Selbstdatenschutz im vernetzten Fahrzeug

Architekturkonzept für Selbstdatenschutz im vernetzten Fahrzeug

Veröffentlichung Nummer: D2

Version 1.0

GEFÖRDERT VOM

Projekt Akronym: SeDaFa
Vollständiger Projekttitel: Selbstdatenschutz im vernetzten Fahrzeug
Projektwebseite: `http://www.sedafa-projekt.de/`

Veröffentlichungsdatum	08.08.2017
Seitenanzahl:	45
Schlagwörter:	Vernetztes Fahrzeug, Privatsphäre, Datenschutz, Selbstdatenschutz, Architektur, Datenschutzmaßnahmen
Autoren:	Matthias Enzmann Fraunhofer SIT Benjamin Lange Fraunhofer SIT Sebastian Mauthofer Fraunhofer SIT Christian Plappert Fraunhofer SIT Daniel Zelle Fraunhofer SIT

Inhaltsverzeichnis

1 Inhalte des APs **5**

2 SeDaFa Architektur **6**
2.1 Abstrakte logische Architektur . . . 6
2.2 Abstrakte technische Architektur . . . 10
2.2.1 Generelle Beschreibung . . . 11
2.2.2 Detailbeschreibung ausgewählter Module . . . 12
2.3 Abbildung auf Fahrzeugarchitektur . . . 14

3 Schutzziele **16**

4 Schutzmaßnahmen **17**
4.1 Benachrichtigung . . . 17
4.2 Verfügbarkeit . . . 18
4.3 Authentifizierung . . . 18
4.4 Autorisierung / Zugriffskontrolle . . . 19
4.5 Verschlüsselung . . . 21
4.6 Lokale Verarbeitung . . . 22
4.7 Anonymität / Pseudonyme . . . 22
4.8 Datenanonymisierung . . . 23
4.9 Bezug zu Anwendungsfällen . . . 24

5 Anwendungsfälle **26**
5.1 Mehrfache Fahrzeugnutzung . . . 26
5.1.1 Car-Sharing . . . 26
5.1.2 Werkstatt . . . 29
5.2 Location-based Services . . . 30
5.3 Smartphone Integration/Drittanbieter-Erweiterungen . . . 32
5.3.1 Android Auto . . . 32
5.3.2 Paket-Auto . . . 33
5.4 Statistische Analysen . . . 35
5.4.1 Umgebung . . . 35
5.4.2 Verschleißanalyse . . . 37
5.5 Elektromobilität . . . 38
5.6 Fahrerverhalten . . . 41
5.6.1 Fahrerüberwachung . . . 42

Literaturverzeichnis **44**

1 Inhalte des APs

In diesem Arbeitspaket (AP) wird anhand der identifizierten Anforderungen eine abstrakte Datenschutzarchitektur entwickelt, die das Ziel hat, die Aspekte *Risikobewertung*, *Transparenz* für den Nutzer und *selbstbestimmte Kontrolle* im Fahrzeugkontext umzusetzen.

Dazu sollen im Hinblick auf die in AP1[1] aufgestellten Anforderungen zunächst Hauptkomponenten und Schnittstellen der SeDaFa Architektur definiert werden. Weiterhin soll für die definierten Anwendungsfälle aus AP1 ein Datenschutz-Maßnahmenkatalog abgeleitet werden, der Methodiken und Techniken enthält, um z. B. Funktionen wie Anonymisierung, Verschlüsselung oder Aggregation unter Berücksichtigung der im Fahrzeug verbauten Hardware umzusetzen, ohne dabei die Realisierung von Mehrwertdiensten zu untergraben. Für die Umsetzung der Maßnahmen werden die notwendigen Architekturkomponenten und Prozesse identifiziert. Die notwendigen Architekturkomponenten und Prozesse werden dann in abstrakte Module zusammengefasst, die die oben genannten Ziele *Risikobewertung*, *Transparenz* und *selbstbestimmte Kontrolle* umsetzen. Ein zentraler Ansatz bei der Umsetzung soll es sein, anfallende Daten wenn möglich auf dem Fahrzeug zu halten und notwendige Übertragungen von Datensätzen nur anonymisiert (z. B. über Aggregation) oder, wenn nicht anders möglich, zumindest verschlüsselt zuzulassen.

Das Dokument gliedert sich wie folgt: In Kapitel 2 wird die sukzessive Entwicklung der SeDaFa-Architektur unter Berücksichtigung der sowohl in AP1 erarbeiteten Ergebnisse als auch den sich aus dem Fahrzeugkontext ergebenden Anforderungen vorgestellt. Anschließend werden in Kapitel 3 Schutzziele definiert, die über die in Kapitel 4 beschriebenen generellen Maßnahmen erreicht werden können, um die technischen Anforderungen aus AP1 zu erfüllen. Diese werden abschließend in Kapitel 5 in die in AP1 definierten Anwendungsfälle integriert.

2 SeDaFa Architektur

Das Ziel dieses APs ist es, eine möglichst allgemein gültige Architektur für den Selbstdatenschutz im vernetzten Fahrzeug zu entwickeln, die herstellerunabhängig auf eine Vielzahl von Fahrzeugen anwendbar ist und auch bereits auf absehbare Entwicklungen im Automobilmarkt eingeht. Um dies zu erreichen, werden die Komponenten der Architektur sukzessiv aus den bisherigen Ergebnissen von AP1 abgeleitet. Dabei werden die resultierenden Zwischenarchitekturen schrittweise in die allgemein technische Domäne überführt und letztlich auf die abstrakte Fahrzeugarchitektur abgebildet.

Wie in Abbildung 2.1 zu sehen, werden dafür in einem ersten Schritt aus den Anforderungen logische Basis-Module wie etwa Transparenz-, Steuerungs- oder Sicherheitsmodule abgeleitet. Durch Strukturierung dieser einzelnen Module wird eine abstrakte logische Architektur abgeleitet, die bereits die sich aus den Anforderungen ergebenden Funktionen enthält, ohne dabei die technische oder die fahrzeugspezifische Domäne zu berücksichtigen.

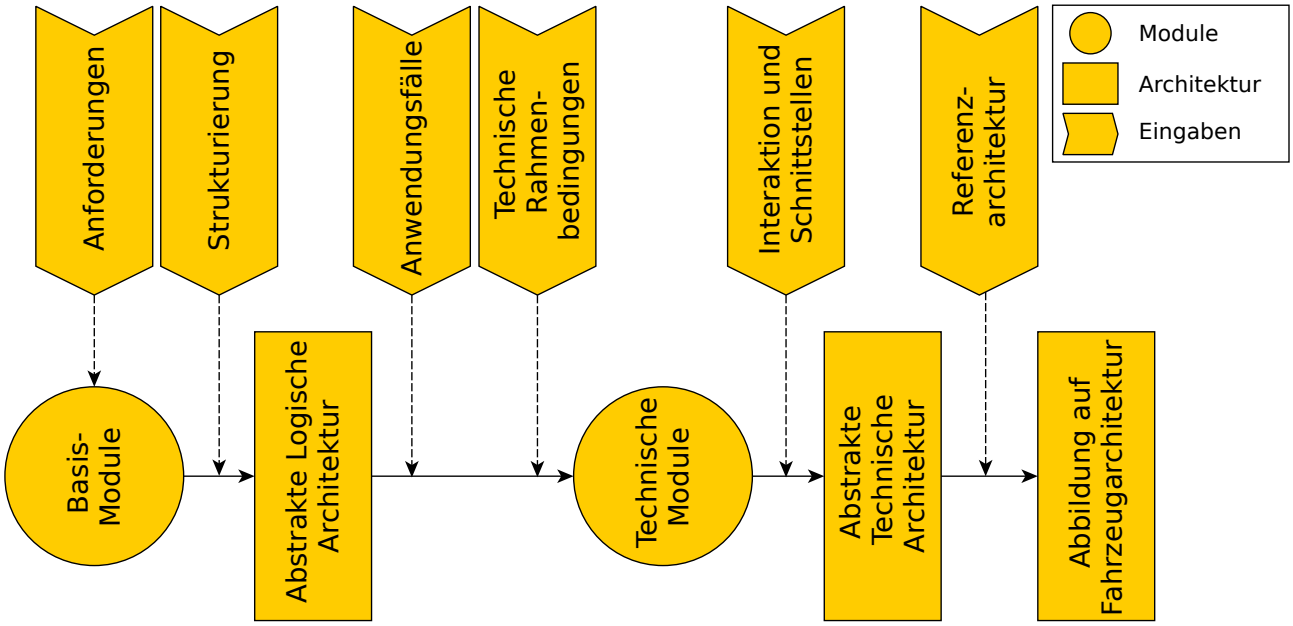

Abbildung 2.1: Vorgehen

Anschließend werden die Basis-Module der logischen Architektur um technische Module ergänzt, die sich aus den konkreten Anwendungsfall-Szenarien und Rahmenbedingungen aus der technischen Domäne ergeben. Unter Berücksichtigung der für die Funktionalität der Anforderungen notwendigen Interaktionen und Schnittstellen zwischen den Modulen wird aus den technischen und Basis-Modulen eine abstrakte technische Architektur erstellt.

Im letzten Schritt wird die technische Architektur dann auf die in AP1 entwickelte Referenzarchitektur abgebildet.

In den folgenden Kapiteln werden die Module der einzelnen erstellten Architekturen detailliert erläutert.

2.1 Abstrakte logische Architektur

Wie bereits im vorigen Kapitel erläutert, leiten sich aus den in AP1 beschriebenen Anforderungen zunächst logische Komponenten ab, die dann zu einzelnen Basis-Modulen zusammengefasst werden und somit die abstrakte logische Architektur bilden.

Die Architektur besteht aus 7 Modulen, die entsprechend der im Fahrzeug üblichen Gliederung in Domänen der Domäne *Selbstdatenschutz* zugeordnet sind (siehe Abbildung 2.2). Die Domäne Selbstdatenschutz umfasst dabei die Module *Sichere Kommunikation*, *Transparenz & Kontrolle*, *Daten(-fluss) Analyse*, *Datenschutz-Policy*, *Sicherheitsmanagement*, *Sichere Informationsverarbeitung*, sowie *Kryptografische Operationen*. Diese sollen nun im Weiteren auch im Hinblick auf ihren Bezug zu der jeweiligen Anforderung beschrieben werden.

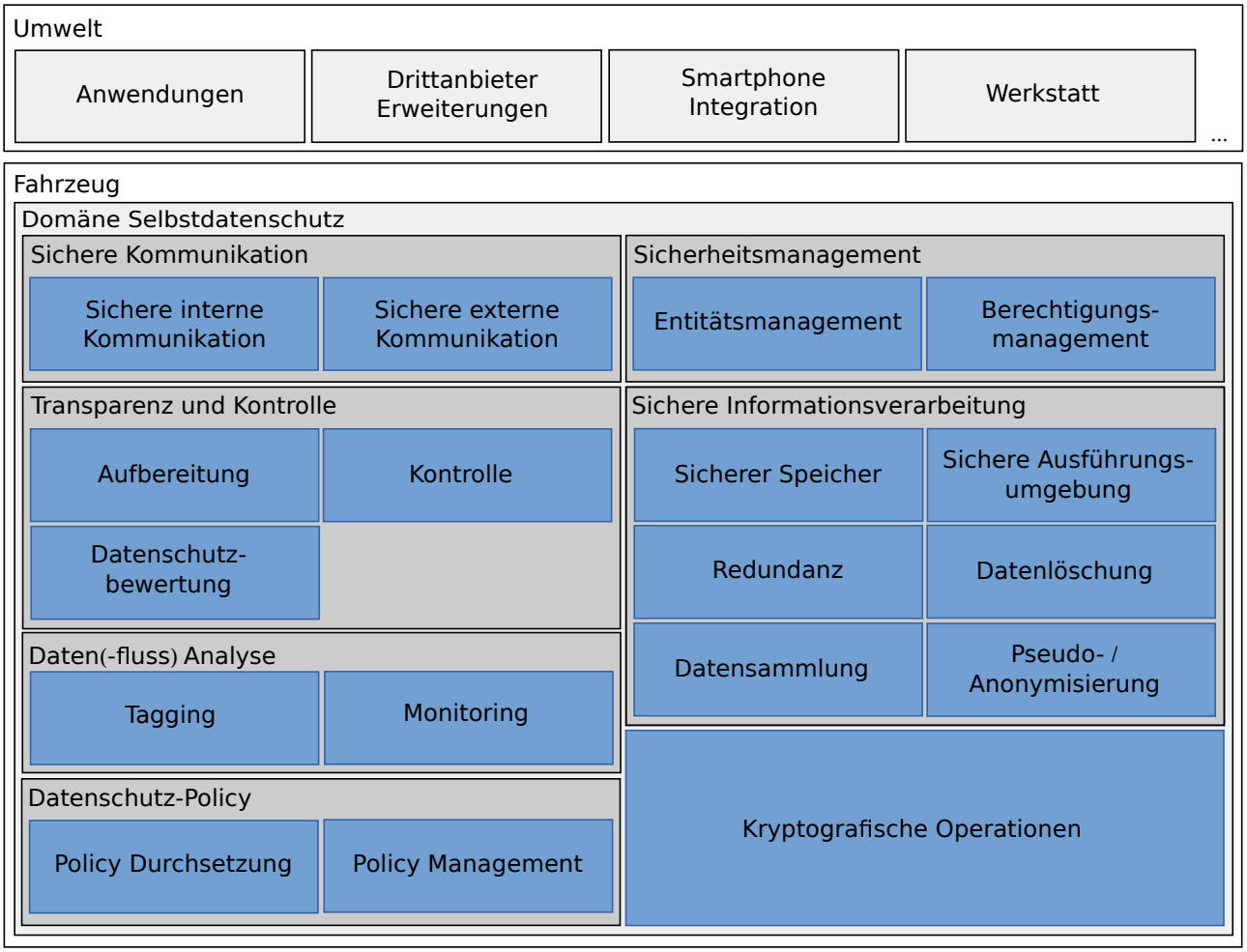

Abbildung 2.2: Abstrakte Logische Architektur

1. Sichere Kommunikation Entsprechend den aus den Anforderungen abgeleiteten Policy Restriktionen setzt das Modul *Sichere Kommunikation* für bestimmte Nachrichten, die entweder intern oder mit externen Kommunikationsteilnehmern ausgetauscht werden, Schutzziele wie Authentizität, Integrität und/oder Vertraulichkeit, um. Interne Kommunikation beschreibt dabei den Nachrichtenaustausch zwischen verschiedenen Entitäten innerhalb des Fahrzeug-Bordnetzes wie sie etwa bei der Aggregation von mehreren Sensorwerten in einem Steuergerät (Electronic Control Units (ECUs)) anfallen, während sich die externe Kommunikation auf den Nachrichtenaustausch des Fahrzeugs mit Kommunikationsteilnehmern außerhalb des Fahrzeug-Bordnetzes (Umwelt), z. B. Anbieter von Mehrwertdiensten (siehe auch AP1, Abstrakte Fahrzeugarchitektur), bezieht.

Die von diesem Modul umgesetzten Schutzziele sind abhängig von den hinterlegten Policies für den jeweiligen Kommunikationsweg und Empfänger. Auf Grundlage von T06 (Einwilligungsnachweis) müssen jedoch alle Daten, die das Fahrzeug verlassen, mindestens signiert sein, um die Einwilligung in die Datenerhebung nachweisen zu können. Weiterhin muss im Hinblick auf T10 (Übermittlung von Verarbeitungsorten) die Integrität von eingehende Nachrichten, die die jeweiligen Verarbeitungsorte beinhalten, sicher gestellt werden, um Manipulationen ausschließen zu können. Außerdem erfordert T16 (Datenintegrität) sichere (integere) interne Kommunikation. Wenn etwa zur Sicherstellung der Datenverfügbarkeit, Daten redundant kopiert werden, muss ihre Integrität auch auf dem Übertragungsweg sichergestellt werden. Schließlich fordert T18 (Vertraulichkeit), dass personenbezogene Daten nicht von Unbefugten ausgelesen werden dürfen. Dies bedingt eine sichere interne als auch externe Kommunikation, indem z. B. Datenflüsse verschlüsselt werden.

2. Transparenz und Kontrolle Das Modul *Transparenz und Kontrolle* ermöglicht dem Nutzer Einsicht und Kontrolle über Datenflüsse, die das Fahrzeug verlassen und somit datenschutzrechtlich relevant sind. Entsprechend des Selbstdatenschutzkonzeptes kann der Nutzer aufgrund der ihm dargestellten Informationen die Datenweitergabe bewilligen oder

ablehnen (Kontrolle) bzw. sich zumindest darüber informieren, zu welchem Zweck und in welchen Intervallen welche Daten zu welchen Parteien übertragen werden (Aufbereitung). Das Untermodul *Aufbereitung* bereitet die angezeigten Informationen so auf, dass der Nutzer diese verstehen kann und gleichzeitig nicht von seiner Fahraufgabe abgelenkt wird. Darüber hinaus wird ihm anhand des Untermoduls *Datenschutzbewertung* die Kritikalität der angeforderten Daten verdeutlicht, um informierte Entscheidungen treffen zu können.

Aktive *Kontrolle* ist in diesem Modul in den Anforderungen T03 (Aktive Einwilligung), T07 (Einwilligungswiderruf), T11 (Beurteilung des Datenschutzniveaus) und T12 (Information über Datenempfänger) gefordert. Während in T03 bzw. T07 dem Nutzer grundsätzlich die Möglichkeit geboten wird, Einwilligungen für bestimmte Daten zu erteilen bzw. diese auch wieder zu entziehen, beziehen sich T11 bzw. T12 auf den informierten Einwilligungsentzug aufgrund einer Diskrepanz des Datenschutzniveaus beim Datenanforderer bzw. auf den informierten Einwilligungsentzug bezüglich des Datenanforderers selbst oder gegebenenfalls Drittparteien an den dieser die Daten weiterleiten will. Durch den informativen Charakter von T07, T11 und T12 als auch T05 (Informationen vor Einwilligung) und T20 (Einfachheit des HMIs) sind in diesen Anforderungen die bereits erwähnten *Aufbereitungen* notwendig, um den Nutzer benutzerfreundlich (Usability) zu informieren. Werden Informationen für den Nutzer aufbereitet, auf deren Grundlage dieser einer Datenweitergabe zustimmen soll (T05, T11, T12), wird zusätzlich in diesem Kontext eine *Datenschutzbewertung* erstellt, um dem Nutzer auf evtl. auftretende Datenschutzrisiken (z. B. die Möglichkeit von Tracking anhand der übermittelten Standortdaten) zu informieren.

3. Daten(-fluss) Analyse Innerhalb des Daten(-fluss) Analyse-Moduls werden die Aktivitäten, die sich mit der Kennzeichnung und Überwachung von Daten bzw. Datenflüssen beschäftigen, zusammengefasst. Daher enthält es die Submodule *Tagging* und *Monitoring*. Das Modul ist eng mit dem *Datenschutz-Policy*-Modul verknüpft, da es die Daten(-flüsse) anhand der dort festgelegten Policies taggt und dann an die *Policy Durchsetzung* weiterleitet. Im Submodul *Tagging* werden einzelnen Datensätzen Metadaten hinzugefügt, um sie entsprechend der in AP1 erstellten Datentaxonomie zu kennzeichnen und vom Untermodul Monitoring „interpretierbar“ zu machen. Das Untermodul *Monitoring* überwacht dann entsprechende Datenflüsse anhand ihrer Tags und leitet diese entsprechend zur *Policy Durchsetzung* weiter, die dann die mit dem Tag verbundenen Policies umsetzt, in dem es die Daten an das jeweilige Modul, z. B. zur *Pseudo-/Anonymisierung*, weiterleitet.

Entsprechend fordern T01 (Datenkategorisierung), T02 (Zwingende Einwilligung), T06 (Einwilligungsnachweis), T13 (Information über Datenspeicherung) und T14 (Zweckgebundene Einwilligung) daher *Tagging*, um Daten grundsätzlich zu kategorisieren (z. B. personenbeziehbar) als auch Metainformationen hinzuzufügen (z. B. Einwilligung erteilt, Zweck der Datenerhebung hinzufügen). *Monitoring* wird an allen Schnittstellen zur “Außenwelt” durchgeführt und explizit in T02 adressiert, da dort automatisiert Datenflüsse unterbunden werden sollen, bei denen keine Einwilligung durch den Nutzer vorliegt.

4. Datenschutz-Policies In diesem Modul werden die Datenschutz-Policies, die sich sowohl aus den in AP1 definierten Anforderungen ergeben als auch diejenigen, die vom Nutzer selbst eingebracht werden, verwaltet und durchgesetzt. Entsprechend beinhaltet das Modul die Submodule *Policy Durchsetzung* und *Policy Management*.

Basierend auf den Anforderungen T02 (Zwingende Einwilligung), T03 (Aktive Einwilligung), T08 (Vorausgehende Einwilligungsüberprüfung) und T12 (Information über Datenempfänger), wird vor Weitergabe eines Datums die Einwilligung des Nutzers überprüft[1]. Falls diese nicht vorliegt, verhindert die *Policy Durchsetzung*, dass die Daten für die keine Einwilligung gegeben worden sind das Fahrzeug verlassen. Auf Grundlage von T14 (Zweckgebundene Einwilligung) stellt die *Policy Durchsetzung* sicher, dass Datenanfragen immer mit dem jeweiligen Zweck der Datenerhebung versehen sind und weist diese daraufhin gegebenenfalls zurück. Weiterhin ist die *Policy Durchsetzung* auch für die Umsetzung von Zugriffssystemen verantwortlich, wie sie in T19 (Zugriffsberechtigungen) gefordert werden. Schließlich wird mit diesem Modul auch T21(Datentrennung) umgesetzt, indem sichergestellt wird, dass Daten, wenn sie für unterschiedliche Zwecke erhoben werden, getrennt versendet werden.

Im Allgemeinen wird das Untermodul *Policy Management* verwendet, um Policies im Fahrzeug zu verwalten, also diese zu erstellen, bestehende abzuändern oder zu löschen. Es ist also indirekt an allen Funktionen beteiligt, bei denen Policies beteiligt sind.

5. Sicherheitsmanagement Das Modul *Sicherheitsmanagement* ist grundsätzlich für die Verwaltung von Berechtigungen und Identitäten von Kommunikationspartnern (z. B. in Form von Zertifikaten) verantwortlich.

[1] Die Einwilligung des Nutzers wird dem Datum als Tag hinzugefügt.

Tabelle 2.1: Zuordnung der technischen Anforderungen zu den Modulen der logischen Architektur

Anforderung	Modul
T01 Datenkategorisierung	DA (Tagging), T (Datenschutzbewertung), P (Policy Management)
T02 Zwingende Einwilligung	DA (Tagging), DA (Monitoring), P (Durchsetzung)
T03 Aktive Einwilligung	P (Policy Management), P (Durchsetzung), T (Kontrolle)
T04 Authentifizierung des Einwilligers	Kryptografische Operation (Auth)
T05 Informationen vor Einwilligung	T (Datenschutzbewertung), T (Aufbereitung), SM (Entitätsmanagement)
T06 Einwilligungsnachweis	SM (Entitätsmanagement), DA (Tagging), SK (Sichere externe Kommunikation)
T07 Einwilligungswiderruf	SI (Sicherer Speicher), SI (Redundanz), T(Aufbereitung), T (Datenschutzbewertung), T (Kontrolle), SI (Datenlöschung)
T08 Vorausgehende Einwilligungsüberprüfung	P (Policy Management), P (Durchsetzung)
T09 Datenverarbeitung ohne Einwilligung	P (Policy Management)
T10 Übermittlung von Verarbeitungsorten	SK (Sichere externe Kommunikation), SM (Entitätsmanagement)
T11 Beurteilung des Datenschutzniveaus	SI (Sicherer Speicher), SM (Entitätsmanagement), T (Datenschutzbewertung), T (Aufbereitung), T (Kontrolle)
T12 Information über Datenempfänger	P (Durchsetzung), SM (Entitätsmanagement), T (Aufbereitung), T (Kontrolle), P (Policy Management), T (Datenschutzbewertung)
T13 Information über Datenspeicherung	DA (Tagging)
T14 Zweckgebundene Einwilligung	P (Durchsetzung), DA (Tagging)
T15 Frühzeitige Anonymisierung/Pseudonymisierung	SI (Anonymisierung/Pseudonymisierung), SI (Datensammlung)
T16 Datenintegrität	SI (Sicherer Speicher), SK (Sichere interne Kommunikation), SI (Sichere Ausführungsumgebung)
T17 Redundanz	SI (Redundanz)
T18 Vertraulichkeit	SI (Sicherer Speicher), SK (Sichere interne Kommunikation), SK (Sichere externe Kommunikation), SI (Sichere Ausführungsumgebung)
T19 Zugriffsberechtigungen	P (Durchsetzung), SM (Berechtigungsmanagement)
T20 Einfachheit des HMIs	T (Aufbereitung)
T21 Datentrennung	P (Policy Management), P (Durchsetzung), SI (Anonymisierung/Pseudonymisierung)
T22 Gezielte und zuverlässige Löschung	SI (Datenlöschung)

Im Untermodul *Entitätsmanagement* werden Berechtigungsnachweise (*Credentials*) des Fahrzeugs (Plattformschlüssel mit zugehörigen Zertifikaten) verwaltet, mit denen sich das Fahrzeug beispielsweise zu anderen Diensten authentifiziert. Dabei werden sicherheitskritische Informationen, beispielsweise private Schlüssel oder Root-Zertifikate, im sicheren Speicher abgelegt, um sie vor unbefugter Einsicht durch Dritte oder Manipulation zu schützen. Weiterhin werden dort auch Zertifikate von internen oder externen Kommunikationsendpunkten verwaltet, damit diese sich untereinander authentifizieren können. Intern können dies etwa Sensoren oder Steuergeräte sein und extern etwa das Backend eines Dienstleisters. Entsprechend der definierten Policies und der Daten(-fluss)analyse kann dann mit Hilfe des Untermoduls der Zugriff von und zu bestimmten Endpunkten kontrolliert werden. Zum Beispiel könnte der Nutzer im Zuge des Selbstdatenschutzes festlegen, dass die Verbindung zu bestimmten Dienstleistern nur verschlüsselt oder aggregiert erfolgen soll[2].

Das Untermodul *Berechtigungsmanagement* kontrolliert dagegen den Zugriff auf das Fahrzeug bzw. Komponenten des Farhezugs und setzt ein Zugriffskontrollsystem um, bei dem bestimmte Rollen (Fahrer, KFZ-Mechaniker, ...) mit verschiedenen Zugriffsrechten ausgestattet werden. Zum Beispiel kann so festgelegt werden, dass der KFZ-Mechaniker nur

[2]Unter Umständen kann durch diese Maßnahmen die Funktionalität der Dienste eingeschränkt oder der Dienst sogar funktionsunfähig werden. Darauf muss der Nutzer hingewiesen werden.

die für die Reparatur und Wartung relevanten Daten, nicht aber beispielsweise synchronisierte Kontaktdaten einsehen darf.

Da dieses Modul eine generelle Verwaltungsfunkion übernimmt und unverzichtbar für die Funktionalität des Gesamtsystems ist, setzt es indirekt eine Vielzahl der definierten Anforderungen um. Insbesondere wird das *Entitätsmanagement* von den Anforderungen gefordert, bei denen Kommunikation mit Entitäten außerhalb des Fahrzeugs stattfindet, also T05 (Informationen vor Einwilligung), T06 (Einwilligungsnachweis), T10 (Übermittlung von Verarbeitungsorten), T11 (Beurteilung des Datenschutzniveaus) und T12 (Information über Datenempfänger), während das *Berechtigungsmanagement* im Speziellen die Anforderung T19 (Zugriffsberechtigungen) umsetzt.

6. Sichere Informationsverarbeitung Das Modul *Sichere Informationsverarbeitung* realisiert den Schutz von allen sicherheitskritischen Informationen, die innerhalb des Fahrzeugs gespeichert und verarbeitet werden. Es besteht aus den Untermodulen, *Sicherer Speicher*, *Sichere Ausführungsumgebungen*, *Redundanz*, *Datenlöschung*, *Datensammlung* und *Pseudo-/Anonymisierung*. Diese Untermodule sorgen in ihrer Gesamtheit dafür, dass Daten bereits im Fahrzeug sicher vorverarbeitet und gespeichert werden können, bevor sie dieses verlassen und auch zuverlässig gelöscht werden können. Dabei kann der Begriff "sicher" abseits von kryptografischer Sicherheit auch organisatorische Sicherheit einschließen, wie sie z. B. durch das *Redundanz*-Modul umgesetzt wird.

Die Untermodule sorgen in ihrer Gesamtheit dafür, dass Daten bereits im Fahrzeug sicher vorverarbeitet (z. B. aggregiert oder anonymisiert/pseudonymisiert) und gespeichert werden können, bevor sie dieses verlassen.

So wird *Sicherer Speicher* von T07 (Einwilligungswiderruf), T11 (Beurteilung des Datenschutzniveaus), T16 (Datenintegrität) und T18 (Vertraulichkeit) gefordert, wobei nur auf Grundlage von T18 auch die Vertraulichkeit der gespeicherten Daten sichergestellt werden muss (z. B. durch Verschlüsselung), während bei den anderen die Integrität der gespeicherten Daten ausreicht. Mit dem Untermodul *Redundanz* soll die generelle Verfügbarkeit der Daten sichergestellt werden. Dies betrifft konkret die Anforderungen T07 und T17 (Redundanz), wobei sich erstere auf die Verfügbarkeit von Einwilligungsnachweisen im Fahrzeug und letztere auf die redundante Auslegung von Backend Systemen bezieht. Das Untermodul *Datensammlung* unterstützt diverse Pseudo-/Anonymisierungstechniken, indem z.B. ein Datum derselben Kategorie (z. B. Positionsdaten) zunächst im Fahrzeug aggregiert wird, um etwa lediglich einen Durchschnittswert zu senden. Das Untermodul wird von T15 (Anonymisierung und Pseudonymisierung) explizit gefordert. Im Fall das Datenintegrität (T16) oder Vertraulichkeit (T18) ist eine *Sichere Ausführungsumgebung* gefordert, innerhalb derer kryptografische Operationen ohne Manipulation oder Einsicht durch Dritte durchgeführt werden können, um etwa die oben genannten Schutzziele umzusetzen. Ein weitere wichtige Funktion des Moduls ist die Löschung von gespeicherten Daten, die je nach Anwendungsfall auch nicht wiederhergestellt werden dürfen. Die Anforderungen T07 (Einwilligungswiderruf) sowie T22 (Gezielte und zuverlässige Löschung bestimmter Datensätze) zielen auf diese Funktion ab. Die letzte Funktion betrifft die Pseudo-/Anonymisierung von Daten und Datenflüssen, wobei insbesondere T15 und T21 (Datentrennung) diese voraussetzen.

7. Kryptografische Operationen Das Modul *Kryptografische Operationen* bietet grundlegende kryptografische Primitiven wie Ver- und Entschlüsselung oder Signaturerstellung und -verifizierung an. Nach Möglichkeit sollten diese Operationen in einer sicheren Ausführungsumgebung (Trusted Execution Environment (TEE)) ausgeführt werden, um z. B. unautorisierte Manipulationen zur Ausführungszeit von kryptografischen Operationen (Verschlüsseln, Signieren, ...) und/oder unautorisiertes Abhören (*Eavesdropping*) zu verhindern.

Ähnlich wie im Modul *Sicherheitsmanagement*, handelt es sich hierbei im eine Kernmodul der Architektur die wesentliche Funktionen bereitstellt. Daher ist es auch indirekt bei der Umsetzung der meisten Anforderungen, jedoch explizit an T04 (Authentifizierung des einwilligenden Nutzers), beteiligt.

2.2 Abstrakte technische Architektur

Die nachfolgende Architektur, die in Abbildung 2.3 dargestellt ist, wird auf einer technischen Abstraktionsebene beschrieben, die sowohl eine einfache Übersicht über die Beziehungen zwischen den verschieden Modulen als auch teilweise Datenflüsse innerhalb der Architektur aufzeigt. Aus diesem Grund werden alle Module als eine Komponente dargestellt, obwohl sich diese unter Umständen auch mehrfach redundant verteilt innerhalb des Fahrzeugbordnetzes befinden können, beispielsweise im Fall des Moduls Policy Durchsetzung[3].

Generell kommuniziert das Fahrzeug über die in Abbildung 2.3 dargestellte Schnittstelle mit der Umwelt. Wie auch in der in AP1 entwickelten Referenzarchitektur [1] zu sehen, besteht die Umwelt aus allen Entitäten außerhalb des Fahrzeugs

[3] Eine beispielhafte Verteilung der einzelnen Module innerhalb des Fahrzeugs findet sich in Kapitel 2.3 ab S.14.

(z. B. der Fahrer selbst, KFZ-Mechaniker, Smartphones, Drittanbieter-Apps, diverse Dienstanbieter, ...), die mit dem Fahrzeug interagieren. Diese Entitäten greifen über verschiedene Technologien auf die Schnittstellen des Fahrzeugs zu. Zum Beispiel kann der Zugriff über das Internet (GSM, UMTS, LTE, ...), Schnittstellen des Infotainmentsystems (WLAN, Bluetooth, USB, DAB, physische Bedienelemente, ...) oder Wartungskanäle (On-Board-Diagnose (OBD) Schnittstelle) erfolgen.

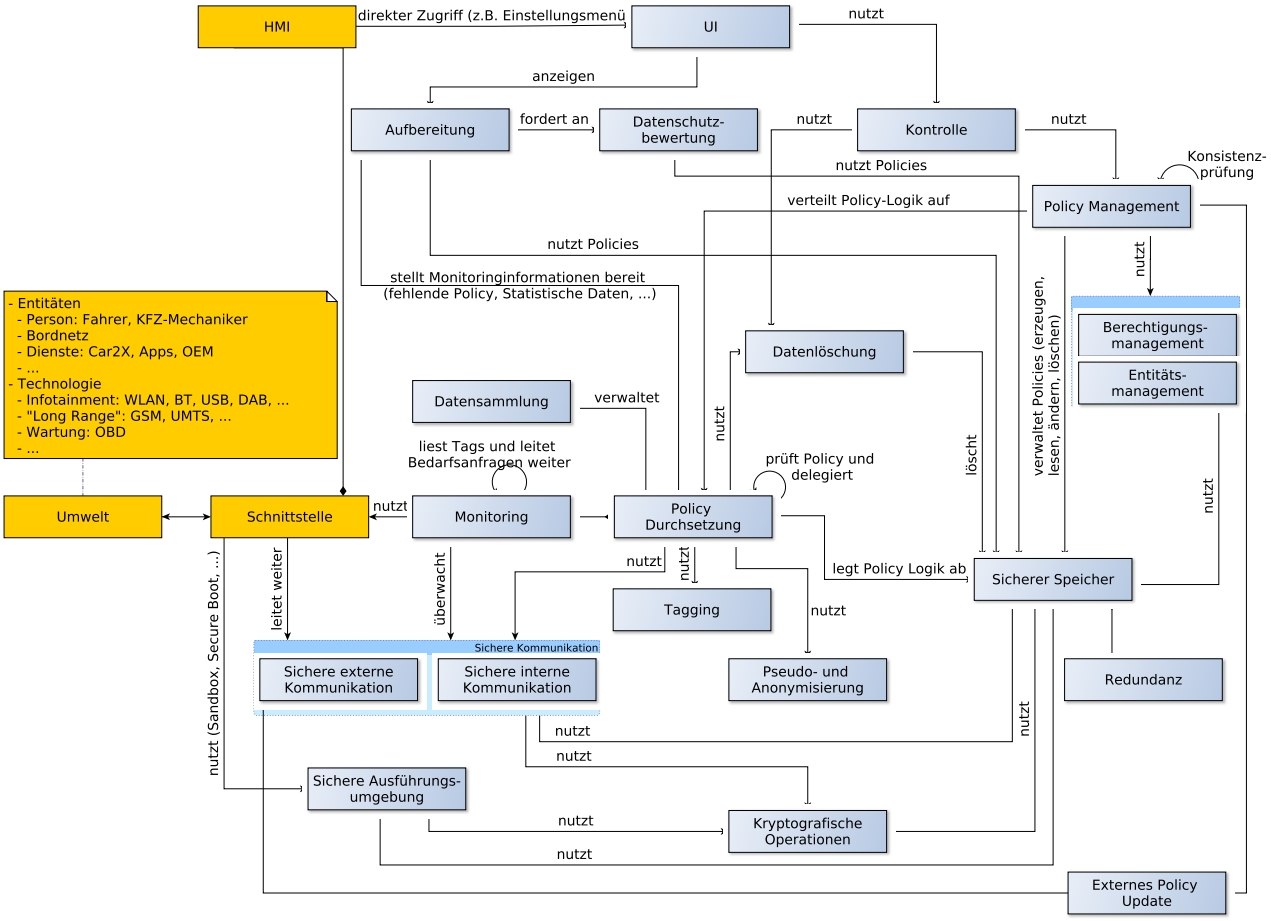

Abbildung 2.3: Abstrakte Technische Architektur

Um die dargestellte Architektur strukturiert beschreiben zu können, soll daher im Weiteren unterschieden werden zwischen der Nutzerkontrolle, bei der der Fahrer Datenschutzeinstellungen einsehen und ändern kann, und einer Datenfluss-basierten Beschreibung, bei der das Fahrzeug unter Berücksichtigung der eingestellten Kriterien mit der Umwelt kommuniziert. Beide Beschreibungen sind dabei lediglich als Einstiegspunkte zur Erklärung der Pfade innerhalb der Architektur gedacht und überschneiden sich daher. Die Nutzerkontrolle umfasst daher die Module *UI*, *Information*, *Datenschutzbewertung* und *Kontrolle* sowie deren Abhängigkeiten, während die Datenfluss-basierte Beschreibung den Pfad über die Module *Monitoring* und *Policy Durchsetzung* sowie deren Abhängigkeiten umfasst.

Im Folgenden soll zunächst die technische Architektur anhand der gerade definierten Kategorien beschrieben werden. Im Anschluss werden dann komplexere Module detaillierter erläutert, die sich in weitere Untermodule gliedern und somit die Abbildung unnötig verkompliziert hätten.

2.2.1 Generelle Beschreibung

Wie bereits erwähnt, soll die Architektur im Weiteren anhand der beiden festgelegten Kategorien, “Nutzerkontrolle” und “Datenfluss-basierte Beschreibung”, grundsätzlich beschrieben werden.

2.2.1.1 Nutzerkontrolle

Wie eingangs erläutert beschreibt die Nutzerkontrolle, wie der Nutzer Datenschutzeinstellungen einsehen und ändern kann. Dabei dient der Bildschirm des Infotainmentsystems dem Fahrer zum einen als Kontrollelement, um bestimmte Datenschutzeinstellungen vorzunehmen, und zum anderen als Informationsanzeige, um datenschutzrelevante Informationen angezeigt zu bekommen. Diese Informationsanzeige erfolgt dabei entweder ereignisgesteuert oder initiiert durch den Fahrer durch die physischen Bedienelemente des Infotainmentsystems. Während sich das nächste Kapitel mit der ereignisgesteuerten Variante befasst, soll hier die Fahrer-initiierte Variante beschrieben werden.

Das zentrale Element ist dabei das Modul *UI*, das die Inhalte darstellt. Hier kann sich der Nutzer seine aktuellen Datenschutzeinstellungen über die *Kontrolle* anzeigen lassen und auch ändern. Für diese Aktionen greift die *Kontrolle* auf das *Policy Management* zurück, das wiederum die Einstellungen (z. B. Policy Regeln (Welche Daten dürfen zu wem wie übertragen werden und welche Datenschutzbewertung leitet sich daraus ab?)) aus dem Speicher ausliest bzw. dort auch neue hinterlegt oder bestehende abändert. Über die Kontrolle ist es dem Fahrer zudem möglich, gezielt Daten (z. B. synchronisierte Adressbücher) über das Modul *Datenlöschung* aus dem Speicher zu löschen. Ändert oder erstellt der Fahrer Einstellungen in Form von Policies, überprüft das *Policy Management* deren Konsistenz, z. B. bzgl. Widerspruch mit anderen Policies, und legt diese im *Sicheren Speicher* ab. Anschließend verteilt es die Policy-Logik, eine maschineninterpretierbare Version der Policy, auf betreffende Module der *Policy Durchsetzung*.

2.2.1.2 Datenfluss-basierte Beschreibung

Bei der Datenfluss-basierten Beschreibung kommuniziert das Fahrzeug mit der Umwelt, wobei für den Selbstdatenschutz im Fahrzeug grundsätzlich alle Datenflüsse relevant sind, bei denen Daten aus dem Fahrzeug in die Umwelt fließen. Der Datenfluss kann entweder durch den Fahrer initiiert werden (z. B. POIs entlang der Route anzeigen) oder aber durch einen Dienst angefordert werden (z. B. Ladesäule fordert ein Vertragszertifikat über ISO 15118 an). Die übertragenen Daten werden dem Nutzer entweder zu einer geeigneten Zeit mit einer entsprechenden Datenschutzbewertung angezeigt oder anhand einer vom Nutzer vorher konfigurierten Policy automatisch behandelt.

Über die jeweilige Schnittstelle übertragene Datenströme (üblicherweise externe Anfragen, um bestimmte Daten zu erhalten) werden, nachdem sie gegebenenfalls vom Modul *Sichere Externe Kommunikation* vorverarbeitet worden sind (z. B. entschlüsselt, Signatur geprüft), zunächst über das *Monitoring*-Modul geleitet, wo die Anfrage auf die geforderten Daten hin überprüft werden. Der jeweilige Urheber der Anfrage und die von ihm geforderten Daten werden mit den Policies im Policy-Speicher abgeglichen. Falls keine entsprechende Policy vorliegt, wird das Modul *Aufbereitung* informiert, das auch eine Datenschutzbewertung zu den geforderten Daten anfragt und diese Information entsprechend aufbereitet. Die Aufbereitung beinhaltet sowohl die Anpassung der Darstellungsform als auch die Festlegung eines günstigen Zeitpunkts zur Anzeige dieser Informationen, um den Fahrer nicht von seiner Fahraufgabe abzulenken. Wenn bereits eine Policy vorliegt, die die Datenerhebung nicht grundsätzlich unterbindet (in diesem Fall wird direkt eine Antwort über diese Unterbindung generiert), wird eine entsprechende Datenstruktur im Modul *Sammlung* angelegt, in der die geforderten Antwortdaten vor dem Versand zunächst zwischengespeichert werden.

An Datenquellen (z. B. Sensoren) erzeugte Daten, die von einer externen Stelle oder vom Fahrer (Fahrer-initiiert) angefordert worden sind, werden durch das *Monitoring*-Modul geleitet, das mit Hilfe des Moduls *Policy Durchsetzung*, einzelne Daten entsprechend den im *Policy Speicher* hinterlegten Regeln taggt (Modul *Tagging*). Liegt keine Policy bezüglich des Taggings vor, wird wieder der Nutzer über die *Aufbereitung* informiert. Die Daten werden in die Datenstruktur, die im Modul *Datensammlung* angelegt worden ist, abgelegt. Evtl. werden auch mehrere Daten der gleichen Kategorie zu Aggregationszwecken zunächst in diesem Modul gesammelt. Enthält die Datenstruktur alle geforderten bzw. die von der Policy freigegebenen Daten, kann diese durch bestimmte Module weiter verarbeitet werden z. B. *Sichere Kommunikation* oder *Anonymisierung/Pseudonymisierung*. Wenn die Vorverarbeitung abgeschlossen ist, werden die Datenpakete an die in Abbildung 2.3 abgebildete Schnittstelle weitergeleitet und gelangen in die Umwelt.

2.2.2 Detailbeschreibung ausgewählter Module

Nachdem im vorigen Kapitel eine generelle Übersicht über die Beziehungen der einzelnen Module der abstrakten technischen Architektur gegeben worden ist, sollen nun komplexere Module detaillierter beschrieben werden.

2.2.2.1 Pseudo- und Anonymisierung

Das übergeordnete Modul *Pseudo- und Anonymisierung* setzt sich aus mehreren Teilmodulen zusammen, die jeweils bestimmte Teilaspekte adressieren. Die *Datentrennung* kümmert sich um die Problemfälle, bei denen einzelne Datensätze nur dann keine Identifikation oder Wiedererkennung zulassen, wenn diese getrennt von bestimmten weiteren Datensätzen übertragen werden. Das Modul soll dabei sicherstellen, dass keine Datensätze miteinander kombiniert werden, die nicht kombiniert werden dürfen bzw. dass bereits kombinierte Datensätze so aufgesplittet werden, dass die einzelnen Komponenten unproblematisch sind. Relevant ist dies insbesondere dann, wenn einzelne Datensätze inhaltlich unverändert übertragen werden sollen. Eng mit dem Modul verknüpft ist das Teilmodul *Ersetzung*. Dieses Modul kommt insbesondere dann zum Einsatz, wenn die Inhalte eines Datensatzes als Folge der Datentrennung nicht im Ganzen übertragen werden dürfen, die Struktur des Datensatzes allerdings zumindest teilweise beibehalten werden soll. Bei der Ersetzung werden einzelne Werte eines Datensatzes ausgetauscht. Abhängig davon, ob auf die zu ersetzenden Werte vollständig verzichtet werden kann, werden sie entweder mit Dummy-Werten überschrieben, oder mit vergröberten Werten, wie sie vom Teilmodul *Vergröberung* bereitgestellt werden. Die *Vergröberung* kümmert sich darum, einzelne Werte so zu modifizieren oder zu verallgemeinern, dass diese inhaltlich noch für den vorgesehenen Zweck verwendet werden können, aber keine weiteren darüber hinausgehenden Informationen bzw. Details enthalten. Ein Beispiel hierfür wäre die Ersetzung einer exakten GPS-Koordinate mit einem groben Kartenabschnitt. Sofern für Werte eines Datensatzes keine dazugehörige Zweckbindung existiert und sie nicht mit Dummy-Werten ersetzt werden, werden diese vom Teilmodul *Löschung* entfernt. Die *Aggregation* kommt dann zum Einsatz, wenn für den Verwendungszweck nicht jeder einzelne Datensatz relevant ist, sondern auch aggregierte Werte mehrerer Datensätze (z. B. Mittelwerte) genügen. Sofern der Zeitpunkt einer oder mehrerer Datenübertragungen ein Datenschutzrisiko darstellt, kommt das Teilmodul *Verzögerung* zur Anwendung. Das Modul kann einzelne Datenübertragungen verzögern und Einfluss auf die Reihenfolge verschiedener Datenübertragungen nehmen. Sofern mehrere Datenübertragungen bewusst miteinander verknüpfbar sein sollen, ohne die Identität des Absenders zu offenbaren, kommen Pseudonyme zum Einsatz. Diese werden von der *Pseudonymverwaltung* verwaltet. Das Modul kümmert sich unter anderem darum, dass Pseudonyme nur so lange wie nötig im Einsatz sind und mehrere Pseudonyme vom Empfänger nicht miteinander in Beziehung gebracht werden können. Neben den zuvor genannten inhaltlichen Pseudo- und Anonymisierungsmaßnahmen gibt es auch Maßnahmen zur Anonymisierung der Kommunikation bzw. Datenübertragung. Diese Funktionen sind im Teilmodul *Kommunikationsanonymisierung* zusammengefasst. Mit Hilfe von organisatorischen und/oder kryptografischen Maßnahmen wird sichergestellt, dass die Kommunikationsmetadaten keine Rückschlüsse auf den Absender zulassen und auch einzelne Datenübertragungen (und damit deren Inhalte) nicht miteinander verkettbar sind.

2.2.2.2 Sicherer Speicher

Das übergeordnete Modul *Sicherer Speicher* fasst alle Module zusammen, die mit der Speicherung verschiedener Datentypen oder Arten der sicheren Speicherverwaltung zusammenhängen. Policies, Zertifikate, Programme, kryptographische Schlüssel und Daten werden jeweils in sicherem Speicher verwaltet. Die entsprechend zuständigen Module sind *Policy Speicher*, *Zertifikatsspeicher*, *Programmspeicher*, *Kryptografischer Schlüsselspeicher* und *Datenspeicher*. Die Module verwenden dabei, soweit erforderlich, technische Maßnahmen (z. B. Verschlüsselung) zum Schutz vor IT-Sicherheitsrisiken wie unbefugtem Zugriff oder Manipulation. Soweit nötig wird auch auf das Modul *Redundanter Speicher* zurückgegriffen. Dieses stellt die Verfügbarkeit gespeicherter Daten sicher, was u. a. datenschutzrechtlich für die gespeicherten Datensätze erforderlich sein kann.

2.2.2.3 Policy Management

Die korrekte und effiziente Verwaltung der Policies ist eine Grundvorraussetzung für das Funktionieren der die Policies umsetzenden Module. Das Modul *Policymanagement* umfasst alle Module, die sich mit der Policy-Verwaltung beschäftigen. Die Teilmodule *Erzeugung* und *Speicherung* kümmern sich darum, neue Policies korrekt zu erstellen und in sinnvoller Form im sicheren Speicher abzulegen. Das Modul *Löschung* ist dafür verantwortlich, veraltete Policies restlos zu entfernen. Sofern bestehende Policies verändert werden sollen, greift das Modul *Anpassung*. Abhängigkeiten und Beziehungen zwischen Policies werden vom Modul *Verknüpfung* verwaltet. Werden Policies erstellt, angepasst oder gelöscht, müssen die Policies auf Konsistenz geprüft werden um ungültige oder sich widersprechene Systemzustände zu verhindern. Das Modul *Beschreibung* dient der Lesbarmachung der Policies, um sie dem Fahrzeugnutzer oder anderen berechtigten Nutzern verständlich präsentieren zu können. Das Modul *Systemkonfiguration* ist schließlich dafür verantwortlich, alle Policyänderungen in maschinenlesbare Form umzuwandeln und die entsprechenden Komponenten, die die Policies umsetzen, zu programmieren.

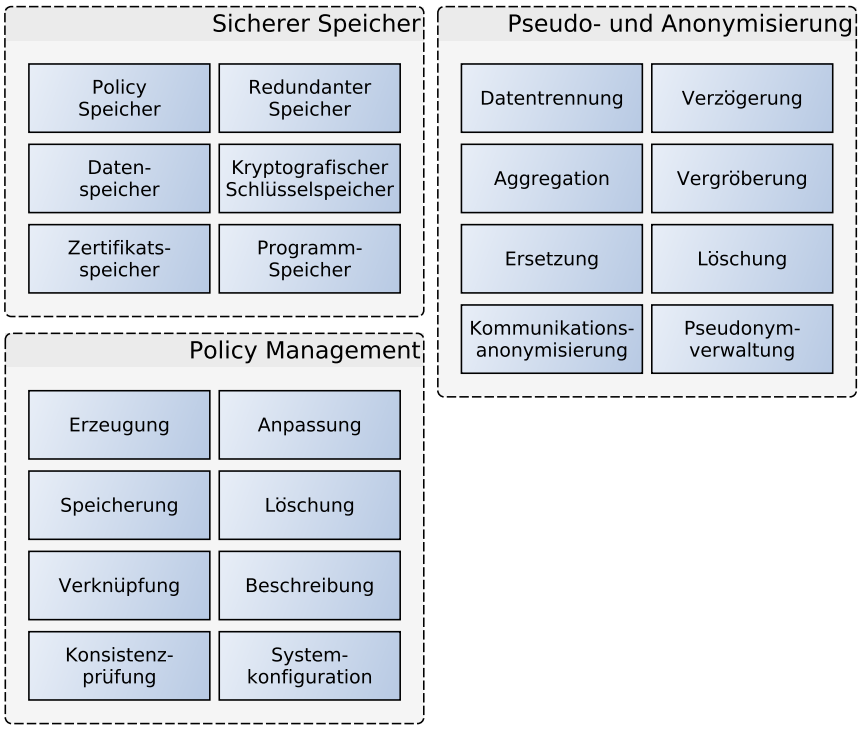

Abbildung 2.4: Moduldetails

2.3 Abbildung auf Fahrzeugarchitektur

Im letzten Schritt wird die entwickelte Datenschutzarchitektur auf die in AP1 definierte Referenzarchitektur [1] abgebildet. Beispielhaft zeigt Abbildung 2.5 nicht nur, auf welche Komponenten sich die Datenschutzarchitektur im Fahrzeug verteilt, sondern bezieht auch Komponenten außerhalb des Fahrzeugs ein, mit denen das Fahrzeug kommuniziert. Dass die Datenschutzarchitektur auch auf Komponenten außerhalb des Fahrzeugs abgebildet werden kann, ist insofern wichtig, als dass z. B. beim verschlüsselten Datenaustausch alle berechtigten Kommunikationspartner über die Ressourcen verfügen müssen (in diesem Fall kryptografisches Schlüsselmaterial), um entsprechend kommunizieren zu können. Weiterhin zeigt die Darstellung nicht nur die Komponenten, auf denen sich einzelne Module der Datenschutzarchitektur realisieren lassen, sondern verdeutlicht im Gegensatz zu den vorherigen Abbildungen auch, dass sich Module teilweise redundant auf verschiedenen Komponenten im Fahrzeug befinden können.

Wie bereits erwähnt stellt die Abbildung eine beispielhafte Implementierung der Module auf die Referenzarchitektur dar. Dabei wurde berücksichtigt, dass Module, die aufwendigere Funktionen erfüllen, (z. B. diverse Umsetzungen des Moduls *Pseudo-/Anonymisierung*), auf Komponenten abgebildet werden, die auch eine adäquate Rechen- bzw Speicherleistung besitzen. Module wie das *Monitoring*, die *Policy Durchsetzung* bzw. *Tagging* sind hauptsächlich an Schnittstellen (Datenquellen bzw. -senken) zwischen Fahrzeug und Umwelt zu finden, um gegebenenfalls (ggf.) direkt auf den Datenfluß einwirken zu können.

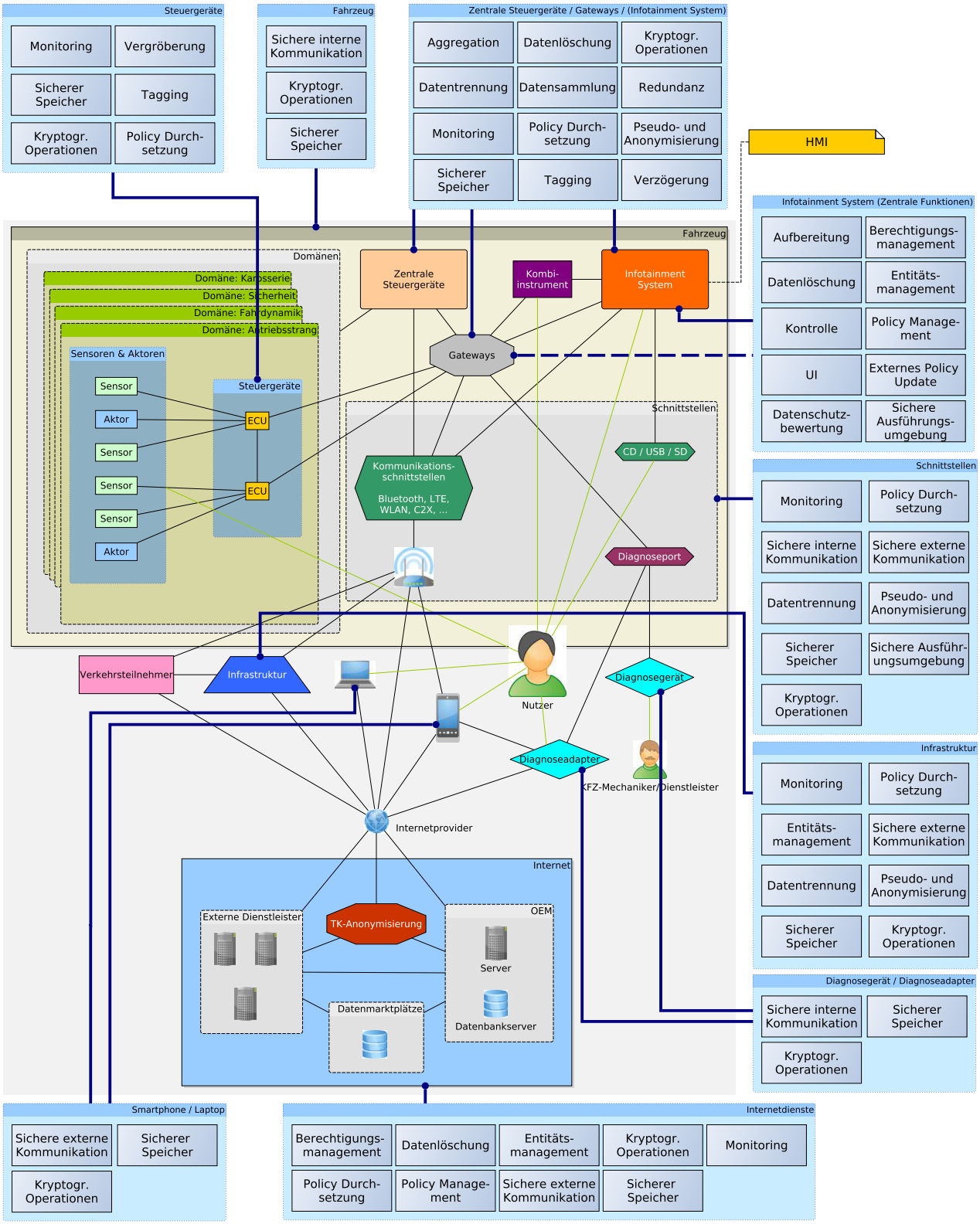

Abbildung 2.5: Beispielhafte Abbildung auf Referenzarchitektur

3 Schutzziele

Die Maßnahmen, die in diesem Dokument erarbeitet werden, dienen vor allem dem Schutz der persönlichen Daten von Nutzern — im Kontext von SeDaFa also vordringlich Fahrern, Fahrzeughaltern und Fahrzeuginsassen. Je nach Anwendungsfall können hierfür unterschiedliche Maßnahmen —alleine oder in Kombination— sinnvoll sein. Jede Maßnahme für sich genommen verfolgt dabei die Erfüllung von ein oder mehr Schutzzielen im Hinblick auf den Schutz der Privatsphäre und/oder der informationstechnischen Sicherheit. Die Ziele wurden bereits im Projektbericht „AP 1: Anforderungsanalyse“ ausführlich dargestellt [1] und sollen deshalb an dieser Stelle nur kurz eingeführt werden.

Datensparsamkeit soll gewährleisten, dass für einen gegebenen Anwendungsfall lediglich die personenbeziehbaren Daten verarbeitet oder gespeichert werden, die für den jeweiligen Anwendungsfall erforderlich sind. Mit anderen Worten soll die Menge der Daten so klein sein, dass ein Weglassen von ein oder mehr Daten dazu führen würde, dass das Ziel der Verarbeitung nicht mehr erreichbar wäre.

Integrität als Schutzziel bezieht sich zum Einen auf die Korrektheit von Daten, sowohl im Sinn von „richtig“ als auch im Sinn von „unverfälscht“, und zum Anderen auf die Korrektheit der Be- und Verarbeitung der Daten, d. h. dass die Datenverarbeitungsprozesse wie angegeben/erwartet ablaufen.

Vertraulichkeit soll sicherstellen, dass Daten vor der Kenntnisnahme durch Unberechtigte geschützt sind. Unberechtigte können hierbei sowohl Dritte als auch Mitarbeiter / Dienste des Unternehmens sein, dem die Daten des Nutzers anvertraut wurden.

Transparenz im Hinblick auf Datenverarbeitungsprozesse meint im vorliegenden Kontext, dass Nutzer erkennen können bzw. darüber informiert sind, wer wann was zu ihrer Person verarbeitet und speichert.

Intervenierbarkeit soll Nutzern erlauben, auf Datenverarbeitungsprozesse Einfluss zu nehmen. Hierbei soll Nutzern die Möglichkeit eröffnet werden, nicht nur Ja/Nein-Entscheidungen hinsichtlich der Verarbeitung ihrer Daten zu treffen, sondern ggf. auch die Art und Weise der Verarbeitung mitzubestimmen.

Verfügbarkeit soll sicherstellen, dass Daten, welche der Nutzer einem Dienst zur Verfügung gestellt hat, durch den Nutzer (jederzeit) abgerufen werden können bzw. ihm zur Verfügung stehen. Dies schließt auf Seiten des Dienstanbieters nicht nur das Sicherstellen der Erreichbarkeit des Dienstes an sich ein, sondern erlegt ihm auch eine Sorgfaltspflicht dahingehend auf, die Daten vor Zerstörung oder Verlust zu schützen.

Nicht-Verkettbarkeit beschreibt das Ziel, eine Verknüpfung von Daten desselben Nutzers, welche in unterschiedlichen Kontexten gewonnen wurden, zu verhindern/unterlassen oder von vornherein zu vermeiden. Kontexte können hier verschiedene Interaktionen eines Nutzers mit demselben Dienst oder Unternehmen sein, bspw. eine Registrierung und eine anschließende Dienstnutzung, oder auch Interaktionen mit unterschiedlichen Diensten. Im ersten Fall geht es meist darum, dass Daten aus einem Vorgang, wie bspw. Name und Anschrift für die Registrierung, nicht mit Daten aus einem anderen Vorgang, bspw. aus der Dienstnutzung gewonnene Daten, zusammengeführt werden können. Der zweite Fall ist ähnlich gelagert, jedoch sind die Kontexte umfassender und beinhalten die gesamte Interaktion eines Nutzers mit den jeweiligen Diensten. Nicht-Verkettbarkeit soll in diesem Fall sicherstellen, dass weder die Dienste selbst noch Dritte erkennen können, ob ein Nutzer a bei Dienst A identisch ist mit einem Nutzer b bei Dienst B. Andernfalls können die Daten von a und b wechselseitig verknüpft werden, sodass ein umfassenderes Bild des Lebenshintergrunds der dahinter stehenden Person geliefert wird.

4 Schutzmaßnahmen

Die hier beschriebenen Schutzmaßnahmen sind dazu bestimmt, die in Abschnitt 3 beschriebenen Schutzziele sicherzustellen. Da das Fahrzeug im Projektfokus steht, sind die Maßnahmen primär für den Einsatz im Zusammenhang mit dem Fahrzeug und der Verarbeitung von Daten inner- und außerhalb des Fahrzeugs ausgelegt. Daneben werden immer noch zusätzliche technische und organisatorische Maßnahmen —bspw. im Backend eines OEM oder bei genutzten Diensten von Dritten— notwendig sein, um die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Insbesondere sind die Anbieter natürlich auch zur Einhaltung gesetzlicher Vorgaben verpflichtet, wie bspw. Maßnahmen, um die Einhaltung der Zweckbindung bei der Verarbeitung von personenbezogenen Daten sicherzustellen. Derlei Maßnahmen können jedoch im Rahmen eines Selbstdatenschutzprojektes nicht behandelt werden.

Die im Folgenden beschriebenen Schutzmaßnahmen werden in abstrakter Form beschrieben, da es hier zunächst um das allgemeine Vorgehen im Rahmen einer Maßnahme geht und noch nicht um eine konkrete technische Ausprägung, wie sie für eine praktische Umsetzung notwendig wäre. Die Beschreibung der technischen Umsetzung wird Gegenstand eines anderen Dokuments sein.

Die vorgeschlagenen Maßnahmen lassen sich unterscheiden in

- technische Maßnahmen,
- organisatorische Maßnahmen und
- ihre Kombination.

Unter organisatorischen Maßnahmen sind Schutzversuche zu verstehen, die durch Handlungsanweisungen sowie Verfahrens- und Vorgehensweisen umgesetzt werden können.[1] Technische Maßnahmen sind demgegenüber Vorkehrungen, die sich auf den Vorgang der Verarbeitung der Daten selbst erstrecken. Dazu gehören bspw. Maßnahmen der Zugriffskontrolle und Verschlüsselung sowie andere Maßnahmen, die den Zugriff Unbefugter verhindern sollen.[2]

Die folgenden abstrakten Beschreibungen der Schutzmaßnahmen stellen die generelle Funktionsweise und Wirkung der Maßnahme vor und zeigen —wo möglich— Varianten auf. Für jede Maßnahme werden die jeweiligen Schutzziele genannt, die durch die Maßnahme erreicht werden. Die Beschreibung der Maßnahmen schließt jeweils mit der Auflistung der technischen Anforderungen T01-T22 aus der SeDaFa-Anforderungsanalyse [1], die durch die Maßnahmen jeweils erfüllt werden.

4.1 Benachrichtigung

Durch die Maßnahme der Benachrichtigung wird erreicht, dass der Nutzer über die vom Fahrzeug übermittelten Daten sowie die im Fahrzeug gespeicherten und verarbeiteten personenbezogenen Daten informiert wird. Auch eine Benachrichtigung im Falle von anonymen Daten ist eine Umsetzung der Maßnahme „Benachrichtigung“. Die Darstellung von Abfragen zur Einwilligung in eine Datenerhebung oder der Bereitstellung von Informationen über Speicherort, Verwendungszweck und Möglichkeiten zum Einwilligungswiderruf sind ebenfalls Teil der Maßnahme.

Technisch wird die Maßnahme durch Dialog- oder Informationsfelder auf dem Infotainmentsystem des Fahrzeugs umgesetzt. Die Maßnahme ist in allen Anwendungsfällen präsent, wird aber je nach Kontext verschiedene der oben genannten Aspekte umfassen.

Durch Benachrichtigung werden die folgenden Schutzziele erreicht:

- Transparenz
- Intervenierbarkeit,

Erfüllte technische Anforderungen:

T01 — Datenkategorisierung

T05 — Informationen vor Einwilligung

T10 — Übermittlung von Verarbeitungsorten

[1] Siehe `https://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Ma%C3%9Fnahmen`

[2] Definition in Anlehnung an [2, Art. 24 Rn. 21-22].

T11 — Beurteilung des Datenschutzniveaus

T12 — Information über Datenempfänger

T13 — Information über Datenspeicherung

4.2 Verfügbarkeit

Die Sicherstellung der Verfügbarkeit korrespondiert als Schutzmaßnahme zum gleichnamigen Schutzziel „Verfügbarkeit“ (siehe Abschnitt 3). Die Maßnahme stellt sicher, dass Daten eines Nutzers durch einen Dienst jederzeit abgerufen werden können und zur Verfügung stehen. Dies betrifft sowohl verarbeitete Daten im Fahrzeug (bspw. in einem Fahrdatenschreiber), die für die berechtigten Personen zugreifbar sein müssen, als auch die Erreichbarkeit von Servern und die Sicherung der Daten vor Verlust. Die Maßnahme der „Verfügbarkeit“ ist daher nicht nur im Fahrzeug selbst, sondern bei Dienstbetreibern anzuwenden. Sie fungiert als übergreifende Maßnahme für alle Anwendungsfälle, in denen Server zur Diensterbringung verwendet werden. Die Art der technischen Umsetzung kann je nach Kontext unterschiedlich sichergestellt werden. Geeignete technische Umsetzungen bestehen in der Herstellung von Backups, der Verwendung von redundanten Servern, Fallbacks u. Ä. Durch geeignete Datenbanken ist ferner eine Organisation der gespeicherten Nutzerdaten notwendig, durch die jedem Nutzer die zu ihm korrespondierenden Daten zur Verfügung stehen. Da die technische Umsetzung in der Regel außerhalb des Fahrzeugs liegt, wird diese im vorliegenden Kontext nicht weiter detailliert.

Die durch die Maßnahme der Verfügbarkeit erreichten Schutzziele sind:

- Integrität,
- Verfügbarkeit

Erfüllte technische Anforderungen:

T17 — Redundanz

4.3 Authentifizierung

Unter Authentifizierung werden technische Maßnahmen verstanden, die gegenüber einem Prüfer —im Folgenden auch als Anbieter bezeichnet— zum Nachweis der Echtheit einer behaupteten Identität oder Eigenschaft einer Person sowie der Urheberschaft von Daten geeignet sind. Eine Authentifizierung muss nicht notwendigerweise personenbeziehbar sein, d. h. sie kann auch dazu dienen, lediglich festzustellen, ob die zu authentifizierende Partei —synonym: Nutzer— eine gewisse Eigenschaft besitzt, bspw. Kunde des Prüfers ist. Im Folgenden werden deshalb die folgenden drei grundsätzlichen Arten der Authentifizierung unterschieden:

(1) Identitätsbasierte Authentifizierung

(2) Pseudonyme Authentifizierung

(3) Anonyme Authentifizierung

Ziele der Maßnahme sind —in Abhängigkeit von den zuvor genannten Varianten—

- Datensparsamkeit,
- Nicht-Verkettbarkeit,
- Integrität,
- Vertraulichkeit.

Identitätsbasierte Authentifizierung. Im Rahmen eines identitätsbasierten Authentifizierungsvorgangs weißt der Nutzer seine Identität aus dem realen Leben nach. Somit ist dem Prüfer die reale Identität des Nutzers bekannt, bspw. durch Nennung von Name und Adresse.

Beispiele für eine identitätsbasierte Authentifizierung sind persönliche Registrierungen mit Nutzername & Passwort, TLS-Client-Authentifizierung mit persönlichen Zertifikaten oder auch die Nutzung der Online-Ausweisfunktion des elektronischen Personalausweises.

Pseudonyme Authentifizierung. Bei einer pseudonymen Authentifizierung wird gegenüber dem Prüfer die reale Identität des Nutzers nicht offen gelegt. Bei häufiger Verwendung desselben Pseudonyms könnte der Prüfer jedoch feststellen, dass es sich beim Authentifizierenden stets um denselben Nutzer handelt, d. h. er wäre in der Lage, den Nutzer *wiederzuerkennen*. Im Unterschied zur identitätsbasierten Authentifizierung können bei einer pseudonymen Authentifizierung *verschiedene Prüfer* für einen bestimmten Nutzer nicht per se feststellen, ob es sich um denselben Nutzer handelt, da ein Pseudonym nur pro Anbieter eindeutig sein muss und verschiedene Nutzer dasselbe Pseudonym bei unterschiedlichen Anbietern nutzen können. Zur Wahrung der Pseudonymität des Nutzers ist es wichtig, dass die *Zuordnungsregel* von Pseudonym zu realer Identität dem Prüfer/Anbieter nicht bekannt wird.

Die zuvor genannten Beispiele für die identitätsbasierte Authentifizierung können ebensogut pseudonym realisiert werden, wenn persönliche Angaben zur realen Identität des Nutzers durch andere Bezeichner (Kennziffern, Pseudonyme, etc.) ersetzt werden. Auch die Online-Ausweisfunktion des elektronischen Personalausweises bietet die Möglichkeit, ein dienstspezifisches Pseudonym bei der Authentifizierung zu verwenden.

Anonyme Authentifizierung. Einer anonymen Authentifizierung liegt zumeist ein kryptografisches Protokoll zu Grunde, mit dessen Hilfe der Nutzer gegenüber dem Prüfer einen behaupteten Sachverhalt bzw. eine behauptete Aussage nachweist. Der Prüfer kann, im Unterschied zur pseudonymen Authentifizierung, durch die Anonymitätseigenschaft nicht feststellen, um welchen Nutzer es sich im Einzelnen handelt. Der Prüfer erhält jedoch „allgemeinere Garantien“, wie bspw. „der Nutzer besitzt Eigenschaft X“, was in einem konkreten Anwendungsfall bspw. zu „Nutzer ist Kunde des Anbieters“ übersetzt werden kann. Maßgeblich für den Grad der Anonymität des Nutzers ist die Größe k der Gruppe möglicher anderer Nutzer, welche dieselbe Eigenschaft haben — diese Gruppe wird als *Anonymitätsgruppe* bezeichnet. Je größer die Anonymitätsgruppe, desto stärker der erreiche Grad an Anonymität [3]. Die Festlegung einer Mindestgröße für k kann in der Praxis eine Herausforderung sein, da ein zu klein gewähltes k möglicherweise zur Identifizierung einzelner Personen führen kann und ein zu groß gewähltes k u. U. nicht zu jeder Zeit erreicht werden kann und damit bspw. ein Prozess so lange verzögert werden muss bis k erreicht ist. Die Anonymitätsgruppe ist stets relativ zu einer bestimmten Partei, hier dem Prüfer. Das hat zur Folge, dass ein Nutzer, der gegenüber einer Partei X anonym ist, nicht notwendigerweise auch gegenüber einer anderen Partei Y anonym sein muss.

Eine Implikation einer anonymen Authentifizierung ist, dass der Anbieter nicht feststellen kann, ob und ggf. wie oft sich ein Nutzer bisher authentifiziert hat, d. h. er ist auf Grund der Authentifizierungsdaten nicht in der Lage, ein Nutzer-/Nutzungsprofil zu erstellen.

Kryptografische Protokolle, welche eine anonyme Authentifizierung ermöglichen, sind bspw. die Familie der Gruppensignaturen [4, 5, 6], anonyme Credentials [7, 8, 9] oder das Protokoll *Direct Anonymous Attestation* (DAA) [10, 11, 12, 13, 14].

Erfüllte technische Anforderungen:

T04 — Authentifizierung des Einwilligers

4.4 Autorisierung / Zugriffskontrolle

Daten sind durch geeignete technische Maßnahmen vor dem Zugriff bzw. der Kenntnisnahme durch Unberechtigte zu schützen. Für den legitimen Zugriff auf Daten bedarf es einer Berechtigung (Engl. *permission*), welche vom *Autorisierer* für eine bestimmte Partei P ausgestellt wird, sodass diese nach Erhalt der Berechtigung zum *Berechtigten* wird. Im Rahmen der hier beschriebenen Maßnahme enthält eine Berechtigung stets eine (nicht notwendigerweise personenbeziehbare) Kennung des Berechtigten P_{ID}, einen Gültigkeitszeitraum t sowie Angaben D, welche die Art der Berechtigung (bspw. Lesen, Schreiben, Ändern) bzw. die darüber zugreifbaren Daten beschreiben. Eine solche Berechtigung wird im Folgenden und in weiteren Abschnitten als Token der Form $Perm(P_{ID}, t, D)$ dargestellt.

Berechtigungen können *zentral* oder *dezentral* verwaltet werden. Bei einer zentralen Verwaltung werden Berechtigungen direkt im System gespeichert, welches den Zugriff auf die angefragten Daten kontrolliert, d. h. der Berechtigte ist nicht „physisch“ im Besitz der Berechtigung. Bei einer dezentralen Verwaltung erhält der Berechtigte das Berechtigungstoken und reicht es zusammen mit der Zugriffsanfrage ein.

Eine Berechtigung muss stets auf ihre Gültigkeit geprüft werden. Konkret heißt das, dass *alle* Bestandteile des Tokens auf ihre Gültigkeit hin überprüft werden müssen. Für den vermeintlich Berechtigten ist deshalb eine Authentifizierung notwendig, sodass festgestellt werden kann, ob der Anfragende tatsächlich die in $Perm(P_{ID}, t, D)$ genannte Identität P_{ID} inne hat. Darüber hinaus muss überprüft werden, ob das Token bereits oder noch gültig ist, d. h. der aktuelle Zeitpunkt

innerhalb des Gültigkeitszeitraums t liegt. Die zuvor genannten Prüfungen sind für den zentralen wie für den dezentralen Fall durchzuführen. Für den dezentralen Fall muss das Zugriffskontrollsystem außerdem die Integrität des Tokens überprüfen, um festzustellen, ob das Token nach seiner Ausstellung manipuliert wurde, bspw. die Identität geändert wurde oder Rechte in D hinzugefügt wurden — bei einem zentralen System ist dies nicht zwingend erforderlich, wenn davon auszugehen ist, dass das Token im Zugriffskontrollsystem hinterlegt und die Integrität des Systems sichergestellt ist.

Autorisierung und Zugriffskontrolle sollen sicherstellen, dass die folgenden Schutzziele erreicht werden:

- Integrität,
- Intervenierbarkeit,
- Vertraulichkeit.

Abstrakt kann eine Autorisierung auch als Form einer datenschutzrechtlichen Einwilligung gesehen werden, sodass durch diese Maßnahme nicht nur sicherheitstechnische Anforderungen erfüllt werden können.

Im Folgenden werden die Schritte der Autorisierung und Zugriffskontrolle im Einzelnen beschrieben.

Berechtigung ausstellen. Im ersten Schritt der Autorisierung legt der Autorisierer fest, wer ($\rightarrow P_{ID}$) wann und wie lange ($\rightarrow t$) auf welche seiner Daten wie ($\rightarrow D$) zugreifen darf. Dies erfolgt durch die Erstellung des Berechtigungstokens $Perm(P_{ID}, t, D)$ und ggf. dessen Integritätsschutz durch Maßnahmen wie bspw. eine digitale Signatur oder einen *Message Authentication Code* (MAC).

Berechtigung erteilen. Im zweiten Schritt der Autorisierung wird die ausgestellte Berechtigung vom Autorisierer im zentralen Fall im Zugriffskontrollsystem hinterlegt oder im dezentralen Fall an den (danach) Berechtigten übergeben. Im zentralen Fall muss das Zugriffskontrollsystem vor der Übernahme der Berechtigung den vermeintlichen Autorisierer authentifizieren, um feststellen zu können, ob dieser selbst die Berechtigung hat, Berechtigungen $Perm(\bullet, \bullet, D)$ hinsichtlich der Daten D auszustellen bzw. zu erteilen.

Berechtigung prüfen. Eine Prüfung der Berechtigung eines Anfragenden hinsichtlich des Zugriffs auf Daten D muss für jede Zugriffsanfrage erfolgen. Dies ist der zentrale Schritt der Zugriffskontrolle. Der Prüfschritt bedingt immer eine vorherige Authentifizierung des Anfragenden, um festzustellen, ob dieser die Identität P_{ID} aus der Berechtigung $Perm(P_{ID}, \bullet, \bullet)$ inne hat. Weiterhin muss für $Perm(\bullet, t, \bullet)$ überprüft werden, ob der aktuelle Zeitpunkt τ innerhalb des Gültigkeitszeitraums $t := [t_1, t_n]$ liegt, also $t_1 \leq \tau \leq t_n$ gilt. Für den dezentralen Fall kommen noch zwei weitere Prüfungen hinzu, nämlich die Prüfung der Integrität von $Perm(\bullet, \bullet, \bullet)$ und die Prüfung, ob der Aussteller im Vorfeld überhaupt die Berechtigung hatte, das Token auszustellen. Letzteres bedingt, dass der Aussteller für das Zugriffskontrollsystem erkennbar ist, was sich bspw. bei Verwendung einer digitalen Signatur durch den Prüfschlüssel des Ausstellers ergibt und sich im Falle eines MAC durch Hinterlegung der Ausstellerkennung in den Daten D realisieren lässt.

Berechtigung entziehen. Der Entzug einer Berechtigung $Perm(P_{ID}, \bullet, D)$ hat unmittelbar zur Folge, dass ein zuvor durch $Perm(P_{ID}, \bullet, D)$ Berechtigter P_{ID} keinen Zugriff mehr auf die Daten D hat. Der Entzug einer Berechtigung kann bspw. durch Löschen aus dem Zugriffskontrollsystem erfolgen (zentraler Fall) oder durch Aufnahme in eine Schwarze Liste (dezentraler Fall). Weiterhin kann eine Berechtigung $Perm(P_{ID}, \bullet, \bullet)$ mittelbar entzogen werden, wenn die darin genannte Identität P_{ID} für Zugriffe gesperrt wird. Eine Berechtigung $Perm(\bullet, t, \bullet)$ kann außerdem „automatisch“ ungültig werden, was einem Entzug gleich kommt, wenn der Gültigkeitszeitraum $t := [t_1, t_n]$ abgelaufen ist, also für den aktuellen Zeitpunkt τ gilt, dass $t_n < \tau$ ist. Berechtigungen, für die die zuvor genannte Bedingung erfüllt ist, können von einer evtl. vorhandenen Schwarzen Liste entfernt werden.

Erfüllte technische Anforderungen:

T02 — Zwingende Einwilligung
T03 — Aktive Einwilligung
T06 — Einwilligungsnachweis
T07 — Einwilligungswiderruf
T08 — Vorausgehende Einwilligungsüberprüfung
T09 — Datenverarbeitung ohne Einwilligung
T14 — Zweckgebundene Einwilligung

T16 — Datenintegrität
T19 — Zugriffsberechtigungen

4.5 Verschlüsselung

Eine der wirksamsten technischen Maßnahmen zum Schutz vertraulicher Daten vor der Kenntnisnahme durch Unbefugte ist die Verschlüsselung der Daten mit Hilfe eines kryptografischen Verschlüsselungsverfahrens. Hierbei gilt es u.a. sicherzustellen, dass das verwendete Verfahren aktuellen Sicherheitsstandards entspricht und die für die Entschlüsselung notwendigen Schlüssel sicher, d. h. für Unbefugte nicht zugänglich, aufbewahrt werden. Verfahren, die als sicher gelten, werden regelmäßig vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als Technische Richtlinie 02102-1 [15] herausgegeben. Für das sichere Speichern von Schlüsseln käme ein so genanntes Hardware-Sicherheits-Modul (HSM) in Frage, welches ein unbefugtes Auslesen eines Schlüssels durch Soft- oder Hardware wesentlich erschwert, da Berechnungen mit geheimen Schlüsseln normalerweise innerhalb des geschützten Speichers des HSM erfolgen und somit Anwendungen keinen unmittelbaren Zugriff auf den Schlüssel erhalten. Durch Softwaremaßnahmen geschützte Schlüssel sind grundsätzlich angreifbarer, da diese zum Zeitpunkt ihrer Verwendung unverschlüsselt im Hauptspeicher des Geräts liegen, sodass neben dem legitimen Programm auch ein Angreifer in der Lage ist, diesen Speicherbereich auszulesen.

Verschlüsselung soll sicherstellen, dass das folgende Schutzziel erreicht wird:

- Vertraulichkeit.

Im Rahmen der hier beschriebenen Schutzmaßnahmen werden zwei generelle, komplementäre Mechanismen zur Verschlüsselung von Daten beschrieben: Ende-zu-Ende-Verschlüsselung und Container-Verschlüsselung.

Ende-zu-Ende-Verschlüsselung. Für die Verschlüsselung von Daten ist eine wesentliche Frage, wer die Daten für wen verschlüsselt. Verschlüsselt ein Sender Daten derart, dass nur der intendierte Empfänger die Daten entschlüsseln kann, wird dies als Ende-zu-Ende-Verschlüsselung (Engl. *end-to-end encryption*, E2E) bezeichnet. In diesem Fall ist es im Hinblick auf die Vertraulichkeit praktisch unerheblich, wie viele Stellen ein verschlüsseltes Datum (Chiffrat) auf dem Weg vom Sender zum Empfänger passiert, da keine der zwischengeschalteten Stellen in der Lage ist, den Klartext des Chiffrats in Erfahrung zu bringen. Wird ein verschlüsseltes Datum auf dem Weg jedoch von einer zwischengeschalteten Stelle ent- oder umgeschlüsselt —unabhängig davon, ob die Stelle das Datum tatsächlich einsieht—, spricht man nicht mehr von Ende-zu-Ende-Verschlüsselung, da davon auszugehen ist, dass der Sender und der intendierte Empfänger nicht mehr alleine Kenntnis von der Nachricht haben. Ende-zu-Ende-Verschlüsselung bietet sich insbesondere für die elektronische *Übermittlung* von Daten an (Engl. *data in transit*).

Container-Verschlüsselung. Unter einer Container-Verschlüsselung wird im Rahmen dieses Dokuments die Verschlüsselung einer Datei für einen Nutzer auf einem lokalen Endgerät verstanden. Der daraus resultierende verschlüsselte Container kann dabei aus logischer Sicht ein oder mehr Dateien enthalten, welche über eine Schnittstelle für Anwendungen geöffnet bzw. entschlüsselt werden. Als Schnittstelle kann bspw. das Dateisystem des Betriebssystems dienen, wenn der Container als Verzeichnis oder als virtuelles Laufwerk in das Dateisystem eingebunden wird. Die Ver- und Entschlüsselung kann dann transparent durch Komponenten im Betriebssystem erfolgen, sodass Endanwendungen hierfür keine besonderen Maßnahmen implementieren müssen. Eine andere Möglichkeit besteht darin, dass eine Endanwendung die Schnittstelle bereitstellt, d. h. die Ver- / Entschlüsselung sowie den Zugriff auf den Container selbst implementiert. Container-Verschlüsselung bietet sich für auf lokalen Medien gespeicherte Daten (Engl. *data at rest*) an. Container-Verschlüsselung kann auch als Umsetzung für Ende-zu-Ende-Verschlüsselung dienen, wenn der Container nicht für den Nutzer selbst, sondern für einen Empfänger verschlüsselt und anschließend verschickt wird.

Datenlöschung. Die Verwendung von Container-Verschlüsselung kann auch beim Problem der „sicheren“ Löschung von Daten weiterhelfen. Im einfachsten Fall werden Daten bei einem Löschvorgang aus Effizienzgründen nur aus den Verwaltungsstrukturen des Dateisystems gelöscht, sodass die Dateien oder Verzeichnisse für den Nutzer nicht mehr sichtbar sind; die eigentlichen Daten bleiben jedoch erhalten und können somit nach der Löschung immer noch extrahiert werden. Wird ein verschlüsselter Container auf diese Weise gelöscht, ist dieses Problem um ein Vielfaches kleiner. Der Container an sich ist zwar ebenfalls extrahierbar, die Daten im Container sind jedoch ohne Kenntnis des Verschlüsselungsschlüssels praktisch nicht lesbar. Da das Ziel der Löschung von Daten primär ist, dass die Daten für niemanden mehr zugänglich sein sollen, kann dies nahezu genauso gut durch die Löschung des Verschlüsselungsschlüssels abgebildet werden. Prinzipiell ist eine physikalische Löschung der Daten immer noch die sicherste Methode, da in diesem Fall keinerlei Anhaltspunkte

für die ursprünglichen Daten übrig bleiben, während der Container immer noch als gültiges Chiffrat einer Verschlüsselung bestimmter Daten vorhanden ist, sodass diese grundsätzlich wieder hergestellt werden können. Jedoch kann sich die physikalische Löschung von *einzelnen* Daten durch den Einsatz verschiedener Techniken zur Verlängerung der Lebensdauer und Fehlerfreiheit von Festplatten, wie bspw. S.M.A.R.T. oder *Wear Leveling*, als schwierig erweisen. Bei der Nutzung von Container-Verschlüsselung reduziert sich das Problem der „sicheren" Löschung der gesamten Daten (im Container) auf das Problem der „sicheren" Löschung des Container-Schlüssels. Dieser ist jedoch speichermäßig klein genug, um in einem sicheren Speicher abgelegt zu werden, wie bspw. einem HSM, sodass dieser dann dafür Sorge tragen kann, dass der Schlüssel „sicher" gelöscht bzw. nicht mehr zugreifbar ist.

Erfüllte technische Anforderungen:

T18 — Vertraulichkeit

T22 — Gezielte und zuverlässige Löschung bestimmter Datensätze

4.6 Lokale Verarbeitung

Die Weitergabe von personenbezogenen Daten stellt grundsätzlich ein Risiko für die informationelle Selbstbestimmung des Einzelnen dar. Gesetzliche Anforderungen sowie technische Maßnahmen, wie die in diesem Dokument beschriebenen, sind dazu gedacht, die Risiken zu senken und Garantien für den Schutz der Privatsphäre zu geben.

Eine Weitergabe von personenbezogenen Daten und eine daraus resultierende Einschränkung der informationellen Selbstbestimmung ist aber nicht immer erforderlich und kann dadurch verhindert werden, dass Verarbeitungsschritte, welche personenbeziehbare Daten erfordern, lokal im Einflussbereich des Nutzers erfolgen.

Durch die organisatorische Maßnahme einer lokalen Verarbeitung sollen die folgenden Schutzziele erreicht bzw. unterstützt werden:

- Datensparsamkeit,
- Transparenz,
- Nicht-Verkettbarkeit,
- Intervenierbarkeit,
- (*Integrität*),
- (*Vertraulichkeit*),
- (*Verfügbarkeit*).

Die vier zuerst genannten Schutzziele werden implizit erreicht, da sich diese im Wesentlichen „gegen" Dateneverarbeiter bzw. Dritte richten, die jedoch im Fall von rein lokaler Verarbeitung nicht existent sind. Integrität, Vertraulichkeit und Verfügbarkeit werden aus ähnlichen Gründen heraus *eingeschränkt* erreicht, da die Daten vor nicht existenten Verarbeitern oder Dritten keinen Schutz benötigen und der Nutzer im Hinblick auf einige Aspekte der Verfügbarkeit, wie bspw. Mobilfunkempfang oder Server-Erreichbarkeit, nicht auf weitere Parteien angewiesen ist. Einschränkend muss bei den letzten drei Schutzzielen jedoch auch berücksichtigt werden, dass ggf. nicht nur der Fahrer/Halter (als Betroffener) selbst Zugang zum Fahrzeug hat, sondern möglicherweise auch weitere Personen, wie bspw. Familienmitglieder, Werkstattangestellte, Freunde, etc. Aus diesem Grund sollten auch bei rein lokaler Verarbeitung zusätzlich technisch Maßnahmen zum Schutz von Integrität, Vertraulichkeit sowie Verfügbarkeit eingesetzt werden.

Die Umsetzung dieser organisatorischen Maßnahme kann auch technische Auswirkungen haben, da ggf. höhere Anforderungen im Hinblick auf Rechenkapazität und Speicherbedarf durch die lokale Verarbeitung entstehen können.

Erfüllte technische Anforderungen:

T16 — Datenintegrität

T18 — Vertraulichkeit

T21 — Datentrennung

4.7 Anonymität / Pseudonyme

Die hier beschriebene Schutzmaßnahme bezieht sich auf anonyme oder pseudonyme Bezeichnungen, die verwendet werden, um die Identität von Personen, Fahrzeugen oder Geräten zu verschleiern. Es kann sich dabei um einmalig (im Falle

von Anonymität) oder mehrfach (im Falle von Pseudonymität) verwendete Nummern, Buchstabenfolgen, Zertifikate o. Ä. handeln. Das hier zu Grunde gelegte Verständnis von „Anonymität“ und „Pseudonymität“ entspricht der Definition von [3]. Demnach ist ein Subjekt einem Beobachter gegenüber *anonym* in einer Anonymitätsgruppe (vgl. Abschnitt 4.3) von Subjekten, sofern es von dem Beobachter nicht von anderen Subjekten der Gruppe unterschieden werden kann. Da sich Anonymität immer auf einen bestimmten Beobachter und eine bestimmte Anonymitätsgruppe bezieht, gilt Anonymität nicht absolut, sondern ist immer auf einen bestimmten Kontext bezogen.

Ein Subjekt ist einem Beobachter gegenüber *pseudonym*, sofern dieser nur ein Pseudonym, aber nicht die Identität des Subjektes kennt. Ein Pseudonym bezeichnet dabei einen Namen ungleich der Identität. Im Gegensatz zu Anonymität erlaubt Pseudonymität Verknüpfbarkeit, also das Wiedererkennen eines Subjektes und damit die Unterscheidung von anderen Subjekten einer Gruppe. Durch den Aspekt der Wiedererkennbarkeit und Verknüpfbarkeit lassen sich Anonymität und Pseudonymität in der Theorie scharf voneinander abgrenzen. In der Praxis ergibt sich jedoch eine gewisse Spannung dadurch, dass „Wiedererkennbarkeit“ auf unterschiedliche Zeiträume bezogen wird. Ob innerhalb mehrerer Interaktionen als Teil eines kurzen Kommunikationsvorgangs (Engl. *Session*) oder erst aufgrund der Wiedererkennbarkeit über zwei verschiedene Sessions von Pseudonymität gesprochen wird, hängt vom jeweiligen Kontext ab.

Anonyme Bezeichner. Anonymität kann je nach Anwendungsfall und konkreten Erfordernissen unterschiedlich umgesetzt werden. Ein spezieller Fall ist die anonyme Authentifizierung (siehe dazu Abschnitt 4.3). In anderen Fällen kann Anonymität einfach dadurch erreicht werden, dass sich eine Person oder ein Fahrzeug nicht durch einen Namen identifiziert oder diesen (bei einer einmaligen Transaktion) mit einer (pseudo-)zufälligen Zeichenfolge ersetzt.

Pseudonyme Bezeichner. Pseudonymität ist dann erforderlich, wenn zwei Parteien mehrfach miteinander interagieren müssen. Auch Pseudonyme können über pseudonyme Zertifikate umgesetzt werden (siehe Abschnitt 4.3). Eine andere Form der Umsetzung besteht in der Verwendung eines Transaktionspseudonyms π, durch das eine Person oder ein Fahrzeug für eine anderer Instanz für die Dauer einer Transaktion/Sitzung wiedererkennbar bleibt, ohne die tatsächliche Identität zu kennen. Ein solches Pseudonym kann ein Benutzername, eine im Rahmen eines Protokolls generierte URL oder eine generierte (pseudo-)zufällige Zeichenfolge sein.

Durch die Verwendung anonymer oder pseudonymer Bezeichnungen sollen die folgenden Schutzziele erreicht bzw. unterstützt werden:

- Datensparsamkeit,
- Nicht-Verkettbarkeit,

Erfüllte technische Anforderungen:

T15 — Frühzeitige Anonymisierung/Pseudonymisierung

T21 — Datentrennung

4.8 Datenanonymisierung

Die Maßnahme der Datenanonymisierung dient der Anonymisierung von inhaltlichen Daten, die in Protokollen oder Datenpaketen übermittelt werden oder für eine spätere Übermittlung gespeichert werden. Im Gegensatz zur Maßnahme „Anonymität/Pseudonyme“, die sich auf anonyme Zeichenfolgen, Zertifikate oder pseudonyme Benutzernamen zur Bezeichnung und ggf. Wiederkennung von Personen oder Geräten in Transaktionen bezieht, zielt die Maßnahme der Datenanonymisierung auf die in Transaktionen verwendeten oder übermittelten Inhaltsdaten. Entsprechend der Definition von Anonymität in [3] sind solche Daten einem Beobachter gegenüber anonym in einer Gruppe von anderen Daten bzw. Absendern, sofern sie innerhalb dieser Gruppe ununterscheidbar sind. Anonymität kann sich je nach Kontext entweder auf die Absender („Senderanonymität“) oder die Daten selbst („Datenanonymität“) beziehen.

Wie im Fall von anonymen Bezeichnern (siehe Abschnitt 4.7) bezieht sich Anonymität nach immer auf eine bestimmte Anonymitätsgruppe sowie auf einen bestimmten Beobachter, dem gegenüber Daten anonym sind. Da die Anonymität der Daten nicht absolut gilt, folgt unweigerlich, dass sie in den allermeisten Fällen bereits dadurch aufgehoben werden kann, dass einem Beobachter neues Wissen zugänglich wird. Die Anonymisierung von Daten setzt daher in Bezug auf einen Beobachter immer einen bestimmten Wissensstand voraus. Sollte sich dieser erheblich ausweiten, ist die Anonymität der Daten nicht mehr garantiert.

Abstrakt besteht die Möglichkeit zur Aufhebung der Anonymität von Daten in der Bildung von *Korrelationen* mit anderen Daten. Durch Korrelationen können bspw. zwei Datenbanken so miteinander verknüpft werden, dass daraus Informationen

abgeleitet werden können, die in keiner der ursprünglichen Datenbanken für sich genommen enthalten waren. Es ist daher notwendig, dass anonymisierte Daten nicht mit anderen Daten (anonymisiert oder nicht anonymisiert) korreliert werden, die nicht als Teil des Wissensstandes des Beobachters vorausgesetzt wurden.

Durch Datenanonymisierung soll sichergestellt werden, dass die folgenden Schutzziele erreicht werden:

- Datensparsamkeit,
- Nicht-Verkettbarkeit.

Anonymisierungsverfahren

Die inhaltliche Anonymisierung von Daten wird algorithmisch durch spezielle Anonymisierungsverfahren erreicht. Solche Verfahren verwenden unterschiedliche Techniken, um offensichtliche Bezüge zu eindeutigen Identitäten zu entfernen:

- Generalisierung von Daten
- Zergliederung innerer Bezüge von Daten
- Beschränkung des Erkenntnisgewinns anhand statistischer Vorgaben
- Statistische Perturbation

Die bekanntesten Anonymisierungsverfahren sind k-*Anonymity* [16] und *Differential Privacy* [17]. k-*Anonymity* ist ein Verfahren, welches Datensätze so generalisiert, dass ein Datensatz unter jeweils k Datensätzen anonym ist. Die Größe von k muss dabei vorgegeben werden und bestimmt die Größe der Anonymitätsgruppe. Je größer die Anonymitätsgruppe, desto stärker ist der erreichte Grad an Anonymität. *Differential Privacy* ist dagegen ein Verfahren, das Anonymität durch statistische Perturbation erreicht. Durch statistische „Rauschwerte“ werden Daten geringfügig entstellt. Die aus Daten gewonnenen Aussagen werden damit mit einem Unsicherheitsfaktor versehen, der in etwa der Unsicherheit aufgrund von statistischen Stichprobenfehlern entspricht.

Anonymisierungsverfahren können unterschiedlich konkrete Ausprägungen haben. Im Fahrzeugkontext sind eine positionelle Generalisierung oder eine zeitlich verzögerte Übermittlung von Daten sehr häufige Anwendungen.

Zeitliche Verzögerung. Eine zeitlich verzögerte Übermittlung durch eine statistische Verzögerung bewirkt, dass ein bestimmtes Datenset von einer großen Anzahl an potentiellen Fahrzeugen übermittelt worden sein könnte. Das sendende Fahrzeug ist damit dem Empfänger gegenüber anonym innerhalb der Gruppe der potentiellen Absender, sofern nicht die Daten selbst weitere Informationen enthalten, die zu einer eindeutigen Identifizierung verwendet werden können.

Positionelle Generalisierung. Eine positionelle Generalisierung ersetzt exakte Positionen durch Positionsbereiche wie bestimmte Ortsquadranten innerhalb von Städten, Postleitzahlgebiete, Bundesländer, etc. Damit werden Rückschlussmöglichkeiten aufgrund einer Fahrzeugposition erschwert. Die Größe der bei der Anonymisierung verwendeten Gebiete ist abhängig von der Vorgabe über die Größe der Anonymitätsgruppe bzw. dem Grad der Anonymität. Je mehr potentielle Fahrzeuge sich innerhalb der verallgemeinerten Positionsangabe befinden, desto stärker der erreichte Grad an Anonymität.

Sonstiges. Neben der Anonymiserung von Zeitpunkten und Geopositionen können prinzipiell alle Arten von Daten anonymisiert werden. Anonymisierungsverfahren können in Abhängigkeit von der Art der zu anonymisierenden Daten gewählt werden, um einerseits einen hohen Grad an Anonymität zu erreichen und andererseits den Nutzwert der Daten so wenig wie möglich einzuschränken.

Erfüllte technische Anforderungen:

T03 — Aktive Einwilligung

T15 — Frühzeitige Anonymisierung/Pseudonymisierung

T21 — Datentrennung

4.9 Bezug zu Anwendungsfällen

Die in den vorangegangenen Abschnitten genannten Schutzmaßnahmen werden in unterschiedlichen Anwendungsfällen verwendet. Die Art der spezifischen Anwendung richtet sich je nach Anwendungsfall und kann von Fall zu Fall variieren.

	Benachrichtigung	Verfügbarkeit	Authentifizierung	Autorisierung und Zugriffskontrolle	Verschlüsselung	Lokale Verarbeitung	Anonymität und Pseudonyme	Datenanonymisierung
Car-Sharing	X	X	X	X	X	X	X	X
Werkstatt	X		X	X				
Ortung und Reaktion	X				X	X		X
Android Auto	X		X	X		X		
Paket Auto	X	X	X	X	X			X
Umgebung	X	X	X		X		X	X
Verschleißanalyse	X	X			X			X
Laden und Bezahlen	X	X	X	X	X		X	
Fahrerverhalten	X	X	X	X			X	X
Fahrerüberwachung	X			X		X		

Abbildung 4.1: Datenschutzmaßnahmen in Anwendungsfällen

Auch die Häufigkeit der Verwendung einzelner Schutzmaßnahmen variiert. Abbildung 4.1 gibt eine Übersicht über die Verteilung der einzelnen Schutzmaßnahmen auf die im nächsten Abschnitt genannten Anwendungsfälle.

5 Anwendungsfälle

In diesem Abschnitt werden die in SeDaFa betrachteten Anwendungsfälle kurz dargestellt und die in Abschnitt 4 beschriebenen Maßnahmen in den jeweiligen Anwendungsfall integriert. Eine detailliertere Beschreibung der Anwendungsfälle ohne Datenschutzmaßnahmen findet sich im Dokument „Anforderungsanalyse“ [1]. Die im Folgenden beschriebenen Anwendungsfälle richten sich jeweils nach der dort gegebenen Beschreibung hinsichtlich Ablauf der Datenübermittlung, Nutzungsbeispielen und erhobenen Daten.

Ziel der folgenden Anwendungsfalldarstellung ist es, einen erweiterten Ablauf zu beschreiben, der die Privatsphäre sowie die Informationssicherheit von Nutzern mit Hilfe der beschriebenen Maßnahmen sicherstellen soll.

Für jeden der im Folgenden beschriebenen Anwendungsfälle ist der Ablauf der Datenübermittlung entsprechend dem Abstraktionsgrad der Maßnahmen schematisch in einer Abbildung dargestellt. Die darin gezeigten Abläufe sind notwendig verkürzt dargestellt, d. h. die explizit erwähnten Datenelemente sind keinesfalls abschließend zu sehen und sollen lediglich Anhaltspunkte für eine praktische Umsetzung liefern.

5.1 Mehrfache Fahrzeugnutzung

5.1.1 Car-Sharing

Beim Car-Sharing (CS) wird ein Fahrzeug von unterschiedlichen Nutzern bei einem CS-Anbieter gebucht und für einen gewissen Zeitraum genutzt. In Bezug auf das Verhältnis von Kunde zu CS-Anbieter findet in Bezug auf die Verarbeitung von personenbezogenen Daten durch den CS-Anbieter das Bundesdatenschutzgesetz (BDSG) auf den gesamten Vorgang Anwendung, da diese zu kommerziellen oder gewerblichen Zwecken erfolgt. Da die Nutzer des CS-Dienstes i. d. R. in keinem persönlichen oder familiären Verhältnis zueinander stehen, findet das BDSG auch im Verhältnis von Kunden untereinander zumindest insoweit Anwendung, dass der CS-Anbieter geeignete technisch-organisatorische Schutzmaßnahmen zu ergreifen hat, um die personenbezogenen Daten einzelner Nutzer voneinander abzuschotten.[1]

Neben der Verarbeitung personenbezogener Daten kann der CS-Anbieter u. U. Zugriff auf eine Reihe persönlicher Daten erhalten, die nicht für die Erbringung seiner Dienste notwendig sind. Ziel der Schutzmaßnahmen ist deshalb, die Preisgabe persönlicher Daten von CS-Nutzern untereinander sowie gegenüber dem CS-Anbieter soweit wie möglich zu vermeiden.

Im Rahmen der Nutzung eines CS-Fahrzeugs können neben den vom Fahrzeug gemessenen und verarbeiteten Daten auch Daten verarbeitet werden, die der Nutzer selbst einbringt, wie bspw. Fahrtziele oder das Übertragen des Telefonbuchs seines Mobiltelefons zur bequemeren Nutzung der fahrzeugeigenen Freisprecheinrichtung.

Im Rahmen des Anwendungsfalls „Car-Sharing“ werden die folgenden Daten betrachtet:

- Übertragung von eigenen Daten, bspw. aus Handy (Kontakte, Audio-/Video-Daten, Playlist, etc.)
- im Auto generierte „Fahrtdaten“, bspw. Fahrtrouten (Ort, Zeit), Fahrverhalten, etc.
- Daten zur Buchung (Buchungsnummer, Dauer und Zeitpunkt der Nutzung, wann, wie lange, Tarif, etc.)
- technische Daten von Geräten des Nutzers, bspw. MAC-Adresse, BT-Adresse, Handy-Modell, etc.
- Daten zu Fahrzeuginsassen, bspw. Fahrerprofil, Anzahl Personen, physiologische Daten

Im Folgenden wird dargestellt, wie der Anwendungsfall „Car-Sharing“ mit Hilfe der Schutzmaßnahmen aus Abschnitt 4 datenschutzfreundlich gestaltet werden kann. In Abbildung 5.1 ist der Ablauf von der Buchung bis zum Abmelden zusammengefasst.

In diesem Anwendungsfall wird davon ausgegangen, dass der Nutzer bereits Kunde des Car-Sharing-Anbieters ist und weiterhin in der Lage ist, sich als Kunde gegenüber dem CS-Anbieter zu legitimieren, ohne seine Identität preiszugeben (etwa in der Weise, in der eine Person sich mit einer Eintrittskarte zu einer Veranstaltung als berechtigter Besucher

[1] Das Bundesdatenschutzgesetz findet gem. § 1 Abs. 2 Nr. 3 2. Halbsatz BDSG keine Anwendung, wenn Daten im familiären und persönlichen Bereich preisgegeben werden. Die Frage nach dem familiären und persönlichen Bereich richtet sich nach der Verkehrsanschauung. Ist der Zweck der Preisgabe objektiv als familiär bzw. persönlich erkennbar, so findet das Bundesdatenschutzgesetz *keine* Anwendung. Dies trifft auch dann zu, wenn die Daten von mehreren Personen genutzt werden, sofern diese Personen dem familiären bzw. persönlichen Kreis zuzurechnen sind [18, § 1 Rdnr. 30–32], [19, § 1 Rdnr. 29, 31], [20, § 1 Rdnr. 2, 21].

Nr.	Funktion	Übermittelte Daten → CS-A	Antwort → Fzg. / Handy	Maßnahme
(1)	Login CS-Anbieter	Anonyme Anmeldung	Transaktions-pseudonym π	Anonyme Authentifizierung als „Kunde bei CS-A“ ⇒ Transaktionspseudonym π
(2)	Fzg. lokalisieren	π, $Anon_{loc}(upos)$	Liste von Fzg.-IDs + Standorte	Datenanonymisierung: Vergröbern des Nutzerstandorts $upos$ auf Planquadrat
(3)	Fzg. reservieren	π, Fzg.-ID (aus Fahrzeugliste)	Reservierungs-bestätigung	—
(4)	Fzg. buchen	π, Fzg.-Kennung F (vor Ort von Fahrzeug), Reservierungsbestätigung, Buchungszeitraum t	Buchungs-bestätigung, Vollzugriffs-berechtigung für F $Perm(\pi, t, F)$	Autorisierung: Berechtigung $Perm(\pi, t, F)$ ausstellen
(5)	Fzg. öffnen	$Perm(\pi, t, F)$	—	Zugriffskontrolle: Berechtigung $Perm(\pi, t, F)$ prüfen
(6)	Schadensmeldung	π, Mängelliste	…	—
		⟨ Fahrzeugnutzung ⟩		
(7)	Checkout	π, Fzg.-Standort	…	De-Autorisierung: $Perm(\pi, t, F)$ entziehen, Daten in Fzg. löschen (insbesondere im Fzg. generierte Daten wie Fahrtrouten)

Abbildung 5.1: Anwendungsfall Car-Sharing

ausweist). Im dargestellten Ablauf in Abbildung 5.1 authentifiziert sich der Nutzer U in Schritt (1) als Kunde des Anbieters und erhält ein Transaktionspseudonym π, welches für einen Zeitraum τ (bspw. 24h) gültig ist.

Mit Hilfe von π kann U Positionen von zur Verfügung stehenden Fahrzeugen beim Anbieter abfragen (Schritt (2)), einen Wagen reservieren (3) und anschließend buchen (4). Der Nutzer bekommt auf seine Anfrage (2) hin eine Liste aller freien Fahrzeuge samt deren genauen Standorten geschickt, welche sich im oder um „sein“ Planquadrat herum befinden. Bei der Lokalisierung von Fahrzeugen des CS-Anbieters wird der Standort des Nutzers auf einem Planquadrat verortet, sodass der Anbieter nicht den genauen Standort des Nutzers erfährt.

Der Nutzer wählt anschließend ein Fahrzeug aus der Liste aus und schickt im Schritt (3) eine Reservierungsanfrage an den Anbieter, welche die eindeutige Bezeichnung des Fahrzeugs (Fzg.-ID) und das Transaktionspseudonym π enthält. Nach Prüfung der Gültigkeit von π sowie der Verfügbarkeit des gewählten Fahrzeugs[2] wird dem Kunden eine Reservierungsbestätigung übermittelt. Ein Kunde kann zu einem Zeitpunkt nur ein Fahrzeug reservieren. Durch diese Restriktion wird verhindert, dass ein Kunde nicht alle verfügbaren Fahrzeuge gleichzeitig reserviert, was zu *Denial-of-Service* für alle anderen Kunden im selben Planquadrat führen würde. Weiterhin muss sichergestellt werden, dass der Nutzer U innerhalb eines gewissen Zeitraums immer dasselbe Transaktionspseudonym erhält, da er ansonsten die zuvor beschriebene Beschränkung leicht dadurch umgehen könnte, dass er sich ein neues Pseudonym π' besorgt.

Am Fahrzeug angekommen tritt der Nutzer mit dem Fahrzeug in Kontakt, um dessen lokale Kennung F zu erhalten, die für den Buchungsvorgang benötigt wird (4). Die Buchung selbst enthält dann das Pseudonym π, die Kennung F, die Reservierungsbestätigung und den vom Kunden festgelegten Buchungszeitraum t. Nach erfolgreicher Prüfung der übermittelten Daten stellt der CS-Anbieter eine Berechtigung $Perm(\pi, t, F)$ für die Nutzung des gebuchten Fahrzeugs für den angegebenen Zeitraum aus. Nach der Übermittlung der Berechtigung an den CS-Anbieter und der erfolgreichen Prüfung entriegelt der Anbieter das Fahrzeug (5). An dieser Stelle soll durch Verwendung der lokalen Kennung F si-

[2] Das Fahrzeug könnte zwischenzeitlich von einem anderen Kunden gebucht worden sein.

chergestellt werden, dass der Nutzer in unmittelbarer Nähe des Fahrzeugs sein muss, um F auszulesen und in der Folge $Perm(\pi, t, F)$ zu verwenden. Hierdurch soll erreicht werden, dass Fahrzeuge nicht in Abwesenheit von Nutzern entriegelt werden. Vor Fahrtantritt kann der Nutzer noch evtl. vorhandene Fahrzeugmängel, wie Beulen, Kratzer o. Ä. festhalten und an den Anbieter übermitteln (6). Der Prüfvorgang zum Öffnen (ggf. auch Starten) des Fahrzeugs (Schritt (5)) wird jedes Mal durchgeführt, sodass das Fahrzeug nach Ablauf der Buchungszeit t nicht mehr bewegt werden kann.

Bei der Rückgabe des Fahrzeugs in Schritt (7) wird dem Anbieter der genaue Standort des Fahrzeugs mitgeteilt, sodass dieser das Fahrzeug wieder für Anfragen (Schritt (2)) freigeben kann und U bzw. π das weitere Nutzungsrecht entzogen wird.

Für den dargestellten Ablauf dürften dem CS-Anbieter allerdings zur Abrechnung keine personenbezogenen Zahlungsinformationen, wie bspw. Kreditkartendaten, übermittelt werden, da dies eine De-Anonymisierung zur Folge hätte. Die Zahlung könnte bspw. durch einen Zahlungsdienstleister erfolgen, bei dem die Zahlungsinformationen von U hinterlegt sind und der statt seiner —unter Verwendung von π als Referenz— die Rechnung beim CS-Anbieter begleicht. Alternativ könnten zur Bezahlung auch Adhoc-Bezahlverfahren oder Prepaid-Karten (vgl. zu diesen Verfahren Abschnitt 5.5) sowie fortgeschrittene Zahlungssysteme [21, 22] oder „Krypto-Währungen“ [23] verwendet werden, welche die Anonymität des Kunden garantieren.

Synchronisation

Wie eingangs erwähnt, gibt es im Anwendungsfall „Car-Sharing“ den Aspekt der „Synchronisation“ des Fahrzeugs mit externen Geräten, wie bspw. Mobiltelefonen. Eine Synchronisation kann dabei persönliche Daten des Nutzers umfassen, wie das Übertragen von Telefon-/Adressdaten ins Fahrzeug oder den Abruf von Daten aus dem Fahrzeug. Beide Fälle sind in hohem Maße für den Schutz der Privatsphäre von CS-Kunden relevant. Abbildung 5.2 stellt einen schematischen Ablauf zum Schutz von im Fahrzeug abgelegten persönlichen Daten dar.

Nr.	Funktion	Übermittelte Daten → Fzg.	Antwort	Maßnahme
(1)	BT-Pairing	BT_ADDR, …	$\langle Key \rangle$	BT_ADDR und andere Geräte-IDs müssen nach *Checkout* (s. Abbildung 5.1) gelöscht werden
(2)	Datenschutzprofil übertragen	Profil	—	Lokale Verarbeitung: Profil von lokalem Gerät laden, statt vom OEM
(3)			⟨ Schlüssel SK_i festlegen/aushandeln ⟩	
(4)	Daten synchronisieren	—	—	Verschlüsselung: Daten als verschlüsselte Container $Enc_{SK_i}(\cdot)$ übertragen, zusammen mit Schlüssel SK_i
		$Enc_{SK_i}(Playlists)$, $Enc_{SK_i}(Telefonnumern)$, …		
(5)			⟨ Datenzugriff ⟩	
(6)	Fzg. verriegeln	Schließen-Kommando	—	SK_i wird bei jedem Verlassen des Fahrzeugs aus dem internen Speicher des Fzg. gelöscht
(7)	Fzg. entriegeln	Öffnen-Kommando, SK_i	—	SK_i wird bei jedem Öffnen des Fahrzeugs (nach initialem BT-Pairing) neu übertragen
(8)			⟨ Datenzugriff ⟩	
			…	

Abbildung 5.2: Anwendungsfall Car-Sharing-Synchronisation

In Schritt 1 wird eine Bluetooth-Verbindung zwischen Fahrzeug und —beispielhaft— einem Mobiltelefon (oder einem ähnlichen Bluetooth-fähigen Endgerät) hergestellt. Im Rahmen der Etablierung der Verbindung —dem sogenannten *Pairing*— überträgt das Endgerät seine weltweit eindeutige Bluetooth-Kennung (BT_ADDR) an das Fahrzeug, sodass Fahrzeug und Gerät sich bei erneutem Kontakt wiedererkennen können. Auf Grund der eindeutigen Kennung und der Zuorden-

barkeit zu einer Person[3] stellt die BT_ADDR ein Langzeitpseudonym dar, das einen Personenbezug leicht ermöglicht. In diesem Sinne darf die BT_ADDR auch nicht mit der realen Identität des Nutzers verknüpft werden, die dem CS-Anbieter bekannt sein könnte. Selbst wenn Letzteres nicht der Fall ist, weil wie im zuvor beschriebenen Anwendungsfall auch die Abrechnung anonym gegenüber dem CS-Anbieter erfolgt, wäre die Speicherung der BT_ADDR problematisch, da auf Grund der Wiedererkennbarkeit der Adresse die beschriebenen Maßnahmen zur Anonymisierung ins Leere laufen würden. Aus diesem Grund muss die Adresse aus dem Fahrzeug gelöscht werden, sobald die Nutzung beendet ist.

Im nächsten Schritt (2) wird das Datenschutzprofil in das Fahrzeug übertragen. Das Profil soll die individuellen Einstellungen zum Schutz der Privatsphäre des Kunden enthalten und durch eine entsprechende Komponente im Fahrzeug gelesen und umgesetzt werden — die zuvor erwähnte Anweisung zur Löschung der BT_Adresse könnte bspw. auch Teil dieser Konfiguration sein.

Der Schritt (3) dient dazu, einen Schlüssel SK_i zu bestimmen, der zur Verschlüsselung von in das Fahrzeug übertragene Daten verwendet werden soll. Persönliche Daten, wie bspw. Telefonnummern & Adressen oder Playlisten für Musikstücke, werden —mit SK_i verschlüsselt— in Form von Containern in das Fahrzeug übertragen und können dort bis zum Ende der Nutzung verbleiben. Für die Systeme/Komponenten im Fahrzeug, die auf die übertragenen Daten Zugriff erhalten sollen (5), werden die Daten durch eine transparente zentrale Schlüsselverwaltungskomponente (u. a. Komponente „Kryptographischer Schlüsselspeicher“, siehe Abbildung 2.4) entschlüsselt, sodass die Anwendungen zum Lesen oder Schreiben der Daten keine eigene Ent-/Verschlüsselungsfunktionalität oder eine eigene Schlüsselverwaltung implementieren müssen.

Verriegelt der Nutzer das Fahrzeug (6), wird der Schlüssel SK_i aus dem „Kryptographischen Schlüsselspeicher“ gelöscht, sodass niemand, der sich Zugang zum Fahrzeug verschaffen würde, Zugriff auf den Schlüssel bzw. die damit verschlüsselten Daten erhalten könnte. Ein positiver Nebeneffekt dieses Vorgehens ist, dass die im Fahrzeug gespeicherten Daten nach der Fahrzeugnutzung —sozusagen nach dem letzten Verriegeln eines Nutzers— nicht explizit durch den Nutzer gelöscht werden müssen, da sie für den nächsten Nutzer —mangels Schlüssel— ohnehin nicht lesbar sind. Daten können dann im Nachgang einfach vom System bei Bedarf gelöscht werden.

Kehrt der Nutzer für seine nächste Fahrt zum Fahrzeug zurück, überträgt sein BT-Gerät den Schlüssel SK_i ins Fahrzeug (7) und gibt dadurch die Daten des Nutzers für die Fahrzeugkomponenten wieder frei (8).

5.1.2 Werkstatt

In einer Kfz-Werkstatt können Fahrzeugdaten hilfreich sein, um Fehler und Probleme mit dem Fahrzeug leichter zu diagnostizieren. Daten sollten aber auch zu diesem Zweck nicht ohne Wissen und explizite Erlaubnis/Einwilligung des Fahrers auslesbar sein. Andernfalls könnte jeder, der sich Zutritt zum Fahrzeug verschafft, die entsprechenden Daten auslesen. Aus diesem Grund wird im folgenden Anwendungsfall „Werkstatt“ eine vom Nutzer ausgehende Autorisierung für den Zugriff der Daten vorgeschlagen. Der schematische Ablauf dieses Anwendungsfall ist in Abbildung 5.3 dargestellt.

Nr.	Funktion	Übermittelte Daten → Fzg.	Antwort	Maßnahme
(1)	⟨ Nutzer U authentifiziert sich ⟩			
(2)	Autorisation von Werkstatt W durch Nutzer U für Zeitraum t bzgl. vordefiniertem oder festgelegtem Datenset D	Autorisierungs-Kommando	$Perm(W, t, D)$	Autorisierung: Berechtigung $Perm(W, t, D)$ erteilen
(3)	⟨ Werkstatt W authentifiziert sich ⟩			
(4)	Auslesen von D durch W	Datenabfrage, $Perm(W, t, D)$	Datenset D	Zugriffskontrolle: $Perm(W, t, D)$ prüfen

Abbildung 5.3: Anwendungsfall Werkstatt

Der hier verfolgte Ansatz soll dem Nutzer erlauben, prinzipiell beliebige zur Verfügung stehende Daten des Fahrzeugs für Dritte zugänglich zu machen und dies auch wieder abstellen zu können. Es erscheint jedoch auf Grund der schieren

[3] Dies gilt unter der Annahme, dass das BT-Gerät stets von derselben Person genutzt wird.

Masse an Datenarten wenig sinnvoll, dem Nutzer alle Daten für die Auswahl zu präsentieren und ihn für jedes einzelne Datum eine Autorisierung ausstellen zu lassen. Zur Vereinfachung kann eine Vordefinition von Datensets D sinnvoll sein, die jeweils eine Menge von Daten für einen bestimmten Anwendungsfall —wie hier „Werkstatt“— umfassen können. Für die Bereitstellung der Daten, genauer der Autorisierung hierfür, ist es erforderlich, dass der Nutzer sich gegenüber dem Bordsystem authentifiziert (1), etwa durch ein Passwort, eine PIN oder ein Hardware-Token o. Ä. — der Fahrzeugschlüssel erscheint jedoch für den Werkstattfall als Authentifizierungs-Token für *den Nutzer* ungeeignet, da der Schlüssel für eine Reparatur i. d. R. in der Werkstatt verbleibt und jeder Werkstattangestellte sich so als *der Nutzer* ausgeben könnte. Für die Autorisierung spezifiziert der Nutzer eine Identität der Werkstatt W, welche durch ein wählbares oder vorgegebenes Authentifizierungsverfahren vom Fahrzeug überprüft werden kann, das Datenset D, auf welches die Werkstatt Zugriff erhalten soll, und schließlich den Zeitraum t für die Dauer der Reparatur (2).

In Schritt (3) authentifiziert sich die Werkstatt bzw. einer ihrer Mitarbeiter mit der zuvor festgelegten Identität W, sodass das Fahrzeug in Schritt (4) feststellen kann, dass die Zugriffsberechtigung $Perm(W, t, D)$ für den Mitarbeiter erteilt wurde. Im Falle einer zentralen Zugriffskontrolle (vgl. Abschnitt 4.4) muss das Autorisierungstoken nicht übertragen werden, da $Perm(W, t, D)$ in diesem Fall im Fahrzeug gespeichert ist und durch Zuordnung der zugriffsberechtigten und authentifizierten Identität W, der Zugriff auf die Daten D —innerhalb des Zeitraums t— gestattet werden kann.

Bei der Übermittlung von (Teilen des) Datenset D bspw. an den OEM, um Fehlerfälle diagnostizieren zu lassen, ist zu beachten, dass dies nur erfolgen kann, wenn die Daten aus D bereits anonymisiert sind bzw. nur in anonymisierter Form an den OEM übermittelt werden oder der Nutzer zuvor für diesen Zweck seine explizite Einwilligung erteilt hat.

5.2 Location-based Services

Der Anwendungsfall „Location-based Services“ fasst verschiedene Unterfälle zusammen, in denen auf die Übermittlung einer Position des Fahrzeugs hin eine Aktion (bspw. Bereitstellung von Informationen durch einen Dienst) ausgelöst wird. Dabei können die folgenden Daten übermittelt werden:

- Fahrzeugposition
- Identität (Pseudonym oder Identität) oder Anonymität
- Dienstparameter

Es werden im Folgenden zwei Anwendungsfälle unterschieden:

1. Point of Interest (POI): Der Nutzer übermittelt seine Position an einen Dienst, um Informationen zu POIs nach vordefinierten Kriterien in seiner Umgebung oder auf einer Fahrtroute zu erhalten.
2. Dienstintegration: Ein vom Nutzer verwendeter Dienst erfragt die Position des Fahrzeugs, um daraufhin Aktionen einzuleiten (bspw. Schließen eines Garagentores) oder um kategorische Informationen zu bekommen (bspw. „Fahrzeug befindet sich innerhalb eines bestimmten Bereiches“).

Beide Unterfälle werden im Folgenden gesondert behandelt.

Anwendung für POIs

Der Ablauf der Datenübermittlung ist in Abbildung 5.4 dargestellt. Um für eine bestimmte Position Informationen von einem Dienst zu bekommen, muss sich der Nutzer zunächst bei dem entsprechenden Dienst einloggen (Schritt (1)). Bei der Anmeldung werden anonyme Credentials verwendet, sodass der Dienst nicht weiß, mit welchem seiner Nutzer er kommuniziert, sondern nur, dass es sich um einen legitimen Nutzer handelt. Der Dienst erstellt daraufhin ein Transaktionspseudonym π für den Nutzer, das in der folgenden Interaktion verwendet wird. In Schritt (2) übermittelt der Nutzer seine derzeitige Position oder eine Position auf einer geplanten Route in anonymisierter Form. Die Anonymisierung führt dazu, dass der Dienstanbieter nur einen Positionsbereich $Area$, nicht jedoch die exakte Position loc des Nutzers erhält. Dies setzt eine vorausgegangenen Anonymisierung der exakten Position zum Positionsbereich $Area = Anon_{pos}(loc)$ im Fahrzeug voraus. Zusätzlich zur anonymisierten Position übermittelt der Nutzer das Transaktionpseudonym π sowie Suchkriterien K, die die Art der gewünschten Informationen (bspw. Restaurantkette, Geo-Caching, etc.) spezifizieren. In Schritt (3) antwortet der Dienstanbieter mit relevanten Orten POI für den Positionsbereich $Area$. Das Der Nutzer (bzw. das Fahrzeug selbst oder ein Nutzergerät wie bspw. Smartphone) filtert anschließend die Menge der erhaltenen Orte, die sich auf die verallgemeinerte Position $Area$ beziehen, im Hinblick auf seine exakte Position loc. Er erhält damit die für ihn relevanten Orte, ohne dass der Dienstanbieter diese kennt.

Nr.	Funktion	Übermittelte Daten → Dienst	Antwort	Maßnahme
(1)	Login bei Service-Anbieter	Anonyme Anmeldung	Transaktionspseudonym π	Verwendung anonymer Credentials
(2)	Übermittlung einer anonymisierten Position $Area = Anon_{pos}(loc)$	$Area$, Suchkriterien K, π	POI für Positionsbereich	Standortvergröberung: $Area$ = Positionsbereich
(3)	Suche nach relevanten POIs für exakte Nutzerposition loc	—	—	Lokale Verarbeitung

Abbildung 5.4: Anwendungsfall POI für ortsbezogene Dienste

Anwendung für Integration weiterer Dienste

Im Fall einer Integration eines weiteren Dienstes in Positionsanfragen wird die Fahrzeugposition durch einen anderen Dienst oder den Nutzer selbst verwendet. Dabei wird die Lokalisierung des Fahrzeugs von einer externen Person (bspw. zur Suche des geparkten Fahrzeugs) oder einem externen System bspw. einem Heimautomatisierungssystem) initiiert, um je nach Position bestimmten Aktionen einzuleiten (bei einem Heimautomatisierungssystem bspw. das Öffnen oder Schließen eines Tores).

Zu Beginn muss der Nutzer bei einem Dienst S (bspw. ein Heimautomatisierungssystem oder eine App zur Lokalisierung des geparkten oder fahrenden Fahrzeugs) registriert sein und dort entsprechende Parameter und Einschränkungen für bestimmte Aktionen eingegeben haben. Für die Positionsabfrage sind nun zwei Szenarien denkbar:

In *Szenario 1* erfragt der Dienst die Fahrzeugposition, weil diese Information selbst relevant ist. Die Abfrage wird über den OEM geleitet, aber Ende-zu-Ende-verschlüsselt zwischen Dienst und Fahrzeug verschlüsselt. Das Fahrzeug antwortet durch Mitteilung der ebenfalls verschlüsselten Position an den Dienst.

In *Szenario 2* ist die Fahrzeugposition selbst nicht wichtig, aber zur Bereitstellung einer gewünschten Information von Bedeutung, die von der Position und speziellen Vorgaben abhängt (bspw. kann das Einfahrtstor geschlossen werden, sofern sich das Fahrzeug auf dem Grundstück befindet). In diesem Fall kann anstelle der Positionsabfrage eine Anzahl von Parametern P vom Dienst an das Fahrzeug übermittelt werden. Diese enthalten eine Anzahl von Bedingungen und möglichen Antworten in Abhängigkeit von der Position des Fahrzeugs. So kann ein Heimautomatisierungssystem erfragen, ob das Einfahrtstor geschlossen werden kann und zwei Antwortmöglichkeiten in Abhängigkeit von der Position des Fahrzeugs vorgeben. Die Übermittlung dieser Parameter erfolgt auch hier verschlüsselt und wird über den OEM geleitet. Im Fahrzeug wird die Position ermittelt und die Antwort entsprechend der Parameter lokal ermittelt. Das Fahrzeug übermittelt anschließend nur die Antwort A (bspw. JA oder NEIN), ohne die Position selbst zu übermitteln.

Nr.	Funktion	Übermittelte Daten → Fzg.	Antwort	Maßnahme
		⟨ Szenario (1): Dienst S erfragt Position ⟩		
(1)	Abfrage der Fzg.-Position durch S	für Fzg. verschlüsselte Positionsanfrage (über OEM)	$Enc_{PK_U}(Pos)$ — von Fzg. für U verschlüsselte Positionsangabe	E2E-Verschlüsselung
		⟨ Szenario (2): Lokale Verarbeitung im Fahrzeug ⟩		
(2)	Abfrage anhand von verschiedenen Parametern P durch S	für Fzg. verschlüsselte Parameter P (über OEM)	$Enc_{PK_H}(P)$ — von Fzg. für D verschlüsselte Antwort A	E2E-Verschlüsselung, lokale Verarbeitung

Abbildung 5.5: Anwendungsfall Heimautomatisierung für ortsbezogene Dienste

5.3 Smartphone Integration / Drittanbieter-Erweiterungen

5.3.1 Android Auto

Im Anwendungsfall „*Android Auto*“ wird ein mobiles Endgerät (Engl. Mobile Device, MD) mit einem Fahrzeug gekoppelt, sodass die Bedienoberfläche des MD auf dem fahrzeugeigenen Bildschirm gespiegelt wird und die Bedienung der Oberfläche bzw. App über fahrzeugeigene Bedienelemente (Touchscreen, Scrollräder, Wippen, etc.) oder Sprachsteuerung erfolgen kann. Voraussetzung hierfür ist, dass das MD unter dem mobilen Betriebssystem Android läuft, die zu nutzende App mit *Android Auto* kompatibel ist und das Fahrzeug selbst *Android Auto* unterstützt.

Nr.	Funktion	Übermittelte Daten → Fzg.	Antwort	Maßnahme
(1)	⟨ Nutzer U authentifiziert sich ⟩			
(2)	Autorisation von Mobilgerät MD durch Nutzer U für Zeitraum t bzgl. Daten D	Autorisierungs-Kommando	$Perm(MD, t, D)$	Autorisierung: Berechtigung $Perm(MD, t, D)$ erteilen (zur internen Verwendung)
		Übermittelte Daten → MD		
(3)	Fzg. übermittelt Daten D	D	—	Vertrauenswürdiges, externes Gerät

Abbildung 5.6: Anwendungsfall *Android Auto*

Android Auto ist zurzeit (Januar 2017) selbst eine App, welche die Interaktion der kompatiblen Apps mit dem Fahrzeug übernimmt. Fahrzeugdaten werden ohne Unterstützung des Fahrzeugherstellers (OEM) jedoch nicht ohne Weiteres an das MD geliefert. Mit Hilfe von Bluetooth-Adaptern für den OBD-Anschluss (Engl. *On Board Diagnose*) können jedoch Fahrzeugdaten bereits von Apps wie bspw. Torque[4] ausgelesen werden — Torque selbst ist allerdings (aktuell) nicht für *Android Auto* verfügbar. Fahrzeughersteller wie bspw. Honda und Hyundai arbeiten jedoch laut AndroidCentral[5] bereits an eigenen Apps für *Android Auto*, um darin Fahrzeugdaten zu nutzen.

Unabhängig davon, ob Fahrzeugdaten direkt über *Android Auto* oder über eine OBD-Schnittstelle in das MD übertragen werden, sollte der Nutzer hierfür den Datentransfer aus dem Fahrzeug *zuvor* autorisieren. Das grundsätzliche Vorgehen entspricht hier dem für die Autorisierung im Anwendungsfall „Werkstatt“ (vgl. Abschnitt 5.1.2) und ist in Abbildung 5.6

[4] `https://play.google.com/store/apps/details?id=org.prowl.torque`
[5] `http://www.androidcentral.com/android-auto-upshifts-it-starts-hit-its-cruising-speed`

für den Anwendungsfall „*Android Auto*“ dargestellt.

Persönliche Daten, die auf dem Smartphone gespeichert sind und im Auto genutzt werden sollen (wie bspw. Playlisten oder Kontakte, vgl. den Anwendungsfall „Synchronisation“ in Abschnitt 5.1.1) müssen nicht mehr „aus der Hand gegeben“ werden, da die komplette Funktionalität auf dem Smartphone verbleibt und eine Übertragung ins Fahrzeug nicht notwendig ist. Das Problem der Löschung von synchronisierten Daten (siehe Abschnitt 5.1.1) besteht insofern nicht mehr. Auf der einen Seite können, abhängig von den innerhalb von *Android Auto* genutzten Apps, unter Umständen Daten, die während der Fahrt anfallen, mit dem ggf. vorhandenen Google-Konto[6] des MD-Nutzers verknüpft werden. Auf der anderen Seite sehen viele Nutzer ihr MD, bspw. ihr Mobiltelefon, als vertrauenswürdig an, da sie ihm ohnehin eine Reihe persönlicher Daten, wie Kontakte oder Fotos, bereits anvertrauen. Hinsichtlich einer möglichen Personalisierung von Daten aus dem Fahrzeug wird es darauf ankommen, in welcher Form die Daten abrufbar gemacht werden und ob die datenverarbeitende Stelle, sei es der App-Hersteller, Google (als Hersteller von Android bzw. *Android Auto*) oder der Fahrzeughersteller, die möglicherweise anonymen Daten mit Hilfe von Kontoinformationen des Nutzers personalisieren wird, was dann in jedem Fall eine vorhergehende Einwilligung des Nutzers erforderlich machen würde.

5.3.2 Paket-Auto

Für den Anwendungsfall „Paket-Auto“ soll der Nutzer die Möglichkeit haben, Paketdienstleistern (oder anderen Dritten) den Zugang zum Kofferraum seines Fahrzeugs zu ermöglichen, sodass diese darin ein Paket für den Nutzer deponieren können. Die Idee ähnelt der von Paketkästen für Wohnhäuser, wie sie bspw. der Paketdienstleister DHL anbietet[7], die im Prinzip ein „Briefkasten“ für Pakete sind und eine Auslieferung von Paketen auch bei Abwesenheit des Empfängers ermöglichen. Im Unterschied zu einem Paketkasten, wie ihn DHL anbietet, hat ein Paketdienstleister „von Haus aus“ keinen Zugriff auf den Fahrzeugkofferraum des Nutzers. Weiterhin ist für die Auslieferung, der Standort des Fahrzeugs i. d. R. im Vorfeld nicht exakt vorherzusehen. Aus diesem Grund bedarf es für ein Auto mit Depotfunktion einer vorherigen Autorisierung des Paketboten zum Öffnen des Kofferraums sowie die Möglichkeit, den aktuellen Standort des Fahrzeugs, d. h. den Lieferort, zum Lieferzeitraum bestimmen zu können. Der technische Ablauf von der Nutzeranmeldung beim Paketdienst bis zur Auslieferung des Pakets ist in Abbildung 5.7 schematisch dargestellt.

In Schritt (1) registriert sich der Nutzer namentlich beim Paketdienstanbieter PD, sodass dieser an den Nutzer adressierte Pakete zuordnen kann. Anschließend (oder zu einem späteren Zeitpunkt nach entsprechender Authentifizierung) übermittelt der Nutzer an PD die eindeutige Nummer des Pakets PNr, welches er in sein Auto geliefert haben möchte, sowie den groben, voraussichtlichen Standort des Wagens im Lieferzeitraum — Schritt (2). Im Zuge dessen erhält er von PD einen kryptografischen öffentlichen Schlüssel PK_{PD}, der im Weiteren als Identität des Dienstes fungiert. Besitzt der Paketdienstleister nur eine Identität in Form von PK_{PD}, nutzen alle Paketboten dieselbe Identität, was bedeutet, dass grundsätzlich jeder Bote des PD den Kofferraum eines Nutzers im Rahmen des Lieferorts/-zeitraums öffnen kann. Alternativ kann die Identität auch in Abhängigkeit von PNr gewählt und nur dem Boten des entsprechenden Pakets zur Verfügung gestellt werden, sodass nur dieser Zugang zum Kofferraum erhält.

Um dem Paketboten den Zugang zu ermöglichen, stellt der Nutzer eine entsprechende Berechtigung für die Identität des Boten bzw. Paketdienstes aus (4), nachdem er sich zuvor selbst gegenüber dem Fahrzeug authentifiziert hat. Die Berechtigung $Perm(PK_{PD}, t, K)$ zum Öffnen des Kofferraums wird anschließend beim Fahrzeughersteller hinterlegt (5), sodass der Paketdienst diese dort zu einem späteren Zeitpunkt abrufen kann. Alternativ könnte die Berechtigung auch im Fahrzeug oder beim Paketdienst hinterlegt werden. In beiden Fällen würde dann die alleinige Überprüfung der Berechtigung im Fahrzeug vorgenommen und das Fahrzeug würde den Kofferraum „autonom“ öffnen — hierfür würde sich der in Abbildung 5.7 gezeigte Ablauf im Schritt 8 insofern ändern, dass die Schließrechte nicht mehr erfragt werden müssten, da sie im Fahrzeug gespeichert bzw. dem PD bereits bekannt wären.

Dem Paketdienstleister wurde in Schritt (2) der grobe Standort des Fahrzeugs bereits mitgeteilt, sodass das Paket (mindestens) im Auslieferungszentrum der richtigen Region bzw. Stadt vorliegt. Um die genaue Position des Fahrzeugs zu erhalten, meldet sich der Paketbote beim Fahrzeughersteller (6), um die Position des Fahrzeugs abzufragen (7). Der Fahrzeughersteller fragt daraufhin die Position des Fahrzeugs beim Fahrzeug selbst an. Das Fahrzeug hat in Schritt (3) die Identität des Paketdienstes/Boten erhalten und verschlüsselt damit die Position des Fahrzeugs sowie Merkmale FD zum leichteren Auffinden des Fahrzeugs (wie bspw. Kennzeichen, Farbe und Modell des Wagens) für den Paketdienst. Durch die Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) werden die zuvor genannten Daten ausschließlich dem Datenempfänger —hier der Paketdienst— zugänglich gemacht und keinem Dritten, wie bspw. dem OEM, der diese Informationen für die Vermittlung der Daten nicht benötigt. Mit Hilfe der zurückgelieferten Daten ist der Bote schließlich

[6] Ein Konto bei Google ist eine Voraussetzung, um Apps für Android, wie bspw. *Android Auto*, aus dem Google-eigenen App-Store heraus zu installieren.

[7] `https://www.dhl.de/de/privatkunden/pakete-empfangen/pakete-zuhause-empfangen/paketkasten.html`

Nr.	Funktion	Übermittelte Daten → PD	Antwort	Maßnahme
(1)			⟨ Nutzer U registriert sich ⟩	
(2)	Paketnummer PNr, Lieferort Loc und Zeitraum t festlegen	PNr, Loc, t	öffentlicher Schlüssel PK_{PD} des Paketdienstes PD (ggf. in Abhängigkeit von PNr)	Standortvergröberung: Loc = Planquadrat (bspw. PLZ-Bereich)
		Übermittelte Daten → Fzg.		
(3)			⟨ Nutzer U authentifiziert sich ⟩	
(4)	Autorisation von Paketdienst PK_{PD} durch Nutzer U für Zeitraum t bzgl. Schließrecht K	Autorisierungs-Kommando, PK_{PD}, t, K	$Perm(PK_{PD}, t, K)$	Autorisierung: Berechtigung $Perm(PK_{PD}, t, K)$ ausstellen
		Übermittelte Daten → OEM		
(5)	U hinterlegt Autorisierung seinen Kofferraum K zu öffnen	— $Perm(PK_{PD}, t, K)$		Autorisierung: Berechtigung $Perm(PK_{PD}, t, K)$ erteilen
(6)			⟨ Bote authentifiziert sich gegenüber OEM mittels PK_{PD} ⟩	
(7)	Abfrage der Fzg.-Position von U durch Bote von Paketdienst PD	Positionsanfrage für Fzg.	$Enc_{PK_{PD}}(Pos, FD)$ — von Fzg. für PD verschlüsselte Positionsangabe Pos sowie Fahrzeugdaten FD	E2E-Verschlüsselung
(8)	Anfrage Schließrechte	Berechtigungsanfrage für Fzg.-Kennung (vor Ort von Fahrzeug)	$Enc_{PK_{PD}}(perm)$ — von Fzg. für PD verschlüsselte Schließberechtigung $perm := Perm(PK_{PD}, t, K)$	E2E-Verschlüsselung
		Übermittelte Daten → Fzg.		
(9)	Bote schickt Öffnen-Kommando	Öffnen-Kommando, $Perm(PK_{PD}, t, K)$	—	Zugriffskontrolle
(10)	⟨ Kofferraum schließen ⟩	—	Benachrichtigung (für U)	De-Autorisierung: $Perm(PK_{PD}, t, K)$ entziehen ⇒ Fzg. sperrt $perm$ bis t vorüber ist

Abbildung 5.7: Anwendungsfall Paketauto

in der Lage, das Fahrzeug zu lokalisieren.

Am Fahrzeug angekommen, erfragt der Bote die Schließrechte für den Fahrzeugkofferraum K (8). Zum Nachweis, dass er an Ort und Stelle beim Fahrzeug ist, sendet er eine Fahrzeugkennung an den Hersteller, welche nur vor Ort am Fahrzeug, bspw. per NFC, auslesbar ist. Gehört die Fahrzeugkennung zum Wagen des Nutzers, antwortet der Hersteller mit der zuvor vom Nutzer erteilten Schließberechtigung, die für den Paketdienstleister PD verschlüsselt wird. Auf diese Weise kann nur ein berechtigter Mitarbeiter des Paketdiensts die Schließrechte nutzen. Alternativ könnte an dieser Stelle der OEM den Kofferraum per „Fernsteuerung“ öffnen, da ihm die in Schritt (5) erteilte Genehmigung des Nutzers für PD bereits vorliegt — in diesem Fall könnte Schritt (9) entfallen.

In Schritt (9) übermittelt der Bote die entschlüsselte Schließberechtigung zusammen mit einem Nachweis seiner Identität PK_{PD} — letzteres kann durch einen vorgeschalteten Authentifizierungsschritt oder ggf. durch eine Signatur mit dem zu PK_{PD} gehörigen privaten Schlüssel erfolgen. Das Fahrzeug prüft dann die Identität sowie die Schließberechtigung und öffnet bei erfolgreicher Prüfung den Kofferraum.

Sobald der Bote den Kofferraum geschlossen hat, kann das Fahrzeug evtl. den Nutzer über die erfolgte Lieferung (via OEM) informieren und die Schließberechtigung bis zu deren Ablaufdatum sperren (10), sodass der Wagen nicht noch einmal mit derselben Berechtigung geöffnet werden kann.

5.4 Statistische Analysen

5.4.1 Umgebung

Durch verschiedene Fahrzeugsensoren werden Daten über die Fahrzeugumgebung gesammelt und anschließend an einen Dienst (OEM oder anderer Drittanbieter) übermittelt. Die Übermittlung kann die folgenden Daten enthalten:

- Freie Parkplätze
- Gefahrenstellen
- Verkehrsschilder
- Fahrbahnmarkierungen
- Verkehrsflussinformationen
- Wetterdaten

Im Folgenden wird der konkrete Anwendungsfall von Daten über Parkplätze betrachtet. Dabei werden auf bestimmte Trigger hin (bspw. bei Unterschreiten einer bestimmten Geschwindigkeit in städtischen Gebieten) automatisch Sensoren zur Registrierung von freien Parkplätzen aktiviert. So können freie Parkplätze erfasst und auch Daten zur Art des Parkplatzes gesammelt werden. In Abbildung 5.8 ist der Ablauf der Datenübermittlung samt den entsprechenden Schutzmaßnahmen dargestellt. Zu Beginn muss das Fahrzeug mit einer Konfiguration zur Datensammlung ausgestattet sein. Es ist davon auszugehen, dass bereits bei der Produktion eine grundsätzliche Konfiguration zur Sammlung von Parkplatzdaten ins Fahrzeug eingebracht wird, die durch unterschiedliche Trigger zu einer lokalen Datensammlung führt. Zur Auslösung des Datensammelauftrags sind unterschiedliche Trigger denkbar:

- Bestimmte geographische Gebiete wie bspw. städtische Gebiete oder speziell zur Sammlung ausgezeichneter Stadtteile, ggf. in Kombination mit Fahrdaten wie bspw. das Unterschreiten einer bestimmten Geschwindigkeit.
- Die Installation eines Dienstes durch den Nutzer, der seinerseits die Datensammlung steuert.
- Direkte Trigger durch den OEM aufgrund von speziellem Informationsbedarf zu einzelnen Gebieten. In diesem Fall ist eine verschlüsselte Kommunikation notwendig, bei der sich der OEM gegenüber dem Fahrzeug mit geeigneten Zertifikaten authentifiziert und zur Beauftragung autorisiert wird.

Die genannten Trigger müssen sich nicht ausschließen: Auch in Folge eines Sammelauftrages durch das Backends oder der Installation eines Dienstes kann die Datensammlung durch Umgebungsdaten als weitere Trigger gesteuert werden. Sobald durch einen Trigger die Sammlung von Parkplatzinformationen ausgelöst wurde (Schritt (1)), sammelt und speichert das Fahrzeug den Ort loc_i, Zeitpunkt t_i und die Art der gefundenen freien Parkplätze P_i (Schritt (2)). Die Übermittlung der Parkplätzen kann auf unterschiedliche Weise erfolgen:

a) Eine Möglichkeit besteht darin, Ort und Parkplatzart exakt zu übermitteln, (Schritt (3)-(a)). Um Rückschlüsse auf die Route und den genauen Aufenthaltsort des Fahrzeugs zu vermeiden, wird der Zeitpunkt der Registrierung des Parkplatzes anonymisiert. Die geschieht durch eine zeitliche Verzögerung der Übermittlung (siehe dazu Abschnitt 4.8).

b) Eine andere Möglichkeit besteht darin, anstelle einer zeitlichen Anonymisierung den Ort der Parkplätze zu anonymisieren (Schritt (3)-(b)). Dabei wird anstelle der exakten Position eine anonymisierte Position $Area = Anon_{loc}(loc_i)$ in Form einer Stadtgebietes $Area$ o. Ä. übermittelt. Sofern dort mehr als ein Parkplatz gefunden wurde, wird zusätzlich die Anzahl an Parkplätzen NR_P übermittelt.

Die an den OEM übermittelten anonymisierten Parkplatzdaten können im letzten Schritt anderen Fahrzeugen zur Verfügung gestellt werden (Schritt (4)). In beiden Formen der Anonymisierung kann als zusätzlicher Schutz für die Übermittlung der Daten an den OEM die Verwendung einer Verschlüsselung sinnvoll sein.

Nr.	Funktion	Übermittelte Daten → Fzg.	Maßnahme
(1)	Datensammelauftrag wird im Fahrzeug durch Trigger T ausgelöst.	Trigger (Umgebungsdaten, Auftrag durch OEM, Dienstinstallation), ggf. kombiniert mit Zertifikat $Cert(T)$	Zertifikat $Cert(T)$
		Übermittelte Daten → OEM	
(2)	Sammlung von Parkplätzen P_i an Position loc_i und Aggregation im Fahrzeug	—	Inhaltliche Anonymisierung durch zeitliche Verzögerung um $t = Anon_t(P_i, loc_i)$ oder lokale Generalisierung $Anon_{loc}(loc_i)$
(3)-(a)	Übermittlung von Parkplatzart P_i mit exakter Position loc_i und anonymisierter Zeit an OEM	$Anon_t(t_i)$, P_i, loc_i	Zeitliche Anonymisierung durch Verzögerung der Übermittlung um $t = Anon_t(P_i, loc_i)$ in Abhängigkeit von den gefundenen Parkplätzen und deren Positionen
(3)-(b)	Übermittlung der Anzahl von Parkplätzen NR_P der in einem Streckenabschnitt bzw. Gebiet $Area$	NR_P, $Anon_{loc}(loc_1, loc_2, ...)$	Positionelle Anonymisierung $Anon_{loc}(loc_i)$ durch Vergröberung des Gebietes

Abbildung 5.8: Übermittlung von Parkplatzdaten

Als zweiter Teil des betrachteten Anwendungsfalles schließt sich der Abruf von Parkplätzen oder die Buchung eines Parkplatzes an. Dabei interagiert das Fahrzeug mit einem Parkplatzanbieter, der entweder selbst Parkplätze zur Verfügung stellt (bspw. kostenpflichtiger Großparkplatz oder Parkhaus) oder lediglich Informationen über freie Parkplätze zur Verfügung stellt. Dieser Teil des Anwendungsfalles ist in Abbildung 5.9 dargestellt.

In einem ersten Schritt meldet sich ein Fahrzeug anonym bei einem Parkplatz-Anbieter an und erhält im Gegenzug ein Transaktionspseudonym π (Schritt (1)). In einem zweiten Schritt kann das Fahrzeug für ein bestimmtes Gebiet $Area$ nach verfügbaren Parkplätzen fragen (Schritt (2)). Der Parkplatzanbieter antwortet darauf mit Informationen über verfügbare Parkplätze.

Sofern ein kostenpflichtiger Parkplatz genutzt werden soll, kann das Fahrzeug eine Buchungsanfrage stellen und die anfallenden Kosten durch eine Bezahlung begleichen. Im Gegenzug erhält es eine Buchungsbestätigung, die gleichzeitig als Autorisierung für die Parkplatznutzung fungiert.

Für die Bezahlung müssen anonyme Bezahlverfahren unter Verwendung von π als Referenz verwendet werden (siehe zu solchen Verfahren Abschnitt 5.1.1), um die Anonymität des Nutzers nicht nachträglich durch Preisgabe seiner Identität beim Bezahlvorgang zu kompromittieren.

Nr.	Funktion	Übermittelte Daten → Parkplatzdienstleister	Antwort	Maßnahme
(1)	Login Parkplatz-Anbieter	Anonyme Anmeldung	Transaktionspseudonym π	Verwendung anonymer Credentials
(2)	Anfrage über verfügbare Parkplatztypen im Gebiet $Area$ für Nutzer π und Zeitraum t	$Area, \pi, t$	Parkplatzangebot (P_i, loc_i, t_i), ggf. mit Nutzungskosten $K_i = K(P_i, loc_i, t_i)$	—
(3)	Reservierungsanfrage zu Parkplatz P_i an Position loc_i für Nutzer π und Zeitraum t	P_i, loc_i, π, t, $Payment(K)$	Buchungsbestätigung $Perm(\pi, P_i, t)$	Anonyme Bezahlung

Abbildung 5.9: Buchen von Parkplätzen

5.4.2 Verschleißanalyse

Im Anwendungsfall „Verschleißanalyse“ werden Daten zu Gebrauch, Abnutzung oder Fehlern einzelner Bauteile oder Sensoren gesammelt und an den OEM oder einen Zulieferer mit dem Ziel der Fehlersuche und Qualitätsverbesserung übermittelt. Die Übermittlung betrifft folgende Daten:

- Steuergerätedaten
- Daten von Außensensoren (bspw. Temperatur)
- Daten von Innenraumsensoren
- Daten von Überwachungssensoren (bspw. Motortemperatur)
- Daten über Bauteile (bspw. Motortyp)

Wie im Fall des Parkdienstes muss eine Konfiguration zur Sammlung von Daten zum Verschleiß bereits im Fahrzeug installiert sein. Diese kann später ggf. durch den OEM modifiziert werden. Die Datenübermittlung selbst wird durch spezielle Trigger ausgelöst. Solche Trigger können sowohl bestimmte Zeitpunkte als auch Außenereignisse oder eine gezielte Abfragen des OEM sein. Der Ablauf der Datenübermittlung und die jeweils verwendeten Schutzmaßnahmen sind in Abbildung 5.10 dargestellt.

In Schritt (1) wird die Datensammlung durch einen Trigger T ausgelöst. Sofern es sich dabei um einen direkten Auftrag des OEM handelt, kann dieser Auftrag durch ein Zertifikat $Cert(T)$ authentifiziert sein. In Schritt (2) werden die Daten D im Fahrzeug entsprechend dem Sammelauftrag gesammelt. Die Daten werden noch vor der Übermittlung im Fahrzeug anonymisiert. Für jedes Datenset D muss eine passende Anonymisierungsstrategie gewählt werden, die sich nach Umfang der Daten, Anzahl und Ausprägung der gesammelten Datentypen, deren Verteilung sowie nach Dauer der Datensammlung und Nutzungszweck der Daten richtet (siehe für Einzelheiten Abschnitt 4.8). Eine solche Anonymisierung im Fahrzeug ist möglich, da die übermittelten Daten von einer Vielzahl von Fahrzeugen gesammelt werden und die Auswertung auf statistischer Basis erfolgen soll. Gezielte Datenabfrage von einem bestimmten Fahrzeug ist dabei nicht vorgesehen (siehe hierzu Abschnitt 5.1.2). Um die Anonymisierung der Daten zu gewährleisten, dürfen die anonymisierten Daten nicht mit nicht-anonymisierten Daten oder einem anderen anonymisierten Datenset D' zusammen übermittelt werden, da sonst durch Analyse und Korrelationsbildung zusätzliches Wissen aus den anonymisierten Daten gewonnen werden kann, das zu einer Identifikation des Fahrzeugs oder zur Enthüllung sensibler Attribute des Fahrers führen könnte (siehe Abschnitt 4.8). In Schritt (3) werden die anonymisierten Daten übermittelt. Als zusätzlicher Schutz wird eine Ende-zu-Ende-Verschlüsselung verwendet.

Nr.	Funktion	Übermittelte Daten → Fzg.	Maßnahme
(1)	Datensammelauftrag wird im Fahrzeug durch Trigger T ausgelöst.	Trigger (Umgebungsdaten, Auftrag durch OEM, Zeitintervall), ggf. kombiniert mit Zertifikat $Cert(T)$	Zertifikat $Cert(T)$
		Übermittelte Daten → OEM	
(2)	Sammlung und Aggregation der Daten D im Fahrzeug	—	Inhaltliche Datenanonymisierung $Anon(D)$ nach vordefinierter Anonymisierungsstrategie in Abhängigkeit des Datensets D
(3)	Datenübermittlung	$Enc_{PK_{OEM}}(Anon(D))$	E2E-Verschlüsselung

Abbildung 5.10: Verschleißanalyse

5.5 Elektromobilität

Elektrofahrzeuge nutzen öffentliche Ladestationen (Engl. *Charge Point*, CP), um ihre Fahrzeugbatterien wieder aufzuladen. Diese Stationen, im Folgenden auch Ladesäulen genannt, werden von speziellen Firmen (Engl. *Charge Point Operator*, CPO) betrieben. Ladestationsbetreiber können für die Abrechnung ihrer Kunden wiederum Verträge mit ein oder mehr Abrechnungsstellen (Engl. *Clearing House*, CH) haben, welche es den Kunden des CPO ermöglichen, verschiedene Zahlungsarten zu nutzen, wie etwa Kreditkarten, Online-Zahlung oder Pre-Paid-Karten. Da unterschiedliche CPOs auch mit unterschiedlichen Abrechnungsstellen (parallel) kooperieren können, könnte dies für Endverbraucher, d. h. den Halter/Fahrer eines Elektrofahrzeugs, dazu führen, dass sie sich für die Abrechnung eines Ladevorgangs bei CPO_1 bei Abrechnungsstelle CH_1 registrieren müssen und beim Laden an einer Station von CPO_m bei Abrechnungsstelle CH_2, was für den Einzelnen mühsam und aufwändig sein kann. Aus diesem Grund kann es einen weiteren Dienstleister, den so genannten E-Mobilitätsdiensteanbieter (Engl. *E-Mobility Provider*, EMP) geben, der wiederum mit verschiedenen Abrechnungsstellen vertraglich verbunden ist und für den Endverbraucher die Abrechnung gegenüber den CHs bzw. CPOs übernimmt. Dieses Modell ist in Abbildung 5.11 dargestellt.

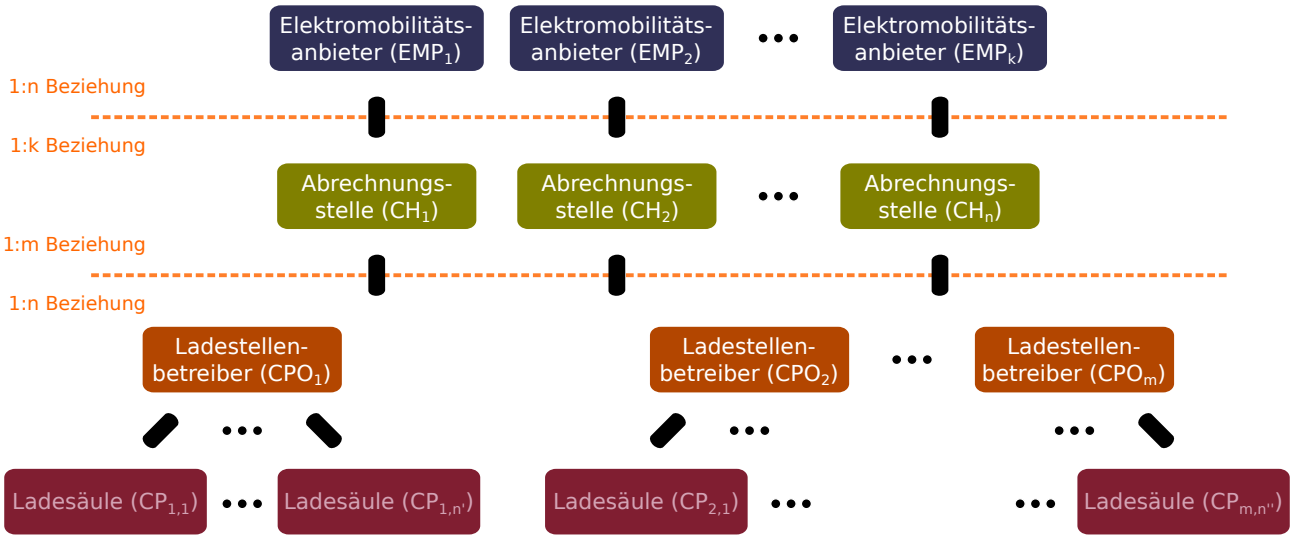

Abbildung 5.11: Zusammenspiel der beteiligten Akteure im Anwendungsfall Elektromobilität

Für den Anwendungsfall „Elektromobilität“ wird in Abbildung 5.12 der schematische Ablauf für die Registrierung und den Ladevorgang gezeigt, wie er sich unter Einsatz der hier vorgeschlagenen Maßnahmen darstellt. Für den Ladevorgang werden die vier Varianten betrachtet, die im Dokument „Anwendungsfälle Elektromobilität“ [1] dargestellt wurden.

In Schritt (1) registriert sich der Nutzer zunächst beim Elektromobilitätsanbieter (EMP). Hierfür sendet er Registrierungs-

Nr.	Funktion	Übermittelte Daten → EMP	Antwort	Maßnahme
(1)	Nutzer U registriert sich	Registrierungsdaten $[Cert(OEM\text{-}P_F)]$	PK_{EMP}, $\{Cert(EMP\text{-}C_U) + PrivKey_{EMP\text{-}C_U} \mid EMAID_U \mid UUID_U\}$	—
		Übermittelte Daten → CPO, CH, EMP (Externe Identifikation)		
(2)	U identifiziert sich mittels EMP	PK_{CPO}, $Enc_{PK_{CPO}}(EVSE\text{-}ID)$, PK_{EMP}, $\{Enc_{PK_{EMP}}(EMAID) \mid Enc_{PK_{EMP}}(UUID)\}$	$Sign_{EMP}(\pi)$ $Perm(\pi, *, EVSE\text{-}ID)$	E2E-Verschlüsselung, Pseudonymisierung: signiertes Transaktionspseudonym $Sign_{EMP}(\pi)$
(3)	Autorisation von CP (Sender) durch CPO bzgl. π	Autorisierungsanfrage bzgl. π, $EVSE\text{-}ID$		Autorisierung: Ladeberechtigung $Perm(\pi, *, EVSE\text{-}ID)$ ausstellen
		Übermittelte Daten → CPO, PP (Adhoc-Bezahlverfahren)		
(4)	U identifiziert sich mittels Zahlungsinformationen BI	$EVSE\text{-}ID$, PK_{PP}, $Enc_{PK_{PP}}(BI)$	$Sign_{PP}(\pi)$ $Perm(\pi, *, EVSE\text{-}ID)$	E2E-Verschlüsselung, Pseudonymisierung: signiertes Transaktionspseudonym $Sign_{PP}(\pi)$
(5)	Autorisation von CP (Sender) durch CPO bzgl. π	Autorisierungsanfrage bzgl. π, $EVSE\text{-}ID$		Autorisierung: Ladeberechtigung $Perm(\pi, *, EVSE\text{-}ID)$ ausstellen
		Übermittelte Daten → CP, CPO (Prepaid-Karte)		
(6)	U autorisiert sich mittels Prepaid-Zahlungsinformationen BI	BI $[EVSE\text{-}ID]$	$[Perm(BI, *, EVSE\text{-}ID)]$	—
		Übermittelte Daten → CPO, CH, EMP (Plug & Charge-Identifikation nach ISO 15118)		
(7)	U identifiziert sich mittels Vertragszertifikat $Cert(EMP\text{-}C_U)$	PK_{EMP}, $Enc_{PK_{EMP}}(Cert(EMP\text{-}C_U))$, $Enc_{PK_{EMP}}(Sign_{EMP\text{-}C_U}(c))$	$Sign_{EMP}(\pi)$ $Perm(\pi, *, EVSE\text{-}ID)$	E2E-Verschlüsselung, Pseudonymisierung: signiertes Transaktionspseudonym $Sign_{EMP}(\pi)$
(8)	Autorisation von CP (Sender) durch CPO bzgl. π	Autorisierungsanfrage bzgl. π, $EVSE\text{-}ID$		Autorisierung: Ladeberechtigung $Perm(\pi, *, EVSE\text{-}ID)$ ausstellen

Abbildung 5.12: Anwendungsfall Elektromobilität

daten wie Name und Vorname sowie ggf. ein *fahrzeugspezifisches* Bereitstellungszertifikat ($Cert(OEM\text{-}P_V)$ — V steht für *Vehicle*) des Fahrzeugherstellers, sofern es sich bei dem Fahrzeug um ein ISO 15118-fähiges Elektrofahrzeug handelt. Der zum öffentlichen Schlüssel (aus $Cert(OEM\text{-}P_V)$) gehörige private Schlüssel ist in diesem Fall im Fahrzeug vorinstalliert.

In der Antwort des EMP erhält der Nutzer den öffentlichen Schlüssel PK_{EMP} des EMP, um ggf. personenbeziehbare oder sensible Nutzerdaten zu schützen. Abhängig davon, wie im späteren Verlauf die Autorisierung des Nutzers für die Ladestation durchgeführt wird, können an dieser Stelle noch ein *nutzerspezifisches* Vertragszertifikat (Engl. Contract Certificate, $Cert(EMP\text{-}C_*)$) zusammen mit dem zugehörigen privaten Schlüssel, eine Kontokennung ($EMAID_*$, Engl. E-Mobility Account ID) oder eine andere eindeutige Kennung ($UUID_*$, Engl. Universally Unique IDentifier) des EMP an den Nutzer übergeben werden. Wird ein Vertragszertifikat $Cert(EMP\text{-}C_*)$ ausgestellt, so wird dieses vom EMP an ein oder mehr mit ihm vertraglich verbundene Abrechnungsstelle (CH) übermittelt, um später die Zuordnung der abzurechnenden Leistungen zu ermöglichen.

Für die Autorisierung an einer Ladestation werden in Abbildung 5.12 die folgenden Varianten [1] betrachtet.

- Externe Identifikation
- Adhoc-Bezahlverfahren
- Prepaid-Karte
- Plug & Charge-Identifikation nach ISO 15118

Externe Identifikation. Vor dem eigentlichen Ladevorgang des Fahrzeugs werden zunächst die Abrechnungsmodalitäten festgelegt. Im Falle der sogenannten externen Identifikation wird die Identität des Ladestellenbetreibers in Form von dessen öffentlichen Schlüssel PK_{CPO}, der Kennung der genutzten Ladesäule (EVSE-ID, Engl. *Electric Vehicle Supply Equipment ID*), der Identität des EMP von U in Form von dessen öffentlichen Schlüssel PK_{EMP} sowie die dem Nutzer zugeteilte EMAID oder UUID (vgl. Schritt (1)) übermittelt. Die EMAID oder UUID werden als persistentes Identitätsmerkmal von U jeweils für den EMP verschlüsselt, sodass weder der Ladesäulenbetreiber noch die Abrechnungsstelle die Nutzeridentität erfahren. Umgekehrt wird ebenfalls die Kennung der Ladesäule verschlüsselt, sodass außer dem CPO niemand den Standort des Nutzerfahrzeugs erfährt. Die verschlüsselten Daten werden jeweils an die Partei übermittelt, für die sie verschlüsselt sind. Da es für die Reihenfolge der kontaktierten Parteien mehrere Möglichkeiten gibt, bspw. CPO→EMP→CPO→CP vs. EMP→CPO→CP [1], werden in der Darstellung alle Daten für die jeweiligen Empfänger verschlüsselt, sodass beim 'Weiterreichen' von Nachrichten in einer Kette keine identifizierenden Daten offen gelegt werden. Der EMP des Nutzers bestätigt durch Ausstellen eines Transaktionspseudonyms π, dass der Nutzer U sein Kunde ist. Durch die Signatur ist gewährleistet, dass die Echtheit des Pseudonyms (auch für Dritte) im Nachhinein überprüfbar ist — $Sign_{EMP}(\pi)$ ist nicht notwendigerweise 'nur' eine Signatur, sondern kann weitere Informationen umfassen, wie bspw. den Gültigkeitszeitraum oder den Zeitpunkt des Signierens. Das Transaktionspseudonym wird an CPO/CP sowie CH als Referenz für den anstehenden Ladevorgang verteilt. In Schritt (3) wird von der Ladesäule CP eine Autorisierungsanfrage an CPO gesendet zur Freigabe des Ladevorgangs. Nach erfolgreicher Prüfung des Pseudonyms sowie der Kennung der Ladesäule stellt der CPO eine Berechtigung aus und autorisiert damit die Ladesäule, den Ladevorgang einzuleiten.

Adhoc-Bezahlverfahren. Bei der Identifikation über ein Bezahlverfahren (4), wie bspw. Kreditkartenzahlung, gibt der Nutzer die Identität seines Bezahldienstleisters (Engl. *Payment Provider*, PP) —für Kreditkarten bspw. Visa oder Mastercard— in Form von dessen öffentlichen Schlüssel PK_{PP} bekannt und verschlüsselt damit seine Zahlungsdaten (Engl. *Billing Information*, BI), sodass der CPO nicht die Identität des Nutzers erfährt. Die verschlüsselten Zahlungsinformationen $Enc_{PK_{PP}}(BI)$ überträgt der CPO an den Dienstleister PP, der nach Prüfung von BI —ähnlich wie der EMP in Schritt (2)— ein Transaktionspseudonym π für CPO herausgibt als Referenz für den Ladevorgang. Schritt (5) ist dann identisch zu Schritt (3) der externen Identifikation.

Prepaid-Karte. Im Falle einer Zahlung mit einer Pre-Paid-Guthabenkarte sind keine Maßnahmen erforderlich, unter der Voraussetzung, dass die Pre-Paid-Karte anonym gegenüber dem CPO bezogen werden kann, bspw. ähnlich wie Guthabenkarten von Mobilfunkanbietern an einer Tankstelle erworben werden können. Es wird deshalb für diese Variante davon ausgegangen, dass das Guthaben entweder auf einer manipulationssicheren Chipkarte gespeichert ist oder zentral durch den CPO ein Guthabenkonto verwaltet wird. Im ersten Fall ist eine Übertragung der Ladesäulenkennung EVSE-ID nicht notwendig, da die Ladesäule auf Grund der durch die Karte gesicherten Informationen BI autonom die Gültigkeit des Guthabens feststellen kann — eine Online-Prüfung durch den CPO ist in diesem Fall nicht notwendig. Im zweiten Fall ist eine Rückfrage der Säule CP beim CPO erforderlich, um prüfen zu können, ob für das Nutzerkonto noch Guthaben

verfügbar ist. Im Falle einer Online-Prüfung überträgt die Ladesäule ihre Kennung sowie die Zahlungsinformation BI der Guthabenkarte an den CPO, der bei positiver Prüfung eine Berechtigung $Perm(BI, *, EVSE\text{-}ID)$ erteilt, welche den Ladevorgang für die Ladesäule freigibt (6), ähnlich wie in den Schritten (3) und (5) zuvor. Ein Unterschied zu den zuvor genannten Varianten besteht allerdings darin, dass der Nutzer U (trotz anonymen Erwerbs der Guthabenkarte) gegenüber dem CPO nicht anonym ist, wenn das Guthaben über ein zentrales Konto (beim CPO) verwaltet wird, da in diesem Fall die Zahlungsinformationen BI stets dieselbe Kontoreferenz —mithin ein Pseudonym— enthalten, über die der Nutzer verfolgbar ist.

Plug & Charge-Identifikation. Unterstützen das Fahrzeug und die Ladesäule einen Ladevorgang nach ISO 15118 [24], kommt das Vertragszertifikat $Cert(EMP\text{-}C_U)$ (siehe Schritt (1)) zum Einsatz. Wie in den Varianten zuvor wird auch hier der EMP mittels seines öffentlichen Schlüssels PK_{EMP} identifiziert und das personenbezogene Vertragszertifikat des Nutzers mit dem Schlüssel des EMP verschlüsselt, sodass der Ladestellenbetreiber den Nutzer nicht identifizieren kann. Zum Nachweis, dass der Nutzer im Besitz des zum Vertragszertifikat gehörigen privaten Schlüssels $PrivKey_{EMP\text{-}C_U}$ ist (vgl. Schritt (1)), signiert er mit diesem eine so genannte *Challenge* c, welche zusammen mit dem Zertifikat vom CPO zur Überprüfung an den EMP übermittelt wird. Die Challenge kann der Nachricht „PaymentDetailsRes“ des PnC-Protokolls aus ISO 15118-2 [25] entnommen oder vom Fahrzeug nachvollziehbar abgeleitet werden.[8] Nach Prüfung der Identität des Nutzers bestätigt der EMP dem CPO die Gültigkeit eines Vertrags und erzeugt für den Ladevorgang ein Transaktionspseudonym π, welches dem CPO zurückliefert wird. Wie in den Schritten (3) und (5) stellt der CPO basierend auf der Identität π eine Berechtigung aus, welche die Ladestelle EVSE-ID autorisiert, den Ladevorgang mit dem Fahrzeug freizugeben.

5.6 Fahrerverhalten

Im Anwendungsfall „Fahrerverhalten“ werden Fahrzeug- und Fahrdaten verwendet, um daraus Metawerte zum Fahrverhalten zu berechnen, die von Versicherungen zur individuellen Anpassung von Tarifen („Pay-As-You-Drive“) verwendet werden können. Zur Bestimmung des individuellen Fahrverhaltens wird aus verschiedenen Fahrdaten ein Score-Wert berechnet, an dem abgelesen werden kann, wie risikoreich ein Fahrer fährt. Dabei werden folgende Daten verwendet:

- Fahrzeugposition
- Geschwindigkeit
- Beschleunigungs- und Bremsverhalten
- Weitere Daten zum Fahrstil wie bspw. ABS-Einsatz

Eine Darstellung des Anwendungsfalles findet sich in Abbildung 5.13. Für die Erfassung der Daten werden von Versicherungen Messgeräte verwendet, die an die OBD-Schnittstelle des Fahrzeugs angeschlossen werden können. Dazu muss sich ein Kunde zunächst bei der Versicherung unter Angabe der dafür notwendigen Daten registrieren (vgl. Schritt (1)) und erhält von der Versicherung in diesem Zuge ein Messgerät (im Folgenden als „Score-Gerät“ bezeichnet), das er an das Fahrzeug anschließen kann. In diesem Gerät können die Vorgaben des Kunden bereits gespeichert sein, sodass das Gerät aufgrund der im Fahrzeug ausgelesenen Daten eine Plausibilitätsprüfung vornehmen kann, die verhindert, dass das Gerät in einem anderen als dem versicherten Fahrzeug eingebracht wird und somit falsche Daten verwendet. Der Fahrzeughalter autorisiert anschließend das Score-Gerät SG für die Verwendung bestimmter Fahrdaten D wie Position, Geschwindigkeit, Bremsverhalten, etc. für einen bestimmten Zeitraum t (Schritt (2)). Diese Daten werden während der Fahrt vom Fahrzeug an das Score-Gerät übergeben (Schritt (3)). Um zu verhindern, dass durch späteres Auslesen des Score-Gerätes Rückschlüsse auf Einzeldaten wie bspw. detaillierte Positionsangaben o. Ä. vorgenommen werden können, können Daten vor Übergabe an das Score-Gerät vom Fahrzeug anonymisiert werden. Die Anonymisierung muss sich in Art und Stärke der Anonymisierung nach den vom Score-Gerät benötigten Daten richten (vgl. hierzu Abschnitt 4.8). Auch eine Übergabe der Daten als Rohdaten ist denkbar, sofern diese nur flüchtig zur Verarbeitung im Score-Gerät gespeichert werden. Im Score-Gerät wird aus den Einzeldaten der Score-Wert zur Fahrweise berechnet. Da die Versicherung nur an diesem Score-Wert interessiert ist, ist eine Übermittlung der Rohdaten oder selbst zuvor anonymisierter Daten an die Versicherung nicht notwendig. Der Score-Wert muss nicht erst auf Servern der Fahrzeugversicherung berechnet werden, sondern kann lokal ermittelt werden. Der berechnete Score-Wert wird anschließend signiert an das Fahrzeug zurückgegeben. Die Signatur schützt vor nachträglicher Manipulation durch das Fahrzeug. Durch die Übermittlung des Score-Wertes bleibt die Transparenz insoweit gewahrt, als der Fahrer den berechneten Wert selbst einsehen kann.

[8] In beiden Fällen muss der EMP überprüfen können, dass c nicht alleine vom Fahrzeug gewählt wurde, um Missbrauch auszuschließen.

In einem letzten Schritt (Schritt (4)) wird der Score-Wert vom Fahrzeug unter Verwendung einer Ende-zu-Ende-Verschlüsselung mit Hilfe des öffentlichen Schlüssels PK_V der Versicherung an diese übermittelt. Diese Verschlüsselung bietet zum einen Schutz gegenüber unbefugten Dritten und ermöglicht es zum anderen, dass die Kommunikation auch über den OEM geleitet werden kann, ohne dass dieser Einsicht in Daten zum Fahrverhalten erhält. Zusammen mit dem Score-Wert wird das Transaktionspseudonym π übermittelt. Ein Pseudonym anstelle einer eindeutigen Identifikationsnummer wie der VIN (Engl. *Vehicle Identification Number*) bietet Schutz davor, dass innerhalb der Versicherungsgesellschaft Daten aus unterschiedlichen Kontexten unnötigerweise zusammengeführt werden.

Nr.	Funktion	Übermittelte Daten	Antwort	Maßnahme
		Übermittelte Daten → Versicherung V		
(1)	Nutzer U registriert sich und sein Fzg.	Registrierungsdaten, $Commit(VIN)$	π	Pseudonymisierung: VIN wird fest- aber nicht offengelegt
		Übermittelte Daten → Score-Gerät SG		
(2)	Autorisation von Score-Gerät SG durch U für Zeitraum t bzgl. Daten D	$Perm(SG, t, D)$	—	Autorisierung: Berechtigung $Perm(SG, t, D)$ erteilen (fzg.-interne Verwendung)
(3)	Übermittlung von anonymisierten Daten D an SG; Antwort ist ein signierter Score-Wert SW	$Anon(D)$	$Sign_{SG}(SW)$	Lokalisierung: Datenverarbeitung erfolgt im Fahrzeug; Tranparenz: U sieht Score-Wert (und nicht nur V); Anonymisierung: SW wird im Fahrzeug gebildet; Lokalisierung: Datenverarbeitung erfolgt im Fahrzeug
		Übermittelte Daten → V		
(4)	Verschlüsselte Übermittlung von signiertem Score-Wert $Sign_{SG}(SW)$ an Versicherung V mit PK_V	$Enc_{PK_V}(\pi, Sign_{SG}(SW))$	—	E2E-Verschlüsselung für Versicherung

Abbildung 5.13: Anwendungsfall Fahrerverhalten

5.6.1 Fahrerüberwachung

Der Anwendungsfall der Fahrerüberwachung sieht vor, dass der Fahrer durch Innenraumsensoren im Fahrzeug überwacht wird und rechtzeitig vor Gefahren gewarnt werden kann. Das umfasst folgende Daten:

- Identität oder Pseudonym
- Innenraumbild, Augenbewegung, Luftzusammensetzung
- Alkoholerkennung, Müdigkeitserkennung

Die Sensordaten können dabei im Fahrzeug ausgewertet werden, eine Serververbindung ist somit nicht erforderlich. Damit wird der Schutz der Daten im Wesentlichen durch die Maßnahme der „lokalen Verarbeitung“ sichergestellt. Ein weitergehender Schutz der Daten durch Autorisierung ist notwendig, um zu verhindern, dass unterschiedliche Fahrer Daten einer anderen Person einsehen oder anhand von Warnungen Rückschlüsse auf solche ziehen können. Es sind folgende Maßnahmen möglich (siehe Abbildung 5.14):

1. Zu Beginn erfolgt nach einer Zustimmung zur lokalen Fahrerüberwachung eine Autorisierung der Fahrerüberwachung durch den Fahrer. Dabei kann die Bezeichnung des Fahrers U entweder sein Name oder ein Pseudonym sein. Bei der Verwendung eines Pseudonyms besteht ein besserer Schutz der Daten, sofern diese als

Profil im Fahrzeug gespeichert bleiben. Die Autorisierung erfolgt in Form einer Berechtigung $Perm(F, t, D)$, die der Nutzer für einen bestimmten Zeitraum t und bestimmte Daten D für sein Fahrzeug F erteilt. Der Zeitraum kann einen Teilabschnitt der Fahrt, die gesamte Fahrt oder mehrere Fahrten umfassen. Im letzten Fall kann die Fahrerüberwachung durch Speicherung der Daten im Fahrzeug und die Zuordnung eines Profils ergänzt werden. Die ausgewählten Daten D können Daten von verschiedenen Sensoren umfassen.

2. Nach Ausstellung der Berechtigung können Innenraumdaten gesammelt und vom Fahrzeug ausgewertet werden. Die Verarbeitung erfolgt ausschließlich lokal (Maßnahme „lokale Verarbeitung“).
3. Nach Ablauf der Zeit t oder einer Handlung des Fahrers wird die Berechtigung zur Datensammlung und -verarbeitung entzogen. Die Zugriffskontrolle kann unter Verwendung von verschlüsselten Containern durchgeführt werden. Damit besteht gleichzeitig ein Schutz für die Daten, sofern solche länger im Fahrzeug gespeichert werden.

Nr.	Funktion	Übermittelte Daten → Fzg.	Antwort	Maßnahme
(1)	Zustimmung zu lokaler Fahrerüberwachung durch Nutzer U für Zeitraum t bzgl. Innenraumdaten D	Autorisierungs-Kommando	$Perm(F, t, D)$	Benachrichtigung; Autorisierung: Berechtigung $Perm(F, t, D)$ ausstellen
(2)	Datensammlung von Daten D	—	—	Lokale Sammlung und Verarbeitung von Daten im Fahrzeug
(3)	Daten löschen	Löschkommando von U für Daten D	Bestätigung der Löschung	Zugriffskontrolle (Entzug von $Perm(F, t, D)$)

Abbildung 5.14: Anwendungsfall Fahrerüberwachung

In diesem Anwendungsfall können die Innenraumdaten D im Fahrzeug verbleiben, sodass keine Autorisierung und Übermittlung an den Hersteller notwendig würde. Hier wäre zu klären, was der Hersteller nach Kenntnisnahme von D veranlassen könnte, was das Fahrzeug nicht autonom durchführen könnte. Weiterhin erscheint eine dauerhafte Speicherung von D nicht notwendig, da D unmittelbar ausgewertet werden kann und eine Reaktion, wie bspw. ein Warnhinweis, direkt erfolgen kann.

Literaturverzeichnis

[1] SeDaFa, "Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug, Deliverable D1," https://sedafa-projekt.de/, Dezember 2016.

[2] B. Paal and D. Pauly, Eds., *Datenschutz-Grundverordnung: DS-GVO*. C.H.Beck, 2017.

[3] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," Technische Universität Dresden, Tech. Rep., 2010.

[4] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitons, simplified requirements, and a construction based on general assumptions," in *Advances in Cryptology - EUROCRYPT '03*, ser. Lecture Notes in Computer Science 2656, 2003, pp. 614–629.

[5] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *Topics in Cryptology - CT-RSA 2005*, ser. Lecture Notes in Computer Science 3376, 2005, pp. 136–153.

[6] M. Manulis, N. Fleischhacker, F. Günther, F. Kiefer, and B. Poettering, "Group signatures: Authentication with privacy," Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep., 2012.

[7] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, pp. 1030–1044, 1985.

[8] L. Chen, "Access with pseudonyms," in *Cryptography: Policy and Algorithms*, ser. Lecture Notes in Computer Science 1029, 1996, pp. 232–243.

[9] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology - EUROCRYPT '01*, ser. Lecture Notes in Computer Science 2045, 2001, pp. 93–118.

[10] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, ser. CCS '04, 2004, pp. 132–145.

[11] J. Camenisch, "Direct anonymous attestation explained," 2007.

[12] ——, "Protecting (anonymous) credentials with the trusted computing groups's tpm v1.2," in *Security and Privacy in Dynamic Environments*, ser. IFIP International Federation for Information Processing 201, 2006, pp. 135–147.

[13] ——, "Better privacy for trusted computing platforms," in *Computer Security –ESORICS '04*, ser. Lecture Notes in Computer Science 3193, 2004, pp. 73–88.

[14] J. Camenisch and J. Groth, "Group signatures: Better efficiency and new theoretical aspects," in *Security in Communication Networks*, ser. Lecture Notes in Computer Science 3352, 2005, pp. 120–133.

[15] Bundesamt für Sicherheit in der Informationstechnik, "Technische Richtlinie TR-02102-1 — Kryptographische Verfahren: Empfehlungen und Schlüssellängen (Version 2014-01)," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.html, Feb. 2014.

[16] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty*, vol. 10, pp. 557–570, 2002.

[17] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, ser. LNCS 4052, 2006, pp. 1–12.

[18] K.-U. Plath, Ed., *BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG*, 2nd ed. Otto Schmidt, 2016.

[19] J. Taeger and D. Gabel, Eds., *Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG*, 2nd ed. Deutscher Fachverlag GmbH, 2013.

[20] L. Bergmann, R. Möhrle, and A. Herb, *Datenschutzrecht*. Boorberg, 2014.

[21] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology*, pp. 199–203, 1983.

[22] S. Srivastava and V. Saraswat, "E-sash payment protocols," *International Journal on Computer Science Engineering*, vol. 4, no. 9, pp. 1603–1607, 2012.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *https://bitcoin.org/en/bitcoin-paper*, 2008.

[24] ISO/IEC 15118, "Road vehicles — vehicle to grid communication interface, first edition 2013-04-15," 2013.

[25] ISO/IEC 15118-2, “Road vehicles — vehicle to grid communication interface — part 2: Network and application protocol requirements, first edition 2013-04-15,” 2013.

SeDaFa

8. August 2017

SeDaFa-D2-1.0