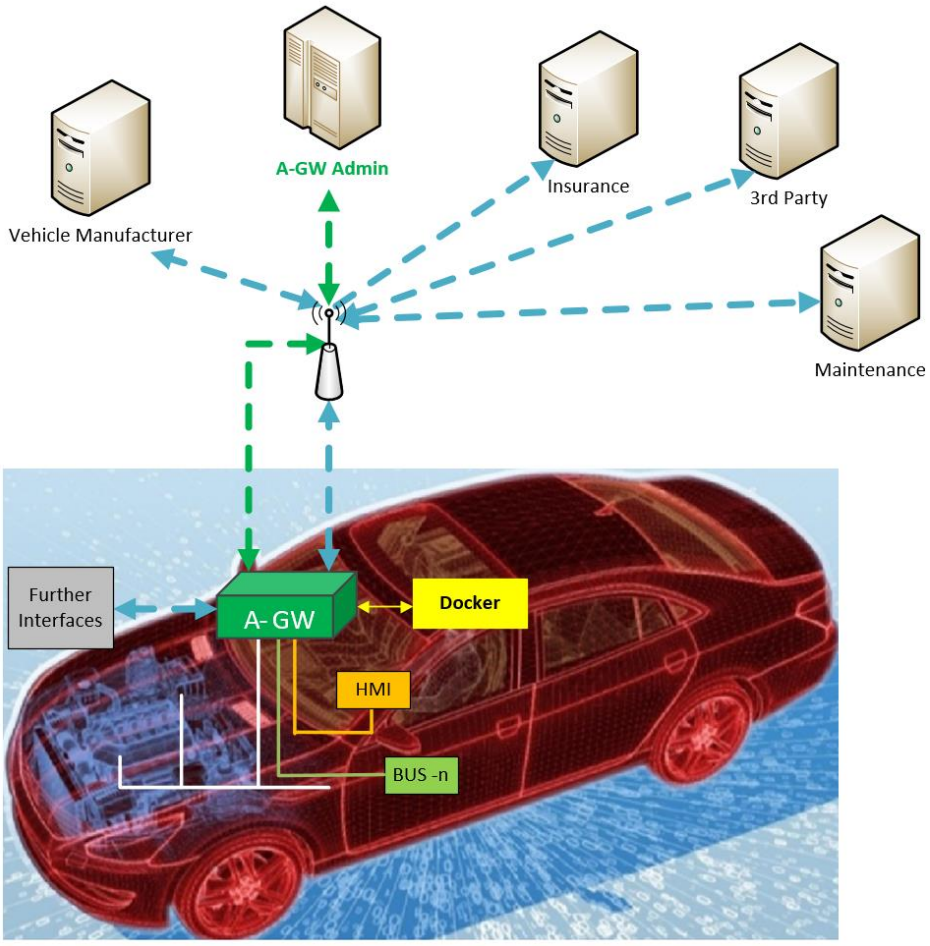
FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA

IT Security
der
On-Board Telematik Plattform[1]



Version: **1.0**

Datum: **16.06.2020**

Autoren: **Markus Bartsch**
Markus Wagner

[1] Basierend auf der englischen Fassung der FIA Studie „On-board Telematics Platform Security“

Inhaltsverzeichnis

Abbildungsverzeichnis

Vorwort

Dieses Dokument basiert auf der englischen Fassung der FIA Studie „On-Board Telematics Platform Security“, die durch die TÜV Informationstechnik (TÜViT – Unternehmensgruppe TÜV NORD) bearbeitet und im Juni 2020 abgeschlossen wurde [FIA]. Gliederung und Struktur des englischen Originaltextes wurden beibehalten. Um Missverständnisse aufgrund der dominanten englischen Sprache in der IT Security Industrie zu vermeiden, wurden viele Anglizismen genutzt, die sich auch in den (zumeist nicht übersetzten) Abbildungen wiederfinden. So wird z. B. das Wort „Security“ konsequent für Thematiken zur Cybersecurity“ verwendet, das Wort „Safety“ im Kontext vom „Schutz für Leib und Leben“ genutzt. Das im Deutschen für beide Thematiken gemeinsam verwendete Wort „Sicherheit“ wird nur dann verwendet, wenn es sich auf beide Aspekte – „Security“ wie auch „Safety“ – bezieht. Darüber hinaus gibt es bei vielen Bezeichnungen keine adäquat verwendbaren deutschen Begriffe oder selten verwendete deutsche Übersetzungen, wie beispielsweise bei „Asset“, „Protection Profile“, „Objective“. Im Abschnitt 4.2.1 – (Benutzer-) Rollen – werden jeweils auch die englischen Begriffe zu den einzelnen Parteien mit aufgeführt.

Im Zweifelsfall gilt der Text aus der englischen Studie.

Zusammenfassung

Die Digitalisierung prägt zunehmend das Umfeld von Menschen und Unternehmen. Das Internet der Dinge (IoT) hat das Potenzial, alles mit allem zu verbinden. Im Automobilsektor werden Fahrzeuge zunehmend mit Backend-Diensten als Vorbereitung für den vernetzten Verkehr der Zukunft verbunden. Die Weiterentwicklung von Kommunikationsnetzen, z. B. das Aufkommen von 5G (bei derzeit über 60 Millionen mit 3G und 4G verbundenen Fahrzeugen), treibt diesen grundlegenden Wandel zwar voran, bietet aber auch neue Möglichkeiten zum Angriff auf die Integrität von Fahrzeugsystemen oder zum Datendiebstahl über Fernzugriff (per remote Zugriff).

Auf der anderen Seite erhalten verschiedene Interessengruppen im Automobilbereich, wie Hersteller (OEM), unabhängige Dienstleister (ISP), Zulieferer, Prüfer oder die Fahrzeughalter selbst, remote Zugriff auf einige Daten, Funktionen und Ressourcen des Fahrzeugs. Dieser Fernzugriff ist derzeit ausschließlich über das Extended Vehicle-Modell des OEMs möglich. Um ein Datenmonopol zu vermeiden und einen fairen Wettbewerb zu ermöglichen, sind andere Zugriffsmodelle auf Daten und Funktionen erforderlich, damit unabhängige Dienstleister im Sekundärmarkt mit dem OEM konkurrieren können.

Für Mobilitätsclubs, die der FIA-Region I angeschlossen sind, ist es von größter Bedeutung, Daten direkt aus dem Fahrzeug zu erhalten. Unabhängige Testeinrichtungen, unabhängige Werkstätten und Mobilitätsclubs benötigen Diagnoseinformationen und Zugriff auf fahrzeuginterne Daten und Funktionen. Der direkte Zugriff auf die Fahrzeugdaten von internen Kommunikationsbussen, Steuerungen und Sensoren trägt entscheidend dazu bei, dass alle Marktanbieter ihre Aufgaben unabhängig und ohne Kontrolle durch den OEM ausführen können.

Natürlich muss solch ein unabhängiger Datenzugriff durch autorisierte ISPs sicher (im Sinne von „Security“) abgebildet werden, was regelmäßige Security Updates durch den OEM erfordert. Wenn Updates für den Hersteller nicht mehr kommerziell interessant wären, z. B. 5-8 Jahre nach dem Verkauf eines neuen Fahrzeugs, wäre die Sicherheit des Fahrzeugs gefährdet, bis es verschrottet wird. Folglich wäre der Verbraucher gezwungen, das Fahrzeug aus dem Verkehr zu ziehen, um sich ein Neues zuzulegen, das mit regelmäßigen Updates unterstützt wird. Daher muss während der Lebenszeit (*Lifetime*) des Fahrzeuges ein Gleichgewicht zwischen dem direkten remote Zugriff auf fahrzeuginterne Daten und Funktionen einerseits und modernsten IT Security Maßnahmen andererseits hergestellt werden. Der Bericht zeigt, dass es möglich ist, den direkten remote Zugriff auf fahrzeuginterne Daten, Funktionen und Ressourcen mit modernsten IT Security Maßnahmen zu kombinieren.

Dieser Bericht beschreibt ein IT Security Konzept für die On-Board-Telematik Plattform (OTP), welches Vertrauen in Schutzmechanismen zugunsten der Privatsphäre von Fahrer und Insassen schafft. Die OTP besteht im Auto aus einem Automotive Gateway (A-GW), das

für die Sicherung des Fernzugriffs zum und vom Fahrzeug zuständig ist sowie Docker Einheiten, auf denen Apps der ISPs ausgeführt werden können, mit denen Fahrzeughalter, Fahrer oder Insassen über eine Benutzerschnittstelle (HMI[2]) interagieren können.

Die OTP besteht zusätzlich aus einem externen System (A-GW: Automotive Gateway Administrator) zur Verwaltung der IT Security Funktionalitäten, das auf einer Public Key Infrastructure (PKI) basiert. Es wird die Idee verfolgt, die Daten des Fahrzeugs möglichst dort zu belassen, wo sie auftreten, nämlich im Auto selbst und nicht auf Backend-Servern wie dem Extended Vehicle. Dabei würden alle Parteien wie folgt hiervon profitieren:

- IT Security by Design als Grundlage für den vernetzten Verkehr der Zukunft und über die gesamte Fahrzeuglebensdauer;
- Privacy by Design (wenn die Daten das Fahrzeug verlassen, werden wichtige Aspekte der Europäische Datenschutzgrundverordnung automatisch eingehalten);
- Manipulationssichere Technologien durch ein eingebettetes, hochsicheres Automotive Gateway;
- Keine Überwachung unabhängiger Dienstleister durch den Fahrzeughersteller als Sekundärmarkt-Dienstleister;
- ISP können zum Nutzen des Verbrauchers (kosten- und qualitätsabhängige Produkt- und Dienstleisterwahl) direkten remote Zugriff auf fahrzeuginterne Daten, Funktionen und Ressourcen erhalten sowie Apps an Bord des Fahrzeugs ausführen;
- Die Benutzerschnittstelle (HMI) des Fahrzeugs – wie die Instrumente oder das Infotainment-Display des Fahrzeugs – ermöglicht die direkte und sichere Kommunikation mit Fahrzeugnutzern und remote Service Providern.

In diesem Sinne steht die OTP für:

- Verbesserungen der Sicherheit und des Umweltschutzes durch Monitoring der entsprechenden Systeme des Fahrzeugs, ohne die Privatsphäre der Fahrzeuginsassen zu beeinträchtigen;
- Vertrauenswürdiger Zugriff auf fahrzeuginterne Daten, deren Funktionen und Ressourcen durch IT Security Mechanismen eines unabhängigen, neutralen A-GWA unter Beachtung des „Separation-of-Duties-Prinzips“ umgesetzt werden;
- Eine zukunftssichere Lösung durch hochsichere und flexible Aktualisierungsoptionen und unter Berücksichtigung von C-ITS[3];
- Schaffung der Voraussetzungen für die freie Wahl der Dienstleister, die dem Verbraucher Leistungen mit Mehrwert zu einem konkurrenzfähigen Preis bieten;
- Die Möglichkeit, dem Verbraucher neue, innovative Dienstleistungen aller Dienstleister, einschließlich des Herstellers in seiner Rolle als Sekundärmarkt-Dienstleister und der ISPs, in einem fairen Wettbewerb anzubieten, von dem der Verbraucher voll und ganz profitieren kann;
- Bestmöglichen Schutz des Autofahrers und der Insassen vor IT-Security Vorfällen und Datenschutzverletzungen;

[2] Human Machine Interface

[3] Cooperative Intelligent Transport Systems (kooperative intelligente Verkehrssysteme)

- Verbraucherseitige Kontrolle des Datenflusses zum und vom Fahrzeug durch Opt-In- und Opt-Out-Funktionen.

Die sogenannten Common Criteria (CC) sollen verwendet werden, um die notwendigen IT Security Funktionen im OTP korrekt zu implementieren. Als internationaler ISO-Standard und durch das SOG-IS-Abkommen in Kombination mit dem neuen Cybersecurity Act (CSA) werden die CC von allen europäischen Mitgliedstaaten sowie von vielen Nationen weltweit akzeptiert. Es wird zusätzlich ein *Protection Profile* (PP) publiziert, dass gemäß den CC die wichtigsten IT Security Merkmale (End-to-End Security, Zugriffskontrolle, …) des A-GWs als zentrale IT Security-Komponente des OTP beschreibt. Zusammen mit einer End-to-end-Verschlüsselung von eingehenden und ausgehenden Fahrzeugnachrichten kann so für moderne, bezahlbare Fahrzeugsicherheit gesorgt werden.

1 Einführung

1.1 Motivation

Verkehrssicherheit und Umweltschutz sind Treiber für Innovation, Investition, Wachstum und Arbeitsplätze in der Automobilindustrie. Einer der heutigen Treiber von Innovation ist die **Informationstechnologie** in vernetzten Fahrzeuge um z.B. die Sicherheit zu erhöhen, die Umwelt weniger zu belasten und den Komfort für den Fahrer zu erhöhen. Safety-relevante Applikationen oder Assistance Systeme sollen Unfälle vermeiden bzw. mildern und aktuelle Verkehrsinformationen im Navigationssystem unterstützen den Fahrer bei der Auswahl geeigneter Routen. Die Vermeidung von Staus, ihre schnellere Auflösung und die unterstützte „smartere“ Anpassung des Fahrverhaltens helfen die Umwelt zu schützen und erhöhen den Fahrkomfort für die Insassen. In den nächsten Jahren wird das Verkehrsaufkommen in der Europäischen Union und speziell den Transitländern erheblich steigen und ihre Grenzen erreichen. Eine Investition in kooperative intelligente Verkehrssysteme (C-ITS) auf Basis des Informationsaustausches von vernetzten, mit intelligenten Assistenzsystemen ausgestatteten Fahrzeugen macht in dem Zusammenhang Sinn.

Zusätzlich erlaubt die Digitalisierung **innovative Ansätze** für unabhängige Service-Dienstleister (ISP). Lokale Diagnosen im Falle von Fahrzeugpannen könnten ersetzt werden durch remote Diagnosen, bei denen der Fahrzeugtechniker über die Benutzerschnittstellen des Fahrzeuges mit dem Fahrer kommuniziert. Direkter Zugriff auf Fahrzeugkomponenten und Daten erlauben dem Diagnostiker möglicherweise, das Problem remote zu beheben. Prognosesysteme unabhängiger Dritter könnten hilfreich für den Halter des Fahrzeuges sein, so dass dieser lange vor dem Auftreten einer Panne über möglicherweise auftretende Probleme informiert wird. Zu diesem Zweck muss ein remote Zugriff für einen autorisierten ISP auf Komponenten und Daten im Fahrzeug möglich sein. Gleichzeitig müssen hochsicher implementierte IT Security-Funktionalitäten während der gesamten Lebenszeit unautorisierte Zugriffsversuche durch Angreifer auf das Fahrzeug unterbinden und Missbrauch feststellen.

Der digitale Wandel bringt jedoch neue Herausforderungen hinsichtlich **IT-Security**-Maßnahmen gegen Hackerangriffe und **Datenschutz** mit sich. Schließlich sind alle Daten, die vom Fahrzeug erzeugt werden und dieses verlassen, personenbezogene Daten, da sie ohne weiteres mit der Fahrzeug-Identifizierungsnummer, dem Fahrzeugkennzeichen oder anderen Identifikatoren des Fahrers oder Fahrzeughalters verknüpft werden können. Zu diesem Zweck sollte der Fahrzeugnutzer in den meisten Anwendungsfällen die Möglichkeit bekommen, individuell und zu jedem Zeitpunkt entscheiden zu dürfen, welche Daten für wen das Fahrzeug verlassen dürfen bzw. wer welche Daten in ein Fahrzeug übertragen darf (opt-in, opt-out) [EDPB1-3]. Dies kann komplexere Szenarien in der Wertschöpfungskette implizieren, bei denen OEM, ISP und Händler in einem weniger gut durchdringbaren Dickicht in Geschäftsbeziehungen zu einander stehen.

Beim Sammeln und Verarbeiten von Fahrzeugdaten nimmt der OEM eine **spezielle Position** ein, da er selbst die Fahrzeug-Software entwickelt und im Fahrzeug installiert hat. Der Hersteller hat tiefergehende Informationen über die verbauten Technologien und auch die Möglichkeiten, eine direkte Verbindung zwischen Fahrzeug und Nutzern selbst aufzubauen. Trotzdem sollte dieser technologische Vorsprung nicht dazu genutzt werden, Herr über alle

anfallenden Daten im Fahrzeug zu sein. Im Zuge von neuen Diensten – wie die Einführung eines automatisierten Emergency Call Systems wie eCall [eCall], dass seit 2018 verbindlich eingebaut werden muss, können Fahrzeughersteller ihren Kunden auch weitere Telematik und Datendienste (value added services) anbieten, wie Zusatzdienste im Navigationssystem, Wartungsservices oder Infotainment-Dienste. Im Zuge der Digitalisierung ist ein Fahrzeughersteller dann nicht nur der traditionelle Designer und Hersteller von hübschen Boliden, sondern auch Datenserviceprovider mit massivem Einfluss auf den Verbrauchermarkt im Automobilsektor.

Der ISP hat nicht diese vergleichbaren Default-Datenzugänge zu den Fahrzeugen und zugehörigen Funktionen – vielleicht gelingt es ihm dennoch unter erheblichen Schwierigkeiten mit Workarounds oder im Zuge von Verträgen mit den OEMs, die dann über ein Datenoligopol herrschen. Jede Innovation findet dann unter ausschließlicher Kontrolle der Hersteller statt. Da die Vernetzung von Fahrzeugen immer weiter zunehmen wird, sollte die freie Auswahl von Diensteanbietern dem Nutzer immer noch ermöglicht werden – so wie es auch bisher bei dem nicht vernetztem Automobil war. Vergleichbare „**Fair-market**"-Konditionen sollten für alle Serviceanbieter mit datengetrieben Modellen geschaffen werden inklusive dem OEM in seiner neuen Rolle als Service Provider. Mit harmonisierten und verbindlichen Spezifikationen für den zukünftigen hochsicheren Datenaustausch über die Kommunikationsschnittstellen des Fahrzeuges wäre dies möglich. Dies ist auch notwendig, um zwei andere Herausforderungen der heutigen Welt des Internets-der-Dinge (IoT) zu adressieren:

1. **Verteilte Funktionalitäten (Distributed Functionalities)**
   Im IoT befinden sich Funktionalitäten und Daten vernetzter Geräte nicht nur auf diesen Geräten selbst, um dann über eine Netzwerkschnittstelle ab und zu mal Daten auszutauschen. Ein IoT Device ist eher nur noch ein *Teil* der digitalen Welt, mit immer weniger eigener Funktionalität. Viele Funktionen und ihre zugehörigen Daten sind dann verteilt
   - in den Backendsystemen der mit dem IoT Gerät zugehörigen Smart Services des Geräteanbieters als auch
   - auf Apps mobiler Endgeräte.

   Diese verteilten Funktionalitäten/Daten erschweren den Aufbau von Securityzonen um sogenannte Assets (Kapitel 3.2) die geschützt werden sollen.
2. **Alles-ist-möglich (Everything is Possible - EiP)**
   Das flexible Zuordnen neuer Funktionalitäten oder Dienste auf ein Gerät ist eines der Hauptvorteile des IoT. Ein heute gekauftes Gerät mit eingeschränktem Use Case Umfang kann morgen bereits Teil eines kompletten Ökosystems mit umfassenden Möglichkeiten sein nur aufgrund von Updates und Vernetzung. Meist wird dies realisiert durch die Kombination der Möglichkeiten der *Distributed Functionalities* (siehe oben) und des vollen Zugriffs auf alle Bestandteile des IoT-Gerätes. Um diesen „vollen Zugriff" möglichst simpel zu gestalten, ist dieser meist wenig bis gar nicht geschützt implementiert. Das ist auch sicherlich tolerabel für ein SmartHome Gerät zum Illuminieren der Wohnzimmerwand, für kritische Anwendungen wäre dies aber nicht tolerabel. Denn wenn jedermann in der Lage wäre, ein solches Gerät in den Administrator-Modus zu schalten, ohne dass es jemand mitbekommt, dann befinden sich diese Geräte im „Alles-ist-möglich"-Zustand: Aufzugstüren in Gebäuden könnten sich öffnen, ohne dass sich eine Kabine dahinter befindet, das

Pedelic Speed-Limit von 25km/h wird aufgehoben und die Sprachsteuerung im Schlafzimmer wird zur Überwachungsstation.

Dies alles trifft natürlich auch auf ein vernetztes Automobil zu – zumeist das komplexeste IoT Gerät, dass ein Bürger privat besitzt: Das vernetzte Fahrzeug sendet Daten zum Backendsystem, manche Information wird weitergeleitet zum Smartphone oder zum Driver Information des Fahrers, wiederum andere Informationen zu 3rd Party Providern. Im vernetzten Verkehr der Zukunft wird die Straßenumgebung geflutet mit Broadcast Messages von Fahrzeugen und Verkehrszeichen – und überall verbergen sich weitere Funktionalitäten für den digitalen Traffic. Den EiP-Modus gilt es zu vermeiden, damit es keine Horror-Nachrichten, wie in [WHICH] beschrieben, geben wird.

Ein erster Ansatz der Automobilindustrie, diesen Herausforderungen zu begegnen, ist das Konzept des "Extended Vehicle" (ExVe) welches nicht als die beste Wahl in einer EU Studie [TRL] angesehen wurde. Denn als die beste Lösung empfand man die “On-Board Application Platform” (OBAP), welches die Kommunikation mit dem Rest der Welt dort steuert und kontrolliert, wo die Daten das Auto verlassen bzw. in diese gelangen: Im Automobil selbst. Die **O**n-Board **T**elematics **P**latform (OTP) skizziert eine konkrete Lösung des dort beschriebenen OBAP aus IT Security Sicht wie auch bezüglich des „Data Protection by Design“ Prinzips.

Als oberste Priorität einer modernen Daten Policy muss auch der Datenschutz, das Recht auf informationelle Selbstbestimmung und die Wahlfreiheit („freedom-of-choice“) für die Verbraucher von Beginn an umgesetzt sein. Um dies zu gewährleisten, benötigt man eine technische Lösung zur Realisierung des “Separation of Duties” Prinzips.

1.2 Struktur des Dokumentes

Der Bericht ist folgendermaßen strukturiert:

- Kapitel 1 – **Einführung**
- Kapitel 2 – **Herausforderungen bei vernetzten Fahrzeugen :** Aktuelle „State-of the-art“ Automotive Kommunikations-Konzepte werden bezogen auf
  - das vernetzte Fahrzeug wie auch
  - den vernetzten Traffic

  vor- und die zugehörigen Herausforderungen herausgestellt.
- Kapitel 3 – **IT Security Modelle** werden als Basis für die dann folgenden Kapitel vorgestellt.
- Kapitel 4 – In “**OTP – Security Konzept**“ wird ein hochsicheres Datenzugriffskonzept vorgestellt, welches durch ein Automotive Gateway (A-GW), basierend auf existierenden Lösungen, realisiert wird.
- Kapitel 5 – Das Kapitel “**Audit und Ratings**“ enthält Vorschläge für mögliche Audit-, Evaluations und Zertifizierungsverfahren bezogen auf die IT Security für das vorgestellte OTP**.**
- Kapitel 6 – Eine **Roadmap** zur Implementierung der sicheren OTP wird skizziert.

2 Herausforderungen bei vernetzten Fahrzeugen

Angesichts der zentralen Rolle des Autos für die Mobilität zahlreicher Menschen wird der zunehmenden Vernetzung und deren Potenzial großes öffentliches Interesse zuteil. Verschiedene Parteien in der Automobilindustrie haben bereits unterschiedliche Konzepte vorgestellt [TRL], wie die Vernetzung der Fahrzeuge bestmöglich realisiert werden kann. In Kapitel 2.1 wird ein Überblick hierzu gegeben während in Kapitel 2.2 drei verschiedene Umsetzungskonzepte vorgestellt werden. Abschließend werden diese Konzepte bewertet.

2.1 Allgemeine Konzepte und mögliche Schwachstellen

Heutzutage sind in Fahrzeugen zunehmend Assistenzsysteme integriert, mit deren Hilfe automatisiert eingeparkt werden kann, der Tempomat den Abstand zum vorausfahrenden Fahrzeug hält oder das Fahrzeug in seiner Fahrspur gehalten wird. Diese hochentwickelten Assistenzsysteme können bereits heute bestimmten Automatisierungsstufen nach [SAE J3016] zugeordnet werden, auf die auch in [ENISA1, 2] Bezug genommen wird:

- Der menschliche Fahrer überwacht die Fahrzeugumgebung:
  0. Keine Automatisierung
  1. Fahrerunterstützung
  2. Teilautomatisiertes Fahren
- Das System zum automatisierten Fahren überwacht die Fahrzeugumgebung
  3. Bedingt automatisiertes Fahren
  4. Hochautomatisiertes Fahren
  5. Voll automatisiertes Fahren

Gemäß dem Wiener Übereinkommen über den Straßenverkehr muss auch bis Automatisierungsstufe 4 der Fahrer jederzeit die Kontrolle über das Fahrzeug haben. Darüber hinaus gibt es bereits Fahrzeuge in den USA und Kanada, die in der Lage sind, sich streckenweise vollautomatisiert auf den Freeways und deren Auf- und Abfahrten zu bewegen - inklusive selbsttätigem Blinken, Spurwechsel und Anpassung der Geschwindigkeit. Zu diesem Zweck ist eine Vielzahl an Kameras, Ultraschallsensoren und Radartechnik bereits im Auto installiert. Zur Verarbeitung und Analyse der gewonnenen Informationen benötigt man noch weitere Hardware, um dem Fahrzeug die richtigen Anweisungen zu geben. Damit wären die ersten Schritte in Richtung einer SAE Level 4 Automatisierung getan.

Für oben dargelegten Stufen automatisierten Fahrens werden viele individuelle Informationen gesammelt und im Fahrzeug ausgewertet. Für die Zukunft wird ein Teil dieser Daten – Geschwindigkeit, Abstände zu anderen Fahrzeugen, Gefährdungspotentiale… – auch anderen Verkehrsteilnehmern zur Verfügung gestellt. Diese Kommunikation wird jetzt bereits realisiert: EU-Staaten, die an dem C-ITS[4] Korridor Projekt [C-ITS-Korridor] teilnehmen, haben beispielsweise spezifiziert, wie Baustellenwarner Informationen über Straßenarbeiten an Fahrzeuge mit entsprechenden Empfangseinheiten schicken können [PP-RWU].

[4] Cooperative Intelligent Transport Systems

Der Informationsaustausch zwischen unterschiedlichen Bestandteilen der Verkehrsinfrastruktur und individuellen Fahrzeugen erfordert den Schutz der übertragenden Daten wie auch der Kommunikationsschnittstellen. Die *Europäische Netzwerk und Informationssicherheitsagentur* (ENISA - *European Network and Information Security Agency*) hat bereits in zwei ihrer Studien [ENISA1, ENISA2] herausgefunden, dass Cyberangriffe mit einem hohen Schadensausmaß an smarten Fahrzeugen (*Smart Cars*) möglich wären.

Ein mögliches Angriffsszenario wäre im Zuge des Aufspielens von Firmware-Updates auf die entsprechenden Fahrzeugsysteme über OEM Backend-Server denkbar. Falls ein Angreifer erfolgreich diese Cloud-Architekturen angegriffen hätte, könnte er möglicherweise veränderte, „bösartige“ Updates (*Malware*) in das Fahrzeug einschleusen, da dieses wiederum annimmt, die Updates wären authentisch, da sie von einem vertrauenswürdigen Server kommen. Die Auswirkung einer solchen Attacke (ggf. unter Ausnutzung des *EiP Modus*) wäre enorm, da an den Backendsystemen eine große Anzahl an Fahrzeugen angebunden wäre und somit das gesamte Ecosystem des OEM betroffen sein könnte. In Abhängigkeit zu den Absichten des Angreifers hätte dies eventuell auch Einflüsse auf die Safety der Insassen in den Fahrzeugen.

Es könnten nicht nur die hochautomatisierten Fahrzeuge der Zukunft von einer Cyberattacke über das Internet betroffen sein. Da mittlerweile mehr als 60 Millionen Fahrzeuge in der EU mit dem Internet verbunden sind, wäre dies auch bei aktuell verfügbaren Fahrzeugen möglich. Bereits vor Jahren wurde auf diese Gefahr hingewiesen, wie beispielsweise im Jahr 2015 in [Jeep] illustriert. Dieser Vorfall führte zu einem großen Rückruf, um die Security-Risiken bei annähernd 1,4 Millionen Autos allein auf amerikanischen Straßen zu beheben. Die Anzahl der Rückrufe in der restlichen Welt ist nicht bekannt. Dies illustriert die eigentliche Problematik einer solchen **Massenattacke**, bei der nicht nur ein einzelnes Fahrzeug, sondern gleich eine ganze Flotte von Fahrzeugen betroffen sein könnte, die sich irgendwo in der Welt auf den Straßen befinden. Die IT Security Risiken müssen deswegen über die gesamte Lebenszeit eines Fahrzeuges, von der ersten Zulassung bis zur Abwrackung, betrachtet werden.

Ansonsten können die Konsequenzen von unzulässigem Zugriff auf Fahrzeugfunktionen auch die Verkehrssicherheit des Fahrzeugs senken und Leib und Leben der Fahrzeuginsassen wie auch der unmittelbaren Umgebung gefährden. Ebenso ist die Integrität von Umweltkontrollsystemen und Verkehrsleitsystemen gefährdet.

Um Schutz im zukünftigen vernetzten Verkehr („(inter)connected Traffic“) zu gewährleisten wird zwischen zwei Anwendungsfällen unterschieden:

1. **Vernetztes Automobil** (“connected car”): In diesem Fall wird der Funktionsumfang um weitere Funktionalitäten durch Backendsysteme von Service-Dienstleistern erweitert. Dieser Anwendungsfall von “distributed services” ist bereits heute in zahlreichen modernen Fahrzeugen implementiert.
2. **Vernetzter Verkehr** („connected traffic“ oder kooperative intelligente Verkehrssysteme – C-ITS) in der Zukunft und speziell für höhere Automatisierungslevel: Die Autos können auf der Straße miteinander und mit der Straßeninfrastruktur durch Versendung und Empfang von geeigneten Messages kommunizieren.

Eine Auswahl möglicher Lösungskonzepte wird im Folgenden vorgestellt.

2.2 Lösungskonzepte

Drei Konzepte (zwei für das vernetzte Automobil und eins für den vernetzten Verkehr) werden vorgestellt sowie die daraus resultierenden Szenarien bei Kombination der vernetzten Anwendungsfälle.

Das Extended Vehicle (**ExVe**) ist primär geeignet für die Rolle des OEM als digitaler Serviceprovider unter seiner vollen Kontrolle. Die On-Board Telematics Platform (**OTP**) gewährleistet dem Fahrzeughalter (oder Fahrer) seine volle Datensouveränität, indem dieser selbst zu jedem Zeitpunkt über opt-in/-out Funktionalitäten entscheiden kann, wer (OEM, ISP, …) welche Daten zu welchem Zweck bekommen soll. Im Vehicle-to-Everything (**V2X**) wird der sichere Message-Transfer auf Basis einer Public Key Infrastructure (siehe [PKI]) für alle im Straßenverkehr in der näheren Umgebung Beteiligte realisiert. Letztlich werden zwei resultierende Kombination zwischen vernetztem Fahrzeug und vernetztem Verkehr vorgestellt.

2.2.1 Extended Vehicle

Das **Extended Vehicle** (ExVe) ist ein Konzept für das vernetztes Automobil, welches zurzeit bei vielen Fahrzeugherstellern umgesetzt ist. Die Fahrzeuge sind hierbei an den Backendsystemen des OEM[5] angebunden. Die ein- und ausgehenden Daten des Fahrzeuges werden über proprietäre und individuell gesicherte Datenfunkverbindungen an die Hersteller-Backendsysteme gesendet. Zusätzliche direkte Datenverbindungen zum Automobil von ISPs oder anderen Drittanbietern sind nicht erlaubt. Diese müssen immer über den OEM erfolgen, der den Datenfluss in seine von ihm gefertigten Fahrzeuge kontrolliert.

Über entsprechende Business-to-Business Schnittstellen können die ISPs auf bestimmte Fahrzeugdaten zugreifen, sofern vertragliche Individualvereinbarungen existieren. Ein direkter Schreib-/Lesezugriff auf Fahrzeugdaten, -funktionen und -ressourcen ist ausschließlich dem OEM vorbehalten. Wartungsarbeiten können nur auf Grundlage bilateraler Vereinbarungen (gegen Bezahlung) zwischen den jeweiligen Marktteilnehmern und dem OEM erfolgen. Der Verbraucher hat somit keine wirkliche Wahl. Dies würde zu einem OEM-Datenmonopol führen, welches gleiche Wettbewerbsbedingungen im Servicemarkt zwischen OEMs und ISPs verhindert (siehe [JRC]) sowie Umfang und Tempo von Innovationen vom Fahrzeughersteller abhängig macht.

Als eine mögliche Lösung kämen sogenannte neutrale Server (NEVADA[6] - siehe [NEVADA]) zum Einsatz, die *downstream* mit Datenmaterial von den einzelnen OEM-Servern versorgt werden und die dann von den ISPs genutzt werden können (siehe Abbildung 1). Die Betreiber dieser `neutralen Server` würden als autorisierte Partner Daten von dem OEM bekommen, verarbeiten und dann an ISPs veräußern. Mit der Zwischenschaltung des `neutralen Servers` soll verhindert werden, dass der OEM in seiner neuen Rolle als Servicedienstleister ohne weiteres die Datenflüsse von und zu den ISPs überwachen und erkennen kann, welcher Wettbewerber am Fahrzeug arbeitet.

[5] **O**riginal **E**quipment **M**anufacturer – in diesem Fall der “Automobilhersteller”.

[6] Neutral Extended Vehicle for Advanced Data Access

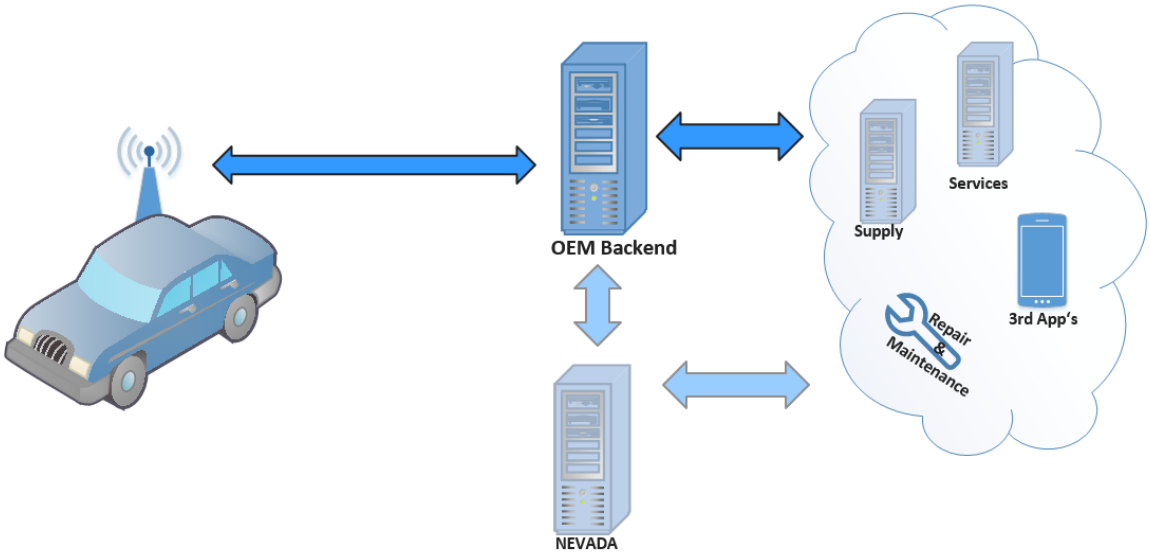


Abbildung 1: Vereinfachte Illustration des Extended Vehicle (ExVe)

Ein direkter Zugriff seitens des ISP wäre auch denkbar, sofern der OEM dies – und wahrscheinlich gegen eine Servicegebühr – zulassen würde. Das “Separation of Duties” Prinzip ist nicht erfüllt, denn dieses erfordert, dass derjenige, der die Daten und den Datenfluss kontrolliert, nicht an den Inhalten der Daten selbst ein Geschäftsmodell knüpft.

ExVe sieht keine Datenkommunikation untereinander zwischen Fahrzeugen (V2V) oder der Straßeninfrastruktur vor, sondern adressiert im Wesentlichen nur den Austausch von Daten zu Servicedienstleistern.

2.2.2 On-Board Telematics Platform (OTP)

Die ***On-Board Telematics Platform*** (OTP) in ihrer ursprünglichen Definition als offene Architektur (*Open Telematics Platform*) adressiert den diskriminierungsfreien Zugriff zwischen Fahrzeug, Servicedienstleistern (ISP und Infrastruktur) und IoT Geräten wie z.B. Smartphones. Demzufolge wird eine standardisierte Kommunikationsumgebung in Bezug auf Soft- und Hardware für Fahrzeuge gefordert: Jedes Fahrzeug soll mit einer On-Board Telematik-Schnittstelle ausgestattet werden, die eine sichere Kommunikation zum und aus dem Fahrzeug abbildet als auch zwischen einzelnen Kommunikationsnetzen im Fahrzeug. Dieses Kommunikationsinterface enthält Integrationsschutzmechanismen und prüft jede Nachricht auf Fehler und bösartige Inhalte. Falls notwendig kann es durch Updates aktualisiert oder ganz ausgetauscht werden, um den Stand der Technik während der gesamten Lebenszeit des Fahrzeuges zu adressieren.

Eine Software Plattform ermöglicht die Ausführung von Applikationen der ISPs. Angeforderte Fahrzeugdaten werden drahtlos an ISP-Server mit Einwilligung des Nutzers übertragen. Der Unterschied liegt darin, dass zwischen Fahrzeug und ISP-Servern kein OEM-Backendsystem mehr erforderlich ist. Die ISP-Applikationen können gleichwertig wie die OEMs in ihrer Rolle als Servicedienstleister direkt auf Dateninhalte im Fahrzeug zugreifen. Damit ein Drittanbieter auf die Plattform als autorisierte Partei zugreifen kann, muss er sich vorab für den Zugang auf die Plattfoirm zertifizieren lassen.

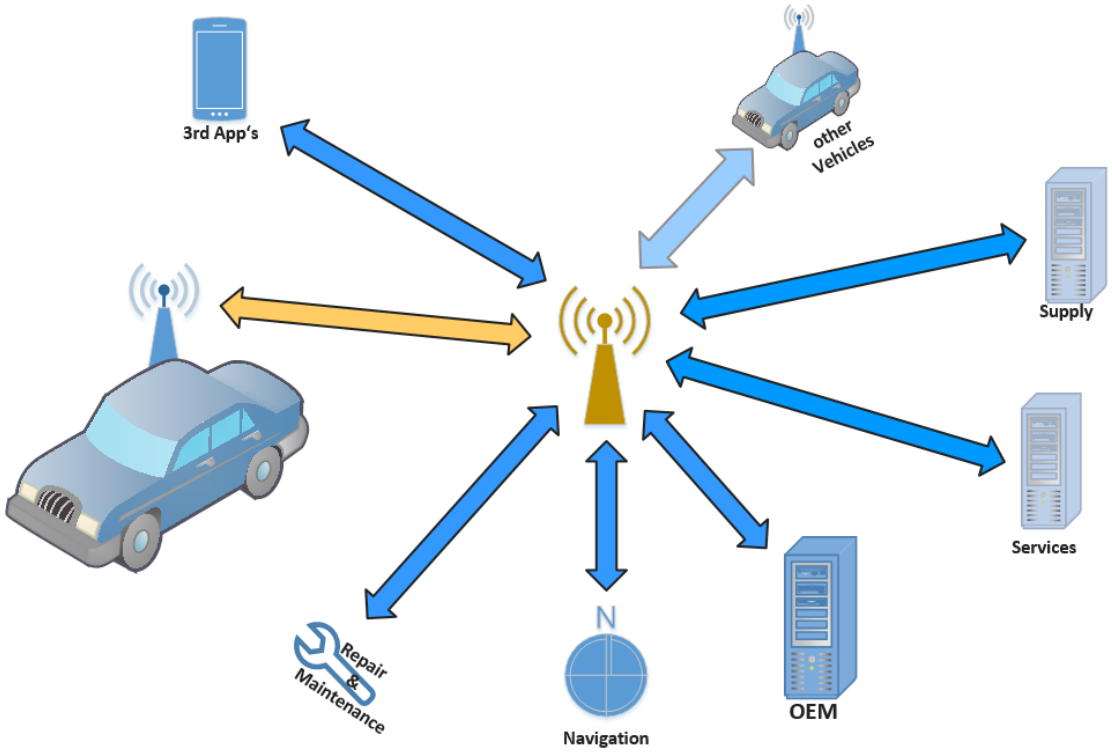


Abbildung 2: Open Architecture OTP

Zusätzlich unterstützt die OTP die digitale Souveränität des Fahrzeughalters. Halter – wie auch Fahrer – sollten die vollständige Kontrolle über ihre personenbezogenen Daten mittels *opt-in*/*opt-out* Mechanismen haben (siehe Abbildung 2).

2.2.3 Vehicle-to-Everything (V2X)

In V2X (Vehicle-to-Everything) wird das Thema *kooperative intelligente Verkehrssysteme* angegangen (C-ITS): Die Fahrzeuge kommunizieren untereinander und mit der sie umgebenden Infrastruktur wie Ampeln und Verkehrszeichen (siehe blaue Pfeile in Abbildung 3). Die sichere Kommunikation basiert auf sogenannte Public Key Infrastrukturen (mehr Information in [PKI], siehe grüne Pfeile in Abbildung 3), die die Authentizität aller V2X Teilnehmer im intelligenten Verkehrssystem (ITS) garantiert. Alle *ITS-Stationen* (ITS-S) inklusive der Fahrzeuge müssen ein standardisiertes Kommunikationsinterface zur Versendung und zum Empfang von V2X-Nachrichten verwenden. Solche Sendeeinheiten (*Transceiver*) werden innerhalb der V2X PKI registriert, die wiederum die zugeordneten Zertifikate in ihrer CA (*Certification Authority*) verwaltet. Somit kann jede ITS-S die Authentizität einer Nachricht prüfen und dabei selbst nur gültige Zertifikate im Transceiver vorhalten.

Das übergeordnete Zertifikate-Management wird unabhängig von den OEMs durchgeführt. Aus Datenschutzgründen wird eine organisatorische Trennung zwischen *Enrolment Authority* (EA) und *Authorization Authority* (AA) innerhalb der CA vorgenommen. Das EA ist verantwortlich für das Management der ITS-S (auch der Fahrzeuge) und das AA für die Generierung der *Authorization Tickets* (AT), die genutzt werden für die eigentliche V2X Kommunikation.

Detaillierte Spezifikationen wurden hierzu von dem Car2Car Communication Consortium (C2C-CC)[7] erstellt.

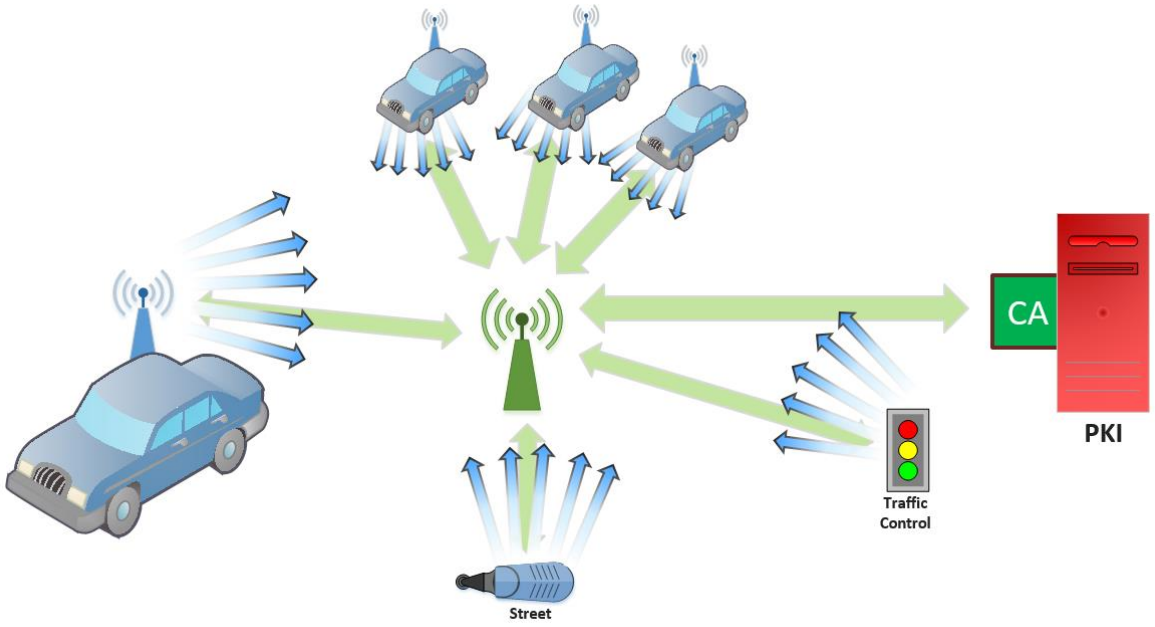


Abbildung 3: Vereinfachte Illustration von V2X

2.2.4 Kombination der Konnektivität

ExVe im C-ITS

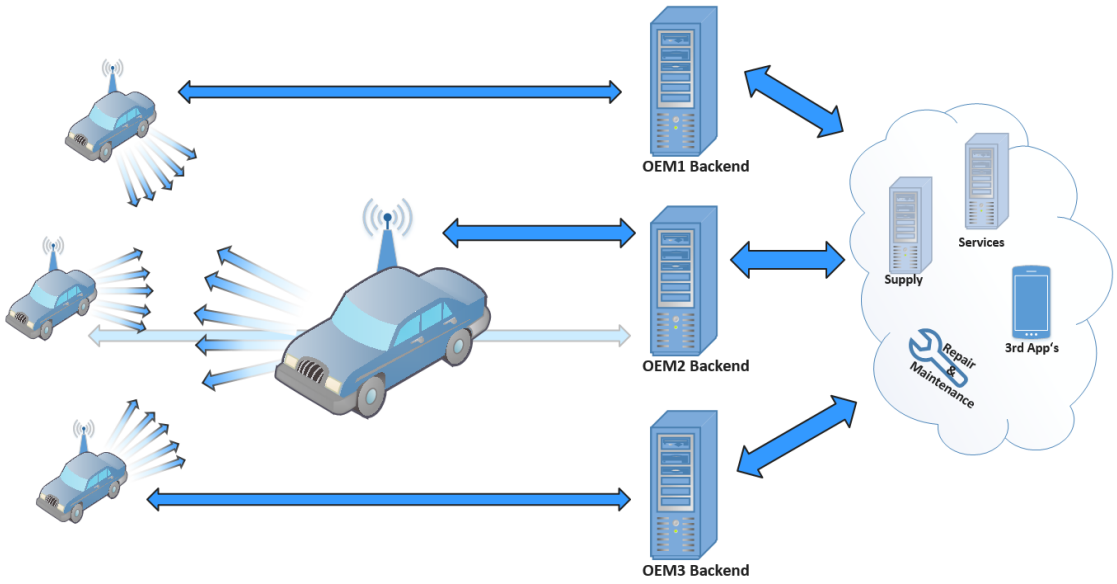


Abbildung 4: ExVe im C-ITS

Bei Verknüpfung der Anwendungsfälle V2X mit dem Extended Vehicle Konzept müsste dieses erweitert werden für ein kooperatives intelligentes Transportsystem wie in Abbildung 4

[7] https://www.car-2-car.org/

mit unterschiedlichen OEMs illustriert. Wahrscheinlich müssten diese beiden Anwendungsfälle durch zwei komplett unterschiedliche Kommunikationstechnologien implementiert werden (Abbildung 5).

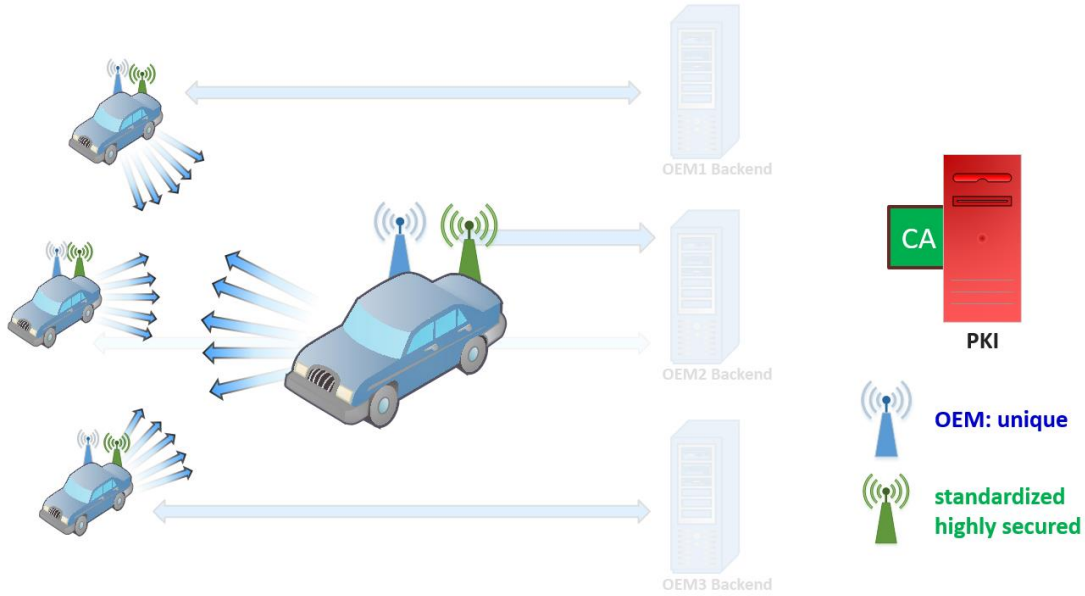


Abbildung 5: ExVe im C-ITS (mit PKI)

Auf der einen Seite gäbe es das proprietäre ExVe-Kommunikationsinterface und auf der anderen Seite eine hochsichere, harmonisierte Schnittstelle zur Abbildung des ITS-S im Fahrzeug.

OTP im C-ITS

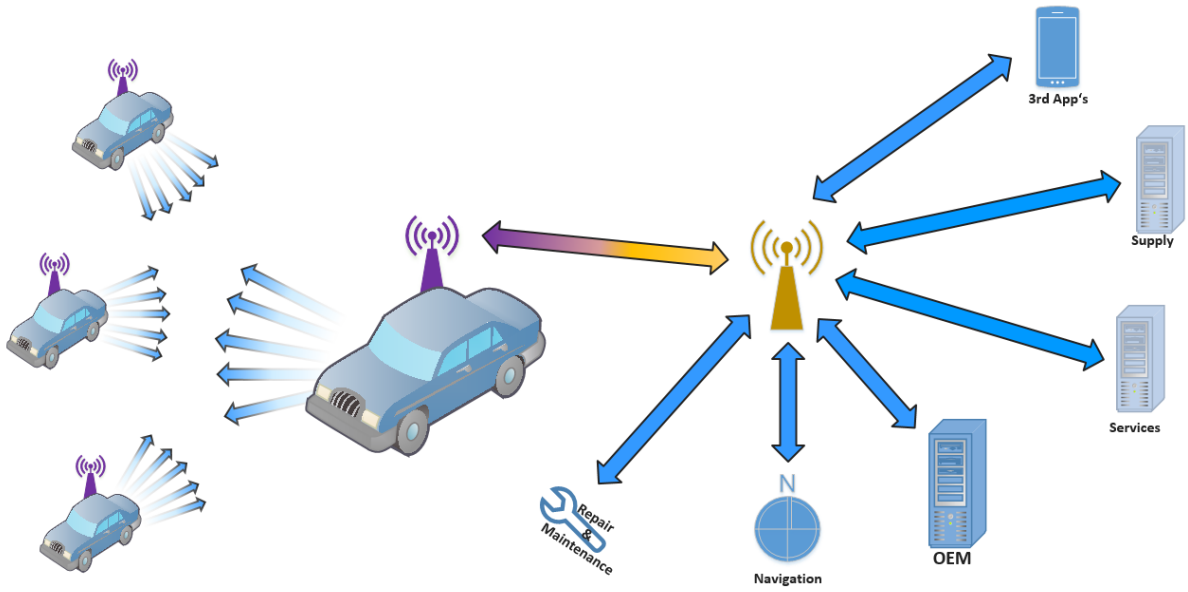


Abbildung 6: OTP im C-ITS

In Gegenzug zu obenstehendem Szenario würde eine Kombination von OTP und V2X nicht zum redundanten Aufbau von Kommunikationsinterfaces im Auto führen. Da beide Anwendungsfälle eine transparente, standardisierte und harmonisierte Schnittstelle erfordern, können diese gut in einer hochsicheren Einheit kombiniert werden: Ein Automotive Gateway (A-GW) wie in Kapitel 4 beschrieben.

2.3 Zukunftsfähigkeit

Obwohl die unterschiedlichen obigen Ansätze für sich allein betrachtet effizient und praktikabel umgesetzt werden können, könnte einer dieser Ansätze in eine technologische Sackgasse führen.

Extended Vehicle (2.2.1)

ExVe verfolgt die Idee, dass 3rd-Party Anbieter zukünftig keinen direkten Zugriff mehr auf das On-Board Diagnose (OBD) Interface benötigen, da sie alle notwendigen Daten dann auch über die ExVe-Backend-Server bekämen. Das Fahrzeug wird um eine *virtuelle Datenzone* erweitert („extended“) und der OEM erweitert seine Rolle als Automobilhersteller zu einem *Automotive Service Provider*. Aus Blickwinkel des OEM ist dies absolut nachvollziehbar – er überlässt das digitale Geschäft nicht den großen IT Providern.

Das Hauptproblem von ExVe ist allerdings dieser – auch von vielen Cloud-Providern – verfolgte Big-Data Ansatz: Der OEM hat die volle Datensouveränität und –kontrolle und auch der Handel von Fahrzeugdaten wird bei ihm gebündelt. Mit permanent vernetzten Fahrzeugen hätte der OEM dann das Datenmonopol aller transferierten Fahrzeugdaten.

Unabhängige Prüfungen der IT Security-Funktionalitäten der ExVe-Kommunikationsschnittstellen durch Dritte nach harmonisierten Standards sind bisher nicht vorgesehen. Dies und die unterschiedlichen proprietären ExVe-Lösungen lassen Zweifel aufkommen, ob diese Implementierungen über die gesamte Lebenszeit des Fahrzeuges abbildbar und robust genug gegen Hackerangriffe sind.

On-Board Telematics Platform (2.2.2)

OTP ermöglicht allen autorisierten Parteien den direkten Zugriff auf Daten, Funktionen und Ressourcen im Fahrzeug und unterstützt damit die Datensouveränität einzelner Marktteilnehmer, die im direkten Vergleich vom OEM zu den einzelnen Marktteilnehmerrollen verschoben wird. Der Halter wie auch der Fahrer eines Fahrzeuges haben die Möglichkeit, zeitbezogene Zuweisungen vorzunehmen, wer auf welche Daten zu welchem Zweck zugreifen darf. Hierzu ist es natürlich auch notwendig, dass bestimmte Möglichkeiten dem Fahrer über die Benutzerschnittstellen im Fahrzeug (HMI) angeboten werden können. Dadurch haben unabhängige Marktteilnehmer die gleichen Möglichkeiten wie der Fahrzeughersteller, dem Verbraucher ihre Anwendungen zu präsentieren.

Auf der anderen Seite könnte einzelne Entscheidungen, wer welche Daten bekommen darf, recht schwierig umgesetzt werden, wenn diese Administration nicht dem einzelnen OEM obliegt. Man benötigt dann eine technische Lösung wie aber auch eine politische Instanz, die die Ansprüche der einzelnen Parteien koordiniert.

V2X und Kombination der Konnektivität (2.2.3, 2.2.4)

V2X bezieht sich auf die kooperativen intelligenten Verkehrssysteme (C-ITS) der Zukunft, ohne die Anwendungsfälle von Servicedienstleistungen wie bei OTP und ExVe mit einzubeziehen. Dabei nutzt man hier standardisierte, hochsichere auf PKI ([PKI]) basierende Kommunikationslösungen aber wiederum keine Datenmodelle, die einen hochsicheren Zugriff auf unterschiedliche Fahrzeugdaten abbilden. Man geht von gleichberechtigten Teilnehmern im C-ITS aus, so dass diese Mechanismen auch nicht notwendig erscheinen. Dadurch gibt es allerding auch keine Rolle wie das des OEM im ExVe, der die ausschließliche Kontrolle über die übertragenen Daten innehat.

Betrachtet man ExVe oder OTP im C-ITS, dann

- mündet ExVe in der derzeitigen Implementierung in redundante Kommunikationstechnologien, die im Fahrzeug verbaut werden müssen,
- während OTP mit einer standarisierten und transparenten Implementierung eines Automotive Gateway (siehe Kapitel 4) beide Kommunikations-Anwendungsfälle in einem Interface im Fahrzeug vereinen kann. Synergien zwischen Nahfeld- (V2X) und Backendkommunikation (ISP) könnten einfach implementiert werden.

Unter Berücksichtigung von zukünftigen Kommunikationstechnologien wie 5G, das unterschiedliche Kommunikationsprotokolle durch *Network Slicing* inkludiert wie

- eMBB[8] als Nachfolger derzeitiger Mobilfunkprotokolle,
- mMTC[9] für die Machine-to-Machine Kommunikation und
- uRLLC[10] für die Sensor-Funkanbindung,

werden Lösungen mit mehreren Kommunikationsschnittstellen für unterschiedliche Anwendungsfälle innerhalb eines Fahrzeugs in eine technologische Sackgasse münden. ExVe in seiner derzeitigen Implementierung scheint nicht zukunftsfähig zu sein.

Zusammenfassung

Betrachtet man die derzeitige Situation in Bezug auf zukünftige Anwendungsfälle wie C-ITS und autonomes Fahren bei gleichzeitigem Einsatz von 5G dann sind die Nachteile von ExVe offenkundig:

- **Unzureichende Transparenz** implementierter Kommunikationsfunktionen
- Mögliche **Security Risiken** aufgrund fehlender Anforderungen
- Mangelende **Interoperabilität** aufgrund fehlender ExVe-Standardisierung

[8] **e**nhanced **M**obile **B**road**b**and

[9] **m**assive **M**achine **T**ype **C**ommunications

[10] **u**ltra **R**eliable and **L**ow **L**atency **C**ommunications

- **„Separation of Duties" Prinzip** ist nicht umgesetzt. Die Kontrolle und das Management von Fahrzeugdaten sollte entkoppelt sein von den dazu gehörenden Businessmodellen – auch in Bezug auf den OEM in einer neuen Rolle als digitalen Serviceanbieter. Dies führte zu:
  - **Volle Kontrolle** des Automobilmarktes **durch den OEM** aufgrund von Lock-In Implementierungs-Policies mit exklusiven Zugriffsrechten zu allen Fahrzeugdaten
  - Fragwürdige Erfüllung der Datenschutzgrundverordnung (DSGVO / **GDPR**)
  - Ergebnisse einer Fahrzeuginspektion (**PTI**[11]**)** durch unabhängige Prüfdienstleister finden unter der vollen „digitalen" Kontrolle durch den OEM statt und können nicht mehr als „*unabhängig*" betrachtet werden
- Durch die fehlende Trennung administrativer Aufgaben ist die Gefahr einer Aktivierung des **EiP-Modus** durch einen Angreifer (Kapitel 1.1) sehr groß.
- Die Separierung unterschiedlicher Kommunikations-Anwendungsfälle (vernetztes Fahrzeug und C-ITS) wird in höhere Kosten und **mangelnde Synergieeffekte** zukünftiger Kommunikationstechnologien münden

Außerdem ist die **IT Security** über die **Lebenszeit** des Fahrzeuges nicht gewährleistet, so dass die Verkehrssicherheit eines Fahrzeugs nicht mehr vom Verbraucher, sondern vom Fahrzeughersteller und/oder Netzbetreiber abhängt. Wenn (IT Security) Updates für einen Hersteller (z.B. 5-8 Jahre nach Verkauf eines Neufahrzeugs) nicht mehr wirtschaftlich interessant sind, ist die IT Security des Fahrzeugs gefährdet, bis es abgewrackt wird.

Der Verbraucher muss dann zwangsläufig das Fahrzeug aus dem Verkehr ziehen und ein neues kaufen, das mit regelmäßigen Updates unterstützt wird. Dies wäre selbst dann denkbar, wenn das Fahrzeug in puncto Verkehrssicherheit und Umweltschutz den Vorschriften noch voll und ganz entspräche. Beschließt der Netzbetreiber ein Netz-Upgrade (von 4G auf 5G) und ist er nicht gesetzlich verpflichtet, dessen Abwärtskompatibilität sicherzustellen, kann die IT Security des Fahrzeugs obsolet werden, da die vom Fahrzeughersteller gesendeten Security-Updates nicht mehr im Fahrzeug ankommen oder zumindest deren Konnektivität deaktiviert ist.

IT Security-Funktionalitäten sind bisher – mit Ausnahme von C-ITS – weniger Bestandteil einer Harmonisierung im Automobilumfeld. Aus dem Grund werden in den folgenden Kapiteln Konzepte aus dem Blickwinkel der IT Security hergeleitet, die darüber hinaus den OTP-Ansatz des vernetzten Fahrzeuges für den Einsatz in einer C-ITS Umgebung erweitert.

[11] Periodical Technical Inspection

3 IT Security Modelle

Dem Ingenieur geht es beim Entwickeln von Produkten und somit beim Implementieren von Software zumeist um eine Lösung für eine bestimmte Aufgabenstellung (*vertikaler Ansatz*)[12]: Jemand hat spezielle Anforderungen für einen konkreten Anwendungsfall und der Entwickler versucht die beste Lösung zur Abbildung dieses konkreten Anwendungsfalls zu finden, der möglicherweise um einige nützliche Dienste ergänzt wird. Dieser *Use-Case* basierte (vertikale) Ansatz ist typisch für die Maschinenbaubranche und Elektronikindustrie: Es gibt Anforderungen, diese werden genauer spezifiziert, implementiert und getestet und danach kann diese konkrete Lösung produziert und vermarktet werden. Im gesamten Entwicklungszyklus werden die einzelnen Schritte der Entwicklung – Spezifikationen, Source Code, Tests – gegenüber dem ursprünglichen Anwendungsfall abgeglichen, der auch konsequent nicht verlassen wird, denn das wäre „außerhalb der Spezifikation".

In der Welt der Cybersecurity bedeutet „**außerhalb der Spezifikation**" die Basis für Geschäftsmodelle von Hackern und Cyberkriminellen[13]. Deren Anwendungsfall ist der *Misuse*-Case[14] oder in anderen Worten: Geschäftsmodelle von Cyberkriminellen können auf Lösungen basieren, die im Vorfeld vom Entwickler eines Produktes nicht vorgesehen waren und somit auch nicht spezifiziert wurden, dem Angreifer aber einen Vorteil bieten – zumeist auf Kosten anderer. Dies kann mit weitestgehend harmlosen Modding von Entertainmentsystemen einhergehen, um den Funktionsumfang auf Kosten der Garantie des Herstellers zu erweitern, aber auch in die juristische Grauzone des Empfangs verschlüsselter TV-Kanäle münden. Spätestens bei der professionellen Vermarktung von copyright-geschützten Inhalten wird es definitiv illegal.

Kriminalität im Automobilsektor bezog sich traditionell auf Diebstahl und Einbrüche, illegalem Tuning (bei gleichzeitigem Verlust der Straßenverkehrszulassung und des Versicherungsschutzes) oder dem Hollywood-bekannten Durchschneiden der Bremsleitung, um es wie „einen Unfall aussehen zu lassen". Jeder dieser Angriffe wird in analoger Weise durchgeführt und ein physikalischer Zugang (ebenso wie in oben aufgeführtem Beispiel „digitaler Angriffe" auf Entertainmentsysteme) zum Fahrzeug ist hierzu notwendig. Die ursprünglich vom Hersteller definierten Anwendungsfälle werden aber auf jeden Fall verlassen.

Mit dem Internet-der-Dinge (IoT) eröffnen sich neue Möglichkeiten. Das Modding der TV-Boxen könnte **remote** erfolgen und eventuell nicht durch den Besitzer des Gerätes. Mit Sprachunterstützung können die Geräte Sprachkommandos empfangen, diese über Smart Services des Geräteproviders auswerten und dies dann auf dem Gerät umsetzen. Vielleicht hört aber noch jemand anderes mit. Auch das vernetzte Automobil eröffnet dem Kriminellen (in diesem Fall „Cyberkriminellen") mehr Möglichkeiten, meist durch umschalten auf den EiP

[12] Im Gegensatz dazu (*horizontaler Ansatz*) implementieren IT Entwickler oft Lösungen zu generischen Anwendungsfällen: Beispielsweise ist der spätere Einsatzzweck eines Betriebssystems oder einer Datenbank dem Entwickler nicht bekannt.

[13] Oft wird bei Hackern differenziert zwischen den *White Hats*, die auf Schwachstellen lediglich aufmerksam machen wollen, und den *Black Hats*, die Schwachstellen für ihren eigenen Vorteil ausnutzen.

[14] „Misuse Case" trifft es besser als der in Deutschland gelegentlich verwendete Begriff „Missbrauch", denn auch der Misuse Case ist ein Anwendungsfall, und somit ein „Use Case" (der allerdings nicht betrachtet wurde).

Modus (siehe Kapitel 1.1): Warum einzelne Komponenten austauschen, wenn man mehr PS durch ein Software Update bekommen kann? Warum Adblue nachfüllen, wenn der Verbrauch außerhalb einer Testsituation ausgeschaltet werden kann? Warum in ein Büro einbrechen, wenn man die Prototypen-Pläne durch einen Angriff auf die Cloud-Services des Herstellers bekommen kann? Warum die Bremsleitungen durchschneiden, wenn safety-relevante Manipulationen remote durchgeführt werden können, ohne dass ein Nachweis dieses Angriffs erfolgen kann?

Mit zunehmender Digitalisierung haben Cyberkriminelle mehr Möglichkeiten (mehr „Misuse Cases“) und mit allgegenwärtiger Vernetzung gibt es einen neuen Angriffsvektor: Den *remote Angriffsvektor*! Remote Attacken geben dem Angreifer mehr Zeit, remote Angriffe sind schwieriger zu detektieren, es ist kaum möglich, die reale Person des Angreifers zu identifizieren und sehr oft ist die Quelle eines solchen Angriffes im Ausland und somit in einem anderen Rechtsraum. Remote Angriffe erweitern die Möglichkeiten für Cyberkriminelle um ein Vielfaches.

Aus diesem Grund müsste jede IT Lösung nicht nur die Anwendungsfälle, sondern auch die „Misuse Cases“ berücksichtigen. Da die Anzahl der „Misuse Cases“ meist viel größer als die Anzahl der definierten Anwendungsfälle ist, macht es allerdings wenig Sinn, diese alle aufzulisten und für die Lösung zu betrachten. Stattdessen sollte jede IT Lösung IT Security-Funktionalitäten enthalten, die sogenannte „**Assets**“ gegen Cybersecurity-Angriffe schützt. Falls dieser Schutz nicht greift, sollten die Angriffe wenigstens erkannt werden, um mit geeigneten Gegenmaßnahmen darauf reagieren zu können [ANA][15]. Es sollte hierbei ein „**Security by Design**“ Prinzip verfolgt werden.

3.1 Security by Design

Viele Veröffentlichungen beziehen sich auf das „**Security by Design**“ Prinzip. [Waidner] definiert “Security by Design” im weiteren Sinne wie folgt: “*The systematically organized and methodically equipped framework that is applied over the lifecycle of secure software*”. Security Anforderungen sollen somit von Anfang an (im „Design“) in der Entwicklung über den Lebenszyklus berücksichtigt werden, damit Schwachstellen später möglichst nicht auftreten. „Security by Design“ gilt somit als Qualitätsgewinn, denn es erhöht die Robustheit von Hard- und Software gegen Angriffe.

Bezogen auf die OTP als Security Architektur eines vernetzten Fahrzeuges ist die gesamte Lebenszeit („Lifetime“) als kritisch anzusehen, da mögliche Manipulationen eine große Auswirkung auf Leib und Leben (Safety) der Insassen von Fahrzeugen und anderen Verkehrsteilnehmern haben könnten. „*Lifetime*“ bezieht sich hierbei auf die Planung, die Entwicklung, die Produktion, den Betrieb – inklusive Wartung und Support – und das finale Vernichten („scrapping“) von OTP-Bestandteilen. Dies bedeutet auch, dass auch die Standorte des OEM oder möglicherweise seiner Zulieferer geeignet geschützt sein müssen, damit Manipulationen und Datendiebstähle nicht bereits hier passieren können.

[15] Im Sinne von „protect-detect-react“.

Synonym zu [EINSA2] wird „**Security by Design**“ in diesem Bericht als Notwendigkeit definiert, dass Security-Aspekte von Beginn der Produktentwicklung über die gesamte Lieferkette bis hin zum gesamten Lebenszyklus des Fahrzeugs zu berücksichtigen sind. Das bedeutet:

- Ein „Security by Design“ Ansatz ist sowohl aus Sicht des **Fahrzeugs** als auch der **Verkehrsinfrastruktur** zu berücksichtigen.
- Die IT Security muss in **jedem relevanten Spezifikationsdokument** behandelt werden, um sicherzustellen, dass Security-Aspekte von Beginn des Entwicklungsprojekts an und nicht erst im Nachgang berücksichtigt werden.
- IT Security muss während der gesamten „**Lifetime**“ betrachtet werden.

Darüber hinaus wird „**Data Protection by Design**“ definiert als:

Die Security Domäne umfasst eine Reihe von Security Maßnahmen zum Schutz personenbezogener Daten, die vom Fahrzeugnutzer erzeugt und durch Dritte gesammelt, verarbeitet und / oder gespeichert werden.

- Die DSGVO (GDPR[16]) muss angewendet werden, um Datenschutzprobleme zu vermeiden.
- Datenschutz-Folgenabschätzungen (DPIA) oder andere gleichwertige Audit-Verfahren müssen unter Berücksichtigung des Verwendungszwecks durchgeführt werden, um etwaige Datenschutzanforderungen zu identifizieren.

3.2 “Assets” und “Threats”

Laut [CC1] und illustriert in Abbildung 7 befasst sich die IT Security mit dem Schutz von Eigenschaften von Objekten – sogenannte „*Assets*“. In dieser Definition sind „Assets Entitäten, die für jemanden einen *Wert* („*Value*“) haben oder bekommen“. Diese Assets können Informationen sein, die von IT Komponenten gespeichert, verarbeitet und übertragen werden, um die vom Eigentümer dieser Informationen („*Asset Owner*“) festgelegten Anforderungen zu erfüllen. Asset Owner können verlangen, dass die Verfügbarkeit, Verbreitung und Änderung dieser Informationen streng kontrolliert wird und dass die Assets durch Gegenmaßnahmen vor Bedrohungen („***Threats***“) geschützt werden.

Die Sicherung der Assets liegt in der Verantwortung des Asset Owner[17], für den das Asset einen Wert hat oder bekommt. Für reale oder mögliche „*Threat Agents*“ (Angreifer wie Hacker, Cyberkriminelle, böswillige Benutzer usw.) können diese Assets ebenso einen Wert darstellen, so dass sie versuchen, Zugriff darauf zu bekommen, was dann möglicherweise gegen die Interessen des Asset Owners wäre – genau das wäre der oben erwähnte Misuse Case.

Die Asset Owner werden solche **Threats** als potenzielle Beeinträchtigung ihrer Assets empfinden, so dass der Wert eines Assets für die Asset Owner abnimmt. Zu den Security relevanten *Wertminderungen* eines Assets (der „Schaden“) gehören zumeist: Verlust der Vertraulichkeit von Assets, Verlust der Asset-Integrität und Verlust der Asset-Verfügbarkeit.

[16] General Data Protection Regulation

[17] In Kapitel 4.2 wird definiert, wer der entsprechende Asset Owner wäre – das muss nicht zwingend immer der Halter eines Fahrzeuges sein.

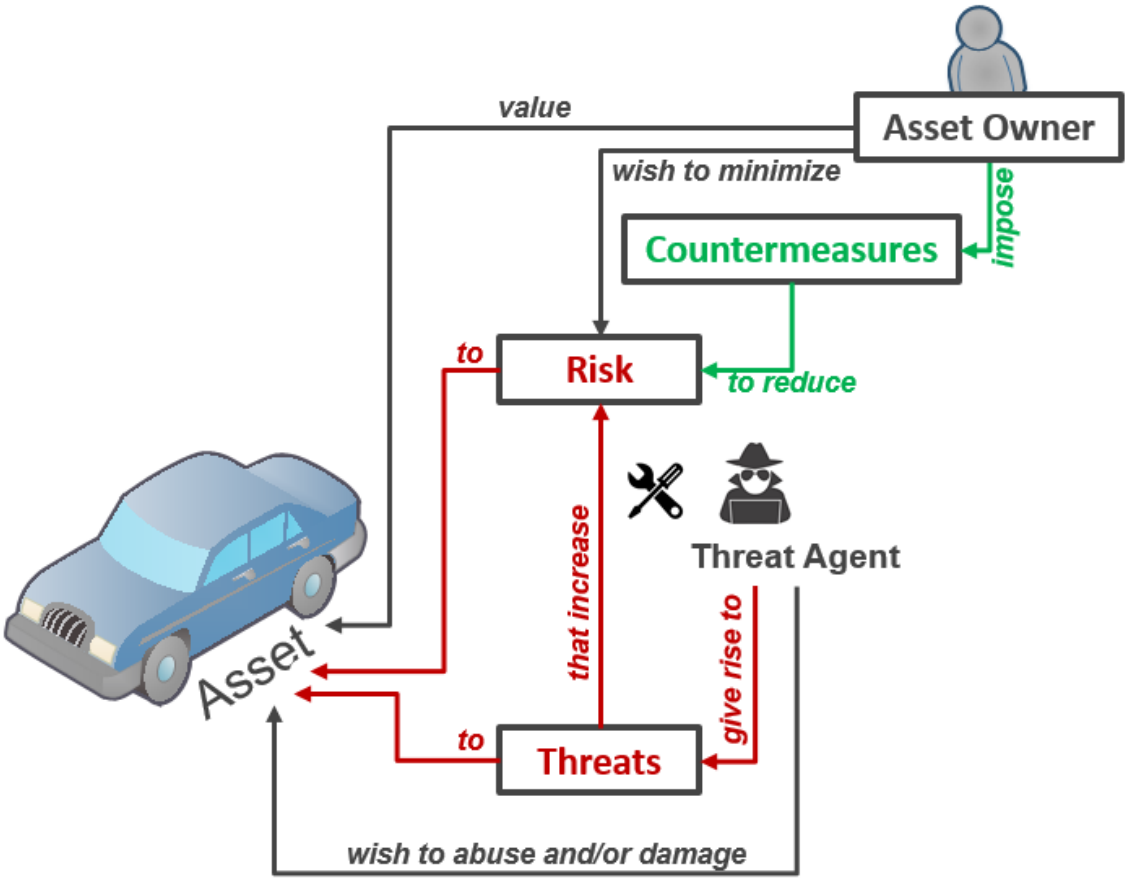


Abbildung 7: Asset & Threats (CC Definition)

Diese Threats bergen daher Risiken („***Risks***“) für die Assets, basierend auf der Wahrscheinlichkeit, dass diese Bedrohung real wird, und des daraus resultierenden Schadensausmaßes auf die Assets. Somit werden Gegenmaßnahmen („Countermeasures“) ergriffen, um die Risiken für Assets zu verringern. Diese Gegenmaßnahmen können technisch (IT Security-Funktionalitäten) umgesetzt und/oder aus organisatorischen Prozessen bestehen und können generisch gruppiert werden (wie oben bereits erwähnt):

1. **Protection** (Maßnahmen zum Schutz gegen Angriffe)
2. **Detection** (Maßnahmen zur Erkennung von Angriffen)
3. **Reaction** (Reaktionen auf Angriffe)

Traditionell konzentriert sich die „Protection“ sehr häufig auf IT Security-Funktionalitäten, die in IT-Security Komponenten implementiert sind, während „Reaction“ meist durch organisatorische Prozesse abgebildet wird.

Es ist nach wie vor zu beachten (dies illustriert Abbildung 7), dass die Ziele eines Threat Agents (Angreifer) nicht unbedingt von der Risikoanalyse des Asset Owners berücksichtigt werden, da seine Motive an einem Asset vielleicht nie von einem Asset Owner im Vorfeld als relevant angesehen worden sind. Dies wäre eine Variante von „*außerhalb der Spezifikation*“ (siehe oben), die auch bei zielgerichteten IT Security-Entwicklungsprojekten unter Berücksichtigung des „Security-by-Design“ Prinzips zwar weniger wahrscheinlich wäre, aber immer noch auftreten könnte.

Die Klassifizierung von Angreifern kann unterschiedlich vorgenommen werden. Wie oben erwähnt, hat sich das Risiko bezüglich remote Angriffen auf IoT-Geräte oder vernetzte Fahrzeuge enorm erhöht. Aus diesem Grund macht es Sinn, Angreifer durch Unterscheidung ihrer **Angriffsvektoren** zu klassifizieren. Wie in Abbildung 8 dargestellt, kann ein Fahrzeug entweder durch lokalen Zugriff, durch „near-field"-Angriffe oder durch remote Angriffe aus sehr großer Entfernung bedroht werden:

- **Lokaler Zugriff**: Lokale Angreifer, die physischen Zugriff auf Komponenten des Fahrzeugs oder einer Netzwerkverbindung zwischen diesen Komponenten haben und versuchen, an Assets heranzukommen oder zu verändern, während sie in Komponenten (z. B. Steuergeräten) gespeichert oder zwischen den Komponenten übertragen werden.
- **"near-field" Angriff**: „near-field"-Angreifer versuchen in unmittelbarer Nähe zum Auto über „near-field"-Protokolle auf Assets im Fahrzeug zuzugreifen.
- **Remote Angriff**: Remote Angreifer versuchen, über Fernzugriffe an die Fahrzeug-Assets zu gelangen. Grundsätzlich können sich diese Angreifer irgendwo in der Welt befinden und ihr Angriffsvektor könnte direkt zum Fahrzeug führen oder aber zu einem Cloud-Dienst, welche Daten (und somit Assets) aus dem Auto speichert oder überträgt.

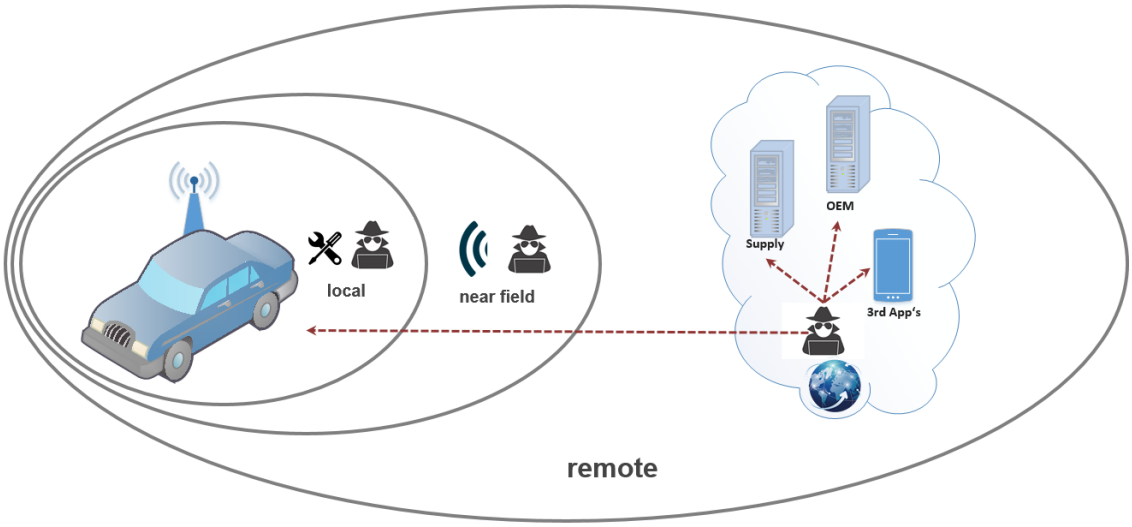


Abbildung 8: Mögliche Angriffsvektoren

Diese Kategorisierung – mit dem Hauptfokus auf den remote Angriff – wird ebenso in dem Protection Profile [PP-AGW] für das Automotive Gateway berücksichtigt, welches zusätzlich zu diesem Bericht veröffentlicht wird. Das Problem der „verteilten Funktionalitäten (*Distributed Functionalities* – siehe Kapitel 1.1)", insbesondere in Bezug auf den remote Angriffs, ist essentiell: Wenn Assets über das Internet verteilt werden, kann ein remote Angreifer die Kontrolle über die Fahrzeugdaten (und wahrscheinlich über das Fahrzeug selbst) erlangen, ohne das Fahrzeug direkt anzugreifen – vielleicht sogar im Rahmen einer remote *Massenattacke* auf eine ganze Flotte. Aus diesem Grund verfolgt das OTP die grundsätzliche Philosophie, die Fahrzeug-Assets möglichst dort zu belassen, wo sie entstehen: Im Auto selbst.

4 OTP – Security Konzept

Zurzeit entwickeln die Automobilhersteller ihre jeweils individuellen IT Security Systeme, die nicht unbedingt zueinander interoperabel bzw. harmonisiert sind, was auch das Testen und somit die Vergleichbarkeit der unterschiedlichen IT Security Lösungen verschiedener OEMs erschwert. Dies bezieht sich im Detail auch auf die Kapitel 2.2 aufgeführten Ansätze.

Außerdem ist es bisher ausschließlich der OEM in seiner neuen Rolle als Service-Provider, der Zugriff auf Fahrzeugdaten über die im Fahrzeug installierten Kommunikationskomponenten hat, was mit der europäischen eCall Regulierung konform ist. Aber im Hinblick auf kommerzielle Anwendungen im vernetzten Automobil sollte die Wahlfreiheit des Endverbrauchers und der faire Wettbewerb garantiert werden und dies auch die Basis für weitere Innovationen sein. Auch unabhängige Werkstätten würden davon profitieren, weil sie dann weniger von den Fahrzeugherstellern abhängig sein würden.

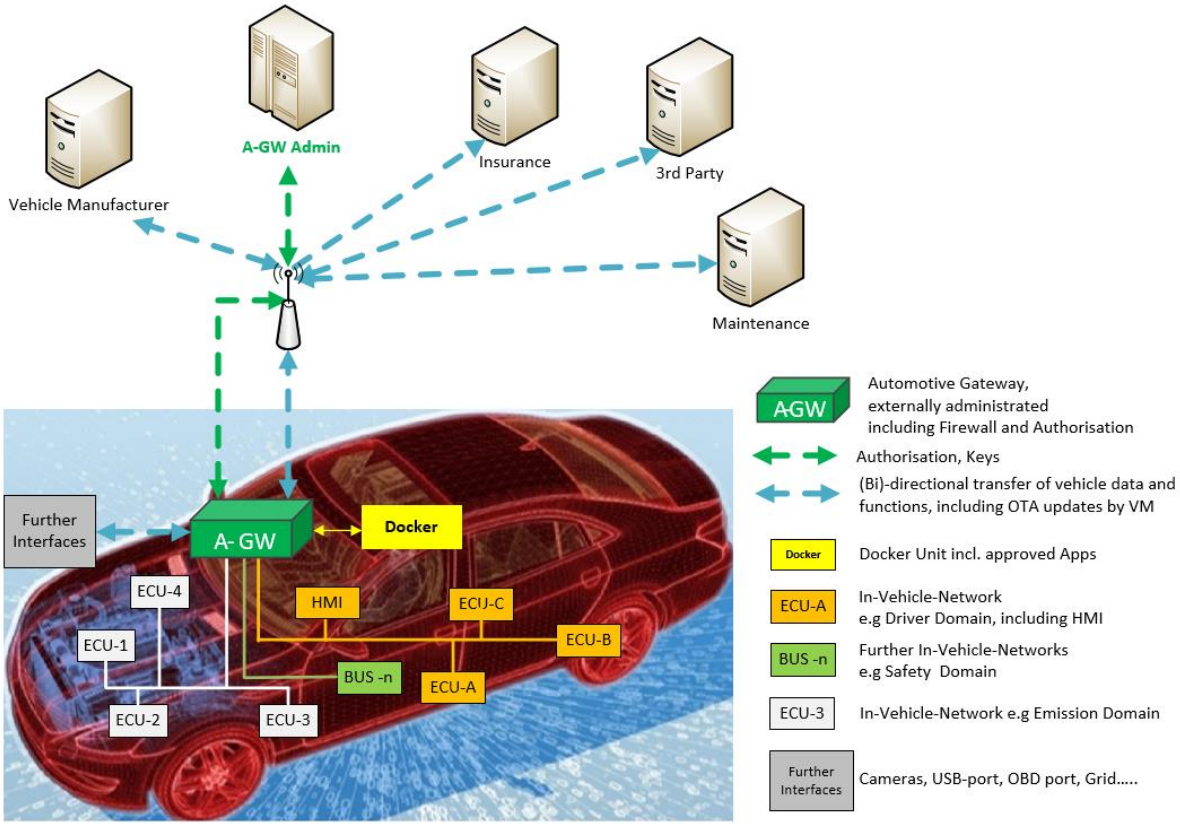


Abbildung 9: OTP mit Automotive Gateway, Docker und HMI

Aus diesen Gründen wird nun eine einheitliche IT Security Architektur für die On-board Telematik Plattform (OTP) vorgeschlagen, die auf Security-Funktionalitäten des C-ITS (bzw. V2X, siehe Kapitel 2.2.3) basiert. Diese IT Security Architektur wird um ein Autorisierungskonzept erweitert, welches privilegierten administrativen Lese- und Schreibzugriff ebenso umfasst wie benutzerbezogene Zugriffe. Hierdurch wird unautorisierter Datenzugriff verhindert, „fair-market“ Konditionen geschaffen, aber zusätzlich auch der Halter oder Fahrer eines Autos in die Lage versetzt, spontan den Datenzugriff zu seinem Fahrzeug anzupassen.

Die On-board Telematik Plattform besteht innerhalb des Fahrzeuges aus einem

- **Automotive Gateway** (A-GW) als Hauptkomponente,
- einer **Docker Unit**, auf welchem ISP-Apps installiert werden können, und
- einer Benutzerschnittstelle (**HMI**).

Das A-GW nutzt kryptographische Primitive (*Credentials*) eines *Hardware Security Moduls* (HSM, siehe [PP-C2C-HSM]), welches Bestandteil des A-GW Controllers ist und hier *Secure Element* (SE) genannt wird. Alle kryptographischen Primitive innerhalb der SEs der Fahrzeuge wie auch von C-ITS Infrastrukturkomponenten werden durch PKIs der OEMs, ISP oder der Kommunikationsprovider verwaltet.

Die OTP erfüllt sowohl Datenschutzanforderungen gemäß DSGVO wie auch die IT Security für das vernetzten Automobil und C-ITS. Damit sind alle angeschlossenen Komponenten und ECUs, Fahrerassistenzsysteme, Sicherheits- und Umweltschutzleitsysteme und Infotainment-Komponenten sowie die Komfortelektronik vor unautorisierten Zugriff von außen geschützt. Das Automotive Gateway innerhalb des Fahrzeugs dient als zentraler Zugangspunkt für die Durchführung von Software-Updates sowie Diagnose-, Reparatur- und Wartungs- sowie Prognoseaufgaben. Gleichzeitig kann das Automotive Gateway innerhalb des OTP die externen Dienste von den für den Fahrer relevanten Informationssystemen (Fahrerdomäne – *Driver Domain*) und von den safety-relevanten Komponenten (*Safety Domain*) separieren. Alle Informationen, die das Fahrzeug verlassen, werden vom Automotive Gateway im Voraus in Übereinstimmung mit bestimmten Benutzer- und Nutzungsprofilen (User-Profile / Usage-Profile) verarbeitet. Dasselbe gilt für alle Informationen, die in das Fahrzeug gelangen.

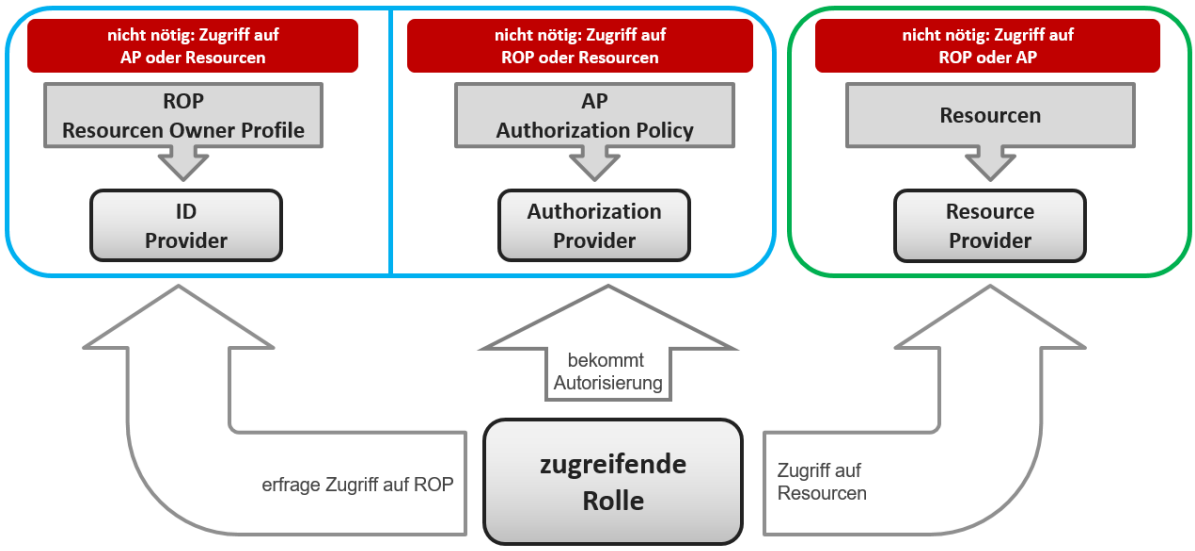


Abbildung 10: '*Separation of Duties*' Prinzip

Ein unabhängiger Dienstanbieter, der als **Automotive Gateway Administrator** (A-GWA, siehe Abbildung 9) bezeichnet wird und der systemische Teil einer OTP ist, kann diese *User / Usage Profiles* in den von ihm verwalteten A-GWs auf Anforderung zentral ändern. Dieser unabhängige Dienstanbieter zieht keinen unmittelbaren Nutzen aus den verarbeiteten Daten. Der A-GWA kann selbst keine Inhalte der transferierten Daten lesen oder verändern. Eine Umsetzung des "Separation of Duties" Prinzips (Abbildung 10) wäre damit realisierbar.

Nach der Einführung eines Security-Modells in Kapitel 4.1, in welchem bestimmte Security-Funktionalitäten einzelnen Layern zugeordnet werden, enthält Kapitel 4.2 Vorschläge zu möglichen Benutzerrollen und -gruppen. Der Automotive Gateway Administrator wird in Kapitel 4.3 ausführlich erläutert und einige Beispiele werden skizziert, wie die richtigen Prozesse definiert werden könnten, dass der A-GWA die "Separation of Duties" auf Basis eines "Multiple-Eyes-Prinzips" erfüllen kann. Im Kapitel 4.4 wird die Lifetime des Automotive Gateways und anderer security-relevanter Komponenten des OTP anhand möglicher Regeln für die einzelnen Lebensphasen erläutert.

4.1 Security Modularisierung und Layer

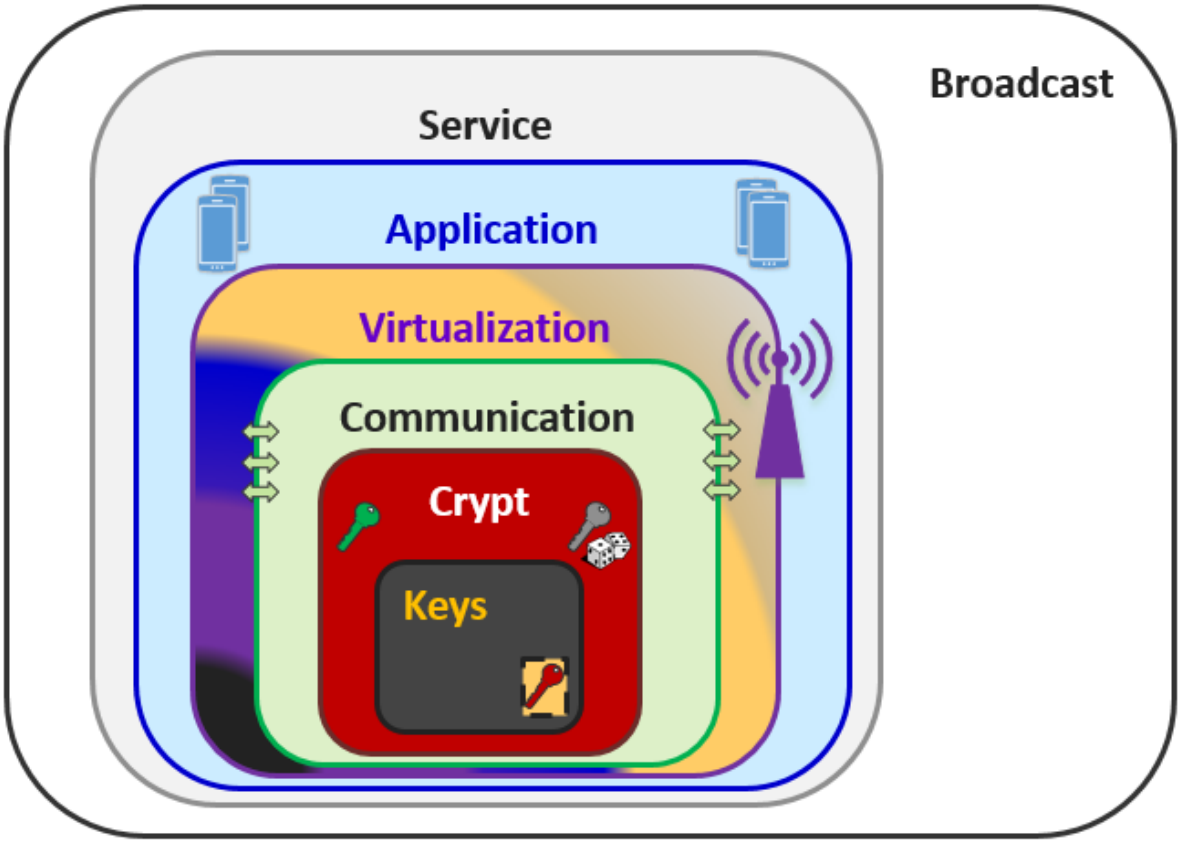


Abbildung 11: Security Layer

Eine Security Architektur für die OTP birgt eine gewisse Komplexität mit einer Vielzahl unterschiedlicher Security-Funktionalitäten. Für eine bessere Struktur und als Basis für mögliche Modularisierungen werden im Folgenden die Security-Funktionalitäten verschiedenen Security Layern (Abbildung 11) zugeordnet, die hierarchisch aufeinander aufbauen.

(1) **Keys**: Der innerste Layer ist verantwortlich für

- das Speichern von privaten Schlüsseln (**Private Keys**) und für Basisfunktionen wie
- **ID's**,
- **asymmetrische Kryptographie** (Verschlüsselung und Signaturen) und
- einem Zufallszahlengenerator (**Random Number Generator** - RNG).

Dieser Layer wird realisiert durch eine kryptographische Hardware (HSM - Hardware Security Module oder alternativ SE – Secure Element), welche diese privaten Schlüssel in einer sicheren, nicht auslesbaren und manipulationssicheren Weise („tamper evident“) speichern kann. Die auf diesen Schlüsseln aufgesetzten Kryptoverfahren laufen ausschließlich in dem HSM/SE ab. Derartige Technologien werden typischerweise in Smart Cards für Bankanwendungen oder ID-Cards eingesetzt.

(2) **Crypt**: Der zweite Layer bildet die Schnittstelle für den kryptographischen Support des oben beschriebenen Key Layer und ist verantwortlich für die

- (symmetrischen) **Session Keys** (basierend auf dem RNG),
- das allgemeine **Key Management (private / öffentliche Schlüssel)**,
- **Identitätschecks** wie auch für die
- SE **Integritätschecks**.

Die kryptographischen Applikationen werden auf dem SE durchgeführt und deren Resultate an den nächsthöheren Level weitergereicht. Typische Anwendungsfälle sind sehr oft Applikationen auf Smart Cards wie Kreditkarten, Signaturfunktionalitäten auf ID Karten oder Security Token. Dieser Layer (und teilweise der Key Layer) bezieht sich auf das HSM, welches in [PP-C2C-HSM] spezifiziert ist.

(3) **Communication**: Der dritte Layer sichert die Kommunikation und regelt den Informationsfluss zwischen einzelnen Security Zonen. Es sind mindestens zwei unterschiedliche Zonen definiert: Eine Zone außerhalb und mindestens einer Zone innerhalb des Fahrzeugs. Als Option könnten weitere Differenzierungen von unterschiedlichen Zonen und deren Separierung innerhalb des Fahrzeuges vorgenommen werden – wie beispielsweise eine Safety-relevante Zone und eine Entertainment-Zone. Für die vertrauenswürdige Kommunikation

- wird eine **Verschlüsselung** basierend auf den Verfahren des Crypt Layers genutzt, um die vertrauliche Datenübertragung zu gewährleisten und werden
- **Signaturen** basierend auf den Verfahren des Crypt Layers genutzt, um die integre Datenübertragung umzusetzen.
- Darüber hinaus sind **Firewall** Funktionalitäten zur Separierung der Zonen implementiert.

Derartige Funktionalitäten sind typischerweise in Firewall- und VPN- (Virtual Private Networks) Produkten implementiert. Dieser Layer ist größtenteils vergleichbar mit dem Transceiver Modul, das in [PP-C2C-TX] spezifiziert ist.

(4) **Virtualization**: Der vierte Layer bildet

- die **Zugriffsrechte** für Fahrzeugdaten,
- das **Monitoring**,
- die **Security Administration** und
- die **Docker** Einheiten ab.

Dies könnte durch unterschiedliche virtuelle Umgebungen oder alternativ durch Benutzer und Nutzungsprofile (User- / Usage-Profile) innerhalb des **Automotive Gateways** – verwaltet durch den **Automotive Gateway Administrator** – abgebildet werden. Derartige IT Security-Funktionalitäten basieren auf Technologien wie sie in State-

of-the-Art Security Lösungen wie der Deutschen Gesundheitstelematik oder dem Deutschen Smart Meter Gateway [PP-SMGW] implementiert sind.

(5) **Application**: Der fünfte Layer ist vorgesehen für separierte Zonen für 3rd–Party Applikationen und ISPs, die in der Regel keinen Zugriff auf Safety-relevante Systeme haben sollten. Einige Benutzerschnittstellen (HMI) oder mobile Endgeräte, die mit dem Fahrzeug verbunden sind, gehören zu solchen Zonen und können auf Docker Einheiten des Layer 4 eingesetzt werden. Durch die Separierung können diese Applikationen auch eigenständige Security Policies verfolgen, die nicht kompatibel sind zu der Fahrzeug Policy[18].

(6) **Service**: Der sechste Layer umfasst Funktionalitäten und Dienste, die nicht öffentlich sind, aber auch geringere Security-Anforderungen haben, wie die Fahrzeug-Konfigurationsdaten des Fahrers oder persönliche Nutzerprofile.

(7) **Broadcast**: Der äußere Layer bezieht sich auf Funktionalitäten oder Information, die für einen kurzen Zeitraum öffentlich zugänglich sind und nicht besonders lesegeschützt sein müssen. Beispielsweise gehören V2X Broadcast- oder Verkehrsinformation für Straßenverkehrsteilnehmer außerhalb des Fahrzeuges dazu.

Durch die Modularisierung der Security-Funktionalitäten kann folgendes automatisch erreicht werden:

- **Hierarchie:** Jede Security-Funktionalität eines höheren Layer sollte nicht die Basisfunktionalitäten des darunterliegenden Layer „überspringen". Ab Layer 4 und darunter dürfen diese nicht umgangen werden.
- **Flexibilität und Zukunftsfähigkeit:** Alle Änderungen von Security-Funktionalitäten können durch lokale oder remote Software Updates durchgeführt werden ohne die Notwendigkeit eines Hardware-Austauschs (Ausnahme: Innerster Layer 1, der nicht zugreifbar sein soll). Dies bezieht sich nicht auf Fragestellungen der Interoperabilität oder Kompatibilität im Allgemeinen[19].
- **Interoperabilität und Wiederverwendbarkeit**: Modularisierung unterstützt Interoperabilitätsanforderungen, Mehrwertdienste (*value-added services*) und neue (zukünftige) Use Cases. Somit ist man flexibler für fortschreitende Innovation.

Die Security Layer wurden außerdem definiert, um besser und strukturierter zu illustrieren, wie man lokale / remote Angriffe verhindern bzw. entdecken kann währen der gesamten Lebensdauer eines Fahrzeuges. Vom Beginn der ersten Fahrzeugnutzung (erste Registrierung) bis zur Abwrackung des Fahrzeugs muss der höchstmögliche Level an IT Security gegeben sein.

Aus diesem Grund sollte der OEM regelmäßige Updates zu angemessenen Preisen auch nach dem Ablauf der Garantie bis zum Ende der Lebenszeit des Fahrzeuges durchführen. Diese Herausforderung kann technologisch mit einem harmonisierten Kommunikationskanal

[18] Ein derartiges Konstrukt ist State-of-the-Art für die Smartphone Integration: Apple's *Carplay* oder *Android Auto* sind populäre Beispiele.

[19] Beispiel: Im Falle, dass ein neues Mobilfunknetzprotokoll ausgerollt wird, ist möglicherweise aus Kompatibilitätsgründen ein Hardwareaustausch notwendig. Aus IT Security Gründen sollte ein Austausch nicht notwendig sein.

durch ein Automotive Gateway (A-GW) auf Layer 4 (Virtualization) gelöst werden. Hardwarebestandteile können kosteneffizient ausgetauscht werden, wenn sich z.B. Mobilfunknetzwerke ändern oder manche Backendserver schnellere Hardware erfordern. Ein Ansatz für den Fall, dass der OEM der Meinung ist, ein kompletter Lifetime-Support wäre wirtschaftlich nicht abbildbar und seine Updates dann irgendwann stoppt, wäre die Unterstützung durch 3rd Party Provider: Die Information über die Bauteile – egal, ob Hard- oder Software – würden dem Provider überlassen, der diesem Support dann nachgehen würde und dies würde im A-GW abgebildet. Hiermit würde verhindert, dass die Lebenszeit eines Fahrzeuges künstlich durch Fahrzeughersteller oder Telekommunikationsprovider reduziert würde.

Zusammengefasst unterstützt ein OTP mit einer Security Architektur, die oben aufgeführte Layer 1-4 abbildet,

- **Security by Design** (Fahrzeug schützt sich selbst gegen Cyberangriffe),
- **Privacy by Design** (Datenschutz der Fahrzeugnutzer ist automatisch durch die implementierte Technologie gegeben) und
- basiert auf eine **tamper-proof Technologie** (aufgrund des enthaltenen SE).

Damit steht OTP im Allgemeinen für

- Steigerung der **Straßenverkehrssicherheit** durch Monitoring von safety- und emissionsbezogenen Komponenten des Fahrzeuges
- **Vertrauenswürdige Security-Administration** durch einen unabhängigen, neutralen Service Provider, der einen freien Wettbewerb im Automotive Sektor unterstützt und selbst nicht in der Lage ist, auf Inhaltsdaten zuzugreifen (A-GWA),
- regulierte **Lebensdauer** und
- eine **zukunftssichere Lösung** durch hochsichere und flexible Update-Optionen und Anwendungen wie V2X Kommunikation.

4.2 Autorisierung

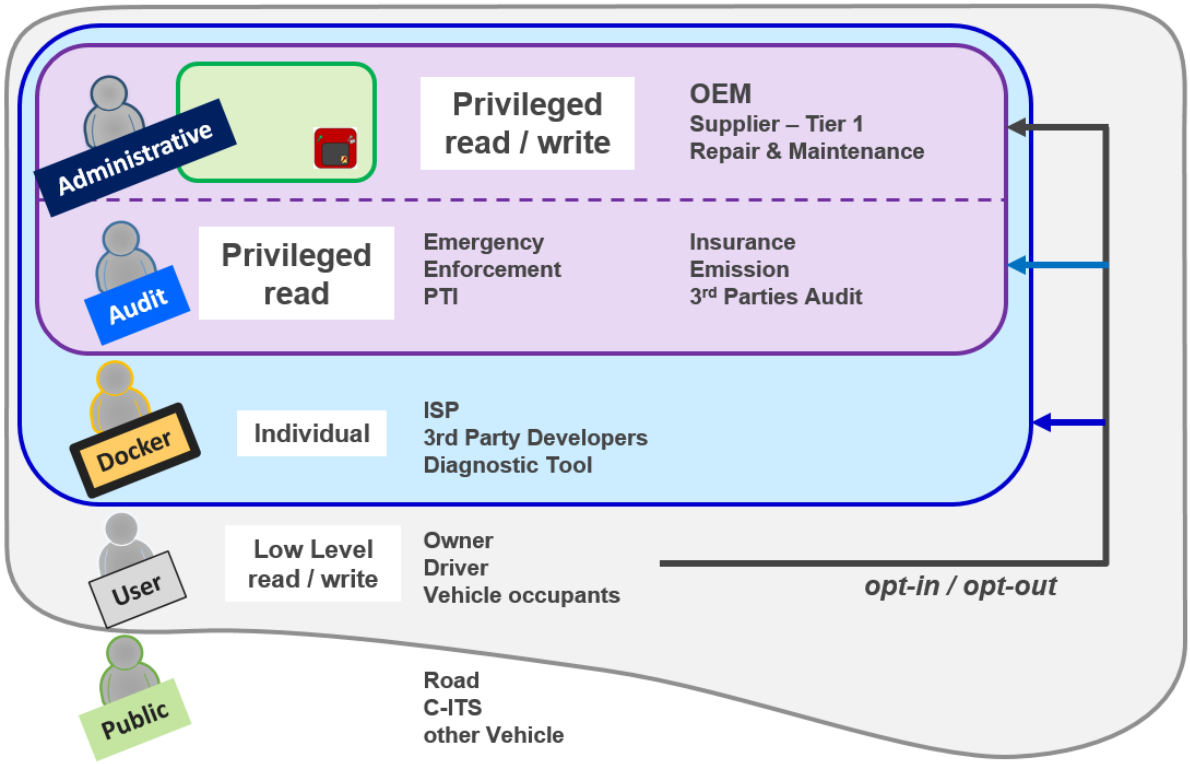


Abbildung 12: Autorisierungs-Hierarchie

Derzeit gibt es wenig Regulierung beim Zugang und bei der Übermittlung personenbezogener Daten im Automotive-Umfeld. Besonders für komplexe Security-Komponenten wie ein Automotive Gateway, das Zugriffsrechte verwaltet, sollte es möglichst weltweit harmonisierte Basisanforderungen für die Autorisierung geben[20], deren Einhaltung regelmäßig im Betrieb überprüft werden kann. Dritten könnte dann ein offener und sicherer Zugriff auf verschiedene Arten von Fahrzeugdaten durch den Fahrzeughalter oder durch den Fahrer gewährt werden. Ein hohes Maß an IT Security für ein Fahrzeug und der Zugriff autorisierter Dritter auf fahrzeuginterne Daten, Funktionen und Ressourcen müssen sich nicht gegenseitig ausschließen.

Das sogenannte 'Separation-of-Duties' Prinzip (Abbildung 10) erfordert, dass Datenflussinhalte bei Erbringung von Dienstleistungen für den Verbraucher von der Kontrolle dieses Datenflusses zwischen den verschiedenen Akteuren getrennt sind. Die Kategorisierung zu übertragender Daten und ihre Beziehung zu verschiedenen Benutzerrollen ist offen zu halten, da das System dies auf flexible Weise übernehmen kann. Der Fernzugriff unterscheidet zwischen Fahr- (*Driving*) und Parkmodus (Parking) des Fahrzeugs (siehe Kap. 4.4.4). Für den Reparatur- und Wartungsmodus (*Maintenance*) gelten – da ein lokaler Zugriff erforderlich ist – besondere Sicherheitsanforderungen, analog zu denen, die im Rahmen des SERMI-

[20] möglicherweise durch UNECE

Schemas [SERMI] für den Zugang zur Reparatur von heute abgesicherten Diebstahlsicherungsgeräten entwickelt wurden, z. B. die Wegfahrsperre oder die Diebstahlwarnanlage des Fahrzeugs.

Für C-ITS sind bereits einige Konzepte für hochsichere Architekturen[21] bis Layer 3 (siehe Kapitel 4.2) entstanden. Für die im Layer 4 aufgeführte Zugriffrechteverwaltung benötigt man einige Basisdefinitionen, die in der OTP abgebildet werden müssen. Zu diesem Zweck werden die potentiellen *Asset Owner* (Siehe Kapitel 3.2) sowie mögliche autorisierte Dritte als Benutzerrollen unten aufgelistet und dann beispielhaft einzelnen Gruppen zugeordnet, die hierarchisch aufeinander aufbauen.

4.2.1 (Benutzer-) Rollen

Automotive Gateway Administrator (A-GWA):

Der Automotive Gateway Administrator verwaltet die Zugriffrechte der verschiedenen Parteien in der Automotive Industrie sowie die zugehörigen Automotive Gateways (A-GW) und er nimmt damit eine zentrale systemische Position in der OTP wahr. Auf Inhalte transferierter Daten zwischen Fahrzeug und Serviceanbietern hat der A-GWA keinen Zugriff. Der A-GWA sollte von einer unabhängigen Instanz betrieben werden. Eine ausführliche Beschreibung befindet sich in Kapitel 4.3.

Fahrzeughersteller (*Vehicle manufacturer* - OEM):

Fahrzeughersteller entwickeln und produzieren Fahrzeuge und bieten zusätzlich weitere Dienstleistungen für die von Ihnen produzierten und zugelassenen Fahrzeuge an (wie R&M oder ISP – siehe unten). In ihrer Rolle als Service-Anbieter konkurrieren die OEMs mit manchen ISPs als „generischer Service-Provider“.

Automobilzulieferer (*Automotive Supplier*) – Tier 1:

Automobilzulieferer sind Unternehmen, die Fahrzeugkomponenten zumeist als direkte Geschäftspartner (Tier X) des Fahrzeugherstellers entwickeln. Es kann auch unabhängige System-, Teile- oder Ausrüstungslieferanten geben, die keinen direkten Vertrag mit einem OEM haben. Automobilzulieferer werden in ihrer Position der Lieferkette (*Supply-Chain*) unterschieden zwischen 3 *Tier*-Leveln (siehe Abbildung 13): Ein *Tier-1 Supplier* liefert direkt an einen OEM und wird beliefert von einem Komponentenlieferanten (*Tier-2*), der wiederum Bauteile von einem *Tier-3 Supplier* bekommt.

Alle Automobilzulieferer müssen bestimmte Schutzmaßnahmen in ihrer Entwicklungs- und Produktionsumgebung einhalten, um Auflagen der OEMs wie auch der Typgenehmigung zu erfüllen. Im Zuge dieses Rollenkonzeptes werden nur Tier-1 Lieferanten betrachtet, da diese vertraglich an den OEM gebunden sind und diese in Folge dessen ggf. remote auf Fahrzeugdaten zugreifen sollten. Dieser Ansatz wird sogar aus Sicht der Security Layer in Kapitel 4.1 verfolgt: Eine Layer-4 Komponente wie das A-GW (Tier-1) beinhaltet eine Layer-3-Netzwerkkomponente (Tier-2), die wiederum auf eine Layer-2 Kryptographie (Tier-3) aufbaut, in der

[21] siehe: [C-ITS-Korridor] als auch Spezifikationen des Car2Car Communication Consortium (https://www.car-2-car.org/)

sich ein Secure Element befindet. Aus Sicht der hier beschriebenen Benutzerrollen (nicht jedoch für die Roll-Out-Prozesse der A-GWs) ist nur der TIER-1 A-GW-Zulieferer relevant.

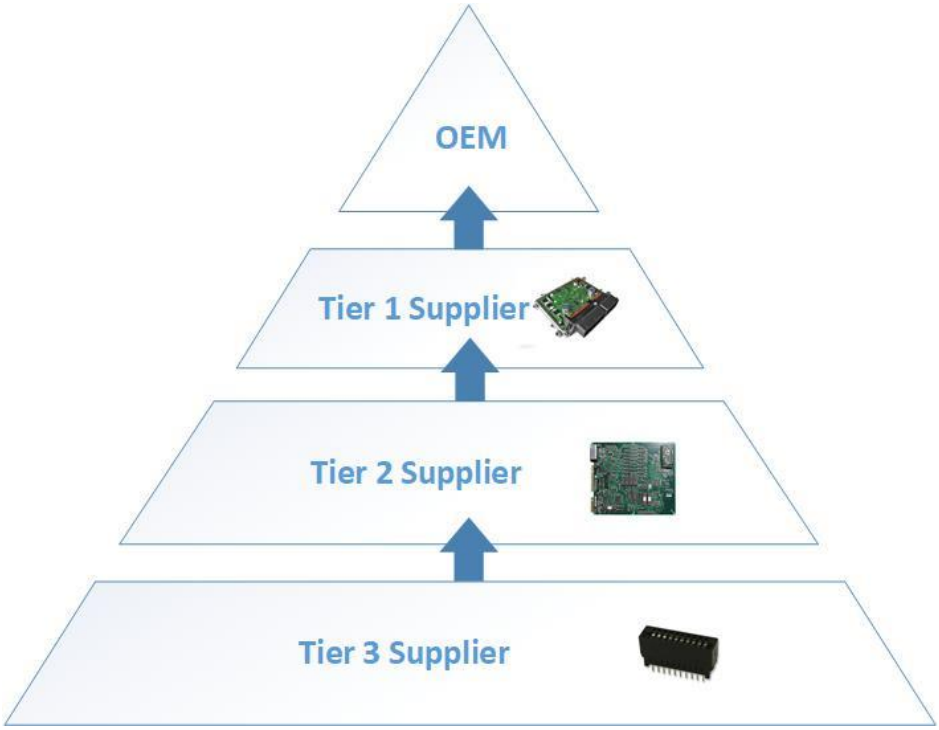


Abbildung 13: *Supplier Pyramide* der Automobilzulieferer

Diagnostik, Reparatur & Wartung (*Repair & Maintenance – R&M*):

Im Zuge der Wartung werden regelmäßige Services und Inspektionen durchgeführt während einer Autoreparatur nur beim Auftreten von Defekten, Störungen oder nach Unfällen stattfindet. Hier sollen sowohl für remote Zugriffe wie auch Diagnosen und deren Auswertungen die gleichen Wettbewerbsbedingungen gelten. Dementsprechend sollte ein OEM in seiner Rolle als R&M-Dienstleister gleichberechtigt gegenüber Vertragswerkstätten oder unabhängigen R&M Dienstleistern angesehen werden. Jeder R&M Anwender eines Diagnosesystems sollte gemäß [SERMI] autorisiert sein, also den Nachweis erbringen, dass es sich um einen „R&M Service für Diagnosezwecke“ handelt.

Entwickler von Diagnose-Tools (*Diagnostic Tool Developer*):

Mit Hilfe von Diagnose-Tools werden Statusdaten der Fahrzeugsensoren und Steuergeräte (ECUs) ausgelesen oder auch beschrieben. Typischerweise findet dies über das OBD-Interface statt. Manche Entwickler von Diagnosetools haben Verträge mit den OEMS, aber es gibt auch unabhängige Entwickler, deren Tools von ISPs wie FIA Mobility Clubs für deren Pannenhilfe und Reparaturservice genutzt werden. Für diese ISPs ist es von großer Bedeutung, dass dieser wettbewerbsfähige Markt für Diagnose-Tools auch in Zukunft für On-Board-Lösungen bestehen bleibt. Derartige Diagnose-Apps könnten Diagnosedaten sammeln und aggregieren und mit ISP-Ferndiagnosediensten kommunizieren.

Fahrer (*Driver*) und andere Fahrzeugnutzer (*User*):

Der Fahrer und ggf. weitere Fahrzeugnutzer sollten über das HMI des Fahrzeugs mit Remote-ISPs kommunizieren können und in der Lage sein, die Opt-In / Opt-Out Funktionen für die Anpassung der User-Profile spontan zu verwenden.

Halter als Nutzer (*User*) eines Fahrzeuges:

Der Halter ist die Person oder der Flottenbetreiber, auf dessen Namen das Fahrzeug zugelassen ist. Der Halter sollte in der Lage sein, jederzeit Opt-In / Opt-Out Funktionen für die Anpassung der User-Profile zu verwenden.

Behörden (*Enforcement Authorities*):

Hierzu gehören neben der Polizei auch Behörden, die die Konformität der Produktion, die Konformität im Betrieb, die Verkehrssicherheit und die Durchführung von Marktüberwachungstests überprüfen. In Deutschland wäre eine solche Durchsetzungsbehörde das Kraftfahrt-Bundesamt (KBA).

Versicherungen (*Insurance*):

Da Versicherungsgesellschaften mittlerweile Tarife anbieten, die das Fahrverhalten ihrer Kunden berücksichtigen, macht es Sinn, dass auch diese vom Halter des Fahrzeuges freigegebene Daten remote erhalten können.

Rettungsdienste (*Emergency*):

Rettungsdienste werden im Falle eines Unfalls remote (über eCall) benachrichtigt.

Straßenverkehrsinfrastruktur (*Road Infrastructure*):

Die Straßeninfrastruktur umfasst Verkehrszeichen und Lichtzeichenanlagen, die Informationen an ein Fahrzeug senden können.

C-ITS (Cooperative Intelligent Transport Systems):

C-ITS umfasst Stauwarner oder Verkehrsmanagementsysteme, die Verkehrsdaten an eine Empfangskomponente im Auto senden.

Prüfunternehmen (*Audit and Inspection Facilities*)

PTI / Roadworthiness:

Zurzeit werden regelmäßige technische Inspektionen (*Periodical Technical Inspection – PTI*) und Prüfungen der Verkehrssicherheit (*Roadworthiness Testing*) lokal im *Maintenance Mode* und unter Nutzung des OBD-Interfaces auf Grundlage verschiedener gesetzlicher Vorschriften durchgeführt. In Zukunft könnte es sein, dass die PTI durch permanentes remote Monitoring (PAI[22]) ersetzt oder unterstützt wird.

Emission Audit:

Bezogen auf die Abgasuntersuchung (Emission Audit) könnten zukünftige Fahrzeuge mit OBM[23] oder OBFCM[24] ausgestattet sein, die die Energieverbrauchsdaten des Fahrzeugs erfassen, um sie an offizielle EU-Behörden weiterzuleiten

[22] **P**ermanent **A**utomated **I**nspection als ein besonderes Einsatzgebiet für ein OBM

[23] **O**n-**B**oard **M**onitoring (in diesem Fall von Emissionen)

[24] **O**n-**B**oard **F**uel **C**onsumption **M**onitoring

3rd-Party Audit:

Nicht gesetzlich vorgeschriebene aber für den Verbraucher informative Tests werden zumeist von Prüfungsorganisationen verschiedener Verbände oder Verbrauchertestorganisationen wie Euro NCAP[25] oder Green NCAP[26] durchgeführt. Meist beziehen sich diese Tests auf die Safety oder auch Umweltauswirkungen und könnten auch als OBM realisiert werden.

ISPs und 3rd-Party Developer:

Independent Service Provider sowie 3rd-Party Entwicklungsunternehmen erstellen Apps, die an Bord des Fahrzeugs ausgeführt werden können, um die Fahrzeugnutzer bei Pannen, Reparaturen, Versicherungen und vielen anderen unabhängigen Mehrwertdiensten zu unterstützten

Fahrzeuge (*Vehicles*):

Letztlich sind auch Fahrzeuge, die am Straßenverkehr teilnehmen (im *Driving Mode*) und im Zuge von V2V mit der Kommunikationseinheit im eigenen Auto interagieren, einer Rolle zugeordnet.

4.2.2 Benutzergruppen

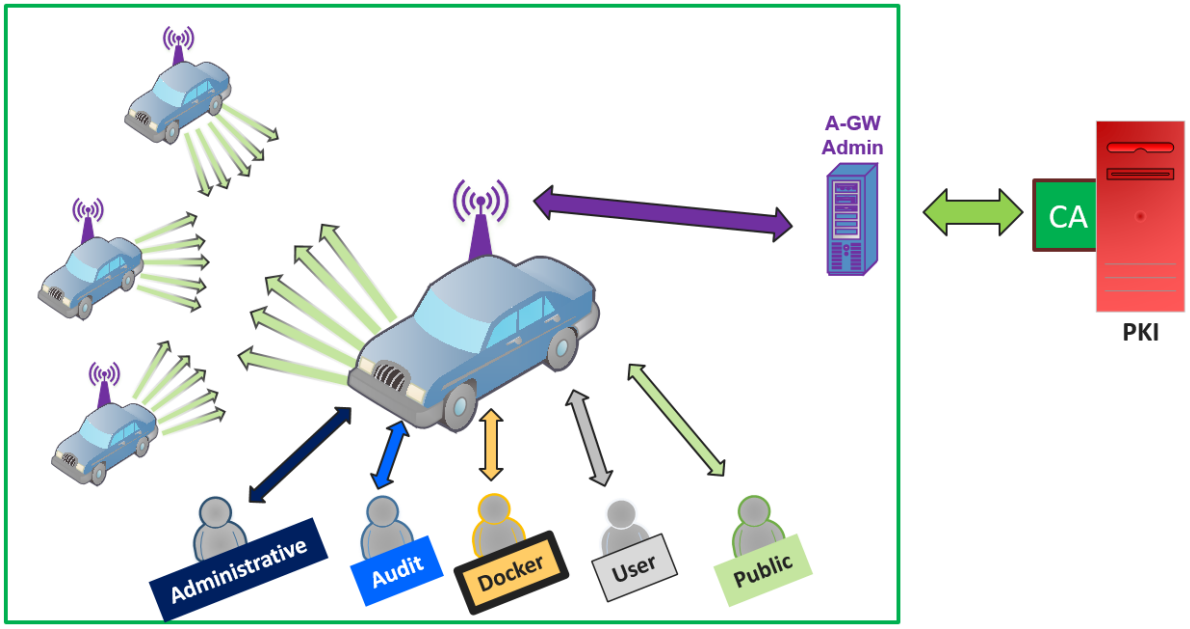


Abbildung 14: OTP – Gruppenbasierte Illustration

[25] https://www.euroncap.com/de

[26] https://www.greenncap.com/

Die oben aufgeführten Rollen werden nun exemplarisch folgenden Gruppen zur Realisierung des „Separation-of-Duties“ Prinzips zugeordnet.

4.2.2.1 Gruppe 0 – A-GWA

Zugewiesene Rolle:

- Automotive Gateway Administrator (A-GWA)

Der A-GWA ist eine zentrale systemische Entität in der OTP, welche die folgenden Gruppen, die zugehörigen User- und Usage-Profile sowie die A-GWs verwaltet. Der A-GWA selbst hat keine Zugriffsrechte auf Inhalte übertragener Informationen und kann User- und Usage-Profile nicht selbstständig, sondern nur auf Anforderung anderer Gruppen ändern. Eine ausführliche Beschreibung befindet sich in Kapitel 4.3.

4.2.2.2 Gruppe 1 – Admin (privilegiertes Lesen und Schreiben)

Zugewiesene Rollen:

- Fahrzeughersteller (OEM)
- Supplier (Tier-1)
- R&M

Gruppe 1 ist für den „administrativen“ und privilegierten Lese- und Schreibzugriff auf Fahrzeugdaten vorgesehen. Dabei ist dieser Zugriff nicht mit dem in der IT-Branche üblicherweise verwendeten Supervisor-Modus (wie „root“ unter Unix) vergleichbar, da im OTP ein „multiple-eyes-principle“ verfolgt wird. Die unter Gruppe 4 aufgeführten „User“-Rollen bekommen das Recht, über opt-in / opt-out Funktionalitäten, den Zugriff von dieser und den anderen Gruppen zu erlauben (opt-in) oder einzuschränken (opt-out). Darüber hinaus unterliegen die Zugriffe einer jeden Rolle der Kontrolle einer anderen Rolle, wie es beispielhaft in Kap. 4.3.1 illustriert ist, so dass ein EiP Modus nicht möglich ist.

Der OEM als Fahrzeugentwickler und –hersteller sowie technischer Servicedienstleister muss über privilegierten Lese- und Schreibzugriff auf Daten und Funktionen des Fahrzeuges verfügen, um damit auch die Bereitstellung von Updates während der gesamten Lebensdauer des Fahrzeugs zu gewährleisten. Aus diesem Grund sollen einige Usage-Profile (Master-Usage-Profil) nicht durch User Profile (Gruppe 4) durch *opt-out* geändert werden können. Für den remote Zugriff, bei denen der Hersteller nach der Fahrzeugzulassung mit ISPs konkurriert, sollten die Rechte zum Zugriff auf Daten und Funktionen mit den konkurrierenden Parteien gleichwertig sein.

Ebenso benötigt ein Tier-1 Automobilzulieferer einige Fahrzeugdaten, um diese zu analysieren, auszuwerten und seine Fahrzeugteile verbessern zu können. Für einen aktiven und schnellen Support zu seinen Fahrzeugkomponenten könnte dieser Supplier auch Schreibzugriff bekommen, um Probleme so schnell wie möglich zu beheben. Der administrative Schreibzugang sollte von den eingebauten Komponenten des Lieferanten abhängen und auf die Bedürfnisse zugeschnitten sein, die sich im Zusammenhang mit diesen Komponenten ergeben.

R&M benötigt für die Fehlerdiagnose, das fahrzeuginterne Auszulesen von Daten und die sichere Kommunikation mit dem Fahrer ebenso privilegierten und anlassbezogenen remote

Lese- und Schreibzugriff auf das Fahrzeug (eine detailliertere Beschreibung weiterer Aufgaben für Diagnose, Reparatur und Wartung findet sich in Kapitel 4.4.4).

4.2.2.3 Gruppe 2 – Audit (nur privilegierter Lesezugriff)

Zugewiesene Rollen:

- Rettungsdienste
- Behörden
- Prüfunternehmen (PTI, Euro NCAP, Green NCAP,…)
- Versicherungen

Gruppe 2 bezieht sich auf die Rollen für Monitoring und Audit-Aufgaben, die somit einen privilegierten Lesezugriff auf das Fahrzeug haben können. Dieser Zugriff sollte jedoch grundsätzlich nicht dauerhaft, sondern auf Ad-hoc-Basis bestehen und nur Informationen enthalten, die für den Zweck dieser Rolle unbedingt erforderlich sind. Hier sollte die Polizei z.B. in der Lage sein, auf Standortdaten zuzugreifen, um gestohlene oder beschädigte Autos zu lokalisieren, wenn dies von einem Gericht angeordnet wurde. Die Rettungsdienste benötigen für den Einsatz Informationen über den Status eines oder mehrerer Fahrzeuge sowie Standortdaten, um mehr Details zu den Unfällen zu erhalten. Während einer PTI / PAI benötigt das Prüfunternehmen bestimmte Fahrzeugdaten. Wenn bei solchen Inspektionen auch die Integrität und Aktualität des A-GW und anderer security-relevanter Komponenten überprüft wird, sind ggf. zusätzliche Informationen erforderlich.

Manche der hier genannten Rollen erfordern für ihre Zwecke nur vorübergehenden und manchmal nur in besonderen Situationen Zugriff auf das Fahrzeug. Ein dauerhafter Zugriff sollte nur eingeschränkt gestattet sein, so vielleicht im Falle von Versicherungspolicen, die das Fahrverhalten der Kunden berücksichtigen. In anderen Fällen, wie z.B. bei Remote-OBFCM oder OBM muss sichergestellt sein, dass die Daten anonymisiert sind und nicht zum Aufspüren des einzelnen Fahrzeugs, Fahrers, Halters oder Insassen verwendet werden können. Darüber hinaus können Rollen aus dieser Gruppe auch zur Realisierung des „multiple-eyes-principle“ als Kontrollfunktion zu Aktivitäten der Gruppe 1 verwendet werden.

4.2.2.4 Gruppe 3 – Docker

Zugewiesene Rollen:

- Independent Service Providers
- 3rd-Party Developer
- Diagnostic Tool Developer

In Gruppe 3 sind Entwickler von Drittanbietern gelistet, die eigene Anwendungen und Produkte für das Infotainmentsystem des Fahrzeugs oder eigene Apps anbieten, mit denen ISPs Ferndiagnosen oder -Prognosen durchführen können. Da dieser Einsatz über den reinen Lese- und Schreibzugriff hinausgeht, sollten die Applikationen in einem vom Rest des Fahrzeugs durch Docker-Technologie separierten Bereich installiert werden, dabei jedoch Zugriff auf einige fahrzeuginterne Daten bekommen. Über das HMI des Fahrzeugs (z. B. Kombiinstrument, Infotainment-Display usw.) können diese Apps dann vom Benutzer genutzt werden. Durch die Separierung können die Apps auch eigenständige Security Policies verfolgen,

die nicht kompatibel zu der Fahrzeug Policy sind, wie dies bei der SmartPhone Integration heute typisch ist.

Im *Maintenance Mode* (siehe Kapitel 4.4.4) sollte über den Docker ein privilegierter Zugriff – vergleichbar mit Gruppe 1 – möglich sein.

Mit dieser Zugangsregelung ist es dem autorisierten Tool-Developer möglich, ISP-Anwendungen und -Zubehör angemessen und effizient zu entwickeln, ohne auf Informationen zuzugreifen, die nicht erforderlich oder nicht freigegeben sind.

4.2.2.5 Gruppe 4 – User

Zugewiesene Rollen:

- Fahrer
- Fahrzeugnutzer
- Halter

Gruppe 4 bezieht sich auf die „direkte Nutzung“. Der Zugriff ist für Fahrer, Fahrzeugnutzer und Halter vorgesehen. Dies geht mit einem nicht privilegierten Lese- und Schreibzugriff auf die Nutz- und Konfigurationsdaten des Fahrzeugs einher, die zum Fahren des Fahrzeugs und Verwenden einzelner Services benötigt werden. Darüber hinaus hat der Halter / Fahrer das Recht, den größten Teil der Usage-Profile aller Gruppen 1-3 über opt-in / opt-out zu kontrollieren, mit Ausnahme von obligatorischen remote Services (Master-Usage-Profil, siehe oben).

4.2.2.6 Gruppe 5 – Public

Zugewiesene Rollen:

- Straßeninfrastruktur
- Fahrzeug
- C-ITS

In Gruppe 5 sind alle Rollen aufgeführt, die zusätzlich zu oben aufgeführten Gruppen Informationen von anderen Verkehrsteilnehmern empfangen und selbst zeitlich begrenzte Messages ortgebunden versenden. Bei den Messages handelt es sich um öffentlich lesbare aber in ihrer Integrität geschützte C-ITS-Informationen an alle ITS Stationen im näheren Umfeld.

4.2.3 Zuordnung: Security Layer - Autorisierung

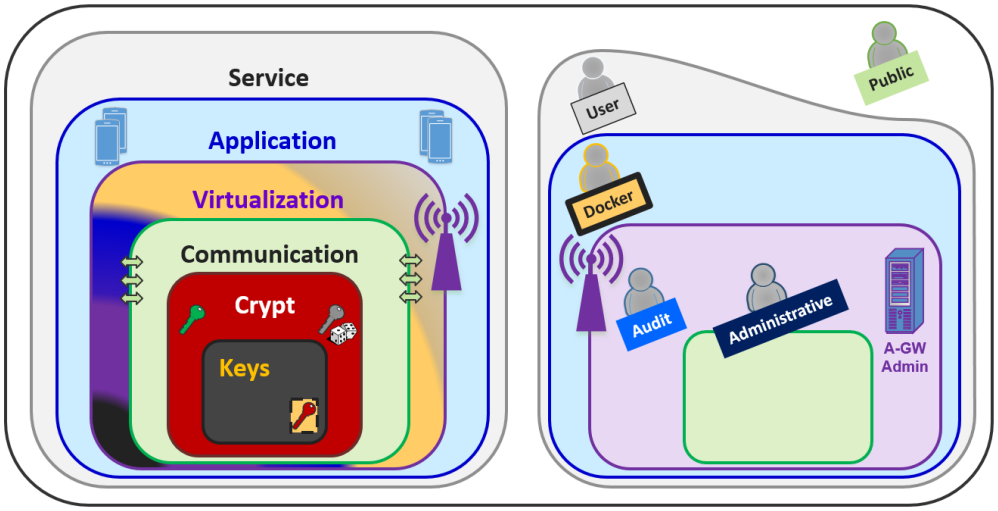


Abbildung 15: Illustration der Abhängigkeiten zwischen Security Layer und Gruppen

Tabelle 1 zeigt eine Zuordnung zwischen den Security Layern und den definierten Gruppen, die auch in obiger Abbildung dargestellt ist.

#	Layer	Gruppe	Kommentar
1	Keys	-	Da diese Layer für die Speicherung von Schlüsseln sowie für grundlegende Funktionen wie Kryptographie und Zufallszahlen-generierung verantwortlich ist, kann nach der Erstellung des SE / HSM keine Berechtigungsgruppe auf diesen Layer zugreifen.
2	Crypt	0. A-GWA	Da diese Layer für die Schlüsselgenerierung, Schlüsselverwaltung, Integritätsprüfungen und die Übertragung von Ergebnissen zwischen dem SE-Layer und des höheren Layer verantwortlich ist, kann nach dem Roll-out des SE / HSM keine Berechtigungs-gruppe auf diesen Layer zugreifen, außer der A-GWA im Zuge von Security-Updates.
3	Communica-tion	0. A-GWA (1. Admin)	Dieser Layer reguliert den Informationsfluss zwischen verschiedenen Kommunikationskanälen über den A-GWA. Da der A-GWA selbst keinen Zugriff auf inhaltsbezogene Daten und Informationen hat, hat er keinen Zugriff auf Inhalte von Layer 4 und darüber. Die Gruppe „Admin“ ist indirekt Teil dieser Ebene, da sie für Aktualisierungen und Fehlerprüfungen der Fahrzeugsoftware verantwortlich ist
4	Virtualization	1. Admin 2. Audit	Die Mitglieder der Gruppe „Admin” haben die höchsten Zugriffsrechte in der OTP, da sie u.a. grundlegende Fahrzeuginformationen sowie Updates durchführen. Zusätzlich werden die User-Profile der Gruppe „Audits“ in dieser Ebene abgebildet. Ein Großteil dieser Zugänge kann vom Halter / Fahrer (Gruppe 4) über opt-in / opt-out angepasst werden.
5	Application	3. Docker	ISPs sowie Entwickler von Drittanbietern und Diagnosetools können Apps in separierten Bereichen (Docker) des Fahrzeugs ausführen.
6	Service	4. User	Die Möglichkeiten der Gruppe 4 beschränken sich auf den „direkten Gebrauch“ und der Nutzung von opt-in / opt-out über User-Profile.
7	Broadcast	5. Public	Der 7. Layer definiert die Verteilung von C-ITS Informationen zwischen ITS-Stationen.

Tabelle 1: Zuordnung von Security Layern zu Gruppen

4.3 A-GWA: Automotive Gateway Administrator

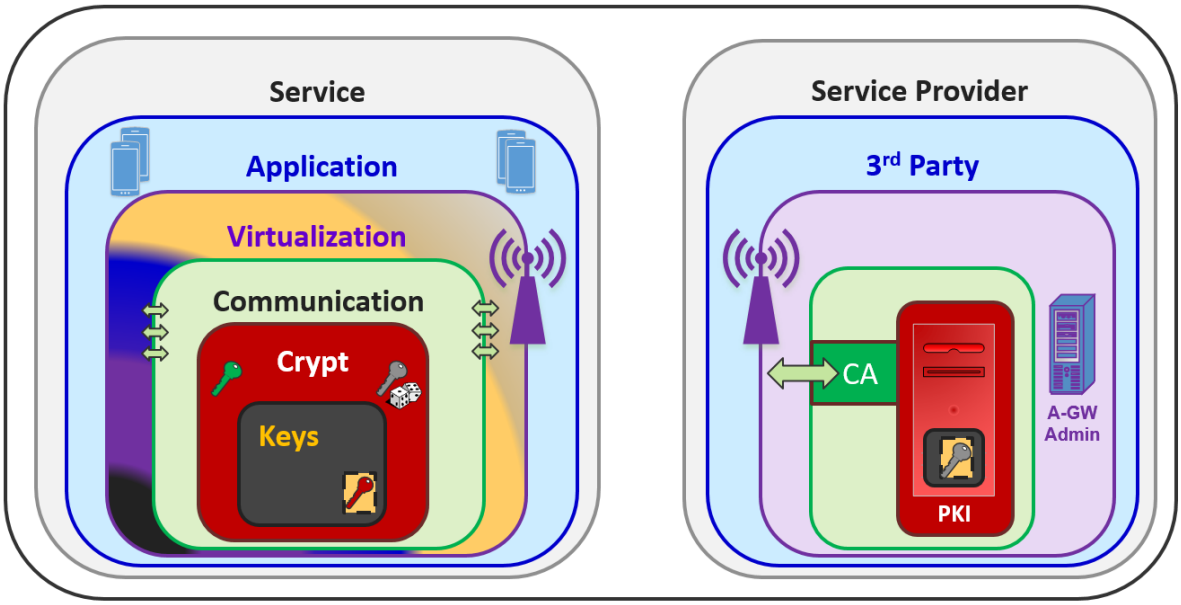


Abbildung 16: OTP - Security Modularisierung

Die Realisierung des “Separation of Duties” Prinzips mit fair verteilen Marktrollen statt nur einer privilegierten Supervisor-Rolle (die allen anderen ihre Regeln auferlegt) - ist technologisch nicht so einfach zu lösen. Das „*Root*-Prinzip“ von Unix-Systemen (der Supervisor-Zugriff) sind im IT-Geschäft gut verankert und wird häufig als „*Gott-Modus*“ bezeichnet: Jedem Benutzer kann jede Art von Zugriff zugewiesen oder verweigert werden, aber *Root* bzw. der Supervisor dürfen immer alles. Darüber hinaus und wie in [ANA] angegeben, ist das Root-Prinzip eine der größten Herausforderungen für die IT Security, da der „Verlust von Rootrechten“ an einen Hacker meist den Verlust von Daten und Kontrolle bedeutet (siehe EiP-Modus in Kapitel 1.1). Zentralisierte Systeme wie ExVe mit privilegiertem Zugriff auf zentrale Rollen sind zwar recht einfach zu installieren, implizieren jedoch auch diese Problematik.

Um einen privilegierten Zugang so auf verschiedene Interessensgruppen zu verteilen, wie dies in den obigen Kapiteln aufgeführt ist, muss man von Supervisor-Ansätze abrücken und stattdessen eine andere Security-Architektur entwerfen. Man könnte eine „*Distributed Ledger*” Lösung aufbauen, die derzeit durch Blockchain-Technologien gehypt wird. Da die meisten Blockchain-Implementierungen jedoch vom zeitaufwändigen „Data Mining“ abhängen, von C-ITS nicht berücksichtigt werden und in den letzten Jahren nicht so viele Erfolgsgeschichten lieferten[27], wurde ein anderer Ansatz verfolgt.

Durch Verwendung der Security-Funktionen der Layer 1-3 (siehe Security Layer in Kapitel 4.1: *sichere Kommunikation basierend auf Kryptographie* – ähnlich wie bei C-ITS) werden in Layer 4 zusätzliche Autorisierungsfunktionen für das A-GW angegeben. Dazu muss auf der Systemseite ebenso eine Layer-4-Komponente erstellt werden, die die bereits für C-ITS ver-

[27] außer im Finanzwesen (BITCOIN) oder in Bezug auf „Smart Contracts”.

wendete PKI bzw. CA wiederverwendet (siehe Abbildung 16). Dies ist der **Automotive Gateway Administrator (A-GWA)**, der für den sicheren Betrieb aller A-GWs zuständig ist, die dem A-GWA zugewiesen sind:

- Management aller **Rollen** und **Gruppen**, wie sie exemplarisch in Kapitel 4.2 aufgeführt sind.
- Management aller User- und Usage-**Profile**
- Management[28] des **Informationsflusses** zwischen den einzelnen Rollen
- **Update** Mechanismen für das A-GW:
  - User- und Usage-**Profile**
  - Security Updates (Layer 2-4)
- **Monitoring** oben aufgeführter Funktionalitäten

Darüber hinaus kann der A-GWA zusammen mit dem A-GW und unter der Kontrolle der relevanten Rolle[29] als hochsicheres (remote) **Zugriffssystem** für u.a. folgende Mehrwertdienste verwendet werden:

- Update der Docker Units
- Update von ECU's
- On-Board-Monitoring (OBM) für unterschiedliche Anwendungsfälle wie PTI / PAI [VDTÜV3], Versicherungen oder Emissionsauswertungen

Für den Fall, dass ein relevantes Usage-Profil eine End-to-End-Security erfordert, ist der A-GWA nicht in der Lage, den Inhalt der übertragenen Daten zu lesen oder User- / Usage-Profile zu ändern, da die kryptografischen Prozesse in den darunterliegenden Layern abgebildet sind.

Es wird empfohlen, dass der Betrieb des A-GWA durch eine neutrale, unabhängige Instanz übernommen werden sollte. Um diese Neutralität zu untermauern und das "Separation of Duties" Prinzip zu erfüllen, sollten dem Betreiber des A-GWA auch keine Zugriffsrechte auf inhaltsbezogene Daten und Informationen gewährt werden.

Vergleichbare Lösungen zum A-GWA werden zurzeit im deutschen Smart Metering System[30] [PP-SMGW, PP-SMGW-SE] spezifiziert und installiert, die zukünftig auch für Ladestationen für Elektrofahrzeuge relevant sein können. Ideen, wie die Rolle des A-GWA in der Realität umgesetzt werden kann, befinden sich im Entwurf des Protection Profiles für das A-GW [PP-AGW], das zusätzlich zu diesem Bericht veröffentlicht wurde.

4.3.1 Beispiele für 'Multiple-Eyes' Zugriffsprozesse mit dem A-GWA

In den vorherigen Kapiteln wird veranschaulicht, wie Security-Funktionen in verschiedenen Layern angelegt werden können und wie verschiedene Rollen verschiedenen Gruppen basierend auf grundlegenden Berechtigungen zugeordnet werden können. Um konkrete User-Profile (relevant für Gruppe 4: Halter / Fahrer) und Usage-Profile (individuell für jede Rolle)

[28] Das A-GWA muss nicht zwingend selbst die Kommunikation durchführen.

[29] opt-in / opt-out durch Halter / Fahrer

[30] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html

zu definieren, sollte für alle Datenobjekte (Asset) im Fahrzeug ebenso entsprechende Gruppierungen vorgenommen werden. Dies wird in diesem Bericht nicht behandelt, ist aber bereits Thema in vielen Verbandsdiskussionen.

Darüber hinaus müssen **Prozesse** definiert werden, auf welcher Basis ein A-GW in einem Fahrzeug, Anfragen für einen remote Zugriff annehmen oder ablehnen muss, damit eine "Separation of Duties" sinnvoll funktionieren kann. Die grundlegenden Schlüsseltechnologien im OTP sind hierbei

- **Digitale Signaturen** (*Signatures*) zur Realisierung eines 'Multiple-Eye Entscheidungsprozesses' und
- **Zeitstempel** (*Time Stamps*) um Deadlocks aufgrund gleichzeitiger Transaktionen zu vermeiden.

Zwei mögliche Beispiele veranschaulichen, wie der Informationsfluss zwischen A-GWA, OEM und dem A-GW innerhalb des Fahrzeuges von der OTP abgebildet werden kann

1.) **Update** eines **OEM Usage-Profils** für einen konkreten Fahrzeugtypen
Annahme: Für einen neuen Service ist es erforderlich, dass ein OEM ein neues Master-Usage-Profil[31] aktualisiert, um Schreibzugriff auf ein ECU in allen Fahrzeugen eines Fahrzeugtyps zu erhalten. Es sei hierbei nicht erforderlich, die Zustimmung des Fahrzeughalters einzuholen, es ist jedoch eine Typgenehmigung erforderlich. Der folgende Workflow muss im OTP abgebildet werden:
   1. Änderungsanfrage des OEM zum Usage-Profil wird zur Typgenehmigungsbehörde[32] gesendet
   2. Typgenehmigung erteilt
   3. Neues Usage-Profil muss an die gesamte Fahrzeugflotte gesendet werden, damit dieses Usage-Profil zu einem bestimmten Zeitpunkt in allen Fahrzeugen aktualisiert werden kann
   4. Das neue Usage-Profil wird vom OEM genutzt

   Der Workflow kann wie folgt im OTP abgebildet werden. Um zu verhindern, dass Hacker im Rahmen einer Man-in-the-Middle-Attacke etwas Ähnliches tun können, werden die Signaturen jeder Nachrichtenübertragung überprüft (Abbildung 17).
      1. Nachricht mit signierter Änderungsanfrage bzgl. des Usage-Profils wird vom OEM zur Typgenehmigungsbehörde gesendet
      2. Check der Signatur, falls OK:
         Typgenehmigung erteilt, diese wird signiert und zurückgesendet
      3. Doppel-signierte Nachricht (OEM mit Typgenehmigung) des neuen Usage-Profils wird an A-GWA gesendet

[31] Im Falle von Security, Safety, Umweltschutz oder anderen Software-Änderungen, die typgenehmigungsrelevant sind. In allen anderen Fällen ist eine Zustimmung des Fahrzeughalters (opt-in) einzuholen, was zusätzlich im Prozess abgebildet werden muss.

[32] oder alternativ einer beliehenen unabhängigen Stelle

4. A-GWA:
   a. Check beider Signaturen, falls OK:
   b. Usage-Profil wird in Referenz-DB gespeichert
   c. Usage-Profil wird vom A-GWA signiert
5. Dreifach-signierte Nachricht (OEM mit Typgenehmigung und A-GWA) des neuen Usage-Profils und dem Aktivierungszeitpunkt wird an alle A-GW der relevanten Fahrzeuge gesendet
6. A-GW
   a. Check aller 3 Signaturen, falls OK:
   b. Update des lokalen Usage-Profils zum definierten Zeitpunkt
7. Signierte Bestätigungsnachricht wird von den A-GW's zurück zum OEM und zu den Typgenehmigungsbehörden gesendet.

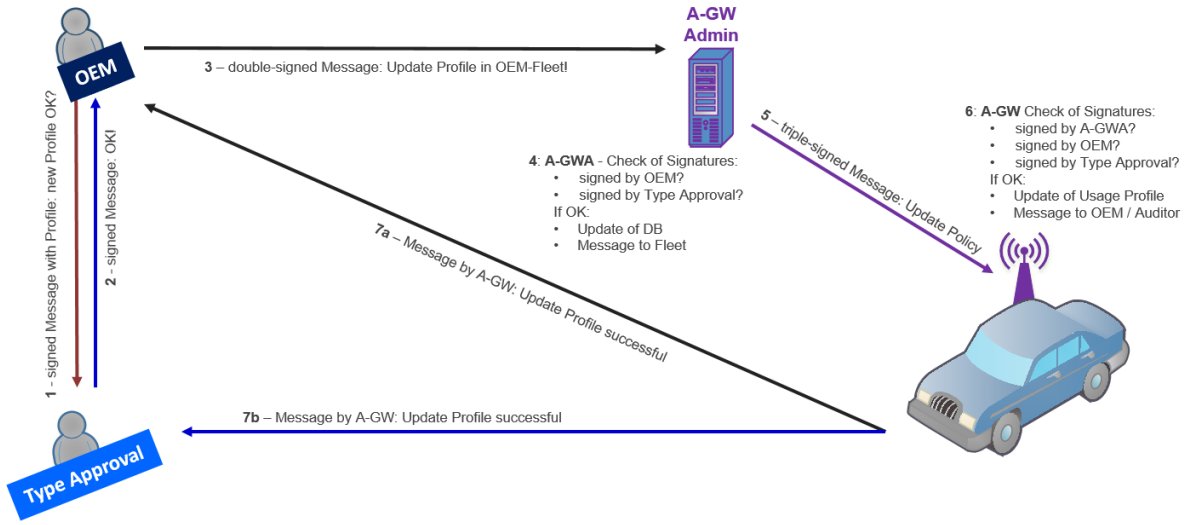


Abbildung 17: Update eines OEM Usage-Profils (vereinfachtes Beispiel)

2.) **Software Update** durch einen OEM (z.B. einer Motorsteuerungseinheit)
Annahme: Ein OEM muss ein Software-Update eines Steuergeräts durchführen. Dieser Vorgang sei compliant zu den OEM-Usage-Profilen aller Fahrzeugen eines Fahrzeugtypen. Es sei zusätzlich nicht erforderlich, dass dieses Update zwingend im *Maintenance Mode* durchgeführt werden muss. Die Fahrzeuge müssen sich aber an einer sicheren Position befinden, ausgeschaltet sein und dürfen sich während des Updates nicht bewegen (*Parking Mode*).
Der Workflow muss wie folgt im OTP unter Kontrolle des A-GWA abgebildet werden:

1. Anfrage des Softwareupdates des OEM wird zur Typgenehmigungsbehörde gesendet
2. Typgenehmigung erteilt
3. Neue Software wird zur gesamten Flotte gesendet, damit dieses Update vorgenommen wird.

Der Workflow könnte wie folgt implementiert werden. Um zu verhindern, dass Hacker etwas Ähnliches tun können (bösartige Code-Injektion), werden die Signaturen jeder Nachrichtenübertragung überprüft (Abbildung 18).

1. Nachricht mit signierter Anfrage zum Softwareupdate wird vom OEM zur Typgenehmigungsbehörde gesendet
2. Check der Signatur, falls OK:
   Typgenehmigung erteilt, diese wird signiert und zurückgesendet
3. Doppelt-signierte Nachricht (OEM mit Typgenehmigung) des neuen Usage-Profils wird an alle relevanten A-GWs gesendet
4. A-GW
   a. Check beider Signaturen, check der Usage-Profil-Compliance, falls OK:
   b. Softwareupdate wird in A-GW zwischengespeichert
   c. Sobald Fahrzeug im *Parking mode*: Softwareupdate wird durchgeführt
   d. Update-Zeitpunkt wird vom A-GW signiert
5. Signierte Bestätigungsnachricht wird mit Zeitstempel von den A-GW's zurück zum OEM und zu den Typgenehmigungsbehörden gesendet

Im Gegensatz zu Beispiel 1 muss der A-GWA keine aktive Rolle in diesem Update-Prozess bekommen. Der A-GWA ist lediglich für die kontinuierliche Überprüfung / Synchronisation von Schlüsseln und Profilen mit den A-GW's erforderlich und kontrolliert den Informationsfluss indirekt über die Schlüsselverfahren.

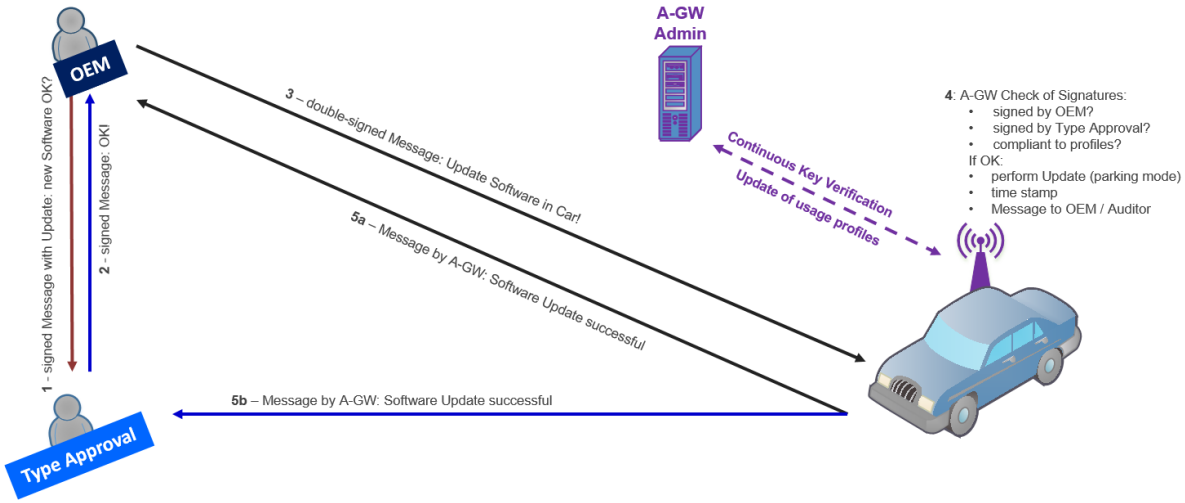


Abbildung 18: Software Update durch einen OEM (vereinfachtes Beispiel)

4.4 Secure Lifetime

Vernetzte Fahrzeuge im C-ITS sowie alle Komponenten eines Fahrzeugs, unabhängig davon, ob es sich um Hardware, Software oder Daten handelt, müssen über die Lebensdauer (*Lifetime*), die in 5 verschiedene Phasen unterteilt ist (Abbildung 19), IT Security-Anforderungen erfüllen. IT Security Software muss manchmal ein Security-Update bekommen und Hardware muss zumeist aufgrund von Alterung oder Aufwärtskompatibilität ausgetauscht werden. Der sichere Betrieb automatisierter Fahrzeuge muss während der Fahrt jederzeit überwacht werden können und der Halter / Fahrer muss jederzeit wissen, ob die IT Security im Fahrzeug erfüllt ist.

End-of-Life und die darauf folgende Abwrackung (*Scrapping*) beziehen sich nicht nur auf das gesamte Fahrzeug. Das Scrapping bezieht sich auf jede einzelne Hardwarekomponente sowie auf jede Software und auch auf Daten.

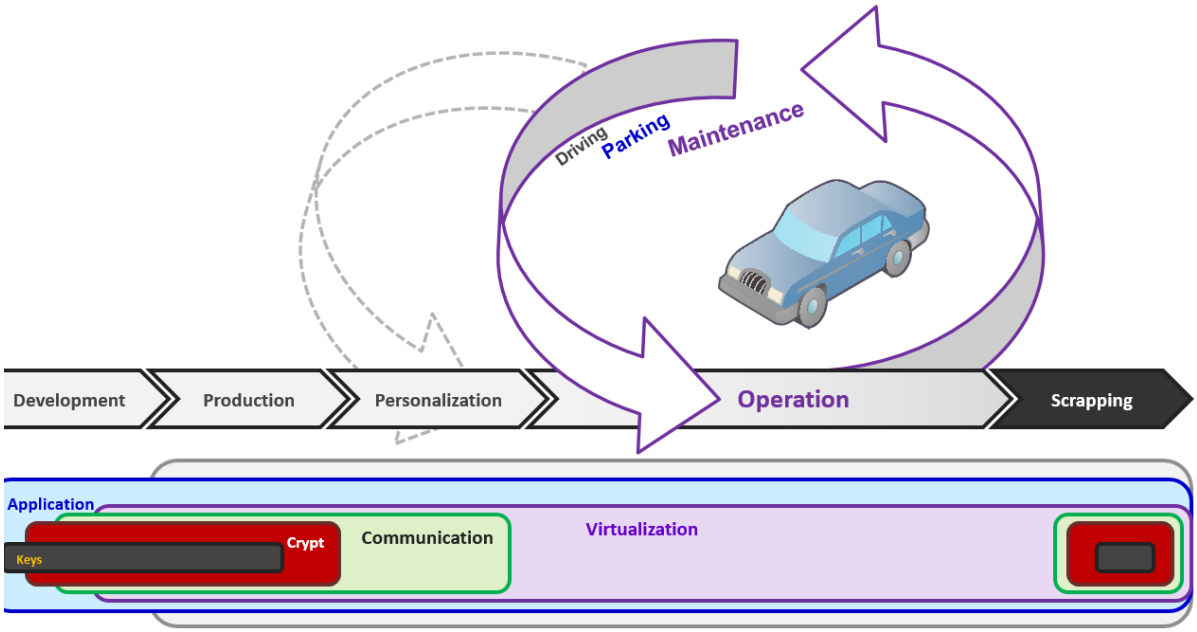


Abbildung 19: OTP Security Lifetime

Es wird ein generisches Regelwerk für die *OTP-Lifetime* anhand der Phasen in Abbildung 19 vorgeschlagen. Ebenso wie das Rollenkonzept in Kapitel 4.2 sollen die hier aufgeführten Vorschläge nur als sinnvolle Beispiel dienen.

4.4.1 Development

Während der Entwicklung von OTP-Security-Komponenten sollten folgende Anforderungen erfüllt sein:

1. Alle Komponenten der OTP müssen in einer sicheren Entwicklungsumgebung entwickelt werden.
2. Ein Cybersecurity Engineering-Prozess wird von den Entwicklern gemäß [ISO21434] verfolgt.
3. Jede Security-Komponente des OTP sollte nach den Common Criteria [CC1, CC2, CC3] evaluiert und zertifiziert werden (siehe Kapitel 5.2). Jede Automotive Gateway

Lösung und deren Security-Teilkomponenten aus tieferen Security Layern müssen nach den Common Criteria gemäß [PP-AGW] evaluiert und zertifiziert werden.

4. Jede Security-Komponente im A-GWA (HSM, Firewall, OS, DB, …) muss nach den Common Criteria evaluiert und zertifiziert sein.

4.4.2 Production

Bei der Endfertigung des Fahrzeugs oder seiner Komponenten werden kryptografische Schlüssel und Initialdaten (jedoch keine benutzerrelevanten Informationen) installiert. Jeglicher Schreibzugriff oder Update auf Layer-1 und Layer-2 Bestandteilen des A-GW ist nach der Produktionsphase nicht mehr zulässig, mit Ausnahme der Deaktivierung von Schlüsseln oder kryptografischen Funktionen.

1. Alle IT Security-Komponenten des OTP müssen in einer sicheren Produktionsumgebung gefertigt werden.
2. Ein Cybersecurity Engineering-Prozess muss von der Produktionsumgebung gemäß [ISO21434] eingehalten werden.
3. Vor Integration in das Fahrzeug wird sichergestellt, dass der Versand von IT Security-Komponenten (TIER 1-3) zwischen verschiedenen Fertigungsstätten innerhalb einer sicheren Lieferkette (*Supply-Chain*) gem. [TISAX] erfolgt.
4. IT Security-Komponenten der Security Layer 1-2 (Layer *Keys* und *Crypt*) sollten die besonderen Anforderungen für die Schlüsselgenerierung, -bereitstellung und -support erfüllen, die für PKI-Rollout-Prozesse zwingend erforderlich sind.
5. Das A-GW muss zum Ende des Fertigungsprozesses der VIN des Fahrzeugs zugeordnet werden.

4.4.3 Personalization

Während der Personalisierung wird ein neuer Halter des Fahrzeugs im A-GW abgebildet. Ein Schreib- oder Aktualisierungszugriff auf Layer-3 Bestandteile des A-GW ist nach der Personalisierungsphase bis zum Wechsel des Halters nicht zulässig, außer im Falle eines Hardwareaustauschs des A-GW. Der Personalisierungsprozess geht mit der offiziellen Zulassung eines Fahrzeuges einher.

1. Beim Halterwechsel werden zunächst alle halterrelevanten User-Profile des A-GWs auf eine ursprüngliche und neutrale Konfiguration zurückgesetzt. Alle Links zu den Daten des letzten Halters werden gelöscht (*gescrappt* → End-of-Life).
2. Das A-GW wird durch Aktualisierungen der neuen User-Profile für den neuen Halter personalisiert.
3. Basierend auf den User-Profilen des Halters können zusätzliche User-Profile für die oder den Fahrer ad-hoc installiert werden.

4.4.4 Operation

Während des Betriebs eines Fahrzeugs können verschiedene Besitzverhältnisse auftreten (siehe Personalisierung), sich User- und Usage-Profile ändern sowie Ersatzteile als auch deren digitale Zuordnungen ausgewechselt werden. Es wird dabei im Allgemeinen zwischen drei verschiedenen Modi unterschieden:

- **Driving (Information) Mode**: Dies ist der safety-relevante Modus, während sich das Auto bewegt. In diesem Modus können nur Konfigurationsaktualisierungen, Fahrerinformationen und C-ITS-Updates vom Fahrzeug empfangen werden
- **Parking (Support) Mode**: Remote-Updates oder Installationen von angedockten Layer-5-Anwendungen können ebenso durchgeführt werden wie Aktualisierungen von User- / Usage-Profilen für das A-GW. Sollten Transaktionen mit komplexen Abhängigkeiten ausgeführt werden müssen, muss das „Alles-oder-nichts-Prinzip“ befolgt werden.
- **Maintenance (Repair) Mode**: Wenn Reparaturen am Fahrzeug bei einem autorisierten R&M-Provider durchgeführt werden, sind Software-Updates des A-GW oder von Komponenten des Fahrzeugs zulässig (unter der Kontrolle des A-GWA bzw. des OEM). Software-Updates mit komplexen Abhängigkeiten müssen dem das „Alles-oder-nichts-Prinzip“ folgen und geeignete Transaktionsschutzmechanismen verwenden.

Die folgenden Regelungen werden zusätzlich bzgl. *Repair & Maintenance* (R&M) vorgeschlagen:

1. **OEM Support**
    a. Der OEM ist verpflichtet, während der gesamten Lebensdauer des Fahrzeugs **Support** und Updates für Security-Komponenten wie das A-GW, Docker-Einheiten (Layer 5) und das HMI bereitzustellen.
    b. Die **Lifetime Anforderungen** (cradle to grave) sollten gesetzlich reguliert sein.
    c. Der OEM hat die Möglichkeit, seine Supportverpflichtungen einem kompetenten und autorisierten Dritten wie z.B. einem **Tier-1 Supplier** zu übertragen.
    d. Nach Ablauf einer definierten *Lifetime* muss der OEM den Quellcode offenlegen oder erklären, dass der A-GW-Support bis zum **Ende der Fahrzeuglebensdauer** fortgesetzt wird.
2. **Service Station**
    a. Eine Service Station wird vom Halter oder Fahrer offiziell für Wartungs- und Reparaturarbeiten über die OTP **registriert**.
    b. Service Stations müssen ein **lizensiertes Diagnosetool** verwenden. Nicht lizensierte Tools werden vom A-GW abgelehnt.
    c. Die **Mitarbeiter** von Service Stations müssen für den Einsatz lizensierter Diagnosetools geschult sein. Das SERMI-Schema [SERMI] könnte hierzu erweitert werden, um Werkstatt-Mitarbeitern für den Zugriff auf fahrzeuginterne Daten, Funktionen und Ressourcen zu zertifizieren.

3. **Updates**
    a. Auftretende Schwachstellen (*Exploits*) beim A-GW oder Layer-5-Anwendungen sollten ausschließlich durch **Security-Updates der Software** behoben werden können. Wenn aufgetretene Security-Exploits dennoch erfordern, dass (Teile) einer Hardware ausgetauscht werden müssen, muss der OEM dies sicherstellen. Bei einem vollständigen Austausch des A-GW muss die VIN mit dem neuen A-GW gekoppelt und eine neue Erstkonfiguration und Personalisierung (siehe oben) durchgeführt werden.
    b. Eine Überprüfung der **Aktualität** der Security-Software muss mindestens bei jeder Wartung in vordefinierten Zeiträumen durchgeführt werden. Ein (remote) OBM des A-GW ist den regelmäßigen Überprüfungen vorzuziehen
    c. **Updates** werden durch den OEM über den **A-GWA** zur Verfügung gestellt.
    d. **Regelmäßige Überprüfungen** des A-GW und anderer Komponenten müssen in vordefinierten Zeiträumen von neutralen Prüfeinrichtungen durchgeführt werden. Ein (remote) OBM mithilfe des A-GW ist gegenüber regelmäßigen Überprüfungen vorzuziehen
4. **Security Incidents**
    a. Es muss ein akustisches Signal ertönen oder auf dem HMI eine **Warnmeldung** aufleuchten, welches auf entdeckte Security-Vorfälle (*Security Incidents*) oder Fehlverhalten des A-GW oder anderer security-relevanter Komponenten hinweist. In diesem Fall und je nach Vorfall ist es obligatorisch, so bald wie möglich eine Service Station aufzusuchen, dabei könnte die Konnektivität unterbrochen werden und jegliche Fahrunterstützung deaktiviert werden.
    b. Jeder Security Incident muss an den **A-GWA** gesendet werden.
5. **Diagnose-Tool**
    a. Es soll **gesetzlich** geregelt werden, dass das OTP über (eine) standardisierte definierte **Diagnoseschnittstelle**(n) verfügt, die unter der Kontrolle des A-GW und/oder der Docker-Unit steht. Diagnosewerkzeuge für im Fahrzeug installierte Komponenten können lokal oder remote genutzt werden.
    b. Zu Diagnosezwecken kann über die **Docker**-Unit ein Zugriff gewährt werden.
    c. Die **Diagnosedaten** und Funktionen (eines Steuergeräts) sind über das A-GW verfügbar zu machen. Die Kommunikation und Interaktion zwischen dem remote ISP und dem Fahrer / Halter muss ebenfalls durch das A-GW sichergestellt werden.
    d. Der OEM stellt ISPs und 3rd Party-Entwicklern ein **Developer-Kit** für Diagnose-Tools zur Verfügung – einschließlich der Spezifikationen der Systeme und der Komponenten, die benötigt werden, um einen innovativen, autorisierten Service zu betreiben.
    e. **Unabhängige Tool-Entwickler** werden als vom OEM unterbeauftragten Entwicklern gleichwertig behandelt.
    f. Diagnose-Tools müssen von einem unabhängigen **Prüflabor** (mit zusätzlicher Validierung durch den OEM) getestet werden.

g. **Innovationen** von Diagnose-Tools dürfen durch den OEM nicht eingeschränkt werden.

4.4.5 Scrapping

Bei Austausch von IT Security-Komponenten oder dem „End-of-Life“ des Fahrzeuges sollten die folgenden Regeln befolgt werden:

1. Die Security-Komponenten sowie das Schlüsselmaterial und alle Daten, die in der Security-Komponente enthalten sind, sind auf sichere Weise zu vernichten.
2. Das Scrapping des A-GW und der entsprechenden Schlüssel wird in der PKI registriert.

Die Richtlinien für das Ende der Nutzungsdauer von User-Profilen und den entsprechenden Daten hängen von den Opt-out-Aktivitäten des Halters oder vom Halterwechsel ab. Wenn dies nicht im Widerspruch zur Gesetzgebung steht, müssen entsprechende Daten unter der Kontrolle des A-GW sowie des A-GWA auf sichere Weise gelöscht werden.

5 Audit und Ratings

Um sicherzustellen, dass eine Implementierung der in Kapitel 4 definierten OTP fehlerfrei und ohne ausnutzbare Schwachstellen erfolgt und somit ein hochsicheres System vorliegt, sind vollständige Prüfungen und Audits der Security-Funktionalitäten über die gesamte Lebensdauer der OTP-Komponenten notwendig.

5.1 Anforderungen an Audit Schemata

Ein geeignetes Prüfschema sollte internationale oder zumindest europäische Anforderungen und Vorschriften erfüllen, da nationale Lösungen für jedes Land, in dem das Produkt genutzt wird, aufgrund der hohen Anforderungen und der damit verbundenen Kosten nicht sinnvoll durchführbar wären.

Um die **GDPR**-Anforderungen zu erfüllen, sollten Datenschutz-Folgenabschätzungen[33] (DPIA) oder andere gleichwertige Audits angewendet werden, die auch den Verwendungskontext betrachten.

Für alle Security-relevanten Prozesse ist [27001] der wichtigste Standard. Die **ISO/IEC 27001** ist Teil der ISO/IEC 27000 Familie. Dabei handelt es sich um eine Sammlung von Standards für Informationssicherheitsmanagement Systeme (ISMS), deren letzte Version 2013 veröffentlicht wurde. ISO/IEC 27001 spezifiziert dabei ein Managementsystem, welches das Ziel verfolgt, Informationssicherheit unter Berücksichtigung spezieller Anforderungen geeignet zu organisieren. Unternehmen, die diese Anforderungen erfüllen, können sich durch akkreditierte Zertifizierungsstellen nach einem erfolgreich durchlaufenen Audit zertifizieren lassen

Auf Grundlage der ISO/IEC 27000 hat der VDA einen Katalog namens **TISAX**[34] [TISAX] für Anforderungen an die Informationssicherheit definiert, der sich auf die Lieferketten bezieht.

Zusätzlich wurde durch ISO und SAE ein Entwurf für ein Auditierungs-Schema (**ISO/SAE 21434** Draft [ISO21434]) vorgelegt, das „Anforderungen für das *Management von Cybersecurity-Risiken* in Bezug auf Konzeption, Entwicklung, Produktion, Betrieb, Wartung und Stilllegung von *elektrischen und elektronischen Systemen* (E / E) für Straßenfahrzeuge, einschließlich ihrer Komponenten und Schnittstellen, spezifiziert".

Mit dem neuen **Cybersecurity Act** [CSA] wird von der europäischen Organisation ENISA ein neues *Framework* zur Zertifizierung von Cybersecurity definiert. Dieses Rahmenwerk legt die wichtigsten horizontalen Anforderungen für die Entwicklung europäischer Zertifizierungssysteme für Cybersecurity fest und bezieht sich auf alle kritischen Infrastrukturen [NIS] – auch auf den Transport- und Verkehrssektor. Hierdurch wird die Anerkennung und Verwendung europäischer Cybersecurity-Zertifikate und EU-Konformitätserklärungen für ICT[35]-Produkte, ICT-Dienste und ICT-Prozesse für alle europäischen Staaten harmonisiert. Dabei werden bereits bestehende nationale wie auch internationale Schemata genutzt und ggf. erweitert. Das **SOG-IS** Abkommen [SOG-IS] zwischen ursprünglich 16 europäischen Mitgliedsstaaten

[33] Data Protection Impact Assessments

[34] Trusted Information Security Assessment Exchange

[35] Information and Communication Technology

wurde dabei im Cybersecurity Act ausdrücklich erwähnt, da die gegenseitige Akzeptanz einer **Common Criteria** (CC) Zertifizierung [CC1, CC2, CC3, CEM] in diesen Ländern bereits besteht. Außerdem werden die CC zusätzlich von vielen weiteren Industrieländern weltweit anerkannt [CCRA]. Aktuell wird das SOG-IS Abkommen zu einem offiziellen Zertifizierungsrahmen für Cybersecurity für alle 27 EU-Mitgliedsstaaten erweitert, um Konformitätsprüfungen bis auf *high-level* für Security-Komponenten zu gewährleisten. Darüber hinaus werden noch weitere Frameworks für Prüfungen auf *substantial-level* wie auch für Cloud-Services definiert.

Da die Common Criteria (CC)

- eine wichtige Rolle als offizielles Rahmenwerk für die Zertifizierung von Cybersecurity in Europa spielen werden,
- die CC in den meisten Industrienationen weltweit offiziell anerkannt sind und
- es derzeit keine Alternativen zu den CC gibt, die methodisch flexibel genug an Anforderungen und Funktionalitäten einer OTP angepasst werden können,

folgt in dem nächsten Kapitel eine Einführung in die Methodik der CC.

5.2 Common Criteria

Abbildung 20: Common Criteria Recognition Arrangement (CCRA) - Teilnehmer

Die Common Criteria (CC) für die *Evaluation der Security von Informationstechnologien* sind ein internationaler technischer Standard für die Bewertung von IT Security-Funktionen von

IT Produkten. Dabei wird das IT-Produkt anhand der zugrundeliegenden Dokumentation sowie durch praktische Tests evaluiert. Die Common Criteria werden bereits seit über 20 Jahren erfolgreich genutzt:

- Version 1.0 der CC wurde zur Kommentierung im Januar **1996** veröffentlicht und auf Basis verschiedener Vorgängerkriterien aus Europa, USA und Kanada entwickelt (ITSEC, TCSEC und CTCPEC).
- Version 2.0 wurde in den folgenden zwei Jahren umfangreich überarbeitet und im Mai 1998 veröffentlicht. Seitdem werden die CC für offizielle Evaluationen von IT Security-Produkten genutzt.
- Version 2.3 (August 2005) wurde als internationaler Standard veröffentlicht (ISO/IEC 15408:2005).
- **Version 3.1** ist die aktuellste Version der CC und wurde im April 2017 in Revision 5 veröffentlicht.

Das Prüfschema der CC unterscheidet zwischen dem Prozess der Evaluation und der Zertifizierung. Die Evaluation ist dabei der Prozess, der als Bewertung des Produktes gegen die definierten Anforderungen gesehen werden kann. Der Zertifizierungsprozess überwacht die Evaluation und endet mit der Vergabe des Zertifikats. Dabei erfordert die CC, dass der Zertifizierungsprozess durch eine von der Prüfstelle unabhängige Stelle durchgeführt wird.

5.2.1 Internationale Anerkennung und Akzeptanz

Wie in [ENISA3] erwähnt, ist die internationale Harmonisierung von CC-Zertifikaten einer der wichtigsten Vorteile bei der Anwendung der CC für die Evaluation von IT Security-Produkten. Zurzeit gibt es zwei unterschiedliche internationale Abkommen für eine länderübergreifende Anerkennung: Das CCRA sowie das SOG-IS [CCRA, SOG-IS].

CCRA

Mit dem ersten internationalen Abkommen über die Anerkennung von IT-Security Zertifikaten, das **C**ommon **C**riteria **R**ecognition **A**rrangement[36] (siehe Abbildung 20) soll sichergestellt werden, dass eine Evaluation auf der Grundlage einheitlicher, international harmonisierter Standards mit einem möglichst hohen Maß an Vertrauenswürdigkeit (*Assurance*) durchgeführt werden kann. Dies soll die Verfügbarkeit hochsicherer IT Produkte für unterschiedlichste Anwendungsfälle verbessern und dabei redundante Evaluationen in mehreren Ländern vermeiden. Mit einem CC Zertifikat für ein IT Produkt sollte keine weitere Security-Bewertung mehr erforderlich sein.

Um die notwendigen Vereinbarungen umzusetzen und die jeweiligen nationalen Systeme (Prüfstellen und Zertifizierungsstellen) hinsichtlich der Anwendung des Kriterienkataloges zu koordinieren und zu synchronisieren, wurde ein Managementgremium aus hochrangigen Vertretern der einzelnen CCRA-Nationen gegründet. Die Anforderungen der CC werden dabei hauptsächlich von einem internationalen Konsortium in zwei Gruppen weiterentwickelt:

- Im Common Criteria Development Board (CCDB) sowie
- im Common Criteria Maintenance Board (CCMB).

[36] https://www.commoncriteriaportal.org/ccra/

Das CCDB verwaltet das technische Arbeitsprogramm für die Wartung und Weiterentwicklung der CC [CC1, CC2, CC3] und der CEM [CEM] und sorgt für eine einheitliche Anwendung der Kriterien bei den CC-zertifikatserteilenden Nationen. Die Aufgabe des CCMB besteht darin, Anträge auf Aufnahme von Änderungsvorschlägen (CP) auf der Grundlage der nationalen CC- und CEM-Entwicklungsanforderungen unter Berücksichtigung der von der CCDB festgelegten CCRA-Anforderungen zu bearbeiten.

SOG-IS

Auf der europäischen Ebene existiert zusätzlich ein weiteres Anerkennungsabkommen: Das SOG-IS[37] (**S**enior **O**fficials **G**roup - **I**nformation Systems **S**ecurity) Abkommen wurde zwischen 16 EU Mitgliedsstaaten[38] als Antwort auf den Beschluss des EU-Rates vom 31. März 1992 (92/242/EEC) im Bereich der Security von Informationssystemen und der nachfolgenden Empfehlung des Rates vom 7. April (1995/144/EC) zu allgemeinen IT Security Evaluationskriterien beschlossen. Die Mitglieder von SOG-IS erkennen CC–Zertifikate gegenseitig an, konzentrierten sich aber – im Gegensatz zu CCRA – auch auf die Koordinierung der Evaluationstätigkeiten in Bezug auf eine gemeinsame europäische Zertifizierung sowie auf die Koordination gemeinsamer *Protection Profiles* (siehe unten).

Um die Anerkennung im Rahmen des SOG-IS-Abkommens zu erreichen, werden eine Reihe unterstützender Dokumente veröffentlicht, die von verschiedenen Arbeitsgruppen im Rahmen des SOG-IS Abkommens entwickelt wurden. Diese „*Joint Interpretation Library* (JIL)“ umfasst verpflichtende Dokumente, die bei der Bewertung eines Produktes zu beachten sind, sofern es unter einen sogenannten technischen (vertikalen) Bereich fällt, der der SOG-IS Vereinbarung unterliegt. Typische Inhalte dieser JIL-Dokumente sind Leitlinien und Interpretationen, wie eine Bewertung zu erfolgen hat.

Die nationalen Zertifizierungsstellen, die Mitglied im Abkommen sind, stellen sicher, dass alle Prüfstellen diese Kriterien zusätzlich zu den vom CCMD und CCDB veröffentlichten CCRA-Kriterien befolgen. Derzeit wird das SOG-IS Abkommen zu einem offiziellen EU-Zertifizierungsrahmen für Cybersecurity erweitert, um Konformitätsprüfungen bis auf *high-level* für Security-Komponenten abzudecken. Darüber hinaus werden noch weitere Frameworks für Prüfungen auf *substantial-level* wie auch für Cloud-Services definiert.

Marktakzeptanz

In den letzten 20 Jahren wurden mehr als 3000 Evaluationen[39] erfolgreich durchgeführt und offizielle Zertifikate hierzu erteilt. Zu den Produkten gehören z.B.:

- Smartcards
- Bankkarten
    - Pässe und Ausweise (ID-Cards)
    - Pre-paid Tickets
    - Kartenlesegeräte

[37] https://www.sogis.eu/

[38] zurzeit nur noch 15 EU Mitgliedstaaten sowie das Vereinigte Königreich und Norwegen

[39] Eine Liste von ca. 1500 veröffentlichten Zertifikaten, die noch gültig sind, ist hier zu finden: https://www.commoncriteriaportal.org/products/

- Biometrische Authentifizierungsprodukte,
- Embedded Devices
    - Teile von Geldautomaten
    - Gesundheitstelematik
    - Smart Meter
    - Tachographen
- Netzwerkgeräte (Firewalls, VPN's)
- Secure Printer
- Detection Devices (IDS)
- Datenbanken
- Betriebssysteme
- Key Management Systeme

Diese zertifizierten IT Security Produkte werden weltweit und nicht nur in den CCRA- oder SOG-IS-Ländern genutzt. Wer beispielsweise irgendwo auf der Welt

- seine Bankkarte an einem Geldautomaten,
- einen Windows-PC oder ein iPhone,
- seinen Reisepass an einer Grenze,
- oder eine U-Bahn in Asien

benutzt, nutzt ein nach den CC zertifiziertes IT Security Produkt. Darüber werden die Daten jedes Anwenders von Cloud-Diensten, deren Backends mit CC-zertifizierten Datenbanken, Betriebssystemen sowie Netzwerkkomponenten und IDS's aufgebaut werden, durch CC-zertifizierte Komponenten geschützt. Dies betrifft

- jeden Online Banking Account,
- Accounts für die meisten sozialen Netzwerke,
- eShops,
- Streaming-Dienste oder auch
- Appstores.

Wenn man jede genutzte Instanz zu den bisherigen CC-zertifizierten Produkten zählt und aufaddiert – also jede Smart Card (impliziert jeweils mehr als ein CC-Zertifikat, da meist zwei Layer einzeln evaluiert wurden – siehe Kapitel 4.1), jede verkaufte Software-Lizenz, jeden einzelnen Online Account zählt, dann sind deutlich mehr als **200 Milliarden zertifizierter Instanzen** in den letzten 20 Jahren auf dem Markt ausgerollt worden. Die CC werden überall auf der Welt genutzt und „*secure IT product*" steht oftmals für ein „*CC certified product*". Aufgrund der weltweiten Verwendung CC-zertifizierter Produkte und der daraus resultierenden weltweiten Akzeptanz nehmen die CC eine besonders herausragende Position auf dem aktuellen IT-Markt ein. Dabei sind die Kosten einer CC-Evaluation bezogen auf die Instanzen sehr gering, nämlich deutlich geringer als **1 Euro pro verkauftem Produkt** oder Lizenz – sehr oft sogar geringer als 1 Eurocent.

5.2.2 CC Paradigmen

Die Common Criteria bestehen aus insgesamt drei Teilen:

1. **Introduction** and general model [CC1]
2. Security **functional** components [CC2]
3. Security **assurance** components [CC3]

Begleitet werden diese Teile durch das Dokument *Evaluationsmethodologie* (**C**ommon **E**valuation **M**ethodology [CEM]), das Prinzipien und Modelle zur CC-Prüfmethodik beschreibt.

Das Hauptziel einer Evaluierung besteht darin, geeignete und verlässliche Nachweise zu sammeln, um – sowohl für den Entwickler als auch den Benutzer – Vertrauen bzw. Vertrauenswürdigkeit (***Assurance***) in IT Security Maßnahmen zu erlangen, die als **IT Security-Funktionalitäten** in einem Produkt (der sogenannte TOE: **T**arget **o**f **E**valuation) implementiert sind. Zusätzlich können die Evaluationsergebnisse eines Produktes B für ein Produkt A wiederverwendet werden, sofern B im Produkt A integriert ist und dessen IT Security-Funktionalitäten somit von A genutzt werden. Die Möglichkeit einer solchen *Composition* steckt hinter der Idee der Security Layer aus Kapitel 4.1 und wird wie folgt in CC angegangen.

5.2.2.1 Composition

Wenn für ein IT Produkt, das aus Teilen verschiedener Anbieter hergestellt wurde, ein Vertrauenswürdigkeitsnachweis erforderlich ist, ist es unter Umständen nicht möglich, die notwendigen Informationen für eine Evaluation eines höheren Evaluation Assurance Level (EAL – siehe unten) zu erhalten. Dies ist darauf zurückzuführen, dass Kooperationsvereinbarungen in der Regel nicht so weit reichen, dass interne Entwurfsunterlagen als Nachweise für den Entwicklungsprozess vorgelegt werden.

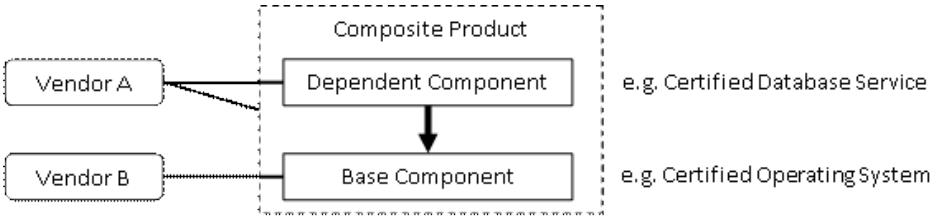


Abbildung 21: Composition

In solch einer Situation kann die Evaluation des "*Composite Products*" entweder

- formal gemäß der "*Composition*"-Klasse der CC oder
- informal neben der reinen CC-Ideologie durchgeführt werden.

Abbildung 21 zeigt die typische Struktur eines Composite-Produktes. Die Evaluation ist auch möglich, wenn ein Produkt aus mehreren Komponenten besteht, oder wenn eine Einteilung in Basiskomponenten und abhängige (*dependent*) Komponenten nicht möglich ist. Nicht nur die Security Layer aus Kapitel 4.1 beruhen auf diesem Ansatz. Vielmehr unterstützt die Möglichkeit der *Composition* auch verschiedene TIER-Level bei Automobilzulieferern (siehe Kap. 4.2.1).

5.2.2.2 Security-Funktionalitäten: ST & PP

Das Herleiten der Security-Funktionalitäten ist bereits in Kapitel 3 beschrieben: Ausgehend von *Assets*, die gegen mögliche Bedrohungen (*Threats*) zu schützen sind, werden Security-Funktionalitäten als geeignete Gegenmaßnahmen definiert. Ein umfassender Satz vordefinierter IT Security-Funktionalitäten wird in [CC2] einschließlich möglicher Abhängigkeiten beschrieben[40]. Diese vordefinierten Security-Funktionalitäten können von einem Hersteller verwendet werden, um die richtigen Security-Anforderungen für sein Sicherheitsprodukt in einem sogenannten **Security Target** (ST) zu spezifizieren: Ein ST beinhaltet die *IT Security Objectives* und Security-Anforderungen für ein **spezifisches IT Security-Produkt**. Dabei definiert das ST sowohl die funktionalen Security-Anforderungen an das Produkt, als auch die Maßnahmen, um Vertrauen in die korrekte und wirksame Implementierung der geforderten Security-Funktionalitäten nachzuweisen. Dabei kann das ST strikte oder nachweisbare Konformität zu einem oder mehreren *Protection Profiles* (PP) fordern und bildet die Grundlage der dann folgenden Evaluation.

Ein solches **Protection Profile** definiert einen implementierungsunabhängigen (herstellerunabhängigen) Satz von Security-Anforderungen und Security Objectives für einen **IT Security-Produkttyp**. Dabei sollte ein solches PP möglichst oft verwendet werden, weshalb in einem PP Anforderungen definiert sind, die zur Erreichung der festgelegten Objectives für diesen Produkttyp nützlich und effektiv sein sollen. Um eine höhere Flexibilität zu erreichen, kann das PP von bestimmten Herstellerprodukten nachweisbare Konformität oder strikte Konformität erfordern. PPs werden speziell für die einheitliche Definition von funktionellen Standards spezifischer IT Security Produkte für ganz bestimmte Anwendungsfälle sowie für die Formulierung von Beschaffungsspezifikationen genutzt.

Eine Vielzahl von PPs ist bereits offiziell zertifiziert[41]. Für den Automobilsektor sind folgende PPs in einigen Ländern gesetzlich vorgeschrieben oder könnten zukünftig relevant werden:

- **Digitaler Tachograph**
  Eine Kombination aus mehreren verschiedenen PP's (*Composition*) bezieht sich auf den Tachographen für LKW's:
  - Vehicle Unit [PP-DT-VU1,2]
  - External GNSS Facility 2017 [PP-DT-EGF]
  - Motion Sensor [PP-DT-MS]
  - Smart Card [PP-DT-TC1,2]
- **On Board Weighing Unit**
  Eine Kombination mehrerer verschiedener PP's (*Composition*) wird zurzeit für „LKW-Wiegeeinheiten" spezifiziert.
- **Taxameter** [PP-Taxi]

[40] Beispiel: *Zugangskontrolle* basiert auf starken *Identitäten* von sogenannten Subjekten die wiederum auf starken *Authentifizierungsmechanismen* basieren,

[41] https://www.commoncriteriaportal.org/pps/

- **V2X / C-ITS**
  Mehrere Schutzprofile wurden bereits oder werden aktuell für das Thema C-ITS spezifiziert (*Composition*):
  - V2X Gateway – Draft [PP-C2C-TX]
  - V2X Hardware Security Module [PP-C2C-HSM]
  - Road Warning Unit [PP-RWU]
  - Cryptographic Service Provider [PP-CSP]
- **Safertec Research Project** [PP-Safertec1,2,3]
  Drei verschiedene PP wurden für typische Anwendungsfälle im Auto spezifiziert:
  - V-ITS-S Base Protection Profile
  - Protocol Control / Communication Unit
  - Sensor Monitor
- **Alcohol Interlock** [PP-Alc]
  Die Alkohol-Wegfahrsperre stellt sicher, dass ein alkoholisierter Fahrer das Fahrzeug nicht nutzen kann.
- **Electric Vehicles** [PP-SMGW, -SE]
  Eine Kombination aus verschiedenen PPs (*Composition*) wird für Smart Metering Lösungen spezifiziert. Zukünftige Versionen dieser Schutzprofile werden das Thema eMobility und Ladestationen beinhalten.
- **FIA AGW** – Draft [PP-Alc]
  Ein Entwurf für ein A-GW PP als Ergebnis dieses Reports.

5.2.2.3 Assurance und EAL

Wie in Teil 3 der Common Criteria [CC3] genauer beschrieben wird die IT Security bzw. das Vertrauen in die Security eines IT-Produktes durch aktive Untersuchungen eines Evaluators erreicht. Dies beinhaltet die Anwendung verschiedener Techniken, wie z.B.:

- Analyse und Kontrolle von **Prozessen** und ob diese angewendet werden[42]
- Analyse ob die verschiedenen **Designdokumente** des IT Security-Produktes die Anforderungen erfüllen
- Analyse der **Handbücher**
- Analyse der funktionalen **Tests** der Hersteller und deren Ergebnisse
- **Unabhängiges** funktionales **Testen** und **Penetrationstests** durch den Evaluator
- **Schwachstellenanalyse**

In der Philosophie der CC wird postuliert, dass man mit steigendem Prüfaufwand (*Evaluation Effort*) mehr Vertrauenswürdigkeit (Assurance) für das IT Security-Produkt bekommt. Dieser ansteigende Prüfaufwand wird erreicht durch:

- **Umfang (*Scope*)**: Je mehr Bestandteile eines IT Produktes in die Evaluation einbezogen werden, desto höher der Aufwand
- **Tiefe (*Depth*)**: Je mehr Design- und Implementierungsdetails offengelegt werden, desto höher der Aufwand

[42] Die Analyse von Prozessen ist auch Gegenstand von [ISO 21434], die anderen Punkte aber nicht.

- **Striktheit (*Rigour*)**: Je mehr Struktur und formale Beschreibungen, desto höher der Aufwand

Die in [CC3] vorgenommene formale Strukturierung von

- ***Assurance Classes***,
- welche aufgeteilt sind in ***Assurance Families***,
- mit tieferem und strikterem formalen Anspruch in **Assurance Components**

spezifiziert präzise die Anforderungen an die 7 unterschiedlichen Vertrauenswürdigkeitsstufen (**E**valuation **A**ssurance **L**evels). Je höher diese EAL-Zahl ist, desto höher ist der Aufwand für die Evaluation (siehe Abbildung 22). Die einzelnen *Assurance Classes* sind:

- **ASE** (**A**ssurance Class **S**ecurity Target **E**valuation):
  Das Security Target (siehe Kapitel 5.2.2.2)
- **ALC** (**A**ssurance Class **L**ife-**C**ycle Support):
  IT Security bei den Lebenszyklusprozessen für das IT Security-Produkt[43] wie IT Security in der Entwicklung, beim Konfigurationsmanagement, bei den Auslieferungsprozessen und dem Fehlerhandling
- **ADV (A**ssurance Class **D**e**v**elopment):
  Entwicklungsunterlagen zur Darlegung des IT Security-Produktdesigns.
- **AGD** (**A**ssurance Class **G**uidance **D**ocuments):
  Benutzerhandbücher und Installationsanweisungen.
- **ATE** (**A**ssurance Class **Te**sts)_
  IT Security Tests, die durch den Hersteller und vom Evaluator durchgeführt werden.
- **AVA** (**A**ssurance Class **V**ulnerability **A**ssessment):
  Zusätzliche Analyse bzgl. dem Level an Widerstandsfähigkeit (*Robustness*) gegen potentielle Angriffe.

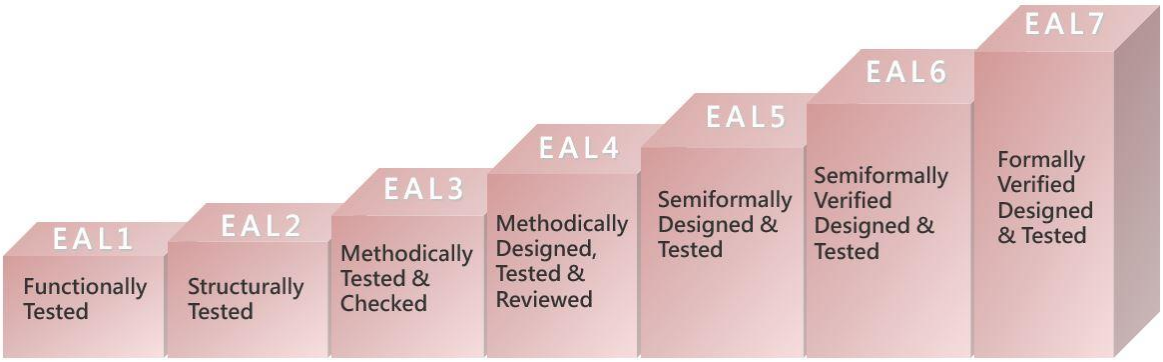


Abbildung 22: Evaluation Assurance Levels (EALs)

Wie bereits beschrieben, sind die *Assurance Classes* in verschiedene *Assurance Families* unterteilt und dahinter verbergen sich die *Assurance Components*, die durch eine angehängte Nummer (hinter der Abkürzung der *Assurance Family*) voneinander unterschieden werden. Die Beschreibungstiefe der vorzulegenden Herstellerdokumente wird mit dieser Nummer der zugehörigen Assurance Component ausgedrückt: Je höher die Nummer, desto mehr Details

[43] Für die Automobilindustrie sind diese in [ISO 21434] beschrieben.

müssen in einer formalen Art und Weise durch den Hersteller beschrieben und durch den Evaluator überprüft werden. Ein definierter Satz an Assurance Components ergibt den Evaluation Assurance Level gemäß Tabelle 2 (alphabetisch aufgelistet). Leere Felder in einer Spalte eines gegebenen EAL sind nicht verpflichtend. Es besteht aber die Möglichkeit, zusätzliche Assurance Components (z.B. aus einem höheren EAL) hinzuzunehmen, was bei der Angabe des EAL mit einem „+" dargestellt ist und als „*Augmentation*" bezeichnet wird, wie z.B. `EAL2+AVA_VAN.3` (gelb in Tabelle 2): Dies wären alle gelisteten Assurance Components in der Spalte zu EAL2 und zusätzlich die Assurance Component `AVA_VAN.3`.

Assurance Class	Assurance Family	Assurance Components						
		EAL						
		1	2	3	4	5	6	7
ADV Development	**ARC** - Security **Arc**hitecture		1	1	1	1	1	1
	FSP - **F**unctional **Sp**ecification	1	2	3	4	5	5	6
	IMP - **Imp**lementation (Source Code)				1	1	2	2
	INT - TSF[44] **Int**ernals					2	3	3
	SPM - **S**ecurity **P**olicy **M**odelling						1	1
	TDS - **T**OE[45] **Des**ign		1	2	3	4	5	6
AGD Guidance Documents	**OPE** - **Ope**rational User Guidance	1	1	1	1	1	1	1
	PRE - **Pre**parative Procedures	1	1	1	1	1	1	1
ALC Life-Cycle Support	**CMC** - **CM**[46] **C**apabilities	1	2	3	4	4	5	5
	CMS - **CM**[46] **S**cope	1	2	3	4	5	5	5
	DEL - **Del**ivery		1	1	1	1	1	1
	DVS - **D**evelopment **S**ecurity (Site Visits)			1	1	1	2	2
	FLR - **Fl**aw **R**emediation							
	LCD - **L**ife-**C**ycle **D**efinition			1	1	1	1	2
	TAT - **T**ools **a**nd **T**echniques				1	2	3	3
ASE Security Target	**CCL** - **C**onformance **Cl**aims ST	1	1	1	1	1	1	1
	ECD - **E**xtended **C**omponents **D**efinition	1	1	1	1	1	1	1
	INT - **Int**roduction	1	1	1	1	1	1	1
	OBJ - Security **Obj**ectives	1	2	2	2	2	2	2
	REQ - Security **Req**uirements	1	2	2	2	2	2	2
	SPD - **S**ecurity **P**roblem **D**efinition		1	1	1	1	1	1
	TSS - **T**OE[45] **S**ummary **S**pecification	1	1	1	1	1	1	1
ATE Tests	**COV** - **Cov**erage of Testing		1	2	2	2	3	3
	DPT - **Dep**th of **T**esting			1	1	3	3	4
	FUN - **Fun**ctional Tests		1	1	1	1	2	2
	IND - **Ind**ependent Testing	1	2	2	2	2	2	3
AVA Vulnerability Assessment	**VAN** - **V**ulnerability **An**alysis	1	2	2	3	4	5	5

Tabelle 2: EAL – Überblick

[44] TOE (Target of Evaluation) Security Functionalities

[45] Target of Evaluation

[46] Configuration Management

Da CC-Evaluationen möglichst entwicklungsbegleitend durchgeführt werden sollten (*concurrent evaluation*), sollte der Evaluations- und Zertifizierungsprozess nicht mehr Zeit als die eigentliche Entwicklungszeit ohne eine Evaluation in Anspruch nehmen (*Time-to-Market*). Hierbei muss deutlich betont werden, dass nie ein komplettes System und alle darin befindlichen Komponenten konform zur CC sein müssen. Bezogen auf die Automobilindustrie kann ein gesamtes Fahrzeug nie Gegenstand einer CC-Evaluation sein. Jedoch sollten die kritischen IT Security Komponenten Teil der CC Evaluation sein – möglicherweise im Rahmen einer *Composition* gemäß der Security Layer aus Kapitel 4.1. In diesem Fall könnte der Aufwand (und die Kosten) zur Entwicklung und Evaluation derartiger IT-Security Komponenten über den Verkauf zahlreicher Instanzen und somit als Massenprodukt auf ein vernünftiges Maß nivelliert werden.

5.3 Empfehlungen

Es steht außer Frage, dass **jede Organisation**, die IT Services anbietet oder IT Security-Komponenten für den Automobilsektor liefert, ein ISMS aufbauen muss, das gemäß **ISO27001** [ISO27001] oder alternativ **TISAX** [TISAX] zu prüfen ist.

Jeder IT-Security Dienstleister, der in der Lifetime-Phase " **Operation**" seine Services zur Verfügung stellt, muss ein hohes Niveau an IT Security (PKI, A-GWA, …) erfüllen und nach den zukünftigen Anforderungen für **Cloud Service Provider** der ENISA geprüft werden. Dies ist im Zuge von End-to-End-Security (durch Verschlüsselung oder Verwendung von Signaturen) und somit für jeden ISP bei der Durchführung von remote Diagnosen von entscheidender Bedeutung.

Während der Lifetime-Phase „**Development**" und „**Production**" von IT Security-Komponenten muss zusätzlich die **ISO/SAE 21434** [ISO21434] erfüllt sein.

- Da die Audit Schemata der ISO/SAE 21434 zukünftig ausschließlich die Prozesse betrachten werden, das technische Testen bzw. die tiefergehende Evaluation des IT-Security-Produktes bei ISO/SAE 21434 somit nicht vorgesehen sind und
- da SOG-IS (und damit die Common Criteria) zunehmend an Bedeutung für die Prüfung von „*high-level*" IT-Security-Produkten gewinnt,

sollten alle IT Security-Produkte der Automobilbranche während der Lifetime-Phase „**Development**" gemäß den Common Criteria evaluiert und zertifiziert werden.

Zusätzlich zu diesem Dokument ist ein Beispielentwurf eines Protection Profiles für ein Automotive Gateway [PP-AGW] erstellt worden. Dieses Protection Profile beschreibt die oben erläuterten IT Security-Aspekte (Assets, Threats, Countermeasures, Security Objectives) für diese wichtige Komponente einer OTP. Zusätzlich zeigt es, wie die Security-Funktionalitäten im Sinne der Common Criteria modelliert werden können.

6 Roadmap

Soll ein System wie die in diesem Dokument vorgeschlagene On-Board Telematik Plattform (OTP) zur Realisierung des „Separation-of-Duties“ Prinzips aufgebaut werden, so müssten vorab viele Parteien und Entscheider überzeugt werden, dass dieser Ansatz die IT Security wie auch die Datenschutzanforderungen gemäß [EDPB1-3] für den zukünftigen vernetzten Verkehr in Europa erfüllen wird. Möglicherweise werden andere Technologien alternativ vorgeschlagen, ggf. belegt durch Buzzwörter wie „Blockchain“ und „KI“, um Aufmerksamkeit zu errege. Vielleicht wird auch argumentiert, dass 5G-Technologien die IT Security Anforderungen von OTP automatisch abdecken würden. Eventuell gibt es auch Meinungen, dass derartig komplexe Security-Architekturen gar nicht notwendig wären für den zukünftig vernetzten Straßenverkehr. In diesem Fall würde es wahrscheinlich umfangreiche Awareness-Kampagnen unter der Kontrolle von Cyberkriminellen geben. Es ist somit wichtig, sich in einem ersten Schritt mit relevanten Parteien, die in der Lage wären, ein solches OTP oder vergleichbare Architekturen[47] zu implementieren, auszutauschen. Falls jemand entscheidet, ein A-GW basierend auf [PP-AGW] und vorliegenden Spezifikationen von Car2Car und C-ITS zu entwickeln, sollte das zugehörige System zum A-GWA im Detail spezifiziert und aufgebaut werden.

Die folgenden Schritte werden als “Roadmap” vorgeschlagen – viele der Aktivitäten können parallel zueinander stattfinden:

1. **Awareness**
    a. Staat (EU): Information auf EU-level an die zuständigen Direktorate
    b. EU-Länder
    c. Standardisierungsgruppen
    d. Automobil- und IKT-Verbände
    e. Aktivitäten bei Automotive Security Veranstaltungen
2. **V2X / C-ITS**
    a. Transceiver Modul im Fahrzeug: Implementierung mindestens einer Lösung gemäß der Definition von C2C-CC (oder alternativ 5GAA)
    b. Transceiver Modul in der Straßeninfrastruktur: Entwicklung mindestens einer Lösung gemäß der Definition von C-ITS [PP-RWU]
    c. C2C-PKI: Betrieb eines Car2Car Pilotprojektes basierend auf einer PKI
3. **OTP**
    a. A-GW-PP: Evaluation und Zertifizierung von [A-GW]
    b. A-GW: Entwicklung mindestens einer Lösung eines A-GW gemäß der Definition von [PP-AGW]
    c. Policies: Spezifikation detaillierter User- und Usage-Profile
    d. Prozesse: Spezifikation aller organisatorischen Prozesse
    e. A-GWA: Installation eines A-GWA basierend auf der C2C-PKI
    f. Roll-Out von A-GW’s
    g. Betrieb eines OTP-basierenden vernetzten Verkehrssystems

[47] wie OBAP in [TRL] oder ein Derivat eines V2X Transceivers aus C2C-CC

4. **3rd Party**
    a. Installation von OTP-konformen ISP's
    b. OBM: Spezifikation und Installation eines OTP-konformen PAI
    c. Diagnose: Entwicklung von OTP-konformen Diagnose-Tools
    d. Installation und Betrieb von OTP-konformen OBM für weitere Dienstanbieter

6.1 Regulierung

Es wäre hilfreich, wenn – nachdem Schritt 1 obiger Liste erfolgt ist – die folgenden 3 Aspekte gesetzlich geregelt würden:

1. **ITS Komponenten** (z.B. A-GW): Für **jede** zukünftige V2X-Kommunikation (Fahrzeug-zu-Fahrzeug, Fahrzeug-zu-Infrastruktur und Fahrzeug zu einem beliebigen Automotive Service im Internet) muss **ein hochsicheres Kommunikationsinterface,** wie das vorgeschlagene A-GW, gemäß der formalen Beschreibung in [PP-AGW] genutzt werden. Dieses Kommunikationsinterface darf nicht umgangen werden, weder durch eine Komponente im Fahrzeug (ECU's, HMI, Docker, eCall,…) noch bei einem anderen externen Interface des Fahrzeugs (wie OBD). Derartige hochsichere Kommunikationsinterfaces müssen Bestandteil der Typgenehmigung gemäß europäischer Cybersecurity Standards wie SOG-IS sein.
2. **ITS Administration**: Das Management und die Administration eines sicheren ITS und seiner Kommunikationsinterfaces wie dem A-GW, aber ebenso hochsichere ITS Komponenten in der Verkehrsinfrastruktur, müssen durch hochsichere **IT Security Systeme** wie das beschriebene A-GWA basierend auf einer PKI umgesetzt werden. Hierzu sollten staatliche Einrichtungen mit der Betreuung des Betriebs dieser ITS Administrationssysteme beauftragt werden.
3. **ITS Zugriffs-Policies**: Zugriffs-Policies (*wer* darf auf *welche* Art auf *was* für Automotive-Daten zugreifen?) müssen definiert und regelmäßig vom Gesetzgeber angepasst werden (ausgehend von den in Kapitel 4.2.2 vorgeschlagenen Gruppen) als regulative Basis für alle User- und Usage-Profile, die in der ITS Administration durch das A-GWA abgebildet werden.

Vereinfacht gesagt muss es regulative Entscheidungen geben zu

1. den eingesetzten **IT Security Produkten**,
2. zu den diese Komponenten verwaltenden **IT Security Systemen** und den zugehörigen
3. **IT Security Prozessen**.

Der Vorschlag zu den Spiegelpunkten 1 und 2 findet sich in diesem Bericht. Die relevanten Entscheidungen (ITS-Zugriffs-Policies) für User- und Usage-Profile und alle zugehörigen Basisprozesse müssen noch definiert werden.

A Anhang

A.1 Abkürzungen

Acronym	Definition
5GAA	5G Automobile Association
A-GW	Automotive Gateway
A-GWA	Automotive Gateway Administrator
ACEA	European Automobile Manufacturers' Association
AA	Authorization Authority
ADV	Assurance Class Development
AFCAR	Alliance for the Freedom of Car Repair in Europe
AGD	Assurance Class Guidance Documents
ALC	Assurance Class Life-Cycle Support
ASE	Assurance Class Security Target Evaluation
AT	Authorization Ticket
ATE	Assurance Class Tests
ATM	Automated Teller Machine
AVA	Assurance Class Vulnerability Assessment
BASt	Bundesamt für Straßenwesen
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2C	Car2Car
C2C-CC	Car2Car Communication Consortium
C-ITS	Kooperative intelligente Verkehrssysteme
CA	Certificate Authority (als Teil einer PKI)
Car2X	Car-to-Everything
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Agreement
CITA	International Motor Vehicle Inspection Committee
CLEPA	European Association of Automotive Suppliers
CM	Configuration Management
DB	Database
DPIA	Data Protection Impact Assessments
DSGVO	Datenschutzgrundverordnung (englisch: GDPR)
EA	Enrolment Authority
EAL	Evaluation Assurance Level
eCall	Emergency Call
ECU	Electronic Control Unit
EiP	Everything is Possible
eMBB	enhanced Mobile Broadband (5G)
ENISA	European Network and Information Security Agency
ExVe	Extended Vehicle
FIA	International Automobile Federation
FIGIEFA	International Federation of Automotive Aftermarket Importers and Wholesalers
GDPR	General Data Protection Regulation (deutsch: DSGVO)
HSM	Hardware Security Module, equivalent to SE
HMI	Human Machine Interface

Acronym	Definition
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet-of-Things
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Independent Service Provider
IT	Information Technology
ITS	Intelligentes Transport System
ITS-S	Intelligent Transport System Station
ITSEF	IT Security Evaluation Facility
IVS	Intelligent Vehicle System
JIL	Joint Interpretation Library
KBA	Kraftfahrtbundesamt
mMTC	massive Machine Type Communications (5G)
NCAP	(European) New Car Assessment Program
NEVADA	Neutral Extended Vehicle for Advanced Data Access
OBAP	On-Board Application Platform
OBD	On-Board Diagnostics
OBM	On-Board Monitoring
OEM	Original Equipment Manufacturer
OBFCM	On-Board Fuel Consumption Monitoring
OTP	On-Board Telematics Platform
OS	Operating System
PAI	Permanent Automated Inspection
PKI	Public Key Infrastructure
PTI	Periodical Technical Inspection
PP	Protection Profile
RNG	Random Number Generator
R&M	Repair & Maintenance
RMI	Repair and Maintenance Information
Safertec	Security Assurance Framework for Networked Vehicular Technology
SE	Secure Element, equivalent to HSM
SFR	Security Functional Requirements
ST	Security Target
SOG-IS	Senior Officials Group Information System Security
TCU	Telematics Control Unit
TOE	Target of Evaluation
TSF	TOE Security Functionalities
UNECE	United Nations Economic Commission for Europe
uRLLC	ultra Reliable and Low Latency Communications (5G)
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCS	Vehicle C-ITS Station
VDA	Verband der Automobilindustrie
VDTÜV	Verband der TÜVs
VIN	Vehicle Identification Number
VPN	Virtual Private Network

A.2 Literatur

[ANA] *Analogue Network Security*
W. Schwartau, 2018
ISBN 978-0-9964019-0-6

[CCRA] *Common Criteria Recognition Arrangement in the field of Information Technology Security*
CCRA-Members[48], July, 2014
https://www.commoncriteriaportal.org/ccra/

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Common Criteria Management Board, Version 3.1, Revision 5, April 2017

[CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Functional security components*
Version 3.1, Revision 5, April 2017

[CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Assurance security components*
Version 3.1, Revision 5, April 2017

[CEM] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*
Version 3.1, Revision 5, April 2017

[CSA] *Cybersecurity Act*
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
http://data.europa.eu/eli/reg/2019/881/oj

[C-ITS-Korridor] *Cooperative ITS Corridor*
Joint deployment of Ministry of Infrastructure and the Environment of the Netherlands, Federal Ministry of Transport and Digital Infrastructure, and Austrian Ministry for Transport, Innovation and Technology
https://c-its-korridor.de

[eCall] Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585

[EDPB1] *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*
European Data Protection Board, V 1.0, January 2020
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[EDPB2] *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*
European Data Protection Board, V 2.0, October 2019
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[48] https://www.commoncriteriaportal.org/ccra/members/

[EDPB3] *Resolution on Data Protection in Automated and Connected Vehicles*
39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, 25-29 September 2017
https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

[ENISA1] *Cyber Security and Resilience of smart cars – Good practices and recommendations*
ENISA, December 2016, ISBN 978-92-9204-184-7

[ENISA2] *ENISA good practices for Security of Smart Cars*
ENISA, November 2019, ISBN 978-92-9204-317-9

[ENISA3] *Overview of ICT Certification Laboratories*
ENISA, V1.1, January 2018, ISBN 978-92-9204-248-6

[FIA] *On-Board Telematics Platform Security*
FIA / TÜViT, June 2020

[FIPS140-3] *FIPS 140-3 Security Requirements for Cryptographic Modules*
National Institute for Standards and Technology, March 2019

[ISO21434] *ISO/SAE DIS 21434 – Road vehicles – Cybersecurity engineering*
International Standardisation Organisation, Committee Draft

[ISO27001] *ISO/IEC 27001 – Information security management systems – Requirements*
International Standardisation Organisation, 2013

[Jeep] *Hackers Remotely Kill a Jeep on the Highway—With Me in It*
Wired, July, 2015
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[JRC] *Access to digital car data and competition in aftersales services*
B. Martens, F. Müller-Lang
European Commission, DG JRC, September 2018
https://ec.europa.eu/jrc/sites/jrcsh/files/jrc112634.pdf

[NEVADA] *Access to the vehicle and vehicle generated data - "NEVADA Share and Secure Concept"*
Graham Smethurst, VDA, 24.10.2017
https://www.vda.de/en/topics/innovation-and-technology/data-security/what-is.html

[NIS] *NIS Directive*
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
http://data.europa.eu/eli/dir/2016/1148/oj

[Oversee] Open Vehicular Secure Platform, OVERSEE Final Report, V 1.0
OVERSEE Concortium, 04.11.2013

[PKI] *Understanding PKI: concepts, standards, and deployment considerations*
Carlisle Adams, Steve Lloyd, Addison-Wesley Professional. 2003, ISBN 978-0-672-32391-1

[PP-Alc] *Alcohol Interlock Protection Profile*
Ministry of Transport, Public Works and Water Management of the Netherlands, V1.0, August 2010
https://www.commoncriteriaportal.org/files/ppfiles/Alcohol%20Interlock%20Protection%20Profile%20v1.00.pdf

[PP-AGW] *FIA Protection Profile - Draft*
A. Bobel, B. Niehöfer, M. Wagner, M. Wahner
TÜViT, May 2020

[PP-C2C-HSM] *Protection Profile V2X Hardware Security Module*
Car2Car Communication Consortium, April 2020

[PP-C2C-TX] *Protection Profile V2X Gateway - Draft*
Car2Car Communication Consortium (in specification)

[PP-CSP] *Common Criteria PP, Cryptographic Service Provider*
BSI, BSI-CC-PP-0104, V.9.8, February 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0104.html

[PP-DT-EGF] *Common Criteria PP, Digital Tachograph – External GNSS Facility (EGF PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0092b_pdf.pdf

[PP-DT-MS] *Common Criteria PP, Digital Tachograph – Motion Sensor (MS PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0093b_pdf.pdf

[PP-DT-TC1] *Common Criteria PP, Digital Tachograph – Smart Card (Tachograph Card)*
BSI, BSI-CC-PP-0070, V1.02, November 2011
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0070.html

[PP-DT-TC2] *Common Criteria PP, Digital Tachograph – Tachograph Card*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0091b_pdf.pdf

[PP-DT-VU1] *Common Criteria PP, Digital Tachograph – Vehicle Unit*
BSI, BSI-CC-PP-0057, V1.0, July 2010
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0057.html

[PP-DT-VU2] *Common Criteria PP, Digital Tachograph – Vehicle Unit (VU PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0094b_pdf.pdf

[PP-RWU] *Protection Profile for a Road Warning Unit*
BASt, BSI-CC-PP-0104, V1.1, July 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html

[PP-Safertec1] *The Protocol Control / Communication Unit Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec2] *Sensor Monitor Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec3] *The V-ITS-S Base Protection Profile*
K. Maliatsos, Safertec, July 2019

[PP-SMGW] *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*
BSI, BSI-CC-PP-0073, V1.3, March 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html

[PP-SMGW-SE] *Protection Profile for a Security Module for Smart Metering Systems (Security Module PP)*
BSI, BSI-CC-PP-0077-V2, V1.03, December 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0077+V2.html

[PP-Taxi] *Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)*
Ministerie van Infrastructuur en Milieu – Netherlands
V1.8, February 2015
https://www.commoncriteriaportal.org/files/ppfiles/[BCT%20PP]%20BeveiligingsprofielBCTV1.8.pdf

[SAEJ3016] *SAE International: Surface Vehicle recommended practice J3016*
2014-01, Revised 2018-06

[SERMI] *Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI)*
SERMI Operations Group, May 2016
https://www.vehiclesermi.eu/

[SOG-IS] *Senior Officials Group Information Systems Security*
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, V 3.0, January 2010
https://www.sogis.eu/

[TISAX] *TISAX (Trusted Information Security Assessment Exchange): Questionnaire for checking Information Security Assessment and Information Security Management*
VDA, Vers. 4.1.1
https://www.vda.de/en/services/Publications/information-security-assessment.html

[TRL] *TRL: Access to In-vehicle Data and Resources, Final report*
M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, F. Ognissanto
European Commission, DG MOVE, 18.05.2017

[VDTÜV1] *Requirements for the telematics interface in vehicles*
R. Goebelt, VDTÜV, January 2017

[VDTÜV2] *Data Protection, IT Security & Compliance as a Basis for New Business Models in Digital Connected Mobility*
R. Goebelt, VDTÜV, January 2018
https://www.vdtuev.de/en/news_policy_statements/position-data-protection-it-security-compliance-for-new-business-models-in-digitally-connected-mobility

[VDTÜV3] *Remote Access to Vehicle Data for ensuring Road Safety and Environmental Protection*
R. Goebelt, VDTÜV, 2020
https://www.vdtuev.de/en/dok_view?oid=779801

[Waidner] *Development of secure Software with Security by Design: Trends and Strategy Report*, M. Waidner, M.Backes, J. Müller-Quade,
Fraunhofer-Institut for Secure Information Technology, 2014

[WHICH] *We hacked a Ford Focus and a Volkswagen Polo*
Which?, 09.04.2020
https://www.which.co.uk/news/2020/04/we-hacked-a-ford-focus-and-a-volkswagen-polo/