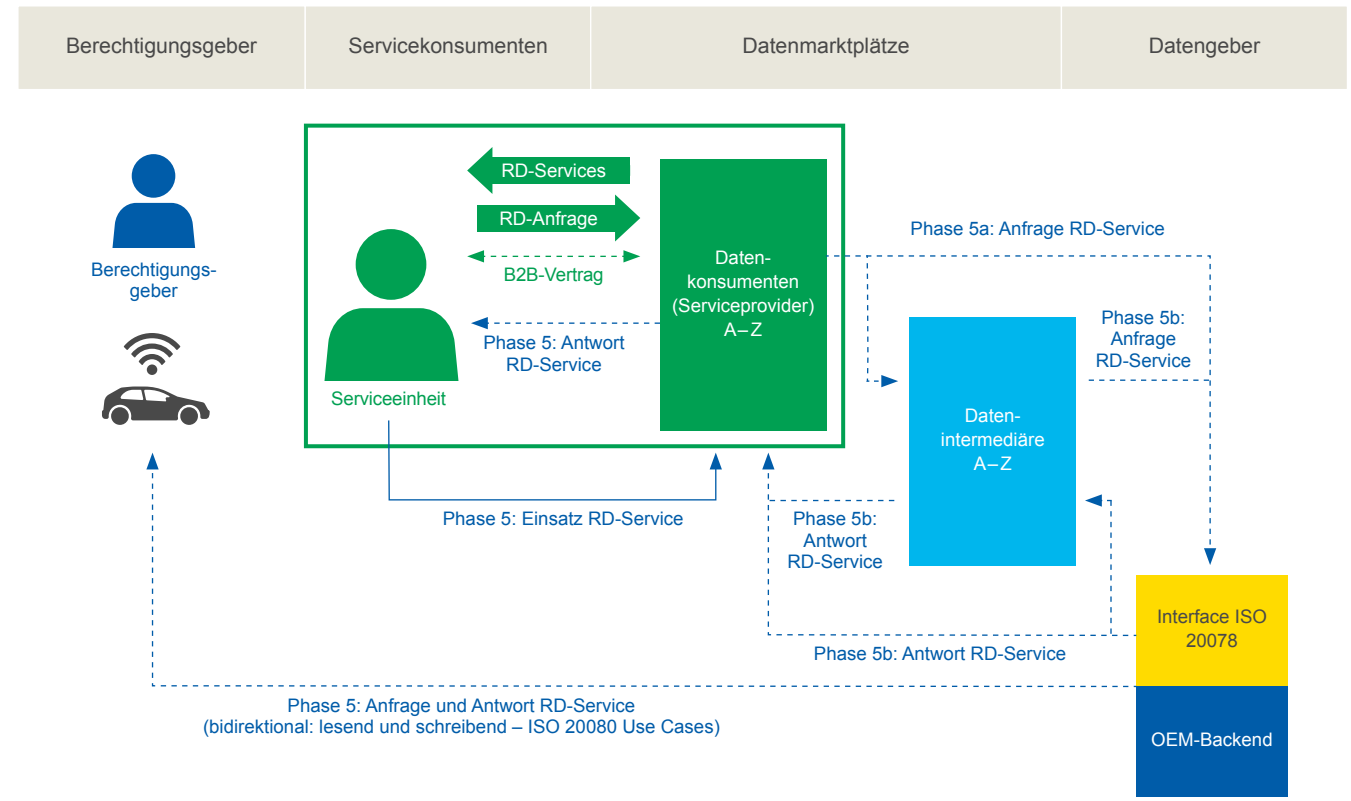
Aktivitätsstufen:	Phase 1***: Auswahl RD-Service **Berechtigungsgeber**	Phase 2: Beauftragung RD-Service **Berechtigungsgeber**	Phase 3: Einverständnis **Berechtigungsgeber**	Phase 4: Einsatz RD-Service durch **Serviceeinheit**
Aktion:	**Berechtigungsgeber** entscheidet sich für RD-Service einer **Serviceeinheit*** über einen RD-**Serviceprovider****	**Berechtigungsgeber** beauftragt die Serviceeinheit* zur RD über RD-**Serviceprovider****	**Berechtigungsgeber** gibt RD **Service Provider**** (ggf. **Intermediär)** Erlaubnis, Daten bidirektional über **OEM** abzufragen (lesend und schreibend)	**Serviceeinheit*** verwendet den durch den RD-**Serviceprovider**** bereitgestellten RD-Service
Berührungspunkt:		• RD-Serviceprovider-Web-Schnittstelle • (Ggf. Intermediär-Web-Schnittstelle)	• RD-Serviceprovider-Web-Schnittstelle • (Ggf. Intermediär-Web-Schnittstelle) • OEM-Web-Schnittstelle via OAuth	• RD-Serviceprovider-Web-Schnittstelle
Akteur:	• Berechtigungsgeber	• Berechtigungsgeber • Serviceeinheit • RD-Serviceprovider (beauftragt ggf. Intermediär)	• Berechtigungsgeber • RD-Serviceprovider (beauftragt ggf. Intermediär) • OEM	• Serviceeinheit • RD-Serviceprovider (beauftragt ggf. Intermediär) • OEM
Umgebung:		• Zugriff auf RD-Serviceprovider Schnittstelle	• Zugriff auf OEM-Schnittstelle	• Zugriff auf RD-Serviceprovider-Schnittstelle • Zugriff auf das Fahrzeug
Beschreibung:	• Berechtigungsgeber entscheidet, dass beauftragte Serviceeinheit* den RD-Service eines RD-Serviceprovider** konsumieren darf • RD-Serviceprovider** ist qualifizierter Serviceprovider für Diagnose (RMI) • Berechtigungsgeber akzeptiert lesenden und schreibenden Zugriff auf das Fahrzeug durch den RD-Serviceprovider** (ggf. Intermediär)	• Berechtigungsgeber beauftragt die Serviceeinheit* mit der Durchführung der RD über den RD-Service des RD-Serviceprovider** und initiiert den Einverständnisprozess • Berechtigungsgeber ist informiert, dass die Serviceeinheit* über den RD-Serviceprovider** eine Diagnosesitzung durchführt	• Berechtigungsgeber gibt Einverständnis, dass RD-Serviceprovider** den RD-Service für die Serviceeinheit* (ggf. über Intermediär) bereitstellen darf	• Berechtigungsgeber nutzt den RD-Service über die Serviceeinheit* durch den RD-Serviceprovider**

* Individuell ausführende Serviceeinheit = Servicekonsument.
** Remote-Diagnose-Serviceprovider = Datenkonsument.
*** Vorausgesetzt: Berechtigungsgeber ist bereits beim OEM registriert und Fahrzeug ist mit Benutzerkonto verknüpft.

Einverständnisprozess Remote-Diagnose (Phase 1 – 4)



Phase 5: Einsatz RD-Service durch Serviceeinheit



V.3. Glossar

Abkürzung	Bedeutung
ADAXO	Automotive Data Access – Extended & Open
API	Application Programming Interface
ASIL	Automotive Safety Integrity Level
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Government
CPU	Central Processing Unit
CSMS	Cybersecurity Management System
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
DSGVO	Datenschutz-Grundverordnung
ECU	Electronic Control Unit, elektronisches Steuergerät
ExVe	Extended Vehicle
FRAND	Fair, Reasonable and Non-Discriminatory
HMI	Human Machine Interface
HW	Hardware
NHTSA	National Highway Traffic Safety Administration
OBD	On-Board-Diagnose
OEM	Original Equipment Manufacturer
RAM	Random-Access Memory

Abkürzung	Bedeutung
RDS	Remote Diagnostic Support
ROA	Remote Online Access
SUMS	Software Update Management System
SW	Software
TRL	Die TRL-Unternehmensgruppe mit Sitz in Crowthorne House, UK, gehört der Transport Research Foundation (TRF) an.
UNECE	United Nations Economic Commissions for Europe
V2V	Vehicle-to-Vehicle-Kommunikation
VO	Verordnung
VSS	Vehicle Signal Specification

Ansprechpartner

Dr. Joachim Damasky
Geschäftsführer
joachim.damasky@vda.de

Matthias Krähling
Abteilungsleiter
matthias.kraehling@vda.de

Dr. Joachim Göthel
Senior Consultant
joachim.goethel@vda.de

Angela Pasch
Senior Consultant
angela.pasch@vda.de

Herausgeber
Verband der Automobilindustrie e. V.
Behrenstraße 35, 10117 Berlin
www.vda.de

Version
Version 1.0, Dezember 2021