Dicht gemacht

Immer mehr Fahrzeughersteller reglementieren den OBD-Diagnosezugang und bauen ihn zu einer gesicherten Schnittstelle aus. K+L-Betriebe tangiert das insofern, weil heute bei einer Unfallschadenreparatur standardmäßig ein Diagnoseprotokoll ausgedruckt werden sollte. Damit ist der Betrieb stets über die elektronischen Systeme des Fahrzeugs im Bilde und kann zugleich gegenüber dem Kunden und der Versicherung dokumentieren, welche Fehlercodes zu Beginn der Reparatur vorhanden waren und wie das Fahrzeug das Unternehmen nach der Reparatur verlassen hat. Darüber hinaus müssen auch Kalibrier- und Einstellarbeiten an modernen Fahrzeugen häufig über Steuergeräte und den entsprechend notwendigen Diagnosezugang angestoßen werden. Die Anbieter universeller Diagnosetechnik arbeiten mit Hochdruck an Lösungen für den freien Markt. Nur so sind auch zukünftig Chancengleichheit für alle Marktteilnehmer und ein fairer Wettbewerb gewährleistet.

Der Diagnosezugang für freie Betriebe wird zunehmend erschwert; Lösungen kommen nur mit Verzögerungen auf den Markt. (Bild: Bosch)

Schon lange erinnert die mehrmarkenfähige Fahrzeugdiagnose an ein Spiel zwischen Hase und Igel oder, um besser im Bild zu bleiben, David gegen Goliath. Zu keiner Zeit waren die Fahrzeughersteller begeistert, dass freie Werkstätten oder findige Tüftler mit teilweise günstigen Diagnosetools die Fahrzeugelektronik überprüfen, resetten oder anders codieren konnten. Selten gelang das auch vollumfänglich auf dem Niveau einer OEM-Diagnose, doch die meisten Diagnosearbeiten und

Fehlercodeauslesungen in der Werkstatt ließen sich bis dato noch immer recht gut mit einem universellen Diagnosesystem von autel, AVL DiTEST, Bosch, Hella Gutmann, Texa etc. erledigen. Dieses bewährte System war zudem notwendig, um den freien Wettbewerb aller am Reparaturmarkt beteiligten Player sicherzustellen.

Inzwischen ticken die Uhren etwas anders. Die Fülle der Fahrzeugelektronik, die Anzahl der Steuergeräte, neue Sicherheitsfeatures und die Vernetzung des Fahrzeugs mit der Umgebung sind auf einem bisher nicht gekannten Niveau angekommen, und diese Entwicklung wird sich künftig noch steigern. Inzwischen ist es so weit, dass selbst OEM-Betriebe das Auto nur noch mit dem Server beim Fahrzeughersteller verbinden und anschließend mehr oder weniger tatenlos zuschauen (müssen) und den Anweisungen des Operators folgen. Fragt der interessierte Kunde später, was denn konkret an seinem Auto gemacht und ggf. verändert wurde, erfolgt nur selten eine zufriedenstellende Antwort. Meist kommt lediglich der lapidare Hinweis auf ein notwendiges Software-Update durch den Hersteller.

Ein kleiner Auszug heute vorhandener Elektroniksysteme im Fahrzeug. (Bild: AVL DiTEST)

Regelmäßige Software-Updates in den Fahrzeugen – teilweise vom Besitzer unbemerkt via Over the Air-Kommunikation[1] – sind ein Indiz dafür, dass sich moderne Fahrzeuge nach der Übergabe an einen Nutzer in einem kontinuierlichen Entwicklungsflow befinden, bei dem der Hersteller die Zügel möglichst fest in der Hand halten will bzw. muss.

[1] Ein Over-the-Air-Update ist eine Software-Aktualisierung, die über eine Funkschnittstelle durchgeführt wird. Man kennt diese Technologie vom Smartphone, doch auch Fahrzeughersteller tauschen auf diese Weise Daten mit dem Fahrzeug aus und spielen neue Software ein.

Fehlercodes: Das Auslesen der Steuergeräte direkt nach der Fahrzeugübernahme und vor der Übergabe sollte Standard im K+L sein, um über den jeweiligen Status des Fahrzeugs im Bilde zu sein und Reklamationen vorzubeugen. (Bilder: AVL DiTEST)

Cyber-Security contra Fairness?

Denn ein einschneidendes Erlebnis für die Branche datiert aus dem Jahr 2015: Damals gelang es Hackern, die Software von Fiat/Chrysler-Fahrzeugen zu manipulieren und während der Fahrt auf Bremse, Einspritzung und Türverriegelung zuzugreifen. In der Folge entschieden einige Fahrzeughersteller – und auch der Gesetzgeber –, Fahrzeuge mit einem gesicherten Zugang auszurüsten. Zur eigenen Produktabsicherung und zum Schutz der Kunden sind die Hersteller stets bemüht, ihre Fahrzeuge nach höchsten Qualitäts- und Sicherheitsstandards abzusichern. Darüber hinaus definiert die UNECE Regularie Work Package 29 die Einführung von Sicherheitsmaßnahmen im Hinblick auf Cyber-Security – siehe auch q-perior.com. Auf EU-Ebene vor allem relevant ist die Verordnung 2018/858 des EU-Parlaments und des Rates vom 30.05.2018. In der seit Herbst 2020 gültigen Richtlinie 2018/858 sind spezielle Zertifikate aus Gründen der Sicherheit (Cyber-Security) erlaubt. Verschlüsselt sind nicht die Daten selbst, für den Zugang, um diese auslesen oder Diagnosedienste durchführen zu können, muss man aber bestimmte Kriterien erfüllen (Authentifizierung).

Das neue gesetzliche Regularium wird gerne dafür herangezogen, die Notwendigkeit einer geschützten Diagnoseschnittstelle plausibler zu machen und in gewisser Weise zur rechtfertigen. Allerdings dürfen niemals die möglichen Auswirkungen für den frei-

en Wettbewerb außer Acht gelassen werden! Wer genau hinschaut, erkennt, dass das in der Verordnung im Anhang X unter den Punkten 2.8 und 2.9 im Prinzip recht klar geregelt ist .

- 2.8: Für die Zwecke von Nummer 2.6.2, falls die Hersteller in ihren Vertragswerkstätten Diagnose- und Prüfgeräte gemäß ISO 22900 „Modular Vehicle Communication Interface (MVCI)“ und ISO 22901 „Open Diagnostic Data Exchange (ODX)“ verwenden, müssen die ODX-Dateien unabhängigen Marktteilnehmern über die Internetseite des Herstellers zur Verfügung gestellt werden.

- 2.9: Für die Zwecke der Fahrzeug-OBD sowie der Fahrzeugdiagnose, -reparatur und -wartung ist der direkte Fahrzeugdatenstrom über einen seriellen genormten Datenübertragungsanschluss gemäß der UN-Regelung Nr. 83, Anhang 11, Anlage 1, Nummer 6.5.1.4 und der UN-Regelung Nr. 49, Anhang 9B, Nummer 4.7.3 bereitzustellen.

Standardisierter Zugriff notwendig

Die momentanen Entwicklungen in der Fahrzeugdiagnose lassen sich allerdings mehr so deuten, dass die geschützte Schnittstelle zur zusätzlichen Diagnosehürde für den freien Markt wird. Harald Hahn (*Bild rechts*), Leiter des ASA[2]-Fachbereichs Diagnose und Abgasmessgeräte in [1]: „In Zeiten der autonomen Fahrstrategien steht die Sicherheit der Fahrfunktionen hoch im Kurs, sodass vom Verordnungsgeber ein ungeschützter und ungewollter Zugriff auf das Fahrzeug und seine Fahrfunktionen nicht erwünscht ist. Wichtig wäre aber trotz aller Restriktionen, dass es einen standardisierten sicheren Zugriff gibt. Jeder Fahrzeughersteller implementiert heute sein eigenes Authentifizierungssystem. Es gibt kein standardisiertes Vorgehen. Dies führt dazu, dass man zukünftig bestimmte Diagnosedienste nur durchführen kann, wenn man autorisiert ist und das Diagnosetool sehr streng an die Herstellerumgebung angebunden ist.“

Inzwischen sind mehrere Fahrzeughersteller dazu übergegangen, die Diagnoseschnittstelle der Autos mit einem gesicherten Zugang auszustatten. Vorreiter war Fiat Chrysler Automobiles (FCA). Mercedes-Benz implementierte sein Sicherheitskonzept CeBAS[3] Mitte 2020 beginnend mit der E-Klasse Facelift. Es folgte die S-Klasse. Volkswagen sichert seit 2020 seine neuen Modelle durch SFD[4], beginnend mit dem

[2] ASA: Der Bundesverband der Hersteller und Importeure von Automobil-Service Ausrüstungen (ASA) vertritt die Interessen der in Deutschland aktiven Werkstattausrüster.

[3] CeBAS: Certificate Based Automotive Security.

[4] SFD: Die Volkswagen Gruppe führt mit der neuen MQB2020 (MQBevo)-Plattform eine neue Sicherheitsfunktion, die sogenannte SFD (Schutz Fahrzeug Diagnose) ein. Um Zugang zu Anpassungen/Codierung zu erhalten, muss das Steuergerät mit einem speziellen Token freigeschaltet werden.

Golf 8. Betroffen sind auch Audi (A3), Seat (Leon) und Skoda (Octavia). Renault hat in den jüngsten Modellen des ZOE, Captur und Clio das sogenannte CAN-Gateway implementiert. Kia, Hyundai und Nissan haben 2020 ebenfalls Fahrzeuge mit eigenen Sicherheitskonzepten auf den Markt gebracht (diese kurze Aufzählung erhebt keinen Anspruch auf Vollständigkeit und wird sich vermutlich in der nächsten Zeit noch verlängern). Was bereits deutlich wurde: So wie die bekannte OBD-Diagnoseschnittstelle zwar optisch standardisiert, aber nicht auf allen Pins gleich belegt ist, unterscheiden sich die geschützten Zugänge und Verschlüsselungen bei den Fahrzeugherstellern. Das macht es für die Anbieter von Mehrmarkendiagnosetechnik kompliziert und vor allem teuer – siehe dazu auch den Kasten am Ende des Beitrags.

Einige Beispiele für Fahrzeughersteller mit Zugangsbeschränkungen bei der Diagnose (ohne Anspruch auf Vollständigkeit). (Bild: AVL DiTEST)

Unterschiedliche Verfahren

Viele Fahrzeughersteller verwenden bei den Security Gateways (SGW) elektronische Authentifizierungsverfahren, die freie Reparaturbetriebe durchlaufen müssen, um Diagnose- oder AU-relevante Daten mit Multimarkentestern aus den Fahrzeugen auslesen zu können. Diese Authentifizierungsverfahren benachteiligen laut ASA-Verband die markenunabhängigen Betriebe im Wettbewerb [2]:

> „Einige Fahrzeughersteller schotten die Zugänge über die OBD-Ports zu Diagnose-, Reparatur- und wartungsrelevanten Daten komplett ab und bieten für den Independent Aftermarket (IAM) bislang keine Zugangsmöglichkeiten. Andere nutzen Security Gateways, um den Zugang zu ermöglichen, doch jeder Hersteller definiert frei und individuell das Authentifizierungsverfahren über sein SGW. Werkstätten und Werkstattausrüster haben es mit zig unterschiedlichen Authentifizierungsverfahren zu tun, da die Verfahren nicht vom Gesetzgeber für die gesamte Automobilindustrie standardisiert vorgegeben sind.
>
> Der Wettbewerbsnachteil wird durch die Preisgestaltung einiger Automobilhersteller für den Datenzugang über SGW verstärkt. Die teilweise verlangten Gebühren für die Authentifizierungsverfahren

über Security Gateways lassen sich kaum mit der gesetzlichen Forderung nach diskriminierungsfreier zur Verfügung Stellung in Einklang bringen. Fahrzeughersteller schützen den OBD-Port über SGW uneinheitlich, welche Daten frei zugänglich und wie sie nutzbar sind. Die Bandbreite reicht von ausschließlich zugänglichen EOBD-Daten (Emission) bis zu Reparatur- und wartungsrelevanten Daten. Diese können teilweise nur ausgelesen werden, schreibender Zugriff ist bei vielen Herstellern nicht möglich, was beispielsweise das Löschen von Fehlercodes und damit Fehlermeldungen, die Fahrzeugführer im Display angezeigt bekommen, unmöglich macht."

Nachgefragt

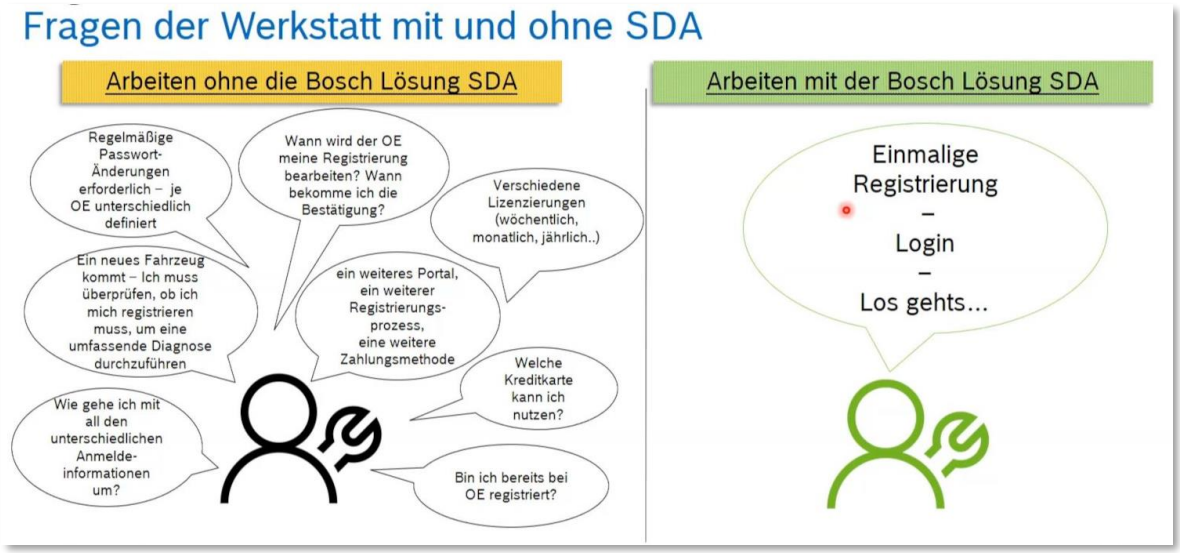
Eine Nachfrage bei Diagnoseanbietern (Bosch und Hella-Gutmann) zur aktuellen Situation und möglichen Lösungen ergab folgendes Bild: Laut Bosch sind passive Diagnosen (z.B. Fehlercodes lesen) in der Regel noch ohne Entschlüsselung möglich. Aktive Diagnosearbeiten wie die Kalibrierung von Fahrerassistenzsystemen können unter Umständen nicht mehr möglich sein. Auch eine Service-Rückstellung kann ggf. nicht mehr erfolgen. Für diese Arbeiten ist bei den Individuallösungen der Hersteller ein kostenpflichtiger Zugang notwendig.

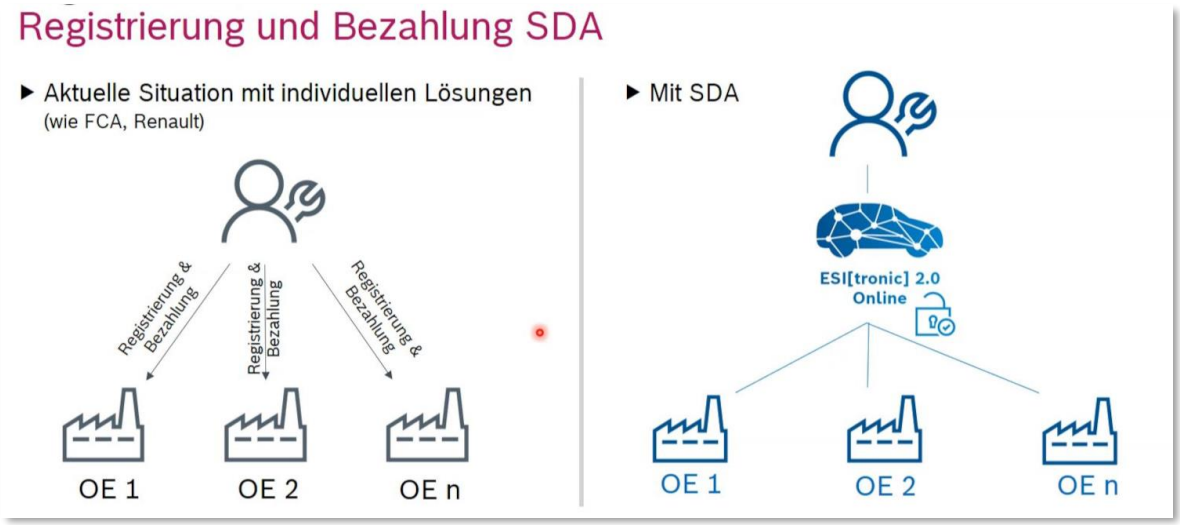
Um diesen auf die Steuergeräte der betroffenen Fahrzeuge zu bekommen, sind bei Bosch ein KTS der neusten Generation (zum Beispiel KTS 560/590), eine lizensierte ESI[tronic] (mindestens Infoart SD-Steuergerätediagnose) und ein Internetzugang erforderlich. Alternativ lässt sich ein KTS 350 oder KTS 250 verwenden. Die Preise dafür starten bei rund 2000 Euro. Die Module sind auch als Bundle mit Laptop erhältlich (KTS 960, KTS 980 oder KTS 995 inklusive Messtechnikmodul FSA 500).

Bosch KTS 250 unterstützt DoIP (Diagnostics over Internet Protocol) – die neue, auf Ethernet basierende Diagnoseschnittstelle. Diese ermöglicht deutlich höhere Daten-Übertragungsgeschwindigkeiten. Immer mehr Fahrzeughersteller setzen Ethernet auch für die Diagnose ein, nachdem die moderne Schnittstelle schon längere Zeit auch für das Flashen der Steuergeräte genutzt wird. Der KTS 250 ermöglicht zudem die parallele Kommunikation mit verschiedenen Steuergeräten auf unterschiedlichen Kommunikationskanälen. (Bild: Bosch)

Bei Bosch gibt es in der Esitronic seit zwei Jahren die Links zu FCA und Renault/Dacia, um sich dort zu registrieren, sowie eine Freischaltfunktion, um sich mit den Autorisierungsdaten dieser Hersteller aus der ESI heraus anzumelden. Seit August hat Bosch seine Lösung „SDA" (Secure Diagnosis Access) in der Esitronic Online 2.0 integriert, mit der nur noch eine einmalige zentrale Registrierung für die sogenannte Bosch-ID erforderlich ist. Zunächst ist geplant, dass über SDA der Zugang zu Fahrzeugen von VW, Audi, Seat und Skoda zur Verfügung steht. Mit weiteren Fahrzeugherstellern soll die SDA-Abdeckung kontinuierlich erweitert werden. Dazu ist Bosch in Kontakt mit den Fahrzeugherstellern und will zeitnah weitere Herstellerlösungen in SDA aufzunehmen.

Loggt der Nutzer sich im Anschluss an die Registrierung mit der Bosch-ID innerhalb der Esitronic ein, erhält er Zugriff auf die geschützten Diagnosefunktionen der teilnehmenden Marken. Dafür fallen zukünftig keine weiteren Kosten außer der Lizenzgebühr für die Esitronic an. Die Kosten für die Nutzung der geschützten Diagnosedaten sind in der Lizenzgebühr für die Steuergerätediagnose enthalten. Bis zur Integration von FCA und Renault/Dacia in die Bosch SDA sind die Kosten allerdings noch bei diesen OE direkt fällig.

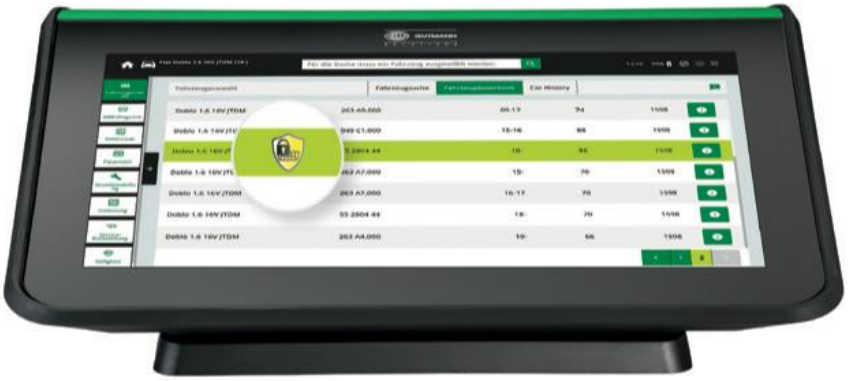




Mit der Lösung „SDA“ (Secure Diagnosis Access) innerhalb der Esitronic Online 2.0 ist nur noch eine einmalige, zentrale Registrierung für die Bosch-ID erforderlich. (Bilder: Bosch)

Hella Gutmann bestätigte, dass das Lesen von Fehlercodes bisher nicht betroffen war. Allerdings soll es bereits ein erstes Top-Modell eines deutschen Herstellers geben, bei dem auch das unmöglich ist. Um Zugang auf die Steuergeräte der gesicherten Fahrzeuge zu bekommen, muss sich der Mitarbeiter, der die Diagnose mit Hella Gutmann durchführen will, persönlich authentifizieren und den Zugriff beantragen. Das Wie wird bei jedem Hersteller anders gehandhabt. Seit Anfang 2021 hat Hella Gutmann eine markenübergreifende Lösung für ein Cyber-Security-Manage-

ment in die mega macs-Software implementiert, mit der der Mitarbeiter in der Werkstatt sich nur ein Mal in seinem Diagnosegerät authentifizieren muss, ohne in ein OE-Portal zu gehen. Das Cyber-Security-Management steht bei den mega macs-Geräten 42SE, 56, 66, 77 und mega macs PC seit dem Update auf die Software-Version 60 zur Verfügung. Nach dem Login kann der Anwender wie gewohnt alle gesicherten Kundenfahrzeuge diagnostizieren.



Das Cyber-Security-Management steht bei Hella Gutmann den mega-macs-Geräten 42SE, 56, 66, 77 und mega macs PC seit dem Update auf die Software-Version 60 zur Verfügung. (Bild: Hella Gutmann Solutions)

Auf Betriebe, die sich selbst bei einzelnen Hersteller-Portalen authentifizieren und für jedes einzelne Kundenfahrzeug Freischaltungen beantragen, kommen in der Regel Gebühren seitens der Hersteller hinzu. Diese variieren: manche Hersteller berechnen eine einmalige Software und Freischaltungen per USB-token oder andere pro Fahrzeugzugang. Mache berechnen Tagesflats. Auf Anwender (reale Personen, nicht ganze Betriebe), die mit Diagnosetechnik von Hella Gutmann arbeiten und sich einmalig online bei dem Anbieter authentifizieren, werden derzeit seitens Hella Gutmann keine Kosten umgelegt. Langfristig ist parallel zur Zunahme der Hersteller und deren Gebühren ein kleiner Obolus nicht ausgeschlossen. Zu den ersten integrierten Marken gehören FCA und Mercedes-Benz, gefolgt von VW und Kia. Hyundai, Nissan und Renault sollen in Kürze folgen. Die Abdeckung wird schrittweise mit den gesicherten Modellen der Hersteller wachsen.

Aus dem Hause AVL DiTEST ist zu hören, dass man sich derzeit mit Volkswagen in der Konzeptphase für einen Zugang in geschützte Fahrzeuge befindet. Wie in [3] berichtet wird, bietet auch die ADIS-Technology GmbH aus Aachen mit dem EuroDFT-Diagnosegerät uneingeschränkten Zugang bei der Fahrzeug-Diagnose. Dazu heißt es in [3]:

> „Zwölf Markensysteme sind auf dem EuroDFT implementiert, darunter auch solche mit SGW, wie Mercedes-Benz oder VW. Nutzer können somit Arbeiten am Fahrzeug vollständig nach Herstellervorgaben ausführen. Um möglichst wenig bürokratischen und technischen Aufwand zu haben, übernimmt ADIS-Technology für die Anwender sowohl die Registrierung bei den Fahrzeugherstellern als auch die Updates der Herstellersoftware.“

Auch die Firma Texa bietet Möglichkeiten, das geschützte Gateway bei Renault-Fahrzeugen zu entsperren, um eine Diagnose durchzuführen. Wie das Unternehmen informiert, muss sich der Anwender dazu auf der Website asos.renault.com registrieren, einen Token (USB-Stick) erwerben und eine spezielle Anwendung herunterladen. Außerdem ist eine Navigator TXTs Fahrzeugschnittstelle notwendig, die im

Pass-Thru-Modus[5] arbeiten kann. Zusammen mit dem Token erhält der Mechaniker eine Benutzer-ID und ein Passwort für den Zugriff auf die Entriegelungsfunktionen des Fahrzeugs.

Fazit

Die aktuellen Lösungen der Diagnosegerätehersteller für den freien Markt könnten suggerieren, dass alles in Ordnung sei. Für Harald Hahn stellt sich das nicht so dar:

> „Die aktuelle Zugangspraxis über die OBD-Ports ist nach unserem Dafürhalten nicht mit den Vorschriften der Typzulassungsverordnung in Einklang zu bringen. Wir stimmen uns hierzu eng mit den Kollegen innerhalb der EGEA[6] und anderen europäischen Verbänden ab. Im Verbund mit AFCAR[7] unternehmen wir intensive Anstrengungen. Auch auf nationaler Ebene gibt es dazu Arbeitskreise, die sich intensiv mit dem Zugriff auf Daten beschäftigen. Aktuell ist nur der Zugang über die OBD-Schnittstelle gesetzlich abgesichert. Anwendungen wie Telematiks oder Diagnostic over the air werden zukünftig noch wichtiger werden. Auch dieses Thema wird aktuell im Rahmen der Cyber-Security-Diskussion mit adressiert. Für künftige „over the air-Zugriffe“ auf Fahrzeuge favorisieren die Fahrzeughersteller das Modell ExVE (extended vehicle). Das lehnt der IAM nicht nur deshalb ab, weil es für den Zugriff auf Echtzeitdaten völlig untauglich ist. Die Hersteller behielten beim Modell ExVE immer die Kontrolle, auch über den Wettbewerb, und würden stets erfassen können, wer gerade mit wem worüber kommuniziert.“

Stattdessen schlagen die Befürworter des freien Marktes für alle Zugriffe auf Fahrzeugdaten die Umsetzung des Modells S-OTP (secure open telematics platform) vor. Hahn: „Dabei kann man den Sicherheitsbedenken der Fahrzeughersteller vor unzulässigem, manipulativen Zugriff auf Fahrzeugsysteme von außen sehr wirksam mit dem Sicherheitszertifizierungssystem SERMI begegnen.“

Zu keiner anderen Zeit war es so schwierig für den freien Markt, ungehinderten Diagnosezugang in moderne und vom Fahrzeughersteller speziell geschützte Modelle zu bekommen. Aus Sicht der GVO und des fairen Wettbewerbs ist das durchaus fragwürdig und auf EU-Ebene zügig zu diskutieren. Unter dem Schlagwort Cyber-Security schottet eine zunehmende Zahl von Fahrzeugherstellern ihre Modelle ab, ohne den freien Markt überhaupt darüber zu informieren oder zeitnahe Lösungen anzubieten. Mitunter wird bei E-Fahrzeugen sogar schon die OBD-Schnittstelle eliminiert, weil im Zuge der AU keine abgasrelevanten Informationen mehr ausgelesen werden müssen. Alle großen Diagnosegeräteanbieter arbeiten an Lösungen, um auch künftig den freien Betrieben das Werkstattgeschäft zu ermöglichen. Der Aufwand und die

---

[5] Die von der Society of Automotive Engineers (SAE) definierte J2534 beschreibt eine Programmierschnittstelle zum hexadezimalen Zugriff auf Diagnoseprotokolle. Wurde sie ursprünglich nur für den Einsatz als Programmierschnittstelle in freien Werkstätten initiiert, wird die PassThru API heute auch für viele andere Aufgaben in der Diagnose eingesetzt, insbesondere für OBD-Aufgaben.

[6] Die European Garage and Test Equipment Association (EGEA) wurde 1980 gegründet und ist der europäische Dachverband und die politische Vertretung der Hersteller von Werkzeugen und Geräten für die Reparatur, Wartung und technische Inspektion von Fahrzeugen in Brüssel.

[7] AFCAR: Alliance for the Freedom of Car Repair in Europe.

Kosten dafür steigen weiter – für die Betriebe und am Ende für den Kunden bzw. alle, die an der Schadenreparatur beteiligt sind.

Wettbewerbsverzerrung

In einem Interview mit der Fachzeitschrift Krafthand vom 23.10.2021 äußerte sich **Jordi Brunet**, Generalsekretär der EGEA, zu den aktuellen Diagnose-Herausforderungen des freien Marktes und vorhandenen Problemfeldern [4]. Die European Garage and Test Equipment Association (EGEA) wurde 1980 gegründet und ist der europäische Dachverband und die politische Vertretung der Hersteller von Werkzeugen und Geräten für Reparatur, Wartung und technische Inspektion von Fahrzeugen in Brüssel. Relevante Inhalte aus dem Interview mit Jordi Brunet in Kurzform:

- Einige Fahrzeughersteller verwenden kein Security Gateway mehr, sondern sogenannte Cyber-Security-Algorithmen an verschiedenen Stellen innerhalb der Fahrzeugarchitektur, die den Zugang erschweren.

- OBD-Zugangsbeschränkungen werden ohne zeitnahe Informationen des freien Marktes installiert; mintunter gibt es Verzögerungen von Monaten bis zu Jahren.

- Verfügbare OEM-Diagnosezugänge basieren auf unterschiedlichen und nicht standardisierten Technologien; werden diese auf einem Rechner installiert, kann es zu Störungen kommen.

- Daten für Reparatur, Diagnose, Wartung und Mechanik werden im OEM-Diagnosetool integriert und unabhängigen Betreibern nicht verfügbar gemacht; teilweise sind die Vorschriften in der Typgenehmigung dafür nicht spezifisch genug formuliert oder werden von den OEMs anders ausgelegt.

- Durch neue UNECE-Vorschriften zur Cybersicherheit kann sich die aktuelle Situation und Beschränkung des freien Marktes künftig weiter verschärfen.

- Die Typgenehmigungsverordnung EU 2018/858 hat Cyber-Security noch nicht vollständig abgedeckt; die EU-Kommission arbeitet an Änderungen, um sicherzustellen, dass keine rechtlichen Lücken bestehen, die ggf. ausgenutzt werden könnten.

- Auch E-Fahrzeuge brauchen einen OBD-Zugang für alle im Fahrzeug verfügbaren Daten, selbst wenn dort keine emissionsrelevanten Daten anfallen und abgerufen werden müssen; momentan wird das teilweise falsch ausgenutzt und bedarf einer umgehenden Klarstellung und sofortigen Lösung.

- Mit der Entwicklung des vernetzten Fahrzeugs und des automatisierten Fahrens versuchen die Fahrzeughersteller die Kontrolle über den Zugang zum Fahrzeug zu bekommen und berufen sich auf Cyber-Security; der Gesetzgeber muss ein Gleichgewicht zwischen Cyber-Sicherheit und freiem Wettbewerb sicherstellen.

Quellenhinweise

[1] Pressestatement des ASA-Bundesverbandes e. V. vom 17.03.2020.

[2] ASA-Pressgespräch 2021 „Hohe Aufgabendichte in der Pandemie“, PI 02-02/2021 vom 25.02.2021.

[3] Fachzeitschrift autoservicepraxis (asp), „Security Gateway: Auf sicheren Wegen“ vom 21.1.2021.

[4] Fachzeitschrift Krafthand: „Freiheit, Gleichheit, fairer Wettbewerb“ in Ausgabe 20/2021.