Sichere Intelligente Mobilität

Testfeld Deutschland

Deliverable D21.5

Spezifikation der IT-Sicherheitslösung

Version	2.0
Verbreitung	Öffentlich
Projektkoordination	Daimler AG
Versionsdatum	08.10.2009

sim[TD] wird gefördert und unterstützt durch

Bundesministerium für Wirtschaft und Technologie

Bundesministerium für Bildung und Forschung

Bundesministerium für Verkehr, Bau und Stadtentwicklung

Dieses Dokument wurde erstellt vom Fraunhofer-Institut SIT

Beiträge wurden verfasst von
Manuel Mattheß – Fraunhofer-Institut SIT
Norbert Bißmeyer – Fraunhofer-Institut SIT
Julian Schütte – Fraunhofer-Institut SIT
Jan Peter Stotz – Fraunhofer-Institut SIT
Matthias Gerlach – Fraunhofer-Institut FOKUS
Florian Friederici – Fraunhofer-Institut FOKUS
Christoph Sommer – Uni Erlangen
Hervé Seudié – Robert Bosch GmbH
Winfried Stephan – T-Systems
Dr. Eric Hildebrandt – T-Systems
Jonas Vogt – Hochschule für Technik und Wirtschaft des Saarlandes
Bechir Allani – Hochschule für Technik und Wirtschaft des Saarlandes
Tobias Gansen – Audi AG
Anke Jentzsch – Volkswagen AG
Hagen Stübing – Adam Opel GmbH
Attila Jaeger – TU Darmstadt / Adam Opel GmbH

Projektkoordination
Dr. Christian Weiß
Daimler AG
HPC 050 – G021
71059 Sindelfingen
Germany

Telefon +49 7031 4389 550
Fax +49 7031 4389 210
E-mail christian.a.weiss@daimler.com

Inhaltsverzeichnis

Abbildungen

Tabellen

Zusammenfassung

Dieses Dokument beschreibt die IT-Sicherheitsarchitektur in sim^{TD}. IT-Sicherheit dient dem Schutz vor Manipulation des Systems, vor Abhören von privater Kommunikation, dem Schutz der Privatsphäre und damit der Einhaltung gesetzlicher Bestimmungen.

In diesem Dokument werden zwei unterschiedliche Lösungsvarianten beschrieben: Eine „optimale“ Lösung beinhaltet Sicherheitsmaßnahmen, wie sie in einem später denkbaren Wirksystem angewandt werden sollten. Für dieses anzunehmende Wirksystem spielen Sicherheit und Skalierbarkeit eine größere Rolle als in sim^{TD}, allerdings können auch teilweise leistungsfähigere Hardware (im speziellen Hardwarebeschleunigung für Kryptografie) und andere Kommunikationskanäle angenommen werden, als sie in sim^{TD} zur Verfügung stehen.

Die zweite Lösungsvariante definiert IT-Sicherheitsmaßnahmen, die für die Absicherung des sim^{TD}-Feldversuchs erforderlich sind. Zugunsten der Anwendbarkeit unter den Rahmenbedingungen von sim^{TD} (keine Hardware-Beschleunigung für kryptografische Operationen, keine Betrachtung der In-Car-Security) wurde der Aufwand für Sicherheitsmaßnahmen reduziert.

Die hier vorgeschlagenen IT-Sicherheitsmaßnahmen sind das unmittelbare Ergebnis einer ausführlichen IT-Sicherheitsanalyse, die in den Kapiteln 3 und 4 beschrieben wird. Diese Maßnahmen konzentrieren sich hauptsächlich auf die folgenden Aspekte:

- Absicherung der Kommunikation von Fahrzeugen untereinander
- Absicherung der Kommunikation zwischen Fahrzeugen und der Infrastruktur
- Absicherung der Kommunikation innerhalb der Infrastruktur
- Pseudonymisierung und Schutz der Privatsphäre

Wesentlicher Bestandteil der IT-Sicherheitsarchitektur ist dabei die Komponente „*Security-Daemon*“, die für das Signieren (und ggf. die Verschlüsselung) von Nachrichten verantwortlich ist. Die dazu verwendeten kryptografischen Schlüssel werden mit Hilfe eine Public Key Infrastructure (PKI) verwaltet. Diese besteht aus mehreren Komponenten zur Schlüsselerzeugung und -verwaltung, sowie Protokollen zum Rückruf kompromittierter Schlüssel (*Revokation*). Zum Schutz der Privatsphäre der Fahrer und aus Performanzgründen werden kurzlebige, asymmetrische Schlüssel (sogenannte *Pseudonyme*) verwendet, die einen Kompromiss aus Sicherheit und Performanz darstellen.

Auch wenn es keine hundertprozentige Sicherheit geben kann, so werden doch die in der IT-Sicherheitsanalyse ermittelten Risiken mit der hier beschriebenen IT-Sicherheitsarchitektur deutlich minimiert und damit der sim^{TD}-Feldtest vor Beeinträchtigungen durch externe Angreifer geschützt.

English summary

Specification of IT Security Solution

This document provides an overview of the IT security architecture of sim^{TD}. IT security aims at protecting the system from manipulation, privacy breaches and eavesdropping of communication. It thereby assures compliance with legal regulations.

In this document, we provide two different approaches on the security architecture: at first, we describe an “optimal” solution, containing security mechanisms we recommend for implementing in a future ITS (Intelligent Transportation System). Such a future ITS has higher demands on scalability and security, but at the same time the restrictions and constraints (no hardware acceleration of cryptography, no consideration of in-car-security, etc.) of sim^{TD} do not apply. The second approach describes a feasible IT security architecture for sim^{TD}. This approach is more lightweight, has reduced complexity and takes the existing constraints into account. On the other side, the approach does not provide an optimal protection level against all kinds of attacks but rather aims at achieving a minimum level of security that is required to maintain correct operation of the system.

The security mechanisms proposed herein are the result of a profound security analysis, as described in chapters 3 and 4. They mainly aim at the following issues:

- Protection of communication between vehicles
- Protection of communication between vehicle and the infrastructure
- Anonymisation and privacy protection

An essential part of the IT security architecture is the so-called *Security Daemon* component, which is responsible for signing and verifying (and encrypting/decrypting, if required) Car2X messages. For signatures and encryption, cryptographic asymmetric keys are required which will be managed by a Public Key Infrastructure (PKI). The PKI consists of several parts, among them components for key generation and -management, as well as protocols for revocation of compromised keys. For the sake of performance and driver’s privacy we will make use of short key lengths, implicating short key lifecycles. This solution requires public keys to be refreshed at a regular basis and is a trade-off of security and performance.

Even if there will be no absolute security, the risks identified by the security analysis will be significantly decreased by the IT security architecture described in this document and therewith the sim^{TD} field test will be protected from most external attacks.

1 Einführung

In einer Car2X-Infrastruktur wie sim^{TD} spielt IT-Sicherheit naturgemäß eine entscheidende Rolle. Wenn die Authentizität von Nachrichten nicht garantiert werden kann, private Daten für jedermann lesbar übertragen werden oder Aufenthaltsorte und Reiserouten von Fahrern öffentlich zugänglich sind, ist sowohl die Funktion des gesamten Systems, als auch die Akzeptanz durch die Benutzer gefährdet. Daher müssen schon beim Systementwurf geeignete IT-Sicherheitsmaßnahmen geplant werden. Aufgrund der besonderen Rahmenbedingungen einer Automotive-Umgebung können jedoch keine Sicherheitslösungen „von der Stange“ verwendet werden: die hohe Mobilität, Anforderungen an die Robustheit von verschiedenen Komponenten und die stark eingeschränkten Speicher- und CPU-Kapazitäten erfordern eine Abwägung zwischen optimaler Sicherheit und ausreichender Performanz.

Allerdings ist bei der sich daraus ergebenden Kompromissbildung immer zu berücksichtigen, dass ein Angreifer diesen Einschränkungen in der Regel nicht unterliegt. Er kann die technischen Mittel nutzen, die ihm zum gegebenen Zeitpunkt zur Verfügung stehen.

Dieses Dokument stellt die IT-Sicherheitsarchitektur des Intelligent Transportation System (ITS) im Projekt sim^{TD} vor. In Kapitel 1 werden zunächst die Rahmenbedingungen vorgestellt, unter denen die IT-Sicherheitsarchitektur entwickelt wurde. In Kapitel 2 werden Vorprojekte und deren Relevanz für sim^{TD} erläutert. In den anschließenden Kapiteln 3 und 4 werden die IT-Sicherheitsanforderungen in sim^{TD} analysiert: Zunächst werden Klassen von unterschiedlichen Angreifermotivationen gebildet und die zu schützenden Komponenten ermittelt. Auf dieser Ausgangsbasis werden dann mögliche Bedrohungen in sim^{TD} erarbeitet, die Risiken abgeschätzt und eine Liste von Anforderungen an die IT-Sicherheit abgeleitet. Diese Anforderungen dienen dann als Richtlinie für den Entwurf der IT-Sicherheitsarchitektur in Kapitel 5. Hierbei unterscheiden wir zwischen einem optimalen Sicherheitskonzept für ein zukünftiges System im Produktiv-Einsatz (im Folgenden *Wirksystem* genannt) und dem Sicherheitskonzept für sim^{TD}, für das geringere Anforderungen an die Sicherheit und die Skalierbarkeit bestehen. Das Dokument schließt mit einer Zusammenfassung und einem Ausblick in Kapitel 6.

Hinweis: Es wird davon ausgegangen, dass der Leser mit den Grundzügen der C2X-Kommunikation vertraut ist und folgende sim^{TD}-Basisdokumente kennt:

- Deliverable D11.3 Funktionsspezifikation
- Deliverable D21.2 Konsolidierter Systemarchitekturentwurf [1]
- Glossar

1.1 sim^{TD} Systemarchitektur

Die allumfassende und nahtlose Vernetzung von Fahrzeugen und Infrastruktur stellt eine signifikante technologische und organisatorische Herausforderung dar. Die Komplexität der sim^{TD}-Architektur rührt unter anderem aus der Tatsache, dass verschiedenste Kommunikationswege, Datenformate und Akteure involviert sind.

Abbildung 1.1 stellt die Systemarchitektur aus der Perspektive der unterschiedlichen Subsysteme, deren Komponenten und Interaktionen dar. Generell lässt die Architektur in zwei Subsysteme einteilen: Das fahrzeugseitige Subsystem beschreibt alle Hardware- und Softwarekomponenten, die im Fahrzeug zu Einsatz kommen. Das Infrastruktur-Subsystem setzt sich zusammen aus dem Infrastrukturteil der Stadt Frankfurt und des Landes Hessen (HLSV), der Versuchszentrale und den ITS Roadside Stations (IRS). Eine detaillierte Beschreibung der Systemarchitektur findet sich in Deliverable D21.2.

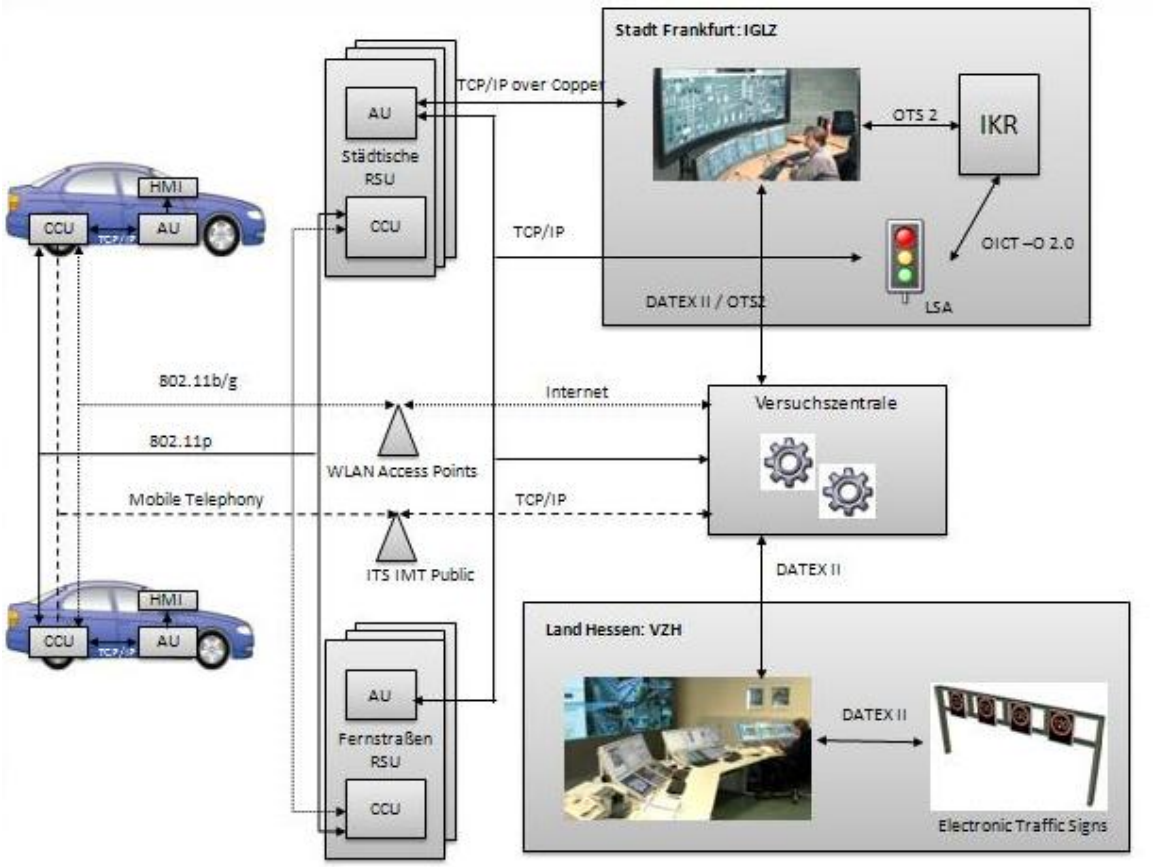

Abbildung 1.1: Gesamtarchitektur

Die sim^{TD}-Architektur integriert grundsätzlich drei verschiedene Kommunikationskanäle, die sich in Technologie und Funktionalität unterscheiden:

- Die direkte Kommunikation zwischen Fahrzeugen untereinander sowie zwischen Fahrzeugen und Infrastruktur erfolgt über den IEEE 802.11p (ITS G5A) Standard. Die meisten Meldungen zur Sicherheits- und Verkehrseffizienz erfordern eine niedrige Latenz und werden daher über diese Verbindung realisiert.
- Weiterhin sind alle Fahrzeuge mit IEEE 802.11 b/g Modulen ausgestattet. Diese werden genutzt, z.B. um auf dem Testgelände über sim^{TD} interne WLAN Access Points u.a. auch, um IP-basierte Kommunikation über das Internet mit dem Test Management Center oder andere Backend-Services herzustellen.
- IP-basierte Kommunikation ist möglich über das gesamte sim^{TD}-Testgebiet unter Verwendung von GPRS, EDGE, UMTS oder HSPA. Zugangspunkte für zellularen Mobilfunk sind in Abbildung 1.1 als ITS IMT Public gekennzeichnet. Über diesen Link wird eine Weiterleitung und Verteilung von Nachrichten zur Sicherheits- oder Verkehrseffizienz zwischen den Autobahn- und Stadt-Szenarien realisiert werden. Auch das Test Management Center nutzt Mobilfunk um Fahreranweisungen an die Fahrer zu übertragen.

Die Verarbeitung aller Nachrichten bis zur Netzwerkschicht wird auf der Fahrzeugseite (ITS Vehicle Station) von der Vehicle CCU (Vehicle Communication Unit) behandelt. CAN-Bus Daten werden von einer zentralen Komponente aufgearbeitet und den Funktionen zur Verfügung gestellt.

Für die ITS Roadside Station (IRS) ist bis auf einige zusätzliche Schnittstellen die gleiche Architektur mit Aufteilung in CCU und AU vorgesehen. Im Gegensatz zu ITS Roadside

Stations entlang der Autobahnen können städtische ITS Roadside Stations das Verkehrsgeschehen direkt über eine Verbindung zu Lichtsignalanlagen steuern.

Die Kommunikationswege in sim^{TD} sind verschiedenen Angriffen auf die Datensicherheit und Privatsphäre der Fahrer ausgesetzt. Um zu verhindern, dass verfälschte Nachrichten Messergebnisse verfälschen und um sicherheitskritische Angriffe zu verhindern, werden eingehende und ausgehende Nachrichten verschiedenen Sicherheitsüberprüfungen unterzogen.

Die ITS Central Station (ICS)[1] ist ein integraler Bestandteil eines ITS. Sie stellt die Verbindung zwischen den klassischen Verkehrszentralen und den neuartigen ITS dar. Diese ICS beinhalten auf ihrer Central Application Unit (CAU) die zentralseitigen Funktionsanteile der Anwendungen, die auf einen solchen angewiesen sind. Eine weitere CAU oder sogar eine weitere ICS beinhaltet das Management der IRS und sonstige benötigte Server. In sim^{TD} laufen in der Versuchszentrale Datenströme aus IGLZ, VZH sowie die über Mobilfunk und WLAN transportierte Daten zur Auswertung und sim^{TD}-Versuchssteuerung zusammen.

1.2 sim^{TD} Funktionen

Funktionen aus dem Bereich Car-2-X werden meist in die drei Bereiche Verkehrseffizienz, Fahr- und Verkehrssicherheit sowie Komfort eingeteilt. Dabei ist diese Einteilung nichttechnischer Natur und spiegelt vor allem die Nutzersicht der Funktionen wieder. Im Projekt *Sichere Intelligente Mobilität – Testfeld Deutschland* (sim^{TD}) sollen durch die Projektpartner über 20 verschiedene Funktionen aus diesen Bereichen implementiert werden. Diese Funktionen wurden vom Projektkonsortium nicht willkürlich gewählt, sondern sind das Ergebnis eines aufwändigen Funktionsauswahlprozesses. Im Laufe dieses Prozesses wurden mehr als 60 Funktionen hinsichtlich zahlreicher Kriterien von Expertengruppen bewertet und die Kriterien partner-individuell gewichtet. Nach der Zusammenführung der Einzelbewertungen wurden schließlich die Funktionen mit den meisten Punkten zur Umsetzung in sim^{TD} bestimmt. Dieser komplizierte Prozess wurde gewählt, um jeder Funktion in sim^{TD} die bestmögliche Unterstützung aller Partner zukommen zu lassen und dem Projekt den größtmöglichen Erkenntnisgewinn zu ermöglichen. Deliverable D11.2 behandelt den Prozess im Detail.

Funktionsentwicklungsteams (FETs) begleiten die jeweiligen Funktionen während der sim^{TD} Projektlaufzeit über die Teilprojekte hinweg durch alle Phasen des Vorhabens. Aufgrund der Projektlaufzeit von vier Jahren ist es nötig, mit dem Systementwurf (TP2) parallel zur Anforderungsanalyse (TP1) zu beginnen. Dies erschwert es einerseits den FETs verbindliche Aussagen zu Funktionsanforderungen zu machen, andererseits sind die Komponentenentwickler gezwungen Annahmen zu treffen und ihre Komponenten flexibel zu gestalten. Die relevanten Prozesse sind im Projekthandbuch (TP0), dem Spezifikationsleitfaden (TP1) und dem Entwicklungshandbuch (TP2) beschrieben.

Kategorie 1: Verkehr
Hauptfunktion 1.1: Basisfunktionen
Basisfunktion 1.1.1: Infrastrukturseitige Datenerfassung
Basisfunktion 1.1.2: Fahrzeugseitige Datenerfassung
Basisfunktion 1.1.3: Ermittlung der Verkehrswetterlage

[1] In sim^{TD} wird die ICS durch die Versuchszentrale realisiert.

Kategorie 1: Verkehr
Basisfunktion 1.1.4: Ermittlung der Verkehrslage
Basisfunktion 1.1.5: Identifikation von Verkehrsereignissen
Hauptfunktion 1.2: Verkehrsinformation und Navigation
Funktion 1.2.1: Straßenvorausschau
Funktion 1.2.2: Baustelleninformationssystem
Funktion 1.2.3: Erweiterte Navigation
Hauptfunktion 1.3 Verkehrssteuerung
Funktion 1.3.1: Umleitungsmanagement
Funktion 1.3.2: Lichtsignalanlagen Netzsteuerung
Funktion 1.3.3: Lokale verkehrsabhängige LSA-Steuerung
Kategorie 2: Fahrerassistenz
Hauptfunktion 2.1 Lokale Gefahrenwarnung
Funktion 2.1.1: Hinderniswarnung
Funktion 2.1.2: Stauendewarnung
Funktion 2.1.3: Straßenwetterwarnung
Funktion 2.1.4: Einsatzfahrzeugwarnung
Hauptfunktion 2.2: Fahrerassistenz
Funktion 2.2.1: Verkehrszeichen-Assistent/Warnung
Funktion 2.2.2: Ampel-Phasen-Assistent/Warnung
Funktion 2.2.3: Längsführungsassistent
Funktion 2.2.4: Kreuzungs-/Querverkehrsassistent
Kategorie 3: Ergänzende Dienste
Hauptfunktion 3.1 Internetzugang und Lokale Informationsdienste
Funktion 3.1.1: Internetbasierte Dienstnutzung
Funktion 3.1.2: Standortinformationsdienste

Tabelle 1.1: Kategorien, Hauptfunktionen und Funktionen

Funktionen der Gruppe 1.1 „Basisfunktionen“ erfassen und interpretieren verkehrlich relevante Daten. Die interpretierten Daten werden dann den anderen Funktionen zur Verfügung gestellt. Da alle anderen, kundensichtbaren Funktionen auf Daten dieser Gruppe basieren, kommt der Qualität und Sicherheit dieser Hauptfunktion im späteren Produktiv-System eine besondere Rolle zu. Werden beispielsweise infrastruktur-basiert gewonnene Daten vor ihrer Verarbeitung manipuliert, sind sie unter Umständen für eine Kette von Fehlfunktionen verantwortlich.

Die Hauptfunktion 1.2 befasst sich mit Funktionen aus dem Bereich „Verkehrsinformation und Navigation“. Hier werden z.B. durch Fahrzeug-zu-Fahrzeug-Kommunikation gewonnene Daten dem Nutzer zur Anzeige gebracht oder durch ein Navigationssystem automatisch verarbeitet. Die Funktion 1.2.2 informiert den Fahrer umfassend über Baustellen, die sich auf seiner Route befinden. Besonders an dieser Hauptfunktion sind der informative Aspekt und die mögliche Beeinflussung der Navigationsaufgabe herauszustellen. Ausgaben dieser Hauptfunktion beeinflussen die längerfristigen Entscheidungen eines Fahrers und führen nicht zu einer unmittelbaren Änderung bei der Bahnführung und Stabilisierung des Fahrzeugs.

Viele Fahrer werden gleichzeitig durch Funktionen der Hauptfunktion 1.3 „Verkehrssteuerung“ beeinflusst. Die Funktionen mit Anteilen in Lichtsignalanlagen haben die Aufgabe,

positiv steuernd auf das Gesamtnetz und auf einzelne, geregelte Knotenpunkte einzuwirken. Dabei kommuniziert die Funktion 1.3.3 nicht direkt mit anderen Verkehrsteilnehmern, sondern ist vornehmlich durch Kommunikation innerhalb der Verkehrsinfrastruktur geprägt.

Die Hauptfunktion 2.1 „Lokale Gefahrenwarnung“ beeinflusst über Warnungen die Bahnführung des Fahrers. Die tolerierbaren Latenzen sind geringer als bei den bisher vorgestellten Funktionen und Falschausgaben können sich unmittelbar und spürbar auswirken.

Höchste Anforderungen an Qualität und Sicherheit der Daten haben die Funktionen der Hauptfunktion 2.2 „Fahrerassistenz“. Diese unterstützen den Fahrer in alltäglichen Situationen mit aufbereiteten Informationen z.B. über Verkehrszeichen, Lichtsignalanlagen sowie in unfallträchtigen Situationen, z.B. beim Überfahren einer ungeregelten Kreuzung oder beim Abbiegen. Dabei dürfen falsche oder fehlende Information (wie sie auch durch fehlerhafte oder unscharfe Sensordaten zustande kommen können) nicht zu einer zusätzlichen Gefährdung des Fahrers führen. Potenziell gefährliche Fahrsituationen werden im Projekt sim^{TD} daher nicht untersucht sondern bleiben Untersuchungsgegenstand eines Car-2-X-Systems der späteren Generation.

Funktionen der Kategorie 3 ermöglichen teilweise die Nutzung oben genannter Funktionen über IP-basierte Kommunikationskanäle – im Gegensatz zur Verwendung von Car-2-X-Kommunikation. Die „Standortinformationsdienste“ allerdings bieten Dritten die Möglichkeit, ihre Dienste im Fahrzeug zur Anzeige zu bringen und sind deshalb geeignet, weitere interessante Aspekte der IT-Sicherheit zu untersuchen.

1.3 Technische Rahmenbedingungen

Folgende Rahmenbedingungen werden für die Sicherheitsanalyse und die Spezifikation der IT-Sicherheitslösung angenommen:

- Es wird davon ausgegangen, dass Detailbeschreibungen der Funktionen bzw. Anwendungsfälle vorliegen, im Idealfall auch schon der (technischen) Szenarien. Wo dies nicht oder nur teilweise der Fall ist, werden, soweit sinnvoll, eigene Annahmen getroffen, was gegebenenfalls spätere Korrekturen der Analyse bzw. des Sicherheitskonzepts nach sich ziehen kann.
- Es wird das Design eines „optimalen, sicheren Konzepts“ eines späteren Wirksystems entworfen. Dieses geht über sim^{TD} hinaus und basiert z.B. auf der Annahme, dass auch kryptografische Hardware verfügbar wäre, die aus Kostengründen in sim^{TD} nicht zur Verfügung steht.
- Ausgehend von diesem „optimalen, sicheren Konzept“ wird das in verschiedener Hinsicht reduzierte Konzept für sim^{TD} entworfen.

Neben den Rahmenbedingungen werden auch noch Abgrenzungen zu bereits bestehenden Systemen vorgenommen. Außerdem werden Fragen der physikalischen Sicherheit bewusst von der Analyse ausgenommen. Die Hintergründe für diese Abgrenzungen werden in den folgenden Abschnitten näher erläutert.

1.3.1 Vorleistungen

Vorleistungen sind Leistungen und die zu ihrer Erbringung notwendigen Dienste und Infrastruktur-Komponenten, die für sim^{TD} zwar benötigt, aber von Dritten bereitgestellt werden und daher außerhalb der direkten Verantwortlichkeit von sim^{TD} liegen. In Tabelle 1.1 werden diese Vorleistungen aufgelistet.

Ref.	Bezeichnung	Beschreibung/Bemerkungen
[V_GPS]	Global Positioning System	satellitengestütztes Navigationssystem des US-Verteidigungsministeriums, das von den Fahrzeugen zur Positionsbestimmung verwendet wird
[V_IP-Zugangsnetz]	Zugangsnetz(e) von ISP	xDSL-basierte Zugangsnetze verschiedener ISPs zu ihrem jeweiligen Backbone-Netz.
[V_IP-Backbone]	IP-Backbone(s) von ISP	Wir unterscheiden hier nicht zwischen IPv4 und IPv6, da IPv6 über IPv4 getunnelt werden kann.
[V_IMT Public]	International Mobile Communications	Herkömmliche GSM bzw. UMTS Mobilfunknetz-Infrastruktur ohne ITS spezifische Anteile
[V_VZH]	Verkehrszentrale Hessen	Alle internen IT-Sicherheitsfragen der VZH obliegen dem Land Hessen und werden daher im vorliegenden Dokument nicht betrachtet.
[V_IGLZ]	Integrierte Gesamtleitzentrale Frankfurt am Main	Alle internen IT-Sicherheitsfragen der IGLZ obliegen der Stadt Frankfurt am Main und werden daher im vorliegenden Dokument nicht betrachtet.
[V_PropNet]	Proprietäre Netzwerkinfrastruktur	Unter diesem Begriff werden existierende Netzwerksysteme oder auch nur einzelne Übertragungsleitungen zusammengefasst, die nicht bereits durch die oben aufgeführten Netze abgedeckt werden. Beispielsweise fallen hierunter die Glasfaser-Strecken zur Anbindung von IRS durch Stadt oder Land.
[V_LSA_VBA]	Lichtsignalanlagen und Verkehrsbeeinflussungsanlagen	Alle entsprechenden Geräte und die sich auf die Anbindung beziehenden IT-Sicherheitsfragen obliegen dem Land Hessen oder der Stadt Frankfurt am Main.
[V_InfStrukSens]	Infrastruktursensoren	Die korrekte Funktionsweise aller infrastrukturseitigen Sensoren zur Datenerfassung wird nicht beachtet.
[V_CarSens]	Fahrzeugsensoren	Die korrekte Funktionsweise aller fahrzeugseitigen Sensoren zur Datenerfassung wird nicht beachtet.

Ref.	Bezeichnung	Beschreibung/Bemerkungen
[V_CarInternal]	Fahrzeug-interne Netze und Komponenten	Im vorliegenden IT-Sicherheitskonzept werden nur die direkt für sim^{TD} vorgesehenen Fahrzeugkomponenten betrachtet.
[V_HW_SecModule]	Hardware-Sicherheits-Modul in der IVS und IRS	Es besteht die prinzipielle Möglichkeit zur Beschleunigung von kryptografischen Operationen und sicheren Speicherung von Geheimnissen ein dediziertes Hardware-Sicherheitsmodul zu verwenden. Ein solches Modul *wird* aber *im Rahmen von* sim^{TD} *nicht eingesetzt*. Daher wird es auch nicht berücksichtigt.

Tabelle 1.2: Vorleistungen

1.3.2 Physikalische IT-Sicherheit

Fragen der physikalischen IT-Sicherheit von Komponenten und Übertragungsleitungen werden in der IT-Sicherheitsanalyse nicht betrachtet, d.h. insbesondere folgende Aspekte werden nicht behandelt:

- Physikalische Abhörsicherheit und Integritätsschutz von Übertragungsleitungen
- Resistenz von Komponenten gegenüber Reverse Engineering
- Extraktion von geheimen Daten bzw. Schlüsselmaterial durch Hardware-Analyse oder Seitenkanalangriffe
- Manipulationsresistenz von Komponenten
- Resistenz von Komponenten gegenüber Zerstörungsversuchen (Vandalismus, Brand, usw.)
- Fragen der Schließtechnik und physikalischen Absicherung von Objekten zur Verhinderung von Diebstahl

Der Ausschluss dieser Aspekte geschieht aus folgenden Gründen:

- Infrastrukturkomponenten liegen größtenteils nicht im Zuständigkeitsbereich von sim^{TD}.
- Bei den Fahrzeugkomponenten müssen die entsprechenden Fragen für das Wirksystem stets anhand der schlussendlich in der Serie verwendeten Komponenten/ Baugruppen geklärt werden. Eine Betrachtung im Vorfeld in sim^{TD} ist demnach nicht sinnvoll.
- Eine Absicherung von Nachrichtenübertragungen erfolgt auf den höheren Ebenen des OSI-Protokoll-Stapels, so dass physikalische Abhörsicherheit und Schutz gegen Manipulation nicht notwendig sind.

1.3.3 In-Car-Security

Mit In-Car-Security sind unter anderen Maßnahmen zum Manipulationsschutz der In-Car-Komponenten (Steuergeräte, Sensoren) und Maßnahmen zur Absicherung der internen

Kommunikation sowohl zwischen In-Car-Domänen als auch zwischen In-Car-Komponenten gemeint. Da es sich in sim^{TD} hauptsächlich um die Absicherung der Kommunikation mit externen Systemen (andere Fahrzeuge, Infrastrukturen) handelt, würde eine Betrachtung der In-Car-Security den Rahmen von sim^{TD} sprengen. Zudem gibt es ein von der europäischen Union gefördertes Projekt, das sich nur mit dieser Thematik beschäftigt. Siehe Kapitel 2 das Projekt EVITA in Abschnitt 2.7.

1.3.4 Verkehrszentrale Hessen

Die Verkehrszentrale Hessen (VZH) ist das aktive System zur Steuerung des Verkehrs auf den Fernstraßen in Hessen. Im Rahmen des Forschungsprojekts sim^{TD} erfolgt kein Eingriff in die Funktionalität der VZH. Die sim^{TD}-Versuchszentrale greift Daten (z.B. FG-Daten[2]) über den sogenannten Infoverteiler der VZH ab. Dazu registriert sie sich beim Infoverteiler, der die gewünschten Daten wie jedem anderen VZH-Kunden in regelmäßigen zeitlichen Abständen über FTP bereitstellt. Aus der Sicht der VZH handelt es sich um einen Push. Die VZH verfügt über eine eigenständige Absicherung. Die Netzwerkanbindung der sim^{TD}-Versuchszentrale an die VZH erfolgt über eine Firewall, deren Regelwerk den Anforderungen des HLSV genügt.

1.4 Definitionen

In Rahmen dieses Dokumentes werden einige Begriffe verwendet, die einer genauen Definition bedürfen, da auf ihnen die nachfolgende IT-Sicherheitsanalyse und das IT-Sicherheitskonzept aufbauen. In diesem Abschnitt werden die für dieses Dokument relevanten Begriffe der IT-Sicherheit definiert, für alle weiteren Begriffe verweisen wir auf das sim^{TD} -Glossar.

1.4.1 Informationssicherheit / Datensicherheit

Mechanismen bzw. Protokolle zur Gewährleistung der Informationssicherheit garantieren bei einem funktionssicheren System, dass nur Systemzustände angenommen werden können, die keine unautorisierte Informationsveränderung oder -gewinnung zulassen. Informationen können als Daten repräsentiert werden, daher spricht man auch von Datensicherheit. Aus Sicht der Datensicherheit bedeutet dies, dass keine unautorisierten Zugriffe auf Daten möglich sein dürfen.

1.4.2 Datenschutz

Mechanismen bzw. Protokolle zum Schutz der Privatsphäre verhindern, dass personenbezogene Daten gesammelt bzw. missbraucht werden können, um z.B. mit Hilfe dieser Daten Verhaltens- oder Bewegungsprofile zu erstellen.

---

[2] FG-Daten sind Nachrichten, die z.B. von den Detektorschleifen und anderen Messstationen herrühren und an die Verkehrszentralen gesandt werden

1.4.2.1 Personenbezogene Daten, Betroffener

Hierbei handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diese wird auch als Betroffener bezeichnet.

1.4.2.2 Erheben, Verarbeiten, Nutzen und Speichern von Daten

Die *Erhebung* von Daten bezeichnet das Beschaffen von Daten über den Betroffenen. *Verarbeitung* enthält die einzelnen Aktivitäten *Speichern*, *Verändern*, *Übermitteln*, *Sperren* und *Löschen* von Daten. Das *Nutzen* von Daten bezeichnet die *Verwendung* von Daten, soweit nicht die *Verarbeitung* vorliegt. Die *Speicherung* von Daten liegt vor, wenn diese *erfasst*, *aufgenommen* oder allgemein *aufbewahrt* werden auf einem Datenträger – gleich welcher Art – zum Zweck der weiteren Verarbeitung oder Nutzung.

1.4.2.3 Anonymität

Die *Anonymität* bezeichnet den Zustand dass Daten eines Betroffenen mit der gleichen Wahrscheinlichkeit auch von einem anderen Betroffenen derselben Menge stammen können. Zur Erreichung dieses Zustandes ist unter Umständen eine Anonymisierung der Daten notwendig. Diese bezeichnet den Prozess der Veränderung von Daten über einen Betroffenen derart, dass diese nicht oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten, Arbeitskraft und Rechtverletzung einem bestimmten oder bestimmbaren Betroffenen zugeordnet werden können.

1.4.2.4 Pseudonymität

Pseudonymität bezeichnet die Ersetzung des Namens oder anderer Identifikationsmerkmale des Betroffenen durch ein anderes Kennzeichen (das Pseudonym) mit dem Zweck, die Zuordnung der Daten zu einem Betroffenen unmöglich zu machen oder wesentlich zu erschweren.

1.4.3 IT-Sicherheitsschutzziele

Auf Grund der hohen Verständlichkeit und der genauen Definitionen übernehmen wir für sim^{TD} die Schutzzieldefinitionen aus [2]. Dort sind die IT-Sicherheitsschutzziele definiert wie folgt:

1.4.3.1 Vertraulichkeit

Ein System gewährleistet Informationsvertraulichkeit, wenn es keinen unautorisierten Informationsgewinn ermöglicht. Für vertrauliche Informationen gelten u.a. auch datenschutzrechtliche Anforderungen (BDSG [3], TDDSG [4]), wie beispielsweise eine zweckgebundene Nutzung der Daten oder auch, dass Daten nicht ohne Einwilligung des Nutzers an Dritte weitergegeben werden dürfen.

1.4.3.2 Authentizität

Unter der Authentizität eines Objekts bzw. Subjekts versteht man die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand seiner eindeutigen Identität und seiner charakteristischen Eigenschaften überprüfbar ist.

1.4.3.3 Integrität

Ein System gewährleistet Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Das bedeutet, dass in Umgebungen, in denen eine solche Manipulation nicht a priori verhindert werden kann (z.B. in Netzen), Techniken erforderlich sind, mit deren Hilfe unautorisierte Manipulationen a posteriori erkennbar sind.

1.4.3.4 Verbindlichkeit / Nicht-Abstreitbarkeit

Ein System gewährleistet Verbindlichkeit bzw. Nicht-Abstreitbarkeit einer Menge von Aktionen, wenn es nicht möglich ist, dass ein Akteur einer Aktion seine Urheberschaft abstreiten kann. Mit der Verbindlichkeitseigenschaft ist die Forderung nach Abrechenbarkeit unmittelbar verbunden. Dies erfordert Maßnahmen zur Überwachung sowie zur Protokollierung einzelner Benutzeraktivitäten.

1.4.3.5 Verfügbarkeit

Ein System leistet Verfügbarkeit, wenn autorisierte Subjekte in der Wahrnehmung ihrer Berechtigung nicht unautorisiert beeinträchtigt werden können. Verzögerungen, die aus „normalen“ Ausführungsverzögerungen Verwaltungsmaßnahmen resultieren, werden als autorisierte Beeinträchtigungen betrachtet. Ein weiterer Aspekt der Verfügbarkeit ist Ausfallsicherheit, also die Resistenz des Systems gegen den unerwarteten Ausfall einzelner Komponenten. Dies schließt Ausfälle aufgrund von Angriffen genauso ein wie Ausfälle, die durch höhere Gewalt verursacht wurden.

1.4.4 Pseudonyme und Identitäten

In diesem Dokument werden die Begriffe *Pseudonym* und *Identität* im Zusammenhang mit der Identifizierung von Fahrzeugen gegenüber der sim^{TD}-Infrastruktur verwendet. Sie sind nachfolgend definiert.

1.4.4.1 Basisidentität

Eine Basisidentität umfasst ein Schlüsselpaar aus öffentlichem und privatem Schlüssel, sowie ein von der Root-CA unterschriebenes, langlebiges Zertifikat (im Text auch als „Basiszertifikat“ bezeichnet). In sim^{TD} ist dieses Zertifikat mindestens für den gesamten Zeitraum des Versuchs gültig, in einem späteren Wirksystem wäre ein Zeitraum von einigen Jahren denkbar. Aufgrund der langen Gültigkeit müssen auch die Schlüssel der Basisidentität ausreichend lang sein. Da eine Basisidentität die eindeutige Identifizierung eines Fahrzeugs erlaubt, darf sie niemals zur Kommunikation mit ITS-Komponenten verwendet werden sondern dient lediglich der Authentifizierung gegenüber der Root-CA.

1.4.4.2 Pseudonym

Ein Pseudonym umfasst ein Schlüsselpaar aus öffentlichem und privatem Schlüssel, sowie ein von der Root-CA unterschriebenes, kurzlebiges Zertifikat. Pseudonyme werden zur Kommunikation mit ITS-Komponenten verwendet und dürfen daher keine dauerhafte Identifizierung eines Fahrzeugs erlauben, um Tracking von Fahrzeugen und Fahrern durch unbefugte Dritte zu verhindern. Aufgrund der kurzen Gültigkeit können die Pseudonymschlüssel deutlich kürzer gewählt werden als die Schlüssel der Basisidentität.

1.4.4.3 Wirksystem

Unter einem Wirk- oder Produktivsystem versteht man den regulären Betrieb eines meist komplexen Systems außerhalb des Probe- oder Testbetriebs. In dem Wirksystem müssen sehr viel stärkere Maßnahmen bezüglich der IT-Sicherheit getroffen werden, da Angreifer eine größere Motivation haben, das System anzugreifen. Außerdem sind sehr viel umfangreichere Skalierungsfragen und Verfügbarkeitsanforderungen zu klären. In einem Probe- oder Testsystem sollen möglichst viele Probleme eines Wirksystems adressiert werden, so dass Erkenntnisse für ein Wirksystem gewonnen werden können.

1.5 Rechtlich regulatorische Rahmenbedingungen

Im Rahmen des Teilprojekts 5 „Bewertung und Rahmenbedingungen“ ist eine externe Studie zur Untersuchung rechtlich regulatorischer Rahmenbedingungen geplant (Deliverable D5.2). In dem vorliegenden technisch orientierten Deliverable werden daher nur grobe Aussagen zu rechtlich regulatorischen Fragestellungen gemacht, die in den entsprechenden Teilen von Deliverable D5.2 weiter detailliert werden müssen. Die folgenden Abschnitte erheben nicht den Anspruch, Rechtsberatung zu sein bzw. zu ersetzen.

1.5.1 Das Bundesdatenschutzgesetz und das Recht auf Informationelle Selbstbestimmung

Personenbezogene Daten unterliegen in der Bundesrepublik Deutschland besonderem Schutz. Dabei sind personenbezogene Daten *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“*[3]. Auch Daten ohne unmittelbaren Personenbezug können zu personenbeziehbaren Daten werden, indem Zusatzinformationen genutzt werden. Diese Zusatzinformationen können auch illegal erlangt worden sein. So ist beispielsweise ein Fahrzeug-Kennzeichen oder eine IP-Adresse kein unmittelbar personenbezogenes Datum, kann aber durch Einbeziehung zusätzlicher Information oder Beobachtung dazu werden. Die Interpretation des Sachverhalts, ob und in welchem Maße die Fahrzeug-zu-Fahrzeug-Kommunikation für das Persönlichkeitsrecht des Einzelnen relevant ist, obliegt Juristen – dennoch ergibt sich für die Realisierung eines Systems zur Fahrzeug-zu-Fahrzeug-Kommunikation die Notwendigkeit, adäquate technische Mechanismen zum Datenschutz vorzusehen.

Der Schutz personenbezogener Daten gipfelt im sog. Recht auf Informationelle Selbstbestimmung des Einzelnen. Es ist ein Persönlichkeitsrecht, gegründet auf dem Grundgesetz der Bundesrepublik Deutschland (GG), dem sog. „Volkszählungsurteil“ von 1983 sowie dem Bundesdatenschutzgesetz (BDSG) und den entsprechenden Landesdatenschutzgesetzen. Das BDSG gilt für alle öffentlichen Stellen des Bundes und für alle nicht-öffentlichen Stellen. Die entsprechenden Landesdatenschutzgesetze finden Anwendung in allen öffentlichen Stellen der jeweiligen Länder.

> Grundgesetz, Artikel 1, Absatz 1:
>
> „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“

[3] BDSG, §3, Abs. 1

Grundgesetz, Artikel 2, Absatz 1:

„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Das Bundesverfassungsgericht (BVG) hat im Volkszählungsurteil festgestellt, dass der Einzelne „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten" bestimmen kann. Dies wird mit den Folgen begründet, die es hätte, wenn der Einzelne nicht wüsste, „(…) welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind (…)". So befürchtete das BVG, dass Bürger in ihrer Verhaltensweise nachhaltig gehemmt und beeinträchtigt würden, aus Angst davor, dass „(...) abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden (…)". So soll das Recht auf Informationelle Selbstbestimmung den Schutz der Privatsphäre ermöglichen und verhindern, das der Einzelne in zu starke Abhängigkeit zu Dritten gerät, weil diese viel von ihm wissen. Aus diesem Grund ist es nur folgerichtig, dass jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten ist, außer ein Gesetz oder eine Rechtsvorschrift verlangen dies *oder* der Betroffene stimmt zu (BDSG §4, Abs. 1).

An die Zustimmung des Betroffenen stellt das BDSG weitere Bedingungen. So muss diese auf der freien Entscheidung des Betroffenen beruhen und in der Regel schriftlich erfolgen. Er muss über Umfang und Zweck der Datenerhebung sowie über die Folgen einer Verweigerung der Zustimmung aufgeklärt werden (BDSG §4a, Abs. 1). Die Freiwilligkeit und die Folgen der verweigerten Zustimmung stellen vor allem bei Monopolen ein Problem dar: Wie kann sich der Einzelne für einen effektiven Datenschutz entscheiden, wenn die Verweigerung der Datenverarbeitung ihn von der Nutzung grundlegender Dienste oder Güter ausschließt?

Die Erhebung von personenbezogenen Daten muss immer offenkundig geschehen, eine geheime Erhebung ist unzulässig. Besonders wird auch die automatisierte Verarbeitung von Daten geregelt.

BDSG §4d Abs. 1:

„Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nichtöffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes (…) dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (…) zu melden."

Die Meldepflicht solcher Verarbeitungen wird sogar noch durch eine vorgeschriebene „Vorabkontrolle" verstärkt, sollten die erhobenen und verarbeiteten Daten „besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen" (BDSG §4d, Abs. 5), was z.B. dann der Fall ist, wenn die Datenerhebung, -verarbeitung und -speicherung dazu dienen, die Persönlichkeit, Leistung oder das Verhalten des Betroffenen zu bewerten.

Personenbezogene Daten dürfen grundsätzlich nur für den Zweck genutzt werden, zu dem sie ursprünglich erhoben wurden. Von diesem Grundsatz kann allerdings nach gesetzlicher Vorgabe abgewichen werden, z.B. zur Durchführung wissenschaftlicher Forschung.

Beim Umgang mit personenbezogenen Daten ist der Grundsatz der Verhältnismäßigkeit zu berücksichtigen. Wo möglich sollen solche Daten vermieden oder nur sparsam erhoben, verarbeitet und gespeichert werden (BDSG §3a). Das Gesetz spricht ausdrücklich davon, dass insbesondere „von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen (…)" ist, soweit dies „möglich ist und der Aufwand in einem

angemessenen Verhältnis zu dem angestrebten Schutzzweck“ steht. Der in diesem Deliverable durchgeführten Bedrohungs- und Schutzbedarfsanalyse kommt also eine besondere Bedeutung zu.

Das BDSG unterscheidet bei den datenerhebenden Stellen zwischen öffentlichen und privat-rechtlichen Stellen. Der Datenaustausch zwischen diesen Stellen ist im BDSG geregelt. Besonders kritisch ist die Datenübermittlung an eine Stelle im Ausland. Die besonderen Regeln zum Austausch von Daten sind z.B. bei der Nutzung von durch IRS erhobenen Daten zu berücksichtigen. Ein denkbares Szenario ist hier die Detektion, Meldung und Weiter-leitung eines Unfalls. Dabei wandern Daten zum Unfallgeschehen und den Beteiligten über verschiedene Stellen und müssen adäquat behandelt werden. Da hier wahrscheinlich ein berechtigtes öffentliches Interesse zur Übermittlung von Daten vorliegt, ist dieser Datenaus-tausch relativ unkritisch zu sehen. Im Gegensatz zum Austausch von Daten mit privat-rechtlichen Stellen. Bei einem ITS könnte dies z.B. ein Anbieter von erweiterten Diensten sein, der zur Abrechnung personenbezogene Daten erfordert. So könnte der Betreiber einer kostenpflichtigen Straße über die automatisierte Auflösung von Pseudonymen Rechnungen für die Straßenbenutzung stellen.

Für privat-rechtliche Stellen ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig (BDSG §28, Abs. 1). Dabei erfolgt allerdings die Einschränkung einer geforderten Zweckbindung. Der Zweck der erhobenen Daten muss dem Betroffenen also vor der Einwilligung erkennbar gemacht werden. Eine Übermittlung oder Nutzung der erhobenen Daten ist allerdings z.B. für die Durchführung wissenschaftlicher Forschung möglich (BDSG, §28 Abs. 3.4).

Neben der Nutzung von personenbezogenen Daten für eigene Zwecke besteht weiterhin die Möglichkeit zur „listenmäßigen“ Übermittlung von Daten. Dabei kann neben Namen, Titel, Graden der Anschrift und dem Geburtsjahr der Betroffenen genau ein sog. „freies Merkmal“ übermittelt werden, z.B. die Eigenschaft „Halter eines deutschen Fahrzeugs“. Die zusätzliche Übermittlung weiterer Eigenschaften, z.B. „Ist größer als 1,85m“ ist unzulässig. Begangene Ordnungswidrigkeiten oder Straftaten („Punkte im Zentralregister“), arbeitsrechtliche Verhältnisse oder Angaben aus vertragsähnlichen Vertrauensverhältnissen dürfen generell nicht listenmäßig übermittelt werden. Gegen diese listenmäßige Übermittlung kann der Betroffene allerdings widersprechen und eine Sperrung der eigenen Daten gegenüber der verantwortlichen Stelle verlangen.

Die genannte „verantwortliche Stelle“ ist diejenige, die Daten erhebt, speichert und nutzt. Bei einem komplexen ITS wird es wahrscheinlich mehrere solcher Stellen geben. So sind sicherlich die Betreiber der Verkehrsinfrastruktur aber auch die Fahrzeughersteller oder deren Beauftragte verantwortliche Stellen im Sinne des BDSG. Auch die Betreiber der für das ITS notwendigen PKI sind zu den verantwortlichen Stellen zu zählen. Da eine übergreifende, zentrale Stelle wahrscheinlich fehlen wird, stellt dies den Betroffenen unter Umstände vor Probleme.

Ob und welche „verantwortliche Stellen“ im Sinne des BDSG in sim^{TD} existieren sollte durch eine entsprechende Prüfung der juristischen Rahmenbedingungen wie sie in AP53 durchgeführt wird ermittelt werden und kann daher an dieser Stelle nicht geklärt werden.

1.5.2 Beauftragter für den Datenschutz

Jede öffentliche und nicht-öffentliche Stelle, die personenbezogene oder personenbezieh-bare Daten automatisch erhebt, verarbeitet und speichert, muss einen Beauftragten für den Datenschutz stellen (BDSG §4f Abs. 1), außer in der nicht-öffentlichen Stelle sind weniger als neun Personen mit der automatisierten Verarbeitung der Daten beschäftigt. Sollte die Art

der Datenverarbeitung eine Vorabkontrolle erfordern, ist in jedem Fall ein Beauftragter für den Datenschutz zu ernennen. Der Beauftragte für den Datenschutz ist dem Leiter der verantwortlichen Stelle direkt zu unterstellen, dennoch ist er in der Ausübung seiner Fachkunde nicht weisungsgebunden. Da der Leiter der verantwortlichen Stelle letzten Endes die alleinige rechtliche Verantwortung für die Einhaltung der relevanten Datenschutzgesetze trägt, kann er sich über das Votum des Beauftragten für den Datenschutz hinwegsetzen.

Beauftragter für den Datenschutz kann nur werden, wer die erforderliche Fachkunde und Zuverlässigkeit zur Erfüllung seiner Aufgaben besitzt (BDSG §4f, Abs. 2). Dabei richtet sich das Maß der erforderlichen Fachkunde nach Art und Umfang der von der verantwortlichen Stelle durchgeführten Datenverarbeitung.

Der Beauftragte für den Datenschutz unterliegt der Verschwiegenheitspflicht, sollte ein Betroffener ein Gesuch an ihn stellen, außer der Betroffene entbindet ihn von dieser Pflicht. Betroffene können sich jederzeit an ihn wenden. Weitere Besonderheit ist, dass der Beauftragte für den Datenschutz das Zeugnisverweigerungsrecht bestimmter Berufsgruppen übernimmt, sollte er während seiner Tätigkeit Kenntnisse von personenbezogenen Daten erhalten, für welche diese Berufsgruppen ein Zeugnisverweigerungsrecht haben. Seine Aufzeichnungen unterliegen einem Beschlagnahmeverbot. Die Rechte und Pflichten des Beauftragten für den Datenschutz erstrecken sich auch auf dessen Hilfspersonal.

Die Aufgaben des Beauftragten für den Datenschutz umfassen unter anderem die Sicherstellung der Einhaltung der relevanten Regelungen für den Datenschutz, mit der Verarbeitung personenbezogener Daten betraute Mitarbeiter mit den relevanten Regelungen vertraut zu machen, die Durchführung einer eventuell notwendigen Vorabkontrolle sowie die Beantwortung von Eingaben von Betroffenen.

Für ein späteres Wirksystem empfehlen wir die Einrichtung eines Datenschutzbeauftragten. Die Rahmenbedingungen in sim^{TD} weichen jedoch in einigen Punkten von denen eines Wirksystems ab: Zum einen werden Daten einer geschlossenen Benutzergruppe erhoben, zu deren Mitgliedern ein vertragliches Verhältnis besteht, dass entsprechend gestaltet werden könnte, so dass die Einrichtung eines Datenschutzbeauftragten nicht erforderlich wäre. Des Weiteren werden in sim^{TD} Daten zum Zwecke der Forschung erhoben und nicht „personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeitet“ (BDSG §4 Abs. 1 S. 5). Eine abschließende Klärung der Frage, ob ein Datenschutzbeauftragter für sim^{TD} erforderlich ist, kann an dieser Stelle nicht geleistet werden. Wir verweisen daher auf die Studie zu rechtlichen und regulatorischen Rahmenbedingungen in AP53.

1.6 Vorgehensweise

sim^{TD} soll ein Testfeld für ein später zu errichtendes ITS sein, so dass die beschriebene IT-Sicherheitslösung gleich auch schon mit Blick auf ein späteres Wirksystem konzipiert wird:

Es wird versucht ein „optimales, sicheres Konzept“ für ein ITS zu entwerfen, das über sim^{TD} *hinaus gültig ist. Dabei wird weiter angenommen, dass im späteren Wirksystem z.B. auch in den Fahrzeugen kryptografische Hardware verfügbar wäre.*

Da die Ergebnisse der Tests im Rahmen von sim^{TD} bei der vorangehenden Spezifikation der Lösung natürlich noch nicht zur Verfügung stehen können, wird die Spezifikation sicherlich nach Abschluss von sim^{TD} noch zu modifizieren sein. In den nachfolgenden Abschnitten wird überdies noch darauf eingegangen, wie sich spezielle Randbedingungen, insbesondere auch die bei sim^{TD}, auf das Umsetzen des Konzepts in die Praxis auswirkt.

Methodisch folgen wir bei der Analyse und der nachfolgenden Spezifikation einer bewährten Vorgehensweise, die folgende Schritte umfasst:

1. Angriffsszenarien (sog. „Dark-Scenarios“) ausarbeiten und daraus Angreifertypen sowie einen "Angriffsbaum" ableiten.
2. Durchführung einer IT-Sicherheitsanalyse auf Basis der Szenarien
    a. Schutzbedarfsanalyse („Welche Güter sind besonders schützenswert?")
    b. Bedrohungs- und Risiko-Analyse („Welche Bedrohungen gibt es? Wie hoch ist das Risiko der einzelnen Bedrohungen?“)
3. Ableiten der IT-Sicherheitsanforderungen aus den relevanten Bedrohungen
4. Ableiten von konkreten Maßnahmen zur Umsetzung (möglichst) sämtlicher identifizierten IT-Sicherheitsanforderungen im sim^{TD} IT-Sicherheitskonzept

Die in Schritt 4 erfolgende Beschreibung, wie sich das ITS sichern lässt, wird in drei Teile gegliedert:

- Zuerst wird in einem allgemeinen Rahmenwerk für die IT-Sicherheit dargelegt, mit welchen Maßnahmen die Sicherheitsanforderungen an ein ITS erfüllt werden können. Hierbei werden auch Varianten dargelegt.
- Anschließend wird mit Blick auf ein späteres Wirksystem eine „optimale" Sicherheitslösung entwickelt, bei der die Spezifikation von sim^{TD} nicht im Vordergrund steht.
- Zuletzt wird dann das optimale Sicherheitskonzept aus dem vorangehenden Schritt auf ein eingeschränktes Konzept reduziert, das sich bei sim^{TD} zeitnah und mit den beschränkten Ressourcen des Projekts auch praktisch umsetzen lässt, aber dennoch die Kernforderungen zur IT-Sicherheit bei sim^{TD} erfüllt.

Die letzten beiden Teilschritte werden in den nachfolgenden Abschnitten noch näher erläutert.

1.6.1 Optimale Sicherheitslösung

Natürlich wird man immer danach streben möglichst viele der identifizierten Sicherheitsanforderungen an ein ITS mithilfe geeigneter Maßnahmen in der Praxis zu erfüllen. Dabei wird man überdies – nicht zuletzt aufgrund der immer wichtigeren Harmonisierung innerhalb der Europäischen Union – versuchen, möglichst konform mit den aktuellen Standardisierungsbestrebungen bei ETSI, C2C-CC und anderen Gremien zu bleiben. Spezielle Sonderlösungen sollten möglichst vermieden werden. Ziel ist es ein Konzept zu erstellen, das auch ohne den (wünschenswerten) Einsatz von kryptografischer Hardware nicht nur sim^{TD} absichert, sondern auch als Basis für das IT-Sicherheitskonzept des Wirksystems dienen kann.

Ein solches IT-Sicherheitskonzept darf dementsprechend keine Maßnahmen enthalten, die sich zwar innerhalb von sim^{TD} umsetzen ließen, aber bei einem späteren Wirksystem nicht, z.B. weil sie nicht hinrechend skalierbar sind.

1.6.2 sim^{TD} spezifische Sicherheitslösung

Gerade im Rahmen von sim^{TD} muss aufgrund der technischen, wirtschaftlichen und zeitlichen Rahmenbedingungen des Projekts damit gerechnet werden, dass nur ein Teil der Maßnahmen, die im Wirksystem umzusetzen wären, implementiert werden können. Zudem gibt es Sicherheitsanforderungen, die im Rahmen eines Tests nicht unbedingt erfüllt werden müssen, beispielsweise die rechtlichen und regulatorischen Rahmenbedingungen, welche in sim^{TD} weniger strikt sind als in einem späteren Wirksystem.

Damit sich Maßnahmen einer vorgeschlagenen optimalen IT-Sicherheitslösung auch auf ihre Praxistauglichkeit testen lassen, müssen Maßnahmen, die für ein Wirksystem zwingend notwendig sind, auch bei sim^{TD} umgesetzt werden. Auch wenn für eine Absicherung von sim^{TD} selbst bestimmte Maßnahmen nicht notwendig sind, so kann doch ein Verzicht auf sie dazu führen, dass sich nur schwer praktisch beurteilen lässt, wie sich die entsprechenden Maßnahmen auf das Wirksystem auswirken werden. Dies gilt insbesondere für solche Maßnahmen, welche die Leistungsfähigkeit von System-Komponenten stark beeinflussen.

Anders als bei der optimalen IT-Sicherheitslösung spielen Standardisierungsbestrebungen nur eine eingeschränkte Rolle: Bei rein sim^{TD} spezifischen System-Teilen kann von Standards abgewichen werden. Die Darstellung der für sim^{TD} spezifischen IT-Sicherheitslösung geschieht zur Vermeidung unnötiger Redundanz durch Angabe der Unterschiede zur optimalen Sicherheitslösung.

2 Relevante Vorprojekte

Dieses Kapitel beschreibt diejenigen Projekte, die für die Entwicklung der Sicherheitslösung in sim^{TD} relevant sind. Eine Übersicht über derzeit laufende Projekte und Standardisierungsaktivitäten bieten Tabelle 2.1 und Tabelle 2.2. Eine Relevanz für sim^{TD} ist gegeben, wenn in dem Projekt

- Konzepte und Verfahren entwickelt wurden, die für die Entwicklung der sim^{TD} IT-Sicherheitslösung relevant sein könnten
- Implementierungen entstanden sind oder in Kürze entstehen, die in sim^{TD} eingesetzt werden könnten.

Eine allgemeine Beschreibung relevanter Vorprojekte für sim^{TD} findet sich in Deliverable D21.1 [5]. Dort wurde in Teilen auch schon auf Projekte eingegangen, die relevant für die Entwicklung der IT-Sicherheitslösung sind. Diese sind in Auszügen im Folgenden wiedergegeben.

Auf der Basis dieser Kriterien werden in diesem Kapitel insbesondere die Ergebnisse der Projekte Network on Wheels, Sevecom, PRE-DRIVE C2X, COMeSafety und des Fraunhofer Innovationsclusters Sichere Identität beschrieben.

Neben relevanten Projekten, die bereits abgeschlossen sind, berücksichtigt dieses Kapitel relevante, aktuell noch laufende Projekte und Aktivitäten passender Standardisierungsgruppen. In diesem Punkt geht dieses Kapitel weiter als Deliverable D21.1 [5].

Die Relevanz für das Wirksystem ist zum gegenwärtigen Zeitpunkt noch nicht bewertbar. Diese Prüfung kann erst im Rahmen seiner Entwicklung durchgeführt werden.

Projekt	**Projekt-ende**	**Kernaspekte**	**Relevanz**
Network on Wheels	2008	Allgemeine Angriffs- und Risikoanalyse. Sicherheitsarchitekturvorschlag. Lösungen für Vertrauenswürdigkeit und Privatsphäre (Context Mixes). Sicheres Routing.	Hoch
SeVeCom – Secure Vehicular Communications	2009	IT-Sicherheitsanalyse auf der Basis von *Spatial Enhanced Cluster Analysis* (SECA). Sicherheitsarchitektur- und Konzeptsvorschlag. Implementierung der Sicherheitslösung auf Basis von ACuP und für das CVIS Projekt	Hoch
Fraunhofer Innovationscluster Sichere Identität Berlin Brandenburg	2010	Allgemeine Projekte zum Thema Identitätsmanagement. Verbesserung und Weiterentwicklung einer IEEE 1609.2 basierten Lösung für “Sichere Identitäten für Fahrzeuge”	Hoch
PRE-DRIVE C2X – Preparation for driving implementation and evaluation of C2X communication technology	2010	Allgemeine Anforderungen und Architektur an eine Sicherheitsarchitektur für Europäisch Intelligente Transportsysteme.	Mittel

Projekt	Projekt-ende	Kernaspekte	Relevanz
EVITA – E-Safety vehicle intrusion protected applications	2011	Sicherheitslösung primär für die interne Kommunikation in Fahrzeugsubssystemen (Steuergerät ⇔ Steuergerät, Sonstiges ⇔Steuergerät) aber auch für die Kommunikation mit Systemen außen des Fahrzeuges.	Niedrig
PRECIOSA – Privacy enabled capability in Cooperative Systems and Safety Applications	2010	Mechanismen zum Schutz der Privatsphäre in ITS Systemen	Mittel bis niedrig

Tabelle 2.1: Relevante Projekte

Standardisierungs-Gruppe	Verfügbare relevante Standards	Kernaspekte	Relevanz
IEEE 1609 (US)	IEEE 1609.2	Demonstration/Implementierungen von 1609.2 im VII PoC[4]. Spezifikation von Sicherheitsdienst für C2X Nachrichten.	Hoch
ETSI ITS (Europe)	Keine	WG 5, Arbeiten zu Sicherheit für ITS G5A, Spezialistengruppe zum Thema Risikoanalyse und Entwurf von Sicherheitsmaßnahmen für ITS G5A	Mittel[5]

Tabelle 2.2: Relevante Standardisierungsgruppen

2.1 Network on Wheels

Das vom BMBF geförderte Projekt NoW (***N**etwork **o**n **W**heels*) hatte eine Laufzeit von Juni 2004 bis Mai 2008. Projektpartner waren Daimler, BMW, Volkswagen, NEC, Fraunhofer FOKUS, Siemens, IMST und Embedded Wireless sowie verschiedenen Unterauftragnehmer.

Schwerpunkte von NoW waren die Entwicklung von Algorithmen für Routing und IT-Sicherheit, die Untersuchung des Funkkanals, die Spezifikation von IT-Sicherheits- und Deployment-Anwendungen, die Ausarbeitung von Szenarien zu Markteinführung und von Geschäftsmodellen sowie eine herstellerübergreifende Demonstration.

Relevanz für sim^{TD}

[4] VII – Vehicle Infrastructure Integration, PoC Proof Of Concept

[5] Für das Wirksystem ist die Relevanz voraussichtlich als hoch einzustufen.

Das NoW Kommunikationssystem enthält eine IT-Sicherheitslösung, die zertifikatsbasiert die Integrität und Authentizität von Nachrichten schützt. Zentraler Bestandteil des Konzeptes ist die Aufteilung in *mutable* und *immutable fields*, also Feldern in den Nachrichten, die von der Datenquelle bzw. von weiterleitenden Knoten auf dem Weg zum Ziel signiert werden müssen.

Daneben wurden weitere Algorithmen und Konzepte zum Thema Sicherheit und Datenschutz entwickelt, die allerdings nicht Bestandteil der Abschlussdemonstration waren z.B. wurden Ideen zur Verwendung von Pseudonymen unter verschiedenen Gesichtspunkten, wie Dichte des Verkehrs, Art des Verkehrs, verschiedenen Algorithmen zum Wechsel von Pseudonymen und einer Mindestzeit, während der das Pseudonym stabil sein soll, untersucht. Hierzu wurden Simulationen durchgeführt und ein Demonstrationstool entwickelt.

2.2 SeVeCom

***Se**cure **Ve**hicle **Com**munication* (01.06.2006 – 03.2009) ist ein Forschungsprojekt, das aus dem EU 6. Rahmenprogramm finanziert wurde. SeVeCom adressierte die IT-Sicherheit von zukünftigen *vehicle communication* Netzwerken, mit Rücksicht sowohl auf Car2Car, als auch auf Car2Infrastructure Kommunikation.

Ziel des Projektes war die Definition einer Sicherheitsarchitektur für Car2x Kommunikationsnetzwerke und darüber hinaus die Empfehlung einer Vorgehensweise für die Einführung von Sicherheitsfunktionen in diesen Netzwerken.

SeVeCom liefert wichtigen Input für die Definition von IT-Sicherheit in anderen Projekten (CVIS) bzw. bei der Standardisierung von Sicherheitsarchitekturen im Rahmen des ETSI-Gremiums. Darüber hinaus liegt ein Demonstrator vor.

Relevanz für sim^{TD}

Die Vorgehensweise zur Erstellung eines Sicherheitskonzepts, und die schon gewonnenen Erfahrungen aus SeVeCom sind“ relevant für die Risikoanalyse in Kapitel 4. Vor allem die ersten Schritte der Anforderungsanalyse entsprechen der allgemeinen Vorgehensweise in sim^{TD}. Darüber hinaus liefert SeVeCom eine Analyse relevanter Signatur Mechanismen für Car2X Anwendungen: RSA, DSA/ElGamal und ECDSA/ECGDSA/ECKCDSA. Die Liste müsste aber aktualisiert und um Ver- und Entschlüsselungsalgorithmen erweitert werden.

SeVeCom hat sich sowohl mit Car2X als auch mit In-Car-Security beschäftigt. Letzteres ist aber nicht im Blickfeld von sim^{TD}. Insofern werden Komponenten wie das In-Car-Security Module und das Tamper Resistent Module (zumindest fahrzeugseitig) keine Rolle spielen.

Die Wiederverwendbarkeit der Sicherheitsarchitektur auf der Infrastrukturseite muss überprüft werden, da sie nicht tiefer gehend in SeVeCom untersucht worden ist. Für die Implementierung wird man auf den Demonstrator von SeVeCom aufsetzen können, falls die Kommunikationslösung ACUp von BMW in sim^{TD} eingesetzt wird.

2.3 IEEE 1609.2

IEEE 1609.2 ist eine Arbeitsgruppe innerhalb des *Institute of Electrical and Electronics Engineers* innerhalb der Arbeitsgruppe 1609, die Protokolle für Anwendungen im Fahrzeugumfeld auf der Basis von IEEE 802.11 standardisiert. Die Gruppe besteht seit 2005, und firmierte vorher unter der Nummer IEEE 1556. Mehr allgemeine Information zu VII und dem PoC finden sich in D 21.1 [5][1].

Mit IEEE 1609.2 hat die Gruppe einen Standard entwickelt, der „Sicherheitsdienste für WAVE“ definiert, und damit sichere Nachrichten- und Zertifikatsformate für die Absicherung von Nachrichten in 1609.2 geschaffen. IEEE 1609.2 definiert eine Authentizitätsabsicherung von Nachrichten auf der Basis digitaler Signaturen mit Elliptischen Kurven (ECC) und Vertraulichkeitsabsicherung auf der Basis von AES.

Relevanz für sim^{TD}

Die Mechanismen von IEEE 1609.2 wurden im Feldtest erprobt und getestet. Es existieren weltweit eine geringe Anzahl von Implementierungen des Standards, eine dieser Implementierungen (der FOKUS Security Daemon) wurde zur Absicherung von Einsatzfahrzeugwarnungen im Car-2-Car Forum 2008 in Dudenhofen verwendet. Die Verfügbarkeit eines Standards und Implementierungen dieses Standards machen diese Aktivitäten relevant für sim^{TD}.

2.4 ETSI ITS WG 5

Das *Technical Committee Intelligente Transportsysteme* (TC ITS) innerhalb der Europäischen Standardisierungsstelle für Telekommunikation (ETSI) wurde 2007 ins Leben gerufen und beschäftigt sich mit der Standardisierung von Protokollen und Architekturen für Intelligente Transportsysteme. Arbeitsgruppe 5 (Security) beschäftigt sich dabei mit dem Entwurf einer Sicherheitslösung für ITS im Allgemeinen.

Relevanz für sim^{TD}

Kern der Arbeiten von ETSI TC ITS WG 5 sind derzeit die Entwicklung einer Bedrohungs- und Risikoanalyse für ITS G5A, die gegen Mitte/Ende 2009 als Technical Report veröffentlicht werden soll. Gegen Ende des Jahres soll dann eine technische Spezifikation der Gegenmaßnahmen (Kommunikationsprotokolle) für sichere ITS Kommunikation veröffentlicht werden. Eine Prüfung auf Relevanz für sim^{TD} kann daher aktuell nicht erfolgen.

2.5 Sichere Identität – Berlin Brandenburg

Der Fraunhofer-Innovationscluster „Sichere Identität“ ist ein Zusammenschluss von fünf Fraunhofer-Instituten, fünf Hochschulen und 12 Wirtschaftsunternehmen. Gefördert wird der Cluster von den Ländern Berlin und Brandenburg.

Ziel der gemeinsamen Forschungs- und Entwicklungsprojekte ist es, Technologien, Verfahren und Produkte anzubieten, die den eindeutigen Nachweis der Identität von Personen, Objekten und geistigem Eigentum in der realen und der virtuellen Welt ermöglichen. Eigentümer und Nutzer von Identitäten sollen dadurch in die Lage versetzt werden, über eindeutig definierte und erkennbare Identitäten selbstbestimmt zu verfügen.

Die Anwendungen reichen von der nächsten Generation fälschungssicherer Personaldokumente über die Sicherung elektronischer Geschäftsprozesse bis hin zur Kommunikation zwischen Autos oder dem Produkt- und Markenschutz.

Relevanz für simTD

Im Rahmen des Fraunhofer Innovationsclusters Sichere Identität wird eine auf IEEE 1609.2 basierende Sicherheitslösung für Fahrzeugkommunikation unter dem Aspekt „Certified C2X“ weiterentwickelt.

Eine frühere Version dieser Lösung wurde schon in der Demonstration des C2C CC 2008 in Dudenhofen verwendet. Teile der Lösung werde im Rahmen des Innovationsclusters unter

einer Open Source Lizenz zur Verfügung gestellt. Dual-Licensing für die Verwendung im kommerziellen Umfeld ist möglich. Ansprechpartner ist Fraunhofer FOKUS.

2.6 PRE-DRIVE C2X

Pre*paration for* ***driv****ing implementation and* ***e****valuation of* ***C2X*** *communication technology* (07.2008 – 06.2010) ist ein Forschungsprojekt, das aus dem EU 7. Rahmenprogramm finanziert wird.

Kern des Projektes ist die Harmonisierung der Pan-europäischen Kommunikationsarchitektur in Zusammenarbeit mit den relevanten Projekten, wie z.B. COMeSafety, CVIS, SeVeCOM. Im Rahmen von PRE-DRIVE C2X ist auch ein separates Dokument entstanden, das eine IT-Sicherheitsarchitektur für die Fahrzeugkommunikation beschreibt.

Relevanz für sim^{TD}

Die Arbeiten im Bereich IT-Sicherheit für C2X innerhalb PRE-DRIVE C2X beschränken sich auf architekturelle Aspekte. Allerdings wird vermulich der im Car-2-Car Forum genutzten Security Daemon im Demonstrator für PreDrive C2X verwendet.

Die Fertigstellung des Demonstrators in PRE-DRIVE C2X liegt innerhalb des Projektzeitraums von sim^{TD}, sodass hier eventuell Erfahrungen mit der Integration von Sicherheit in das Kommunikationssystem relevant sein könnten.

2.7 EVITA

E*-Safety* ***V****ehicle* ***I****ntrusion pro****T****ected* ***A****pplication* (07.2008 – 06.2011) ist ein Forschungsprojekt im 7. Rahmenprogramm der Europäischen Union. Partner im Projekt sind BMW, Bosch, Continental, escrypt, EURECOM, Fraunhofer SIT, Fujitsu, Infineon, Institut TELECOM, KU Leuven, MIRA, und TRIALOG.

Ziel des Projektes ist die Entwicklung einer Hardware für den Einsatz im Automotive Umfeld, die als Basis für Sichere e-Safety Anwendungen verwendet werden kann. Kernbestandteil dieser Lösung ist die Entwicklung eines *ECU Trust Module* ETM, also eines Trusted Modules für Steuergeräte im Fahrzeug.

Relevanz für sim^{TD}

Die Arbeiten von EVITA haben 2008 begonnen. Eine Referenzimplementierung in Software und Hardware wird Anfang 2011 abgeschlossen sein. Diese soll zum Projektende (Juni 2011) dann als offene Spezifikation publiziert werden. Die EVITA Lösung ist primär ein In-Car-Sicherheitssystem. Sie basiert auf den Einsatz einer zusätzlichen Hardware, die in sim^{TD} nicht vorgesehen ist. Teilergebnisse (Angriffsszenarien, Risikoanalyse, Bedrohungsanalyse) aus EVITA könnten für die Sicherheitsanalyse in sim^{TD} verwendet werden, da es bei den Partnern im Konsortium aus EVITA und sim^{TD} Überschneidungen gibt.

2.8 PRECIOSA

Pr*ivacy* ***e****nabled* ***c****apability* ***i****n* ***Co****operative* ***S****ystems and Safety* ***A****pplications* (03.2008 – 02.2010) ist ein im 7. Rahmenprogramm der EU gefördertes Projekt. Partner sind TRIALOG, ORACLE, ptv, Humboldt Universität zu Berlin, und die Universität Ulm. Es beschäftigt sich mit dem Schutz der Privatsphäre und der Datenhaltung für Intelligente Transportsysteme.

Schwerpunkt des Projektes sind kooperative Systeme und Forschung im Bereich des Schutzes der Privatsphäre für Intelligente Transportsysteme. Hier soll im Allgemeinen die Privatsphäre untersucht und eine „privacy aware“ Architektur entwickelt werden. Weiterhin sollen im Rahmen des Projektes Richtlinien zum Schutz der Privatsphäre in kooperativen Systemen erarbeitet werden.

Relevanz für sim^{TD}

Die Arbeiten von PRECIOSA haben 2008 begonnen und werden vermutlich nicht mehr im Rahmen von sim^{TD} relevant sein, da es keine Überschneidung bei den Partnern gibt.

3 Motivation

IT-Sicherheitsmaßnahmen sind teuer – Entwicklung, Implementierung und Betrieb eines sicheren Systems benötigt zusätzliche Entwicklungszeit, Rechenleistung und Übertragungskapazität und erhöhen zusätzlich die Komplexität des Systems. Dass dieser Aufwand nicht ungerechtfertigt ist, demonstriert dieses Kapitel anhand einer Auswahl potenzieller Bedrohungsszenarien und deren Auswirkungen auf ein ITS ohne wirksame und vollständige IT-Sicherheitsmaßnahmen. Die dargestellten Auswirkungen demonstrieren die Notwendigkeit von IT-Sicherheitsmaßnahmen für sim^{TD} sowie für das avisierte Wirksystem.

Kategorisiert man mögliche Angriffsszenarien, die den Betrieb des ITS gefährden bzw. die zu einem Scheitern des Feldversuchs führen können, so sind im Wesentlichen drei Klassen von Szenarien zu unterscheiden. Sie zielen im Einzelnen auf: Die Übertragung falscher Daten (3.1, Übertragung falscher Daten), eine Sabotage des Systems (3.2, Sabotage des Systems) und den unbefugten Zugriff auf Daten (3.3, Unbefugter Zugriff auf Daten). Mögliche Angriffe aus diesen Klassen sind im Folgenden aufgeführt.

3.1 Übertragung falscher Daten

Das Gros technischer Szenarien, die den Betrieb des ITS oder die Durchführung des Feldversuchs gefährden, umfassen die Übertragung falscher Daten, d.h. das Einbringen gefälschter Daten oder eine Verfälschung der durch Teilnehmer übertragenen Daten.

Angriffe, die das Einbringen gefälschter Daten in das System zur Folge hätten, würden den Regelbetrieb des ITS unmittelbar gefährden und hätten damit insbesondere auch das direkte Scheitern des Feldversuchs zur Folge. Dies kann durch eine unbefugte Teilnahme von Angreifern am System – etwa mit eigener Hardware, durch Impersonation bekannter Teilnehmer oder durch die gleichzeitige Teilnahme unter mehreren Identitäten geschehen. Vergleichbar mit der Einbringung falscher Daten ist die Verfälschung von übertragenen Daten. Dies beinhaltet die Veränderung von Nachrichtenteilen, beispielsweise der Fahrzeugposition, der Fahrrichtung oder der Fahrzeuggeschwindigkeit. Ebenso führt in vielen Fällen auch die gezielte Verzögerung zu übertragender ITS-Nachrichten zu einer Verarbeitung nicht mehr gültiger Daten und damit zu einer Gefährdung des ITS.

Im Rahmen des Feldversuchs zählen dazu zusätzlich alle Szenarien, die bereits in der Versuchszentrale gesammelte Daten während oder nach der Zusammenstellung löschen oder korrumpieren können.

3.1.1 Angriffsszenario „Verfälschung übertragener Nachrichten“

Einer der weitreichensten Angriffe auf das ITS ist die aktive Verfälschung von übertragenen Nachrichten. Betreibt ein Angreifer etwa erfolgreich eine eigene ITS Vehicle Station, so beziehen andere Nutzer in unmittelbarer Nähe Nachrichten von dieser Station. So ist es einem Angreifer ohne weiteres möglich, falsche Verkehrs-, Baustellen- und Reisezeitinformationen auszusenden, etwa um die Routenwahl anderer Fahrer beliebig zu beeinflussen. Desweiteren könnten Angreifer falsche oder nicht plausible Nachrichten verschicken um die Systeme anderer Fahrzeuge oder Roadside Stations zu stören.

3.1.2 Angriffsszenario „Impersonation anderer Teilnehmer“

Impersation bedeutet, dass sich ein Teilnehmer mit einer fremden oder mehreren IDs gleichzeitig authentifiziert. Ein Angreifer könnte gleichzeitig mehrere Absender-IDs verwenden um anderen Teilnehmern mehrer reale Teilnehmer vorzutäuschen.

Der Betrieb einer eigener ITS Vehicle Station ist jedoch unter Umständen gar nicht notwendig, falls es einem Angreifer gelingt, durch Impersonation anderenn Teilnehmern ein schlüssiges, aber fiktives Straßenszenario vorzuspiegeln. Der Aufenthaltsort des Angreifers wäre in diesem Fall noch nicht einmal örtlich eingeschränkt wodurch der Täter entsprechend schwer zu fassen wäre. Der Verlauf und die Folgen des Angriffs wären vergleichbar mit den unter Abschnitt 3.1.1 (Angriffsszenario „Verfälschung übertragener Nachrichten“) genannten. Der Angriff wird alternativ auch als Sybil-Attacke bezeichnet.

3.1.3 Angriffsszenario „Selektive Unterdrückung von Nachrichten“

Oft ist ein aktives Fälschen von Nachrichten nicht einmal nötig, um den Betrieb des ITS zu gefährden. Gelingt es einem Angreifer, selektiv im ITS übertragene Nachrichten zu unterdrücken, so ist er ebenfalls in der Lage, die Sicht aller Teilnehmer auf das Verkehrsgeschehen zu beeinflussen, wenn auch nicht derart frei, wie das in den vorgestellten Szenarien 3.1.1 (Angriffsszenario „Verfälschung übertragener Nachrichten“) und 3.1.2 (Angriffsszenario „Impersonation anderer Teilnehmer“) möglich ist.

Als Sonderfall dieses Angriffs führt im Feldversuch eine selektive Unterdrückung von Fahranweisungen mit hoher Wahrscheinlichkeit unmittelbar zum Scheitern des Versuchs, da dann nur ein Teil der Fahrer nur die gestellten Anweisungen ausführt.

3.1.4 Angriffsszenario „Selektive Verzögerung von Nachrichten“

Doch auch durch die simple Verzögerung von Nachrichten lassen sich in manchen Fällen Teilnehmer des ITS massiv gefährden. Gelingt es etwa einem Angreifer, eine Warnung vor Rotlichtverstoß oder vor einer Vollbremsung so weit zu verzögern, dass sie erst zu einem für den Angreifer günstigen Zeitpunkt ausgesendet oder empfangen wird, so wird der Fahrer dadurch ggf. irritiert, was schwere Auffahrunfälle zur Folge haben könnte. Auch wenn der Fahrer stets die Möglichkeit hat, die Situation zu beherrschen und selbst für das sichere Führen seines Fahrzeugs verantwortlich ist, können Angriffe auf die Nachrichtensicherheit auf diese Weise indirekt die Wahrscheinlichkeit von Unfällen erhöhen.

3.1.5 Angriffsszenario „Infektion des Systems mit Malware“

Alle unter 3.1.1 (Angriffsszenario „Verfälschung übertragener Nachrichten“) bis 3.1.4 (Angriffsszenario „Selektive Verzögerung von Nachrichten“) genannten Angriffe sind problemlos auch ohne physikalische Präsenz eines Angreifers durchführbar, falls er Systemkomponenten durch eine Infektion mit Malware unter seine Kontrolle bringen konnte. Ähnlich den aus dem Internet bekannten Angriffen durch dezentral koordinierte Botnetze wären solche Angriffe kaum nachzuverfolgen und nach erfolgter Infektion einer ausreichender Anzahl von Systemkomponenten nur mit extremem Aufwand einzudämmen [6].

3.1.6 Angriffsszenario „Veränderung von Daten in der Versuchszentrale“

Ein Feldversuch-spezifisches Angriffsszenario stellt die Veränderung von Daten nach ihrer Aggregation in der Versuchszentrale dar. Lassen sich Manipulationen durch das Hinzufügen, Weglassen, Verändern oder Verdoppeln von gespeicherten Daten nicht ausschließen, so ist ein Angreifer in der Lage, mit einem Schlag die gesammelten Daten für die Auswertung wertlos zu machen. Fällt die Manipulation auch während der Konsolidierung der Ergebnisse nicht auf, so lässt sich durch diesen Angriff sogar erreichen, dass das Projekt sim^{TD} zu falschen Endergebnissen gelangt.

3.1.7 Angriffsszenario „Feldversuch mit inkonsistenter Software“

Die in 3.1.6 (Angriffsszenario „Veränderung von Daten in der Versuchszentrale“) genannten Angriffsziele ließen sich auch erreichen, falls ein Angreifer in der Lage ist, in sich konsistente Softwarebestandteile des ITS in einzelnen Teilnehmern so zu kombinieren, dass letztendlich ein inkonsistentes Gesamtsystem betrieben wird [7]. Standardisiertes Systemverhalten muss von allen Komponenten korrekt umgesetzt werden. Wenn neue Versionen von Softwarekomponten eingesetzt werden sollen, muss sichergestellt werden, dass entweder alle Komponenten ausgetauscht werden oder dass die neuen Versionen abwärtskompatibel sind. Falls Systemkomponenten eingesetzt werden, die nicht zueinander kompatibel sind, kann es im schlimmsten Fall zu mittlerem bis grobem Fehlverhalten führen.

3.2 Sabotage des Systems

Der Betrieb des ITS lässt sich durch die Verfälschung von übertragenen Daten stören – wesentlich einfacher kann ein Angreifer dieses Ziel jedoch durch Sabotage erreichen.

Zu Angriffen dieses Szenarios zählen neben der trivialen Störung von Straßenverkehr und der Zerstörung von Infrastruktur alle Angriffe, die geeignet sind, die Verfügbarkeit des Diensts einzuschränken (Denial of Service, DoS). Neben der physikalischen Veränderung oder Zerstörung von Systemkomponenten, die im Folgenden nicht weiter betrachtet wird, ist ein möglicher DoS-Angriffsvektor das Jamming des Funkkanals durch strategische Störsender. Ebenso sind Angriffe, die an verschiedenen Stellen des ITS Überlast erzeugen, vorstellbar. Schließlich kann der Betrieb des ITS durch Sabotage des Routings im Kernnetz gestört werden.

3.2.1 Angriffsszenario „Jamming des Funkkanals“

Ein großes Problem der drahtlosen Netzwerke, wie denen im C2X-Umfeld, ist das Management wer zu welchem Zeitpunkt den Funkkanal nutzen darf oder etwas senden darf. Da es keinen zentralen Koordinator gibt, der den Zugriff regelt, muss jeder Teilnehmer selber entscheiden wann er den Funkkanal belegt. Andere Teilnehmer sollten dabei nicht gestört werden. Trotzdem kann es zu Kollisionen kommen, wenn zwei Teilnehmer zur gleichen Zeit senden, d.h. die beiden Übertragungen überlagern sich und werden damit unbrauchbar. Deshalb unterbrechen die Sender ihre Übertragungen sofort, sobald sie eine Kollision auf dem Funkkanal feststellen. Nach einer kurzen zufälligen Wartezeit versuchen es beide Sender noch einmal (Retry-Mechanismus).

Durch einen eigenen Sender kann ein Angreifer dies nutzen um gezielte Kollisionen zu erzeugen. Ab einer gewissen Dichte von Fahrzeugen verursacht der Retry-Mechansimus zusätzliche Kollisionen, was die Auswirkungen des Angriffs noch verstärkt. Der Angreifer kann so mit verhältnismäßig geringem Aufwand das System stören. Des Weiteren ließe sich auf

diese Art ein Angriff, wie er in Abschnitt 3.1.3 (Angriffsszenario „Selektive Unterdrückung von Nachrichten“) beschreiben wird durchführen oder verschleiern.

3.2.2 Angriffsszenario „Überlastung des Systems“

Ähnlich dem in 3.2.1 (Angriffsszenario „Jamming des Funkkanals“) vorgestellten Angriff lassen sich in einem ungeschützten System einzelne Komponenten auch dazu instrumentieren, wiederum mit vergleichsweise geringem Aufwand die Systemlast so weit zu erhöhen, dass potenziell Angriffe wie der in Abschnitt 3.1.3 (Angriffsszenario „Selektive Unterdrückung von Nachrichten“) vorgestellt, möglich ist. Manipulierte Systemkomponenten können zum Beispiel mit einer hohen Frequenz und einer hohen Priorität Nachrichten per Broadcast aussenden um den Funkkanal zu blockieren. Andere Ziele von diesem Angriffszenario könnten auch zum Beispiel Puffer oder Datenbanken sein, die durch übermäßige Datenmengen blockiert werden könnten.

3.2.3 Angriffsszenario „Sabotage des Routings“

Ist ein Angreifer in der Lage, Routingentscheidungen im ITS zu beeinflussen, so ist er in der Lage, die Verbindung zwischen Komponenten des Systems gezielt auf Transportschicht zu unterbrechen und so einen Angriff der in 3.1.3 (Angriffsszenario „Selektive Unterdrückung von Nachrichten“) genannten Art und Weise vorzubereiten oder zu verschleiern

Ebenfalls wäre ein Angreifer in die Lage versetzt, Datenverkehr über eigene Netzknoten umzuleiten und so eine Vielzahl der in 3.1 (Übertragung falscher Daten) beschriebenen Szenarien herbeizuführen.

3.3 Unbefugter Zugriff auf Daten

Die letzte Klasse von Szenarien umfasst alle Angriffe, die nicht auf eine Sabotage oder die Übertragung falscher Daten abzielen, sondern auf den unbefugten Zugriff auf Daten. Unbefugter Zugriff kann entweder zur Vorbereitung weiterer Angriffe dienen oder derart verheerenden Einfluss auf die Wahrung der Privatsphäre aller Nutzer haben, dass die Akzeptanz und damit ein langfristiger Betrieb des ITS massiv gefährdet wird.

Die Angriffe, beschrieben in Abschnitt 3.2 können kombiniert werden, so dass Schwachstellen der Verschlüsselungsverfahren ausgenutzt werden oder ein Zugriff auf kryptografisches Schlüsselmaterial möglich wird.

Ebenso sind Angriffe vorstellbar, die zu einer Kompromitierung der Mechnismen zum Schutz der Privatsphäre führen. Die Zuordnung von Basisidentitäten zu Fahrzeugen und damit auch zu Personen durch unbefugte Dritte muss verhindert werden. Schon die Zuordnung mehrerer vorübergehend verwendeter Pseudonyme kann die Privatsphäre der Benutzer gefährden: Denkbar ist einen Angriff, bei dem pseudonymisierte ITS-Nachrichten zentral gesammelt werden, um globale Bewegungsprofile „von Haustür zu Haustür“ zu erstellen.

3.3.1 Angriffsszenario „Abhören von Kommunikation“

Da Teilnehmer am ITS auch mit dem Internet kommunizieren, ergeben sich durch das Abhören vertraulicher Kommunikation zwischen Teilnehmern und Servern IT-Sicherheitsprobleme: Der Verlust der Privatsphäre, unautorisierte Kontobewegungen oder der Diebstahl

von Firmengeheimnissen ist denkar. Ebenso können ITS-spezifische Informationen, etwa über Routen und Reiseziele, zur Vorbereitung weiterer Angriffe abgehört werden.

3.3.2 Angriffsszenario „Auflösen der Basisidentität“

Ist ein Angreifer in der Lage, die verwendete Basisidentität eines Teilnehmers aufzulösen, so versetzt ihn das in die Lage, diesen Teilnehmer nicht nur momentan, sondern potenziell zu jeder Zeit im System zu identifizieren und seinen Aufenthaltsort zu ermitteln.

3.3.3 Angriffsszenario „Zuordnung mehrerer Pseudonyme“

Wenn einem Angreifer der Startpunkt eines Fahrzeuges bekannt ist, kann automatisiert mit relativ geringem Aufwand eine Personengruppe erstellt werden, welche das Fahrzeug führen. [8].Einen Zuordnung zwischen Personen und Fahrzeugen kann zunächst nur relativ ungenau erstellt werden. Sind darüber hinaus jedoch Start-Ziel-Kombinationen bekannt, so lässt sich selbst bei extremer Ungenauigkeit der Quelldaten von mehreren Quadratkilometern noch sehr zuverlässig auf die Identität einer Person schließen.

Gelingt es einem Angreifer, mehrere verwendete Pseudonyme eines Teilnehmers einander zuzuordnen und so die Bewegungsspur eines Fahrzeugs bis zum Start einer Fahrt zurückzuverfolgen, kann die Pseudonymität dieses Teilnehmers aufgehoben werden.

4 IT-Sicherheitsanalyse

Am Anfang des Entwurfs einer Sicherheitsarchitektur für sim^{TD} steht die Analyse möglicher Gefahren und bedrohter Güter. Die Ergebnisse dieser Analyse dienen dann als Grundlage für Designentscheidungen während des Architekturentwurfs, da sie Aussagen darüber erlauben, welche Verbindungen und Daten besonders schützenswert sind und Hinweise darauf geben, welche möglichen Angriffe unterbunden werden müssen.

Die IT-Sicherheitsanalyse gliedert sich in vier Bestandteile: In Abschnitt 4.1 wird zunächst der Schutzbedarf für unterschiedliche Güter in sim^{TD} (Daten, Komponenten, Verbindungen, etc.) ermittelt. Des Weiteren werden in Abschnitt 4.2 mögliche Angreifer auf das sim^{TD}-System in verschiedene Klassen kategorisiert, entsprechend ihren Fähigkeiten und ihrer Motivationen. Auf Grundlage der Schutzbedarfsanalyse und des Angreifermodells wird dann in Abschnitt 4.3 eine Analyse der möglichen Bedrohungen in sim^{TD} durchgeführt und die sich daraus ergebenen Risiken abgeleitet. In Abschnitt 4.4 werden schließlich konkrete Anforderungen an sim^{TD} formuliert und anhand der jeweils adressierten Risiken priorisiert. Ergebnis dieses Kapitels ist eine Liste von umzusetzenden IT-Sicherheitsanforderungen, die während des Architekturentwurfs berücksichtigt werden müssen. Die im nachfolgenden Kapitel 5 entwickelten Maßnahmen wurden des besseren Überblicks halber in die Liste in Abschnitt 4.4 eingetragen, so dass der Leser dort einen direkten Überblick über die IT-Sicherheitsanforderungen und die entsprechenden Maßnahmen erhält.

4.1 Schutzbedarfsermittlung

Die Ermittlung des Schutzbedarfs erfolgt anhand einer Strukturanalyse von sim^{TD}, bei der die einzelnen Systeme, Daten, Kommunikationsverbindungen und Funktionen hinsichtlich ihrer Schutzwürdigkeit analysiert werden.

Auch wenn die Ermittlung des Schutzbedarfs anhand von sim^{TD} geschieht, so dürfte sie in weiten Teilen dennoch auch für das spätere Wirksystem zutreffend sein. Wenn allerdings bei der vorliegenden Analyse bereits erkennbar ist, dass der Schutzbedarf für ein Gut im Wirksystem anders als in sim^{TD} sein könnte, so wird entsprechend differenziert darauf eingegangen.

Als Basis für die Einordnung der schützenswerten Güter dienen die Auswirkungen von Ausfällen und erfolgreichen Angriffen auf die schützenswerten Güter, wie sie in Kapitel 3 beschrieben sind. Die detaillierte Betrachtung der Bedrohungen, Schwachstellen, Schadenshöhen und Eintrittswahrscheinlichkeiten erfolgt in Abschnitt 4.3.

4.1.1 Beschreibung der Schutzbedarfskategorien

In diesem Dokument beschränken wir uns auf die drei Schutzbedarfskategorien nach IT-Grundschutz-Handbuch des BSI.

Schutzbedarfskategorien	
1= Niedrig bis Mittel	*Die Schadensauswirkungen sind begrenzt und überschaubar*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen und Konventionalstrafen. 2. Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige

Schutzbedarfskategorien	
	Auswirkungen auf die davon Betroffenen und würden von diesen daher toleriert. 3. Die persönliche Unversehrtheit der Kunden wird nicht beeinträchtigt. 4. Mithilfe des Mobilitätssystems realisierte Dienste werden allenfalls unerheblich gestört. Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. 5. Das Ansehen der Betreiber des Mobilitätssystems bei Kunden und Partnern wird nicht beeinträchtigt. 6. Der finanzielle Verlust für den Betreiber ist tolerabel
2 = Hoch	*Die Schadensauswirkungen können beträchtlich sein*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen erhebliche juristische Konsequenzen und hohe Konventionalstrafen. ▪ Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten starke Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert. 2. Die persönliche Unversehrtheit der Kunden kann bei unglücklicher Verkettung mit externen Faktoren beeinträchtigt werden. 3. Mithilfe des Mobilitätssystems realisierte Dienste werden erheblich gestört. Die Beeinträchtigung würde von den Betroffenen als nicht akzeptabel eingeschätzt werden. 4. Eine nicht geringe Zahl von Kunden oder Partnern wird verärgert. 5. Der finanzielle Verlust für den Betreiber ist nicht tolerabel.
3 = Sehr hoch	*Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen massive juristische, insbesondere auch strafrechtliche Konsequenzen und drastische Konventionalstrafen. 2. Das informationelle Selbstbestimmungsrecht ist de facto aufgehoben und der Missbrauch personenbezogener Daten massiv gegeben. 3. Die persönliche Unversehrtheit ist direkt gefährdet. 4. Mithilfe des Mobilitätssystems realisierte Dienste werden über längere Zeit massiv gestört bzw. fallen ganz aus. 5. Eine sehr große Zahl von Kunden und große Partner werden verärgert, es resultiert ein bleibender Vertrauensverlust in das Mobilitätssystem. 6. Der finanzielle Verlust für den Betreiber ist existenzbedrohend.

Tabelle 4.1: Schutzbedarfskategorien nach IT-Grundschutz-Handbuch des BSI inhaltlich auf sim^{TD} angepasst

Diese Schutzbedarfskategorien werden auf die einzelnen IT-Sicherheitsschutzziele (siehe Abschnitt 1.4.3), angewendet, was zu jeweils drei Schutzbedarfsklassen pro Sicherheitsziel führt, aufgeführt in Tabelle 4.2. Die Bezeichner der Schutzbedarfsklasse bestehen aus einem Kürzel für das Sicherheitsziel und einer angefügten Zahl (1,2 oder 3), welche den Schutzbedarf anzeigt.

Sicherheitsziel	Schutzbedarfsklassen
Authentizität	**Atz1**: Authentizität ist hier nicht erforderlich, da gefälschte Nachrichten keine oder nur geringe Konsequenzen hätten.
	Atz2: Gefälschte Nachrichten könnten strafrechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen haben.
	Atz3: Nicht authentische Nachrichten können für den Betreiber ruinös oder den Fahrer Existenz bedrohend sein.
Autorisierung	**Atg1**: Autorisierung ist nicht erforderlich, die entsprechende Aktion (z.B. Senden einer Nachricht) kann von jeder Komponente, die dazu in der Lage ist, ausgeführt werden, ohne dass dies ein Problem darstellte.
	Atg2: Das unautorisierte Ausführen einer Aktion könnte: - strafrechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen haben. - zu lokalen Systemstörungen oder gar Systemausfällen führen.
	Atg3: Das unautorisierte Ausführen einer Aktion: - bedroht die Stabilität des Systems und führt zu massiven Störungen oder Ausfällen mit entsprechenden Auswirkungen auf den Verkehr. - könnte für den Betreiber ruinös sein oder für den Fahrer Existenz bedrohende Folgen haben.
Vertraulichkeit	**V1**: Informationen sind öffentlich. Eine Verbreitung hätte keine oder nur geringe negative Konsequenzen.
	V2: Informationen dürfen nur einem definierten Personenkreis zugänglich sein. Eine Verletzung könnte rechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen haben.
	V3: Eine Verletzung der Vertraulichkeit kann für den Betreiber ruinös und für den Fahrer Existenz bedrohend sein.
Anonymität	**An1**: Die Aufhebung der Anonymität ändert wenig oder nichts, da der Teilnehmer bereits anderweitig identifizierbar ist.
	An2: Die Aufhebung der Anonymität führt zu massiven Verletzungen des Rechts auf informationelle Selbstbestimmung der Teilnehmer. Die demokratische Gesellschaftsordnung wird durch Aushöhlung von Verfassungsgrundsätzen geschädigt.
	An3: Das Recht auf informationelle Selbstbestimmung ist nicht mehr existent, es existiert keine unüberwachte Bewegungsfreiheit mehr, die Teilnehmer werden in ihren Bewegungen und ihrer (fahrzeuggebundenen) Kommunikation total überwacht.
Pseudonymität	**Ps1**: Die Aufhebung der Pseudonymität ändert wenig oder nichts, da der Teilnehmer bereits anderweitig identifizierbar ist.
	Ps2: Die Aufhebung der Pseudonymität führt zu massiven Verletzungen des Datenschutzes und die Privatsphäre der Teilnehmer wird stark beeinträchtigt. Die demokratische Gesellschaftsordnung wird durch Aushöh-

Sicherheitsziel	Schutzbedarfsklassen
	lung von Verfassungsgrundsätzen geschädigt.
	Ps3: Das Recht auf informationelle Selbstbestimmung ist nicht mehr existent, es existiert keine unüberwachte Bewegungsfreiheit mehr, die Teilnehmer werden in ihren Bewegungen und ihrer (fahrzeuggebundenen) Kommunikation total überwacht.
Verfügbarkeit	**Vg1**: Ausfälle sind so kurz, dass keine oder nur geringe negative Konsequenzen daraus resultieren.
	Vg2: Ausfälle beeinträchtigen die Systemfunktionalität so stark, dass rechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen resultieren können.
	Vg3: Massive Ausfälle führen zu einer für den Betreiber ruinösen oder für den Fahrer Existenz bedrohenden Situation.
Verbindlichkeit	**Vb1**: Verbindlichkeit ist für den entsprechenden Dienst nicht notwendig oder das Fehlen der Verbindlichkeit führt zu keinen oder nur geringen negativen Konsequenzen.
	Vb2: Verbindlichkeit ist für den entsprechenden Dienst zwar prinzipiell notwendig, aber fehlende Verbindlichkeit führt nur zu Unterbrechungen bzw. zu einem Rückfall auf einen Dienst ohne Verbindlichkeit. Hieraus könnten allerdings rechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen resultieren.
	Vb3: Verbindlichkeit ist essentiell für einen Dienst und ihr Ausfall führt daher zu einem Totalausfall der mit dem Service verbundenen Funktionen.
Integrität	**I1**: Veränderte oder korrumpierte Nachrichten haben keine oder nur geringe Konsequenzen.
	I2:Veränderte oder korrumpierte Nachrichten haben erhebliche Konsequenzen, die zu großer Kundenunzufriedenheit führen und rechtliche, finanzielle oder das Image beeinträchtigende Konsequenzen haben können.
	I3: Veränderte oder korrumpierte Nachrichten führen zu einer für den Betreiber ruinösen oder den Fahrer Existenz bedrohenden Situation.

Tabelle 4.2: Schutzbedarfsklassen der einzelnen Sicherheitsziele

4.1.2 Strukturanalyse

Bei der Strukturanalyse im Rahmen der Schutzbedarfermittlung werden die wesentlichen schützenswerten Güter identifiziert, wobei die Analyse bei einem Detaillierungsgrad auf Ebene der groben Systemarchitektur aufsetzt. Die sich hierbei ergebenen komplexen Objekte wären natürlich noch weiter analysierbar, aber i. Allg. würde dies keinen großen Gewinn für die Sicherheitsanalyse erbringen.

Vorleistungen, d.h. Standard-Komponenten und -Systeme, die in sim^{TD} verwendet werden und für die Diensterbringung notwendig sind, aber nicht weiter analysiert werden, sind in Abschnitt 1.3.1 aufgeführt.

Im Rahmen der Schutzbedarfsanalyse betrachteten Objekte werden mit Bezeichnern der Form [Präfix_Kürzel] ausgezeichnet, wobei das Präfix auf den Typ des Gutes verweist. Folgende Typen existieren:

- Vorleistungen, mit Präfix "V", s. a. Abschnitt 1.3.1.
- Systeme bzw. Komponenten, mit Präfix "S"
- Daten, mit Präfix "D"
- Kommunikationsverbindungen, mit Präfix "K"
- Funktionale Güter, mit Präfix "F"

Eine Übersicht über die grundlegenden Akteure in sim^{TD} und ihrer Kommunikationsverbindungen zeigt Abbildung 4.1.

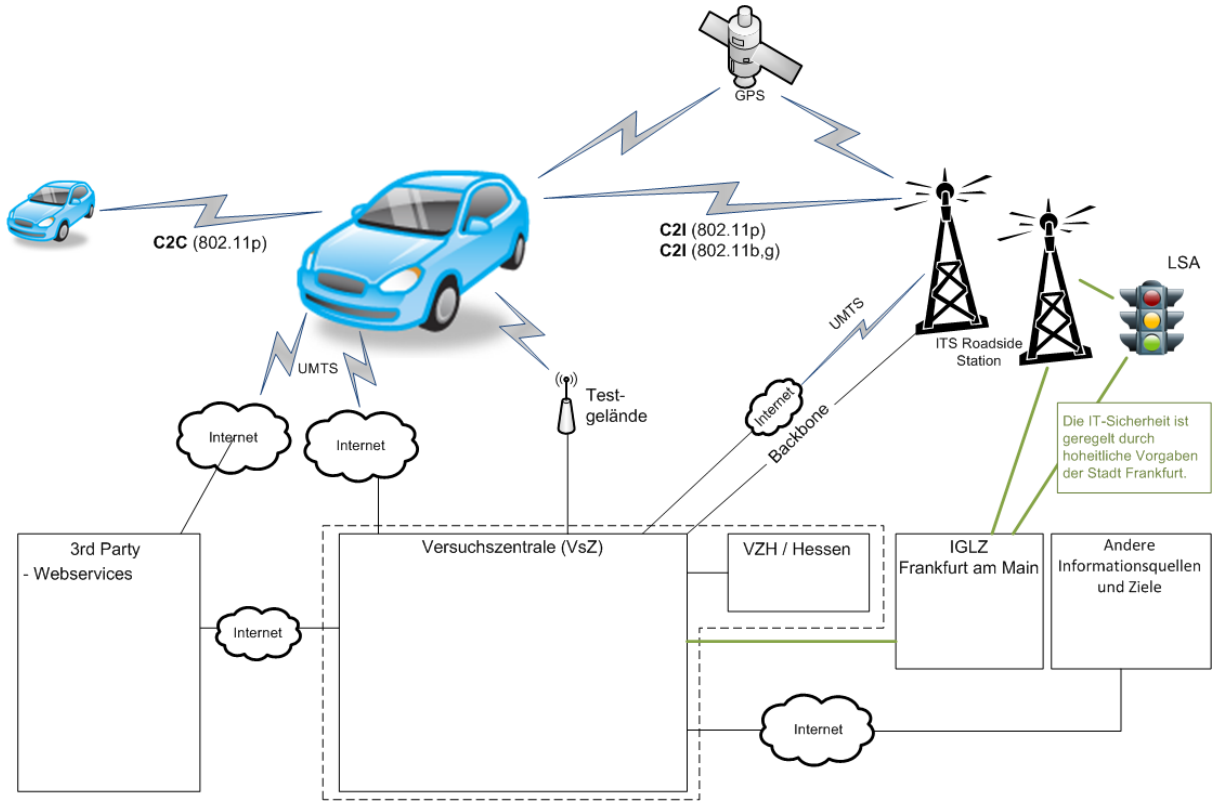

Abbildung 4.1: Referenzmodell – Akteure und Dienste in sim^{TD}

In der folgenden Analyse wird unterschieden zwischen Objekten, die stets Bestandteil eines Mobilitätssystems sein werden, und solchen, die spezifisch für das Testfeld sind und daher nur im Rahmen von sim^{TD} relevant sein werden.

4.1.2.1 Vorleistungen

Vorleistungen sind Leistungen, die von Dritten bereitgestellt werden und daher außerhalb der direkten Verantwortlichkeit von sim^{TD} liegen. Desweiteren fallen darunter Dienste und Infrastruktur-Komponenten, die zur Erbringung der Leistungen benötigt werden. Eine vollständige Auflistung aller Vorleistungen befindet sich bereits in Abschnitt 1.3.1. Daher wird auf eine erneute Auflistung im Rahmen der Strukturanalyse verzichtet.

4.1.2.2 Systemen/Komponenten – Kommunikationsakteure

Sicherlich ist in einem ITS die körperliche Unversehrtheit der Fahrer und der anderen Verkehrsteilnehmer im weitesten Sinne das höchste schützenswerteste Gut. Da sich die Gefährdungen der körperlichen Unversehrtheit allerdings im Rahmen eines ITS nicht direkt, sondern durch Beeinträchtigungen des ITS oder Fehler in diesem ergeben, kann dieses Gut nicht direkt betrachtet werden, sondern indirekt über den Schutzbedarf der Komponenten, der Kommunikationsbeziehungen und der funktionalen Güter. Somit wird nicht der Fahrer selbst betrachtet, sondern das Fahrzeug bzw. die für das ITS-relevanten Komponenten in ihm und ihre Kommunikationsbeziehungen zu anderen ITS-Komponenten.

Für die Schutzbedarfsanalyse werden die Akteure, soweit es sich um technische Objekte handelt, durch ihre wesentlichen Systeme bzw. Komponenten, die in das ITS eingebunden sind, dargestellt. Dementsprechend werden auch die Kommunikationsverbindungen nach den Komponenten benannt, an denen die Verbindungen jeweils enden.

Fahrzeuge: ITS Vehicle Station (IVS)

Bei den Fahrzeugen kann es sich um PKW, LKW, Motorräder handeln. Für die Schutzbedarfsanalyse werden die Fahrzeuge auf den Teil abstrahiert, der mit dem ITS wechselwirkt. Es handelt sich hierbei um die IVS. Diese besteht aus zwei Teilen: Einer Communication & Control Unit (CCU) und einer Application Unit (AU):

- **[S_IVS_CCU]** Vehicle Communication & Control Unit
- **[S_IVS_AU]** Vehicle Application Unit

Infrastruktur-Akteure: ITS Central Station (ICS) und ITS Roadside Station (IRS)

Auf Infrastrukturseite des ITS lassen sich auf der obersten Architekturebene (siehe Abbildung 4.1) zwei Akteure identifizieren: die ITS Roadside Stations (IRS) und die ITS Central Stations (ICS).

- ITS Roadside Stations (**IRS**): Im Wirksystem wird es wahrscheinlich verschiedene IRS Typen geben. In sim^{TD} hingegen gibt es nur einen Typ: die IRS (betrieben vom Land Hessen und der Stadt Frankfurt am Main), die mit der Versuchszentrale – auf verschiedenen Wegen (verschiedene Übertragungstechnik und Wege) – verbunden werden.
  - **[S_IRS_CCU]**: Straßenseitige Kommunikationseinheit, Roadside Communication & Control Unit (Roadside CCU) ist der Router, der sich um grundlegende Kommunikationsaspekte der Station kümmert. Im Falle einer IRS, die direkt via UMTS an die Versuchszentrale angebunden sind, verfügt die CCU noch zusätzlich über eine UMTS-Schnittstelle.
  - **[S_IRS_AU]**: Straßenseitige Application Unit, auf dem die verschiedenen Funktionskomponenten ausgeführt werden.
  - Infrastruktur-Sensoren, wie z.B. Straßenzustand- und Straßenwetter-Informations-System (SWIS), sie werden unter die Vorleistungen gezählt, s. Abschnitt 1.3.1.
  - Verkehrsbeeinflussungs- und Lichtsignalanlagen VBA/LSA: die VBA/LSA sind zum Teil direkt an ITS Roadside Stations angeschlossen. Es gibt zwei verschiedene Anbieter von VBA/LSA: die Stadt Frankfurt und das Land Hessen. Die VBA/LSA, unabhängig von Anbieter, zählen zu den Vorleistungen, da sie kabelgebunden und mit proprietären Protokollen kommunizieren, s. Abschnitt 1.3.1.
- ITS Central Stations (**ICS**): In sim^{TD} wird es nur eine ITS Central Station geben, welche die zentralen Backendkomponenten umfasst. Es handelt sich hierbei in sim^{TD}

um die Versuchszentrale VsZ. In einem Wirksystem würde es sich um Verkehrszentralen oder (integrierte) Gesamtleitzentralen von Großstädten handeln. Eine ICS besteht aus ein oder mehreren AU und Backend-Systemen.

- Die Versuchszentrale von sim^{TD} wird für die Schutzbedarfsanalyse in folgende Bestandteile zerlegt:
  - **[S_ICS_VsZ_IRS_Man]**, IRS-Management-System
  - **[S_ICS_VsZ_AU]**, weitere Software-Systeme der Versuchszentrale, z.B. für die Fahrzeugverwaltung.
  - **[S_ICS_VsZ_DB]**: Datenbank zur Speicherung der verschiedenen Versuchsdaten.
  - **[S_ICS_VsZ_PKI]**, Server auf dem die PKI-Software läuft. Die PKI wird separat betrachtet, da PKI-Systeme sicherheitskritisch sind, und deshalb in der Regel besonders technisch, physisch und organisatorisch geschützt werden müssen. Dies gilt insbesondere für das Wirksystem, das wahrscheinlich eine größerer Zahl regionaler PKI-Systeme, aber nur „eine“[6] relativ zentrale PKI haben wird.
  - **[S_ICS_VsZ_DNS]**, DNS-Server. Für Zertifikate, die Domänennamen beinhalten, muss sichergestellt sein, dass entsprechend DNS-Server erreichbar sind.
- Verkehrszentrale: Die Verkehrszentrale Hessen (VZH) wird komplett vom Land Hessen abgesichert: sie wird unter den Vorleistungen gezählt, s. Abschnitt 1.3.1.
- Die Integrierte Gesamtleitzentrale der Stadt Frankfurt am Main (IGLZ), wird komplett von der Stadt Frankfurt am Main abgesichert: sie wird unter die Vorleistungen gezählt.
- Verkehrstelematiksysteme: Diese Systeme werden für eine spätere Einführung in das Wirksystem wichtig sein, aber nicht in sim^{TD}. Für eine genaue Analyse des Schutzbedarfs müssten allerdings die entsprechenden Systeme bekannt sein. In der Schutzbedarfsanalyse wird daher nur ihre Kommunikationsschnittstelle zur Zentrale generisch berücksichtigt, s. Abschnitt 4.1.2.5.

Zur Infrastruktur gehört selbstverständlich auch die nachrichtentechnische Infrastruktur, allerdings wird bei sim^{TD} - und sicherlich auch später im Wirksystem - auf bereits vorhandene Netzwerkinfrastruktur zurückgegriffen. Diese wird ebenfalls unter zu den Vorleistungen gezählt und daher hier nicht explizit berücksichtigt.

Externe Diensteanbieter

Bei den externen Diensten (Web-Dienste) handelt es sich um solche, die nicht im Rahmen des ITS selbst, sondern von Dritten erbrachte Dienste, die eine Internet-Verbindungen zwischen Diensteanbieter und Fahrzeug verwenden. Typischerweise wird es sich um Web-Dienste handeln, die über Internetstandardprotokolle (HTTP, HTTPS, IMAP,...) mit einer Anwendung im Fahrzeug kommunizieren.

- **[S_ExtService]** Systeme externer Dienstleister, wie z.B. Flottenmanagement, Gebäudedienste, Mehrwertdienste, etc.

[6] Zur Erhöhung der Ausfallsicherheit wird man hier natürlich stets mindestens zwei Systeme auf unterschiedlichen Liegenschaften vorsehen.

Die Systeme der Anbieter externer Dienste werden als Blackbox betrachtet. Primär interessant sind die Kommunikationsverbindungen zwischen ITS-Komponenten und den externen Diensten, siehe Abschnitt 4.1.2.5.

4.1.2.3 Daten

IVS und IRS Daten

Die Daten aus dem IVS und IRS werden in diesem Abschnitt gemeinsam beschrieben, da beide Stationen in weiten Teilen identische Funktionalitäten und Komponenten besitzen.

Schlüsselmaterial

[D_IVS_Keys] und **[D_IRS_Keys]**: Hierbei handelt es sich um das langfristig gültige kryptografische Schüsselmaterial innerhalb von IVS bzw. IRS.

Umfeldtabelle

Die Umfeldtabelle ist eine der zentralen Komponenten auf der IVS- und IRS-AU (Application Units) (siehe Deliverable D21.2 [1] für die Aufbereitung und Deliverable D21.4 [9] für die Nachrichtenformate). Alle empfangenen C2X-Nachrichten werden hier verwaltet und für die Funktionen bereitgestellt. Die Funktionen können sich für die benötigten Informationen bei der Umfeldtabelle registrieren. Sobald die gewünschte Information verfügbar ist, wird diese an die Funktion weitergeleitet. Des Weiteren kann über die Umfeldtabelle die Nachbarschaftstabelle abgerufen werden. Diese beinhaltet alle CAMs der im Empfangsbereich liegenden Fahrzeuge und IRS.

In sim^{TD} werden C2X-Nachrichten definiert, von denen alle weiteren Formate abgeleitet werden. Es werden 3 Datentypen in der Umfeldtabelle unterschieden:

- CAM (Cooperative Awareness Messages): diese werden in Form einer Nachbarschaftstabelle gespeichert. Die Tabelle enthält Daten der aktuellen Kommunikationspartner, die im Empfangsbereich liegen.
- DENM (Decentralized Environmental Notification Message): diese sind Warnmeldungen oder Ereignisse im C2X-Netzwerk (siehe Kapitel Datenbasis in Deliverable D21.2).
- Alle anderen Nachrichten, die in Deliverable D21.4 definiert sind.

Wir teilen die in der Umfeldtabelle gespeicherten Daten in folgende Kategorien ein:

- **[D_IVS_CCU_U_CAM]**
- **[D_IRS_CCU_U_CAM]**
- **[D_IVS_CCU_U_DEN]**
- **[D_IRS_CCU_U_DEN]**
- **[D_IVS_CCU_U_OTHER]**
- **[D_IRS_CCU_U_OTHER]**

Logdaten

Die Logdaten bestehen aus den Live- und Messdaten der Funktionen und Systemkomponenten. **[D_IVS_Log]** und **[D_IRS_Log].**

VAPI Client (nur IVS)

- Objektliste **[D_IVS_CCU_VC_List]**: Dies ist die Liste aller Informationen, die vom VAPI Service zur Verfügung gestellt werden. Es handelt sich hierbei um eine große

Anzahl verschiedener Informationen, die von Navigation bis hin zu aktuellen Fahrzeugsteuerungsinformationen reichen, für Details, siehe Deliverable D21.2 [1]. Die Can-Bus Daten werden temporär von dem VAPI Client auf dem CCU gespeichert.

- **[D_IVS_CCU_VC_Acc]**: Zugriff auf CAN-Bus Daten: Der Zugriff auf den VAPI Service (Daten, siehe Deliverable D21.2 [1]) erfolgt über den VAPI Client. Dieser erlaubt das direkte Abrufen (Request/Response) sowie Abonnieren (Publish/Subscribe) von VAPI-Informationen.

Software

Sowohl auf der CCU als auch auf der AU sind verschiedene Softwareprogramme eingesetzt. Diese Programme haben dabei verschiedene Aufgaben: Funktionalitäten für die Kommunikation mit externen Systemen zur Verfügung stellen, Car2X Anwendungen ausführen und die Verwaltung der AU und CCU gewährleisten. Auf den CCU werden dabei fast ausschließlich native C/C++ Programme eingesetzt. Auf der AU liegen die Car2X Anwendungen als Java OSGi Bundles vor. Die Verwaltungsfunktionalitäten können sowohl durch Bundles als auch durch native (C/C++, Java, ...) Anwendungen realisiert werden. Alle zusammen repräsentieren einen großen Teil des Know-hows der verantwortlichen Institutionen. Die Anzahl der unterschiedlichen Softwarekomponenten auf der CCU und AU ist sehr hoch. Für die Strukturanalyse gruppieren wir sie anhand des Systems, auf denen sie ausgeführt werden in **[D_IVS_CCU_SW]**, **[D_IRS_CCU_SW]**, **[D_IVS_AU_SW]** und **[D_IRS_AU_SW]**. Wir nehmen hierbei an, dass bei allen ein ähnlicher Schutzbedarf besteht.

4.1.2.4 ICS Daten

Wir beschränken uns weitgehend auf die Versuchsdaten (von der Versuchszentrale), da eine Verallgemeinerung auf das Wirksystem aufgrund der fehlenden Spezifikation nicht sinnvoll wäre.

Kryptografisches Schlüsselmaterial

- **[D_ICS_Keys]** langfristig gültiges kryptografisches Schüsselmaterial der zentralen Systeme, z.B. CA-Root-Schüssel.

Versuchsdaten

Es werden hier in wesentlichen 3 Datentypen[7] unterschieden: Logdaten als Messdaten, Monitoring-Daten als Livedaten und Steuerungsdaten für die Durchführung von Tests. Darüber hinaus sind noch die Software selbst und die DGPS Daten zu nennen.

Messdaten **[D_ICS_AU_Mess]** werden von allen Quellen (IVS, IRS, ICS) gesammelt und werden nach Auswertung zur Verfügung gestellt. Beispielsweise wird der Abstand zum vorausfahrenden Fahrzeug bei der sim^{TD}-internen Flotte per LIDAR erfasst.

Livedaten **[D_ICS_AU_Live]** dienen der Versuchsverwaltung für die Auswertung des Versuchs. Es sind auch die Daten, die zeitnah weitergegeben werden (z.B. an den Leitstand).

Steuerungsdaten **[D_ICS_AU_SD]** sind Daten, die für das Drehbuch, die Ad-Hoc Anweisungen, Versuchsanweisungen, Versuchsüberwachung und Defektmeldungen benutzt werden.

Software Bundles **[D_ICS_AU_SW]** repräsentieren Funktionen zur Planung, Durchführung und Bewertung von Versuchen.

---

[7] Zur Benennung der Kürzel: ICS steht für die (Versuchs) Zentrale, AU für Application Unit, d.h. als die Anwendung, und das Kürzel dahinter für den jeweiligen Typ von Daten.

Differential GPS **[D_ICS_AU_DGPS]** sind Daten, die von einem Drittanbieter in sim^{TD} zur Verfügung gestellt werden, um die Positionierung von IRS und IVS zu verbessern.

4.1.2.5 Kommunikationsverbindungen

Im Rahmen von sim^{TD} sollen verschiedene Arten von Übertragungstechniken auf ihren Einsatz in einem ITS getestet werden. Im Wirkbetrieb eines ITS werden möglicherweise auch heterogene Übertragungstechniken eingesetzt werden. Dem wird dadurch Rechnung getragen, dass in der Schutzbedarfsfeststellung die Kommunikationsverbindungen bei Bedarf anhand der Übertragungstechnik differenziert werden. Im folgenden Abschnitt werden zuerst die Kommunikationsverbindungen aufgeführt, die sowohl im ITS (voraussichtlich) vorhanden sein werden, als auch in sim^{TD} existieren; danach folgen die für sim^{TD} spezifischen Kommunikationsverbindungen.

Fahrzeugseitige Kommunikation

Hierbei handelt es sich um alle Kommunikationsverbindungen, welche von und zum Fahrzeug gehen. Im Fahrzeug ist die Vehicle Communication & Control Unit (Vehicle CCU) für die gesamte Kommunikation im Rahmen des ITS und die Kommunikation zu Drittanbietern via ITS zuständig. Folgende Kommunikationsverbindungen können auftreten:

- **[K_C2C_11p]** Kommunikation zwischen zwei Fahrzeugen, verwendet stets IEEE 802.11p
- **[K_C2I_11p]** Kommunikation zwischen Vehicle CCU und Roadside CCU, verwendet IEEE 802.11p
- **[K_C2I_VsZ_cell]** direkte Kommunikation zwischen Vehicle CCU und der (Versuchs)Zentrale via ITS IMT Public (UMTS/GPRS): z.B. für den Upload von Testprotokollen. Im Rahmen von sim^{TD} wird hierdurch die im Wirksystem vorhandene Kommunikationsbeziehung zwischen einem Fahrzeug und einem externen Dienstanbieter ebenfalls abgedeckt, da die externen Dienste von Drittanbietern durch einen Server in der Versuchszentrale emuliert werden.
- **[K_C2I_ExtServ_cell]** Kommunikation zwischen Vehicle CCU und externen Diensten/Mehrwertdiensten via ITS IMT Public (UMTS bzw. GSM)

Nur in sim^{TD}:

- **[K_C2I_ExtServ_11bg]** Kommunikation zwischen Vehicle CCU und externen Diensten/Mehrwertdiensten via Consumer-WLAN (IEEE 802.11 b/g), aller Voraussicht nach wird dies im Rahmen vom sim^{TD} höchstens für die Überspielung von Daten aus den Fahrzeugen in die Versuchszentrale verwendet, während die Fahrzeuge auf dem Testgelände geparkt sind.
- **[K_C2I_11bg]** direkte Kommunikation zwischen Vehicle CCU und der Infrastruktur, insbesondere einfache Verkehrsbeeinflussungsanlagen (z.B. Verkehrszeichen und Baustellenausschilderungen), verwendet teilweise Consumer-WLAN (IEEE 802.11 b/g), die Kommunikation wird häufig unidirektional von der Infrastruktur ausgehen (Broadcasts). Beispielsweise werden von der Funktion 3.1.2 Standortinformationen via Broadcast übertragen.

Infrastrukturseitige Kommunikation

Bei der infrastrukturseitigen Kommunikation steht die Versuchszentrale von sim^{TD} stellvertretend für eine ITS-Zentrale (ICS).

- **[K_I2I_IRS_VsZ_cell]** Kommunikation zwischen Roadside CCU und Versuchszentrale. Diese verwendet ITS IMT Public (UMTS bzw. GPRS)

- ***[K_I2I_IRS_IGLZ]*** Kommunikation zwischen Roadside CCU und IGLZ wird nicht betrachtet. Diese Kommunikation läuft über Kupferadern, siehe Vorleistungen, Abschnitt 1.3.1.
- ***[K_I2I_IRS_VZH]*** Kommunikation zwischen Roadside CCU und VZH. Diese Kommunikation verwendet Glasfaser. Die Verbindungen über Glasfaser werden hier nicht betrachtet, siehe Vorleistungen, Abschnitt 1.3.1.

Verbindungen Dritter zu einer ITS-Zentrale

- **[K_SimPart_VsZ]** Kommunikation zwischen den sim^{TD} -Partnern und der Versuchszentrale. Diese Kommunikation wird über das öffentliche Internet laufen. Bei der Zentrale eines ITS könnte diese Verbindung z.B. einem Wartungsfernzugang entsprechen.

[*K_ExtServ_VsZ*] Kommunikation zwischen externen Diensteanbietern und der (Versuchs)Zentrale, diese Verbindung existiert bei simTD nicht, da externe Dienste durch einen Server in der Versuchszentrale emuliert werden.

Verbindungen zwischen ITS-Zentralen

- **[*K_I2I_IGLZ_VsZ*]** Kommunikation zwischen IGLZ und der Versuchszentrale. Diese Kommunikation läuft über eine dedizierte Glasfaser und ist dadurch nicht Teil der IT-Sicherheitsbetrachtung. Siehe Vorleistungen, Abschnitt 1.3.1.
- **[*K_I2I_VZH_VsZ*]** Kommunikation zwischen VZH und der Versuchszentrale. Diese Kommunikation wird in Rahmen von sim^{TD} nicht betrachtet, da sich die Versuchszentrale und das VZH innerhalb der gleichen Liegenschaft befinden, siehe Vorleistungen, Abschnitt 1.3.1.

Nur in sim^{TD}:

- **[K_I2I_VsZ_TestgInd]** Kommunikation zwischen der Versuchszentrale und ihrem Ableger auf dem Testgelände.

4.1.2.6 Funktionale Güter

Als funktional schützenswerte Güter werden Dienste/Funktionen bezeichnet, die auf Basis von sicheren, intelligenten Mobilitätssystemen, hier also von sim^{TD}, realisiert werden. Bei Störungen des unterliegenden Mobilitätssystems aufgrund von Ausfällen, Fehlern oder Angriffen kann es daher auch zu Beeinträchtigungen oder Fehlfunktionen dieser funktional schützenswerten Güter kommen.

Im Deliverable D11.4 werden Funktionen des ITS beschrieben sowie in Hauptfunktionen und Unterfunktionen eingeteilt. Im Rahmen der Schutzbedarfsanalyse wird die Bewertung nur auf Basis der Hauptfunktionen vorgenommen. Der Schutzbedarf der Hauptfunktion wird dabei bestimmt durch den jeweils höchsten Schutzbedarf der dazugehörigen Unterfunktionen.

[F_VLage] ***Erfassung der Verkehrslage***

Diese Hauptfunktion ermittelt Daten zur Verkehrslage basierend auf infrastrukturseitiger und fahrzeugseitiger Datenerfassung und stellt diese den anderen Hauptfunktionen zur weiteren Verarbeitung zur Verfügung. Es handelt sich um einen Basisdienst.

[F_VInfoNavi] ***Verkehrsinformation und Navigation***

Diese Hauptfunktion stellt Informationen zu Verkehrsereignissen und der Verkehrslage sowie zum Straßenwetter unbewertet auf Anzeigen im Fahrzeug dar oder verwendet diese zur Dynamischen Routenplanung.

[F_VSteu] ***Verkehrssteuerung***

Diese Hauptfunktion ermittelt aus Daten, die in der Verkehrsinfrastruktur gewonnen werden, zusammen mit Daten, die die Fahrzeuge melden, optimierte, verkehrsabhängige Steuerstrategien für Lichtsignalanlagen in Verkehrsnetzen oder an Knotenpunkten sowie für ein Umleitungsmanagement in Gebieten mit hoher Verkehrslast.

[F_LokWarn] ***Lokale Gefahrenwarnung***

Diese Hauptfunktion beinhaltet Funktionen zur Warnung des Fahrers vor lokalen Gefahren. Gemeinsames Element ist die autonome Detektierung von lokalen Gefahren durch die Fahrzeuge und das Aussenden entsprechender Gefahrenmeldungen.

[F_FahrAssist] ***Fahrerassistenz***

In dieser Hauptfunktion sind Assistenzfunktionen zusammengefasst, die den Fahrer bei seinen „normalen“ Fahraufgaben unterstützen sollen.

[F_IntNet_LokInf] ***Internetzugang und lokale Informationsdienste***

In dieser Hauptfunktion wird der Internetzugang im Fahrzeug genutzt, um Verkehrsdaten und Kommunalinformation sowie Informationen zur Parksituation im Fahrzeug verfügbar zu machen. Diese Funktionen sind stellvertretend für vielfältige Nutzungsmöglichkeiten des Internets im Fahrzeug.

4.1.3 Feststellung des Schutzbedarfs

In den folgenden Abschnitten wird für die verschiedenen Arten von schützenswerten Gütern in tabellarischer Form der Schutzbedarf für ein Wirksystem und sim^{TD} dargestellt. Hierbei werden für die einzelnen Sicherheitsziele die in Tabelle 4.2 aufgeführten Kürzel für die Schutzbedarfskategorien verwendet.

In den folgenden Tabellen steht in der übergeordneten Spalte „Schutzbedarf“ der entsprechende Schutzbedarf für ein Wirksystem, abgekürzt mit ITS, und für das Versuchssystem sim^{TD}.

Für den Feldversuch im Rahmen von sim^{TD} wäre es ausreichend den für sim^{TD} eingetragenen und notwendigen Schutzbedarf zu berücksichtigen. Es ist aber sehr empfehlenswert stattdessen für sim^{TD} den Schutzbedarf des Wirksystems zugrunde zu legen, damit etwaige Probleme mit Absicherungsmaßnahmen, die nur im Wirksystem notwendig sind, bereits im Feldversuch bemerkt werden und nicht erst später beim Betrieb eines ITS.

Bei einigen Gütern kann noch nicht auf den Schutzbedarf bei einem Wirksystem geschlossen werden oder die entsprechenden Güter sind ohnehin stark sim^{TD}-spezifisch. In diesen Fällen steht in dem entsprechenden Feld „n.a.“.

Angesichts der großen Anzahl von Schutzzielen, werden in den Feldern für den Schutzbedarf nur die Ziele eingetragen, bei denen ein mittlerer oder hoher Schutzbedarf vorliegt.

4.1.3.1 Systeme und Komponenten

Der Schutzbedarf bei den Systemen ist stark abhängig davon, ob es sich um ein „einzelnes“ zentrales System handelt oder um ein vielfach vorhandenes (wie IVS oder IRS).

Generell wird das Schutzziel Verfügbarkeit, das bei zentralen Elementen eines Wirksystems äußerst wichtig ist, bei einem Testsystem wie sim^{TD} nur eine kleine Rolle spielen, daher finden sich dort auch keine Einträge.

Eine PKI wird im Fall eines Wirksystems sehr wahrscheinlich auf Basis eines (dedizierten) Trustcenters aufgebaut werden, daher wird hier die PKI *mit allen Daten* als ein System betrachtet.

In Tabelle 4.3 wird für das fahrzeugseitige System ein hoher Grad an Anonymität bzw. Pseudonymität gefordert. Bewusst wurde dabei auch der Aspekt der Anonymität für ein ITS berücksichtigt. Dies geschah mit dem Ziel, die Anforderungen an ein ITS mit maximaler informationeller Selbstbestimmung aufzuzeigen. Ein solches ITS schließt jegliche[8] Möglichkeit der Fahrzeugortung und der Erstellung von Bewegungsprofilen aus.

Allerdings ist dies im Rahmen der bisherigen ITS-Planung nicht vorgesehen. Hier wird lediglich Pseudonymität angestrebt. Dies bedeutet, dass die Infrastruktur im Normalfall die Identität eines Fahrzeugs nicht erkennt, da dieses Pseudonyme verwendet. Anhand von Protokollierungsdaten der PKI könnte ein Pseudonym jedoch bei Bedarf der Identität des jeweiligen Fahrzeugs und damit einer Person zugeordnet werden.

Man kann sich durchaus legitime Anwendungen einer solchen Pseudonymauflösung vorstellen, beispielsweise nach einem Unfall oder einer massiven ITS-Störung könnte im Nachhinein festgestellt werden, von welchem Fahrzeug (absichtlich) fehlerhafte Daten gesendet wurden.

Die Auflösung von Pseudonymen zur zugehörigen Basisidentität wird oft mit der Zuordnung von Kraftfahrzeugkennzeichen zu dem zugehörigen Halter verglichen, da auch diese Zuordnung nur unter bestimmten Bedingungen zulässig und überdies auf staatliche Stellen beschränkt ist. Dieser Vergleich hinkt allerdings, da die Pseudonym-Auflösung ein erheblich größeres Missbrauchspotential mit sich bringt.

Deshalb empfiehlt es sich, dringend die entsprechenden Fragen im Rahmen eines Sicherheitskonzeptes für ein ITS (Wirksystem) noch einmal gründlich zu diskutieren und technisch schwer zu überwindende Barrieren einzubauen, die den oben angedeuteten Missbrauch eines ITS verhindern können.

Systeme und Komponenten	**Schutzbedarf**		**Begründung**
	ITS	**sim^{TD}**	
[S_IVS_CCU]	**An3**, **Ps3**, **I3**, **Vb3**	**Ps2**, **I2**	Das System ist wichtig für die Übermittlung von Informationen, welche die Sicherheit des Fahrers und des Fahrzeugs betreffen, daher die hohe Anforderung an die Ausfallsicherheit. Es dürfen keine Informationen das System verlassen, die eine Zuordnung zu einer statischen Identität (z.B. der Basisidentität) zulassen. Statische Identitätsinformationen sollten minimal sein. Integrität und Verbindlichkeit sind wichtig im Falle von juristischen Auseinandersetzungen bei Unfällen usw.
[S_IVS_AU]	**An3**, **Ps3**, **I3**,	**Ps2**, **I2**	Das System ist wichtig für die Übermittlung von Informationen, welche die Sicherheit des Fahrers und des Fahrzeugs betreffen, daher die hohe

[8] Dies bedeutet, dass es selbst dann nicht möglich wäre, wenn ein Angreifer Zugriff auf alle Daten der infrastrukturseitigen Systeme samt PKI hätte.

Systeme und Komponenten	Schutzbedarf		Begründung
	ITS	sim^{TD}	
	Vb3		Anforderung an die Ausfallsicherheit. Es dürfen keine Informationen das System verlassen, die eine Zuordnung zu einer statischen Identität zulassen. Integrität und Verbindlichkeit sind wichtig im Falle von juristischen Auseinandersetzungen bei Unfällen usw.
[S_IRS_CCU]	**I3**, **Vb3**	**I2**	Verfügbarkeit ist i. Allg. nicht kritisch, da nur einzelne IRS lokal ausfallen. Integrität und Verbindlichkeit sind wichtig im Falle von juristischen Auseinandersetzungen bei Unfällen usw.
[S_IRS_AU]	**I3**, **Vb3**, **Atg3**	**I2**, **Atg2**	Verfügbarkeit ist i. Allg. nicht kritisch, da nur einzelne IRS lokal ausfallen. Integrität und Verbindlichkeit sind wichtig im Falle von juristischen Auseinandersetzungen bei Unfällen usw.
[S_ICS_VsZ_IRS_Man]	**Vg3**, **I3**, **Atg3**	**Atg2**, **I2**	Die Managementsysteme müssen stets verfügbar und integer sein. Zudem darf nur autorisierter Zugriff möglich sein.
[S_ICS_VsZ_AU]	**Vg3**, **I3**, **Atg3**	**Atg2**, **I2**	Die Anforderungen für die Managementsysteme lassen sich auf die Anwendungsserver übertragen, da sie eine kritische Komponenten zur Erbringung der Dienste sind.
[S_ICS_VsZ_DB]	**Vg3**, **I3**, **Atg3**	**Atg2**, **I2**	Für die Datenbank ist wie üblich ein Rollenkonzept notwendig.
[S_ICS_VsZ_PKI]	**Vg3**, **I3**, **V3**, **Ps3**, **Atg3**	**Atg2**, **I2**, **Ps2**	Die PKI ist ohne zusätzliche Maßnahmen stets in der Lage die Pseudonymität, welche durch Pseudonyme gewährleistet wird, aufzuheben, deshalb muss sichergestellt werden, dass dies nicht geschieht.
[S_ICS_VsZ_DNS]	**Vg3**		Authentizität und Integrität der DNS-Nachrichten wird nicht gefordert, da diese Sicherheitsziele anderweitig (durch Zertifikate) realisiert werden.

Tabelle 4.3: Feststellung des Schutzbedarfs – Systeme

4.1.3.2 Daten

Daten	Schutzbedarf		Begründung
	ITS	sim^{TD}	
[D_IVS_CCU_U_CAM] **[D_IVS_CCU_U_DEN]**	**Atz3**, **Vg3**, **I3**, **Ps3**	**Ps2**, **I2**	Es handelt sich hierbei um Broadcast-Nachrichten, so dass Vertraulichkeit per se unnötig ist (und auch nur schwer zu realisieren wäre).
• **[D_IRS_CCU_U_CAM]** • **[D_IRS_CCU_U_DEN]**	**Atz3**, **Vg3**, **I3**,	**I2**	Die IRS haben öffentliche Funktionen und sind keiner Person zuordenbar, Pseudonymität ist nicht notwendig.
[D_IRS_Log]	**Atz3**, **I3**	**Atz2**, **I2**	Es darf nicht möglich sein, unerkennbar Logdaten fälschen zu können.
[D_IVS_Log]	n.a.	**Atz2**, **I2**	Es darf nicht möglich sein, unerkennbar Logdaten fälschen zu können. (Es handelt sich hierbei um die Logdaten speziell für Test in sim^{TD}.
[D_IRS_Keys]	**Atz3**, **I3**, **V3**		Es darf nicht möglich sein, eine IRS zu fälschen bzw. zu kopieren. Hardware Schutzmechanismen gegen Auslesen von Schlüsselmaterialen sind für das Wirksystem sehr wichtig, für sim^{TD} allerdings nicht erforderlich.
[D_IVS_Keys]	**Atz3**, **I3**, **V3**		Hardware Schutzmechanismen gegen Auslesen von Schlüsselmaterialen sind für das Wirksystem sehr wichtig, für sim^{TD} allerdings nicht erforderlich.
[D_IVS_CCU_VC_List]	**Atz3**, **I3**,	**Atz2**, **I2**	Diese Daten stellen die fahrzeugseitige Basis für viele Funktionen des ITS dar, da müssen die authentisch und integer sein.
[D_IVS_CCU_VC_Acc]	**Atg3**	**Atg2**	Der Zugriff auf die CAN-Bus-Daten darf nur autorisiert durchgeführt werden.
[D_ICS_Keys]	**Atz3**, **I3**, **V3**,	**V2**	Die PKI ist ohne zusätzliche Maßnahmen stets in der Lage die Pseudonymität, welche durch Pseudonyme gewährleistet wird, aufzuheben, deshalb muss sichergestellt werden, dass dies nicht geschieht.
[D_ICS_AU_Mess]	n.a.	**Atz2**, **I2**	Die entsprechend Daten in sim^{TD} müssen authentisch und integer sein, damit die Versuchsauswertung sinnvoll möglich ist.

Daten	Schutzbedarf		Begründung
	ITS	sim^{TD}	
[D_ICS_AU_Live]	n.a.	**Atz2**, **I2**	Die entsprechend Daten in sim^{TD} müssen authentisch und integer sein, damit die Versuchsauswertung sinnvoll möglich ist.
[D_ICS_AU_SD]	n.a.	**Atz2**, **I2**	Die entsprechend Daten in sim^{TD} müssen authentisch und integer sein, damit die Versuchsauswertung sinnvoll möglich ist.
[D_ICS_AU_SW] **[D_IRS_AU_SW]** **[D_IVS_AU_SW]** **[D_IVS_CCU_SW]** **[D_IRS_CCU_SW]**	**Atz3**, **I3**, **Atg3**	**Atz2**, **I2**, **Atg2**	Software-Manipulation muss vermieden werden.

Tabelle 4.4: Feststellung des Schutzbedarfs – Daten

4.1.3.3 Kommunikationsverbindungen

Kommunikations-verbindungen	Schutzbedarf		Begründung
	ITS	sim^{TD}	
[K_C2C_11p]	**Atz3**, **I3**, **Vg3**	**Atz3**, **I3**	Sichere Mobilität lässt sich nur mit einer authentischen, integeren und stets verfügbare Inter-Fahrzeug-Kommunikation erreichen.
[K_C2I_11p]	**Atz3**, **I3**, **Vg3**	**Atz3**, **I3**	Es gelten hier die gleichen Maßstäbe wie bei der Fahrzeug-zu-Fahrzeug-Kommunikation.
[K_C2I_11bg]	n.a.	**Atz2**,**I2**, **V2**	Im Rahmen von sim^{TD} werden hierüber umfang-reichere Logdaten usw. übertragen. Für das Über-tragen anderer Daten im Ad-Hoc-Modus wird in sim^{TD} keine Vertraulichkeit benötigt.
[K_C2I_VsZ_cell]	**Atz3**, **V3**, **I3**, **Vg3**,	**Atz2**, **I2**, **V2**	Zwischen Fahrzeug und der Zentrale müssen vertrauliche Daten, glaubwürdig und integer ausgetauscht werden.
[K_C2I_ExtServ_11bg]	**Atz2**, **I2**, **V2**	**Atz2**, **I2**, **V2**	Der genaue Schutzbedarf hängt stark von der Anwendung ab. Es handelt sich um Übertragun-gen, welche für die Verkehrssicherheit nicht relevant sind.
[K_C2I_ExtServ_cell]	**Atz2**, **I2**, **V2**	**Atz2**, **I2**, **V2**	Der genaue Schutzbedarf hängt stark von der Anwendung ab. Es handelt sich um Übertragun-gen, welche für die Verkehrssicherheit nicht relevant sind. Grundschutz ist teilweise durch das Mobilfunk-Netz gegeben.
[K_I2I_IRS_VsZ_cell]	**Atz2**, **I3**, **V3**, **V2Vg2**	**Atz2**, **I2**, **V2**	IRS, die nicht über Glasfaser angeschlossen sind, kommunizieren via Mobilfunk mit der Zentrale, daher muss hier zusätzlich noch die Vertraulichkeit geschützt werden.

Kommunikations-verbindungen	Schutzbedarf		Begründung
	ITS	sim^{TD}	
[K_SimPart_VsZ]	**Atz3**, **I3**, **V3**	**Atz3**, **I3**, **V3**	Eine mangelnde Absicherung dieses Zugriffs zur Zentrale könnte bei einem Angriff zur vollständigen Systemkompromittierung führen.
[*K_ExtServ_VsZ*]	**Atz3**, **I3**, **V3**, **Vg3**	**Atz2**, **I2**, **V2**	Über diese Verbindung werden u.a. sicherheitskritische Zertifikatsinformationen laufen.
[K_I2I_VsZ_TestgInd]	n.a.	**Atz3**, **I3**, **V3**	Diese Verbindung muss als prototypisch für eine Verbindung zwischen Zentralen (ICS) in einem ITS gesehen werden. Diese Verbindungen sind nur zwischen berechtigten Endpunkten, vertraulich und integritätsgeschützt aufzubauen. Die Verfügbarkeitsanforderungen sind im Wirkbetrieb eines ITS natürlich höher als bei sim^{TD}.

Tabelle 4.5: Feststellung des Schutzbedarfs – Kommunikationsverbindungen

4.1.3.4 Funktionale Güter

Bei den funktionalen Gütern wird der Schutzbedarf nur auf Basis der Hauptfunktionen analysiert, da eine Darstellung mit allen Unterfunktionen viel zu unübersichtlich wäre. Dementsprechend wird der Schutzbedarf für eine Hauptfunktion durch den jeweils maximalen Schutzbedarf der Unterfunktionen bestimmt, was gerade beim Wirksystem zu hohen Werten für den Schutzbedarf führt.

Generell gilt, dass die funktionalen Güter eines ITS eine hohe Verfügbarkeit haben müssen, da sich die Fahrer (und auch die Verkehrsleitzentralen) nach hinreichender Abdeckung sehr schnell an die Funktionen gewöhnen werden.

Generell muss bei allen Funktionen auch sichergestellt sein, dass die zu ihnen gehörenden Informationen bzw. Aktionsvorschläge authentisch und integer sind. Zudem muss Verbindlichkeit gegeben sein.

Eine wichtige Rolle nimmt bei den Funktionen auch die Anonymität bzw. Pseudonymität ein, da häufig Daten vom Fahrzeug übertragen werden, die bei laufender Nachverfolgung oder in Korrelation mit anderen Datensätzen Rückschlüsse auf private Belange der Fahrer zulassen, somit also sein Recht auf informationelle Selbstbestimmung gefährden könnten.

Funktionale Güter	Schutzbedarf		Begründung
	Wirksystem	sim^{TD}	
[F_VLage]	**I3**, **Atz3**, **Vb3**, **Ps3**, **Vg3**, **V3**	**Atz2**, **I2**, **V2**	Einige Funktionen dieser Klasse übertragen schützenswerte persönliche Daten (z.B. Reiseziele), deren Vertraulichkeit gewährleistet sein muss. s.a. Text im Vorspann
[F_VInfoNavi]	**I3**, **Atz3**, **Vb3**, **Ps3**, **Vg3**	**Atz2**, **I2**,	s.o. Text im Vorspann
[F_VSteu]	**I3**, **Atz3**, **Vb3**,	**Atz2**, **I2**,	s.o. Text im Vorspann

Funktionale Güter	Schutzbedarf		Begründung
	Wirksystem	**sim^{TD}**	
	Ps3, **Vg3**		
[F_LokWarn]	**I3**, **Atz3**, **Vb3**, **Ps3**, **Vg3**	**Atz2**, **I2**,	s.o. Text im Vorspann
[F_FahrAssist]	**I3**, **Atz3**, **Vb3**, **Ps3**, **Vg3**	**Atz2**, **I2**,	s.o. Text im Vorspann
[F_IntNet_LokInf]	**I3**, **Atz3**, **Vb3**, **Ps3**, **V3**, **Atg2**	**Atz2**, **I2**, **V2 Atg2**	In sim^{TD} werden zwar nur kostenfreie Dienste betrachtet, aber in einem Wirksystem werden häufig kostenpflichtige Dienste angeboten. Daher spielen Vertraulichkeit und Autorisierung hier eine größere Rolle.

Tabelle 4.6: Feststellung des Schutzbedarfs – Funktionale Güter

4.2 Angreifermodell

Ein wichtiger Teil einer IT-Sicherheitsanalyse ist die Betrachtung der potenziellen Angreifer. Diese unterscheiden sich hinsichtlich ihrer Motivation, ihres Zieles und der zur Verfügung stehenden Mittel (Geld, Zeit, Rechenkapazität, …). Diese Eigenschaften eines Angreifers begrenzen dessen Möglichkeiten, Verwundbarkeiten in einem IT-System auszunutzen.

4.2.1 Angreiferfähigkeiten

Die Fähigkeiten eines Angreifers entsprechen dessen zur Verfügung stehenden Möglichkeiten auf das ITS in kommunikationstechnischer, physischer und sozialer Hinsicht einzuwirken. Im Rahmen der Betrachtung der Angreiferfähigkeiten werden Klassen von Angreifern identifiziert und zusammen mit den ihnen zugrunde gelegten Fähigkeiten vorgestellt. Eine solche Angreiferklasse beinhaltet insbesondere auch das herrschende Vertrauensverhältnis zwischen Teilnehmer und Angreifer. Die erfolgte Kategorisierung ist kurz in Tabelle 4.7 (S. 49) zusammengefasst.

4.2.1.1 [P_0] Angriffe aus dem Internet

Angriffe aus dem Internet finden von außerhalb des ITS statt.

Diese Angreifer haben zwar Kenntnis von der Funktionsweise der beteiligten Komponenten, sie sind jedoch physisch nicht anwesend und damit lediglich in der Lage, über das Internet auf den Feldversuch bzw. auf Benutzer des ITS einzuwirken.

4.2.1.2 [P_1] Angriffe durch anwesende Dritte

Auch Angriffe anwesender Dritter finden aus logischer Sicht von außerhalb des ITS statt.

Sie sind jedoch bedingt durch ihre unmittelbare physische Präsenz durchaus in der Lage, auch Kommunikation auf der Endbenutzerseite von 802.11p und Consumer-WLAN zu manipulieren, sowie eigene Endgeräte an eine bestehende Netzwerkinfrastruktur anzuschließen.

4.2.1.3 [P_2] Angriffe durch Teilnehmer

Bei Angriffen von Teilnehmern des sim^{TD}-Feldversuchs, bzw. Benutzern des ITS kann angenommen werden, dass sie ein gültiges Basisidentität besitzen.

Sie verfügen damit zusätzlich über jederzeit aktuelles, gültiges Schlüsselmaterial und sind in der Lage, eigene UMTS-Übertragungen zu senden sowie den Inhalt generierter Datenpakete beliebig zu manipulieren.

4.2.1.4 [P_3] Angriffe durch mit der Kfz-Wartung betraute Personen

Personal, das mit der Wartung der Fahrzeuge betraut ist, die am ITS teilnehmen verfügt prinzipbedingt nicht nur über physikalischen Zugriff auf die Komponenten, sondern auch das für gezielte Eingriffe nötige Fachwissen. Dies ist insbesondere der Fall, falls die Wartung sich auf die fahrzeugseitigen Komponenten IVS-CCU und IVS-AU erstrecken soll.

Angreifer dieser Klasse sind somit in der Lage, in den Besitz gültiger, fremder Basisidentitäten zu gelangen.

4.2.1.5 [P_4] Angriffe durch Wartungstechniker

Personal, das mit der Wartung infrastrukturseitiger Komponenten des ITS betraut ist verfügt darüber hinaus auch über Zugang zu diesen Komponenten.

Angreifer dieser Klasse werden damit in die Lage versetzt, zusätzlich in fremde UMTS-Übertragungen einzugreifen, den Systemaufbau des Gesamtsystems zu ihren Gunsten zu verändern, Netzwerk-Übertragungen zwischen Infrastrukturkomponenten aktiv zu verändern, sowie umfassende Informationen über den aktuellen wie auch vergangenen Status aller Teilnehmer zu empfangen und zu speichern.

4.2.1.6 [P_5] Angriffe durch in der Mächtigkeit dem Betreiber gleichzusetzende Personen

Diese Klasse von Angreifern bildet die Oberklasse aller bisher genannten Angreifertypen und schließt darüber hinaus all solche potenziellen Angreifer ein, denen ein universeller und zeitlich fast unbegrenzter Zugriff auf das ITS möglich ist.

Zusätzlich zu den bereits genannten Angriffen ist diese Klasse von Angreifern jederzeit in der Lage, unabhängig von den tatsächlich registrierten Benutzern eine beliebige Anzahl gültiger Basisidentitäten zu generieren.

	P_0	P_1	P_2	P_3	P_4	P_5
Kenntnis des Systemaufbaus	☑	☑	☑	☑	☑	☑
Zugriff über Internet	☑	☑	☑	☑	☑	☑
Eingriff in fremde 802.11p-Übertragungen		☑	☑	☑	☑	☑
Eingriff in fremde C-WLAN-Übertragungen		☑	☑	☑	☑	☑
Zugang zur Netzwerkinfrastruktur		☑	☑	☑	☑	☑

	P_0	P_1	P_2	P_3	P_4	P_5
Besitz einer personalisierten Basisidentität			☑	☑	☑	☑
Eingriff in eigene UMTS-Übertragungen			☑	☑	☑	☑
Besitz fremder Basisidentität				☑	☑	☑
Eingriff in fremde UMTS-Übertragungen					☑	☑
Eingriff in den Systemaufbau					☑	☑
Eingriff in LAN-Übertragungen					☑	☑
Kenntnis des Status der Teilnehmer					☑	☑
Erzeugung neuer Basisidentitäten						☑

Tabelle 4.7: Angreifermodell für das ITS: Mittel und Fähigkeiten verschiedener Klassen von Angreifern.

4.2.2 Angreifermotivation

Neben den Fähigkeiten eines Angreifers spielt auch seine Motivation eine entscheidende Rolle. Angreifer verfolgen unterschiedliche Ziele, die sich auf ihr Angriffsverhalten auswirken. In der folgenden Tabelle werden unterschiedliche Kategorien von Angriffsmotivationen, wie sie in der nachfolgenden Bedrohungsanalyse verwendet werden dargestellt.

Angriffsmotivation	**Beschreibung**
Vandalismus	Angreifer, die dieses Ziel verfolgen sind auf eine maximale Beeinträchtigung des sim^{TD}-Systems aus. Für die Erreichung dieses Angriffziels sind Methoden geeignet, die die sim^{TD}-Funktionen möglichst lange und wirksam sabotieren.
Wissenschaftlicher Anreiz	Angreifer die das Ziel *Wissenschaftlicher Anreiz* verfolgen, sind an Angriffsmethoden interessiert, die hohe wissenschaftliche Reputation versprechen oder die durch „sportlichen Ehrgeiz“ motiviert werden. Um dieses Ziel zu erreichen werden daher Angriffe gewählt, die auf möglichst drastische Ergebnisse zielen oder welche die Verwundbarkeit von sicher geglaubten Komponenten aufzeigen.
Finanzieller Anreiz	Durch die Verfolgung des Ziels *Finanzieller Anreiz* erhoffen sich Angreifer einen möglichst großen finanziellen Profit von der Durchführung des entsprechenden Angriffs. Beispiele hierfür sind zum einen Angriffe zur Erlangung verwertbarer Daten (z.B. Versuchsergebnisse) sowie Angriffe, die für Erpressungen geeignet sind, also z.B. auf persönliche Daten zielen oder eine Beeinträchtigung der sim^{TD}-Funktion androhen (insofern kann es hier ggf. Überscheidungen mit dem Angriffsziel *Vandalismus* geben).

Tabelle 4.8: Definition der Angriffsziele

4.3 Bedrohungs- und Risikoanalyse

Ziel der Bedrohungsanalyse ist es, mögliche Ursachen (organisatorisch, technisch und durch Benutzer hervorgerufene Ursachen) zu identifizieren, die zum Fehlschlagen des sim^{TD}-Versuchs führen könnten. In der daran anschließenden Risikoanalyse wird für jede Ursache das damit verbundenen Risiko ermittelt.

Um für die Bedrohungsanalyse zumindest die kritischsten Ursachen vollständig zu erfassen, bedarf es eines systematischen Vorgehens, dessen Umsetzung in diesem Abschnitt beschrieben wird. Zur Ermittlung der möglichen Bedrohungsursachen wird zunächst ein Bedrohungsbaum erstellt, der ausgehend von der allgemeinen Bedrohung *Versuch fehlgeschlagen* untergeordnete Bedrohungen und ihre Ursachen ableitet. Die möglichen Ursachen werden anschließend den in Abschnitt 4.1 ermittelten schutzbedürftigen Gütern zugeordnet, um einen Überblick über besonders bedrohte Güter zu erhalten. Es werden während der Bedrohungsanalyse nur die schutzbedürftigen Güter mit Schutzbedarf mittel bis sehr hoch berücksichtigt (für eine Übersicht der Güter und ihrer Schutzbedarfklassen siehe Abschnitt 4.1). Anschließend wird für jede Bedrohung das resultierende Risiko ermittelt. Hierzu werden unter Berücksichtigung des in Abschnitt 4.2 erarbeiteten Angreifermodells Wahrscheinlichkeiten für entsprechende Angriffe so wie der ggf. daraus resultierende Schaden abgeschätzt. Die genaue Vorgehensweise der Risikoanalyse wird weiter unten in Abschnitt 4.3.3 erklärt.

4.3.1 Ermitteln der High-Level Bedrohungen

Für die Analyse möglicher Risiken und Bedrohungen in sim^{TD} ist es zunächst erforderlich, alle möglichen Gefährdungen des Systems zu identifizieren. Hierzu werden die aus den Angriffsszenarien in Kapitel 3 hervorgehenden Bedrohungen in eine Baumstruktur übertragen und schrittweise verfeinert, um letztlich möglichst alle Angriffsursachen zu finden. Der resultierende Bedrohungsbaum ist in Abbildung 4.2 dargestellt. Für sim^{TD} wurden – wie in Abschnitt 1.1 erläutert – Vorannahmen getroffen, durch die einige der Bedrohungen von vornherein ausgeschlossen werden, weil sie entweder nicht im Rahmen der sim^{TD}–Architektur beeinflusst werden können (z.B. Dienste externer Anbieter oder Mobilfunk-Infrastrukturen) oder im Rahmen des sim^{TD}-Versuchs nicht umgesetzt werden (z.B. Trusted Platform Modules (TPM), die den unberechtigten Zugriff auf das kryptografische Schlüsselmaterial verhindern). Um den Umfang der Bedrohungsanalyse überschaubar zu halten und gleichzeitig eine für den Versuch relevante Risikoeinschätzung zu erhalten, werden solche Bedrohungen in der nachfolgenden Analyse nicht betrachtet. In Abbildung 4.2 sind solche Bedrohungen ausgegraut dargestellt. Weiter werden für die Analyse nur Bedrohungen bis zur vierten Ebene des Baumes (beginnend mit Ebene 1: *Versuch fehlgeschlagen*) berücksichtigt. Alle feingranulareren Bedrohungen dienen dem besseren Verständnis, werden aber in der Risikoanalyse zusammengefasst bearbeitet.

Abbildung 4.2: Bedrohungsbaum mit Ebenen 1 bis 6

Die allgemeine Bedrohung des Projektes ist mit *Versuch fehlgeschlagen* beschrieben. Sie wird in die drei Hauptbedrohungen unterteilt, die sich aus den Angriffsszenarien in Kapitel 3 ergeben. Die Bedrohung *Versuch sabotiert* beinhaltet dabei Angriffe, die von außen die Funktionsweise des Systems gezielt stören. Dies bedeutet jedoch nicht, dass alle Möglichkeiten, den sim^{TD}-Versuch zu sabotieren unter dieser Bedrohung zusammengefasst sind. Eine Sabotage des sim^{TD}-Versuchs kann durchaus auch Folge einer der anderen Bedrohungen (z.B. *Aufzeichnung falscher Daten*) sein, jedoch sind diese primär auf gezielte Angriffe von innerhalb des Systems bezogen.

4.3.2 Bedrohungen schützenswerter Güter

Die folgende Tabelle enthält alle Bedrohungen bis zur dritten Ebene. Dies sind die Bedrohungen, die im Hinblick auf sim^{TD} untersucht werden.

Kürzel	Beschreibung	Funkt. Güter	Daten	System /Kom.	Komm.Verbindungen
B_Sab	**Versuch sabotiert**				
B_SabDosÜbe	Überlast	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]			[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_SabDosRou	Routing	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]		**[S_IVS_AU] [S_IRS_CCU] [S_IRS_AU] [S_IVS_CCU]**	[K_C2I_11p] [K_C2I_11bg] [K_I2I_IRS_VsZ_cell]
B_Versfehler	**Versuchsdaten fehlerhaft**				
B_VersfehlerFFahranw	Falsche Fahranweisungen	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]	[D_ICS_AU_SW] [D_IRS_AU_SW] [D_IVS_AU_SW] [D_IRS_CCU_SW] [D_IVS_CCU_SW]	**[S_IVS_AU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell]
B_VersfehlerNbaFahranw	Nichtbeachtung von Fahranweisungen	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]	[D_IVS_AU_SW] [D_IVS_CCU_SW]	**[S_IVS_AU] [S_IVS_CCU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell]
B_VersfehlerUnbfTeiln	UnbefugteTeilnahme • Eigene Hardware • Impersonation • Sybil-Angriffe	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]	[D_ICS_AU_SW] [D_IVS_CCU_SW] [D_IRS_CCU_SW] [D_IVS_AU_SW] [D_IRS_AU_SW]	**[S_IVS_CCU] [S_IRS_CCU] [S_IVS_AU] [S_IRS_AU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2C_11p]
B_VersfehlerAufzUnvstDaten	Aufzeichnung unvollständiger Daten	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]	[D_ICS_AU_SW] [D_IVS_CCU_SW] [D_IRS_CCU_SW] [D_IVS_AU_SW] [D_IRS_AU_SW]	**[S_IVS_CCU] [S_IRS_CCU] [S_IVS_AU] [S_IRS_AU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2C_11p]

Kürzel	Beschreibung	Funkt. Güter	Daten	System /Kom.	Komm.Verbindungen
B_VersfehlerManipvSoftw	Manipulation von Software • Malware • Eigene/Veränderte OSGi-Bundles	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]	[D_ICS_AU_SW] [D_IVS_CCU_SW] [D_IRS_CCU_SW] [D_IVS_AU_SW] [D_IRS_AU_SW]	**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2C_11p]
B_VersfehlerManipvÜbertr	Manipulation von Übertragungen • Manipulation von sim^{TD} Übertragungen	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]	**[D_IVS_CCU_U_CAM]** **[D_IRS_CCU_U_CAM]** [D_IVS_CCU_U_DEN] **[D_IRS_CCU_U_DEN]** [D_IVS_Log] [D_IRS_Log] [D_ICS_AU_Mess] [D_ICS_AU_Live]	**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_VersfehlerÄnderAufgzDat	Veränderung der aufgezeichneten Daten	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]	**[D_IVS_CCU_U_CAM]** **[D_IRS_CCU_U_CAM]** [D_IVS_CCU_U_DEN] **[D_IRS_CCU_U_DEN]** [D_IVS_Log] [D_IRS_Log] [D_ICS_AU_Mess] [D_ICS_AU_Live]	**[S_IRS_CCU]** **[S_IRS_AU]**	[K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2C_11p] [K_I2I_IRS_VsZ_cell]
B_VersfehlerÄnderBÜbertr	Veränderung bei Übertragung	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]	**[D_IVS_CCU_U_CAM]** **[D_IRS_CCU_U_CAM]** [D_IVS_CCU_U_DEN] **[D_IRS_CCU_U_DEN]** [D_ICS_AU_Mess] [D_ICS_AU_Live]	**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_VersfehlerÄnderBZsmstl	Veränderung beim Zusammenstellen der Daten	[F_VLage] [F_VInfoNavi][F_VSteu]	**[D_IVS_CCU_U_CAM]** **[D_IRS_CCU_U_CAM]**	**[S_IRS_CCU]** **[S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg]

Kürzel	Beschreibung	Funkt. Güter	Daten	System /Kom.	Komm.Verbindungen
		[F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]	[D_IVS_CCU_U_DEN] **[D_IRS_CCU_U_DEN]** [D_ICS_AU_Mess] [D_ICS_AU_Live] [D_IVS_CCU_VC_List] [D_IVS_CCU_VC_Acc]		[K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_VersfehlerÄnderDZsmgstID	Veränderung der zusammen-gestellten Daten	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]	**[D_IVS_CCU_U_CAM]** **[D_IRS_CCU_U_CAM]** [D_IVS_CCU_U_DEN] **[D_IRS_CCU_U_DEN]** [D_ICS_AU_Mess] [D_ICS_AU_Live]	**[S_IRS_CCU]** **[S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_UnbefDaten	**Unbefugter Zugriff auf Daten**				
B_UnbefDatenAusl	Auslesen von Versuchsdaten • gespeichert • während Übertragung • nach Zusammenstellung	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]		**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]
B_UnbefDatenZuordnPersPseu	Zuordnung Person/Fahrzeug ←→ Basisidentität	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]		**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	
B_UnbefDatenZuordnPseuPseu	Zuordnung Pseudonym ←→ Pseudonym	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist]		**[S_IVS_CCU]** **[S_IRS_CCU]** **[S_IVS_AU]** **[S_IRS_AU]**	

Kürzel	Beschreibung	Funkt. Güter	Daten	System /Kom.	Komm.Verbindungen
B_UnbefDatenMithrnVertrlKom	Mithören vertraulicher Kommunikation • Fahranweisungen • C2C-Kommunikation • C2I-Kommunikation • VsZ-Kommunikation	[F_VLage] [F_VInfoNavi][F_VSteu] [F_LokWarn] [F_FahrAssist] [F_IntNet_LokInf]		**[S_IVS_CCU] [S_IRS_CCU] [S_IVS_AU] [S_IRS_AU]**	[K_C2C_11p] [K_C2I_11p] [K_C2I_11bg] [K_C2I_VsZ_cell] [K_C2I_ExtServ_11bg] [K_I2I_IRS_VsZ_cell] [K_SimPart_VsZ]

Tabelle 4.9: Bedrohungen schützenswerter Güter

4.3.3 Risikoabschätzung

In vorherigen Abschnitt wurden die Bedrohungen ermittelt aber nicht bewertet. Um die Bewertung durchführen zu können, wird im Rahmen der Risikoanalyse für jedes der identifizierten Bedrohungsszenarien die Eintrittswahrscheinlichkeit und die Schadenshöhe ermittelt. Die Eintrittswahrscheinlichkeit und die potenziellen Schadenshöhe ist jeweils mit Ziffern von 1 (niedrig), 2 (mittel) oder 3 (hoch) klassifiziert[9].

4.3.3.1 Ermitteln der Eintrittswahrscheinlichkeit

Um eine möglichst gute Abschätzung der Eintrittswahrscheinlichkeit zu erreichen, wird zum einem die Attraktivität des Angriffes und zum anderen der erforderliche Aufwand abgeschätzt. Die Attraktivität eines Angriffes wird – abhängig von der Motivation des Angreifers – anhand der in Abschnitt 4.2 definierten Ziele *Vandalismus*, *Wissenschaftlicher Anreiz* und *Finanzieller Anreiz* eingestuft.

Jede Bedrohung wird im Hinblick auf ihre Attraktivität für eines der drei Angriffsziele auf einer Skala von 1 (irrelevant) bis 3 (sehr attraktiv) bewertet. Analog wird der benötigte Aufwand für die Durchführung eines Angriffs von 1 (geringer Aufwand) bis 3 (sehr hoher Aufwand) abgeschätzt.

Die Eintrittswahrscheinlichkeit wird nicht nur durch die Attraktivität eines Angriffs im Hinblick auf ein Angriffsziel bestimmt, sondern auch durch die Fähigkeiten eines Angreifers. Hierzu verwenden wir die Klassifizierung der Angreifer (P_0 bis P_5) wie sie im Angreifermodell in Abschnitt 4.1.2.1 erarbeitet wurde.

Um die gesamte Eintrittwahrscheinlichkeit für eine Bedrohung zu ermitteln, wird in einem ersten Schritt die Eintrittwahrscheinlichkeit für jeden Angreifertyp ermittelt: Hierzu wird für jeden Angreifertyp i das Verhältnis Attraktivität AT_j zu Aufwand AU_i berechnet und der Mittelwert ermittelt.

$$E_i = \frac{1}{3}\left(\sum_{j=1}^{3}\frac{AT_j}{AU_i}\right)$$

Anschließend wird die gesamte Eintrittswahrscheinlichkeit E wie folgt berechnet:

$$E = \frac{1}{6}\left(\sum_{i=1}^{6} E_i\right)$$

Tabelle 4.10 listet einzelne Bedrohungen nach der Schwere des Schadens und der Angriffswahrscheinlichkeit bewertet auf. Bedrohungen der ersten und zweiten Ebene sind nicht

[9] Aufgrund der Tatsache, dass die Eintrittswahrscheinlichkeiten nicht im Bereich zwischen 0 und 1 liegen, handelt es sich strenggenommen nicht um Wahrscheinlichkeiten im mathematischen Sinne. Der Wertebereich von 1 bis 3 wurde gewählt um die Lesbarkeit zu erhöhen und ist ohne Belang für die nachfolgende Risikoabschätzung. Eine Skalierung der Eintrittswahrscheinlichkeiten mit dem Faktor 0,1 würde der mathematischen Definition genügen ohne das Ergebnis zu verändern.

enthalten, ihre Angriffswahrscheinlichkeiten und Schadensauswirkungen ergeben sich aus den untergeordneten Bedrohungen.

Bedrohung	Aufwand/ Schwierigkeit für Angreifertyp						Attraktivität für Angreifer			E
	P_0	P_1	P_2	P_3	P_4	P_5	Vandalismus	Wissenschaft	Finanz.	
B_Sab										
B_SabDosÜbe	3	2	2	2	1	1	3	1	3	1,49
B_SabDosRou	3	2	2	2	1	1	3	2	3	1,70
B_Versfehler										
B_VersfehlerFFahranw	3	3	3	2	1	1	2	1	1	0,78
B_VersfehlerNbaFahranw	3	3	3	2	1	1	2	1	1	0,78
B_VersfehlerUnbfTeiln	3	3	2	1	1	1	2	2	1	1,16
B_VersfehlerAufzUnvstDaten	3	3	2	1	1	1	3	2	1	1,39
B_VersfehlerManipvSoftw	3	2	2	1	1	1	3	3	2	1,93
B_VersfehlerManipvÜbertr	3	2	2	2	1	1	3	3	1	1,49
B_VersfehlerÄnderAufgzDat	3	2	2	1	1	1	3	2	1	1,44
B_VersfehlerÄnderBÜbertr	3	3	2	2	1	1	3	2	1	1,22
B_VersfehlerÄnderBZsmstl	3	3	2	2	1	1	3	2	1	1,22
B_VersfehlerÄnderDZsmgstlD	3	2	2	1	1	1	3	2	1	1,44
B_UnbefDaten										
B_UnbefDatenAusl	3	2	2	1	1	1	1	3	3	1,69
B_UnbefDatenZuordnPersPseu	3	3	2	1	1	1	1	2	3	1,39
B_UnbefDatenZuordnPseuPseu	3	3	2	1	1	1	1	2	3	1,39
B_UnbefDatenMithrnVertrlKom	3	3	2	2	2	1	1	3	3	1,23

Tabelle 4.10: Eintrittswahrscheinlichkeit aller Bedrohungen

4.3.3.2 Ermitteln der Schadenshöhe

Um ihre Kritikalität abzuschätzen, werden Bedrohungen unterschiedlichen Schadenklassen zugewiesen. Eine Schadensklasse stellt dar, wie hoch der mögliche Schaden ausfiele, der

durch eine Bedrohung hervorgerufen würde. Analog zu Abschnitt 4.1 werden an dieser Stelle mögliche Schäden in drei unterschiedliche Schadenshöhen klassifiziert:

Schadensklasse	Beschreibung
1= Niedrig bis Mittel	*Die Schadensauswirkungen sind begrenzt und überschaubar*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen und Konventionalstrafen. 2. Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen daher toleriert. 3. Die persönliche Unversehrtheit der Kunden wird nicht beeinträchtigt. 4. Mithilfe des Mobilitätssystems realisierte Dienste werden allenfalls unerheblich gestört. Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. 5. Das Ansehen der Betreiber des Mobilitätssystems bei Kunden und Partnern wird nicht beeinträchtigt. 6. Der finanzielle Verlust für den Betreiber ist tolerabel
2 = Hoch	*Die Schadensauswirkungen können beträchtlich sein*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen erhebliche juristische Konsequenzen und hohe Konventionalstrafen. ▪ Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten starke Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert. 2. Die persönliche Unversehrtheit der Kunden kann bei unglücklicher Verkettung mit externen Faktoren beeinträchtigt werden. 3. Mithilfe des Mobilitätssystems realisierte Dienste werden erheblich gestört. Die Beeinträchtigung würde von den Betroffenen als nicht akzeptabel eingeschätzt werden. 4. Eine nicht geringe Zahl von Kunden oder Partnern wird verärgert. 5. Der finanzielle Verlust für den Betreiber ist nicht tolerabel.
3 = Sehr hoch	*Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen*, d.h.: 1. Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen massive juristische, insbesondere auch strafrechtliche Konsequenzen und drastische Konventionalstrafen. 2. Das informationelle Selbstbestimmungsrecht ist de facto aufgehoben und der Missbrauch personenbezogener Daten massiv gegeben. 3. Die persönliche Unversehrtheit ist direkt gefährdet. 4. Mithilfe des Mobilitätssystems realisierte Dienste werden über längere Zeit massiv gestört bzw. fallen ganz aus.

Schadensklasse	Beschreibung
	5. Eine sehr große Zahl von Kunden und große Partner werden verärgert, es resultiert ein bleibender Vertrauensverlust in das Mobilitätssystem. 6. Der finanzielle Verlust für den Betreiber ist existenzbedrohend.

Tabelle 4.11: Definition der Schadensklassen

Jeder der Bedrohungen wurde bereits eine Liste betroffener Güter zugewiesen (siehe Tabelle 4.9: Bedrohungen schützenswerter Güter). Weiterhin wurde jedem Gut ein Schutzbedarf zugeordnet (siehe Tabelle 4.3, Tabelle 4.4, Tabelle 4.5 und Tabelle 4.6). Aus diesen Daten wurde die maximale Schadenshöhe einer Bedrohung nun wie folgt abgeleitet: Für jede Bedrohung wurde die Gesamtheit aller von ihr betroffenen Güter sowie deren Schutzbedarf ermittelt. Aus dem höchsten Schutzbedarf ergibt sich jeweils die maximale Schadenshöhe, die in Tabelle 4.12 dargestellt ist. Da es sich um den jeweils maximalen anzunehmenden Schaden handelt, bewegen sich die Werte größtenteils im oberen Bereich der Skala 1 – 3.

Bedrohung	Schadens-höhe	Begründung
B_Sab		
B_SabDosÜbe	3	Durch DoS-Angriffe können sim^{TD} -Funktionen außer Kraft gesetzt werden und so indirekt, bei Verkettung unglücklicher Verkettung von Umständen, eine Gefahr für die körperliche Unversehrtheit der Fahrer darstellen.
B_SabDosRou	3	Durch DoS-Angriffe können sim^{TD} -Funktionen außer Kraft gesetzt werden und so indirekt, bei Verkettung unglücklicher Verkettung von Umständen, eine Gefahr für die körperliche Unversehrtheit der Fahrer darstellen.
B_Versfehler		
B_VersfehlerFFahranw	3	Das Erteilen falscher Fahranweisungen kann im Einzelnen zu verfälschten Versuchdaten führen. Der Schaden bleibt jedoch begrenzt und überschaubar.
B_VersfehlerNbaFahranw	3	Die Nichtbeachtung von Fahranweisungen kann im Einzelnen zu verfälschten Versuchdaten führen. Der Schaden bleibt jedoch begrenzt und überschaubar.
B_VersfehlerUnbfTeiln	3	Eine unbefugte Teilnahme am sim^{TD} -Versuch könnte Kunden und Partner verärgern, das Ansehen des Betreibers schädigen und zu Beeinträchtigungen einzelner sim^{TD} -Funktionen führen. Obwohl keine unmittelbare Gefahr für Teilnehmer droht und der direkt finanzielle Schaden wahrscheinlich gering bliebe, wird diese Bedrohung daher mit 2 eingestuft.
B_VersfehlerAufzUnvstDaten	3	Die Aufzeichnung unvollständiger Daten kann – je nach Umfang der Datenmenge – zur Beeinträchtigung oder zum Fehlschlagen des Versuchs führen. Die Unvollständigkeit großer Datensätze stellt daher ein nicht akzeptables Risiko dar.

Bedrohung	Schadens-höhe	Begründung
B_VersfehlerManipvSoftw	3	Eine Manipulation der verwendeten Software – etwa ein Austauschen von OSGi-Bundles in der IVS durch bösartige Software hätte gravierende Folgen die, je nach Absicht des Angreifers, zur Preisgabe vertraulicher Daten bis hin zur Fälschung von Versuchsergebnissen oder DoS-Angriffe auf andere Fahrzeuge. Aufgrund des hohen Schadenspotentials wurde diese Anforderung mit 3 eingestuft.
B_VersfehlerManipvÜbertr	2	Eine Manipulation von übertragenen Daten kann zur Beeinträchtigung des Versuchs führen. Dies stellt ein hohes Risiko dar.
B_VersfehlerÄnderAufgzDat	3	Nachträgliches Ändern von bereits aufgezeichneten Daten birgt ein höheres Risiko als eine Modifikation während der Übertragung, da hierdurch eine größere Datenmenge bedroht ist. Sollten wesentliche Teile der sim^{TD} -Versuchsdaten manipuliert werden so ist ein Fehlschlagen des Versuchs möglich und das damit verbundene Risiko daher nicht akzeptabel.
B_VersfehlerÄnderBÜbertr	2	Die Schadenshöhe ist analog zu B_VersfehlerManipvÜbertr.
B_VersfehlerÄnderBZsmstl	3	Die Schadenshöhe ist analog zu B_VersfehlerÄnderAufgzDat.
B_VersfehlerÄnderDZsmgstlD	3	Die Schadenshöhe ist analog zu B_VersfehlerÄnderAufgzDat.
B_UnbefDaten		
B_UnbefDatenAusl	3	Auslesen unbefugter Daten kann zum einen zur Verletzung von Verträgen führen und zum anderen eine unautorisierte Veröffentlichung der Versuchsergebnisse zur Folge haben. Daher wurde diese Schadenshöhe mit 3 bewertet.
B_UnbefDatenZuordnPersPseu	2	Eine Zuordnung von Pseudonymen durch unbefugte Dritte stellt eine Verletzung der Privatsphäre von Fahrern dar und könnte in einer Vertragsverletzung sowie negativen Reaktionen führen. Der potenzielle Schaden wurde daher mit 2 bewertet.
B_UnbefDatenZuordnPseuPseu	2	Eine Zuordnung von Pseudonymen durch unbefugte Dritte stellt eine Verletzung der Privatsphäre von Fahrern dar und könnte in einer Vertragsverletzung sowie negativen Reaktionen führen. Der potenzielle Schaden wurde daher mit 2 bewertet.
B_UnbefDatenMithrnVertrlKom	3	Mithören vertraulicher Kommunikation kann zum einen zur Verletzung von Verträgen führen und zum anderen eine unautorisierte Veröffentlichung der Versuchsergebnisse zur Folge haben. Daher wurde diese Schadenshöhe mit 3 bewertet.

Tabelle 4.12: Schadenshöhe aller Bedrohungen

4.3.3.3 Ermitteln des Gesamtrisikos

Der endgültige Wert für das Risiko ergibt sich aus der Eintrittswahrscheinlichkeit einer Gefährdung, bezogen auf den Zeitraum eines Jahres, und der Schadenshöhe bei erfolgtem Eintritt. Die Ermittlung des Risikos ist anhand folgender Beziehung durchzuführen (siehe auch [2]):

*Risiko = Schadenshöhe (S) * Eintrittswahrscheinlichkeit (E)*

Aufgrund der für Eintrittswahrscheinlichkeit und Risiko definierten Skala von 1 bis 3 liegen die möglichen Werte für das Risiko zwischen 0,33 und 9.

Bedrohung	Schadenshöhe (S)	Eintrittswahrscheinlichkeit (E)	Risiko (S · E)	Sicherheitsanforderung
B_Sab				
B_SabDosÜbe	3	1,49	4,47	SIMTD-48 Rechtzeitigkeit von CAMs und DENMs SIMTD-28 Plausibilitätsprüfung von Nachrichten
B_SabDosRou	3	1,70	5,1	SIMTD-28 Plausibilitätsprüfung von Nachrichten
B_Versfehler				
B_VersfehlerFFahrmnv	3	0,78	2,34	SIMTD-59 Authentizität von ICS Steuerungsdaten SIMTD-47 Rechtzeitigkeit von Fahrerinformationen
B_VersfehlerNbaFahranw	3	0,78	2,34	SIMTD-47 Rechtzeitigkeit von Fahrerinformationen
B_VersfehlerUnbfTeiln	3	1,16	3,48	SIMTD-43 Autorisierung aller Teilnehmer (widerrufbar) SIMTD-27 Erkennung von Pseudonymmissbrauch SIMTD-26 Authentizität des Nachrichtenerstellers SIMTD-25 Authentizität von CAM-Nachrichten SIMTD-4 Revokation von Pseudonymen SIMTD-2 Authentizität von DENM-Nachrichten

Bedrohung	Schadenshöhe (S)	Eintrittswahrscheinlichkeit (E)	Risiko (S · E)	Sicherheitsanforderung
B_VersfehlerAufzUnvstDaten	3	1,39	4,17	SIMTD-44 Vollständigkeit der Logging-Daten
B_VersfehlerManipvSoftw	3	1,93	5,75	SIMTD-63 Autorisierung für Zugang zur ICT Central Station SIMTD-62 Autorisierung für Zugang zur IRS SIMTD-61 Autorisierung für Zugang zur IVS SIMTD-60 Integrität der verwendeten Software
B_VersfehlerManipvÜbertr	2	1,49	2,98	SIMTD-13 Authentische Baustelleninformationen von IRS an Fahrzeug SIMTD-12 Authentizität der Straßenvorausschau-Kartendaten SIMTD-64 Absicherung der Verbindungen über "öffentliche" Netze
B_VersfehlerÄnderAufgzDat	3	1,44	4,32	SIMTD-62 Autorisierung für Zugang zur IRS SIMTD-61 Autorisierung für Zugang zur IVS SIMTD-58 Authentizität von ICS Livedaten SIMTD-57 Authentizität von ICS Messdaten SIMTD-53 Authentizität von IRS Logging-Daten SIMTD-38 Integrität der IVS Daten internetbasierter Dienste SIMTD-37 Autorisierter Zugriff auf die Daten internetbasierter Dienste in ICS SIMTD-36 Integrität der Daten internetbasierter Dienste in ICS SIMTD-31 Integrität von Standortinformationen auf IRS SIMTD-30 Integrität von Standortinformationen auf IVS

Bedrohung	Schadenshöhe (S)	Eintrittswahrscheinlichkeit (E)	Risiko (S · E)	Sicherheitsanforderung
B_VersfehlerÄnderBÜbertr	2	1,22	2,44	SIMTD-59 Authentizität von ICS Steuerungsdaten SIMTD-58 Authentizität von ICS Livedaten SIMTD-57 Authentizität von ICS Messdaten SIMTD-50 Authentizität von Daten der Standortinformationsdienste SIMTD-35 Integrität der Informationen internetbasierter Dienste SIMTD-34 Authentizität von Daten der Internetbasierten Dienste SIMTD-25 Authentizität von CAM-Nachrichten SIMTD-24 Authentizität von Straßenwetterwarnungen SIMTD-17 Sichere Anbindung externer Webservices SIMTD-13 Authentische Baustell-eninformationen von IRS an Fahrzeug SIMTD-12 Authentizität der Straßenvorausschau-Kartendaten SIMTD-2 Authentizität von DEN-Nachrichten SIMTD-64 Absicherung der Verbin-dungen über "öffentliche" Netze
B_VersfehlerÄnderBZsmstl	3	1,22	3,66	SIMTD-58 Authentizität von ICS Livedaten SIMTD-57 Authentizität von ICS Messdaten SIMTD-53 Authentizität von IRS Logging-Daten
B_VersfehlerÄnderDZsmgstlD	3	1,44	4,32	SIMTD-63 Autorisierung für Zugang zur ICT Central Station SIMTD-62 Autorisierung für Zugang zur IRS SIMTD-58 Authentizität von ICS

Bedrohung	Schadenshöhe (S)	Eintrittswahrscheinlichkeit (E)	Risiko (S · E)	Sicherheitsanforderung
				Livedaten SIMTD-57 Authentizität von ICS Messdaten SIMTD-53 Authentizität von IRS Logging-Daten SIMTD-38 Integrität der IVS Daten internetbasierter Dienste SIMTD-37 Autorisierter Zugriff auf die Daten internetbasierter Dienste in ICS SIMTD-36 Integrität der Daten internetbasierter Dienste in ICS SIMTD-32 Integrität von Standortinformationen in ICS SIMTD-31 Integrität von Standortinformationen auf IRS SIMTD-30 Integrität von Standortinformationen auf IVS
B_UnbefDaten				
B_UnbefDatenAusl	3	1,69	5,07	SIMTD-45 Vertraulichkeit der Logging-Daten (gespeichert) SIMTD-39 Autorisierter Zugriff auf die Daten internetbasierter Dienste auf IVS SIMTD-16 Black Box Funktion in der IVS nur mit Einwilligung des Benutzers
B_UnbefDatenZuordnPersPseu	2	1,39	2,78	SIMTD-45 Vertraulichkeit der Logging-Daten (gespeichert) SIMTD-20 Keine Rückverfolgbarkeit von Personen durch Positionsketten in DEN-Nachrichten SIMTD-18 Wechsel von Pseudonymen SIMTD-16 Black Box Funktion in der IVS nur mit Einwilligung des Benutzers SIMTD-11 Anonymisierte Speicherung persönlicher Daten in der

Bedrohung	Schadenshöhe (S)	Eintrittswahrscheinlichkeit (E)	Risiko (S · E)	Sicherheitsanforderung
				RSU SIMTD-8 Nicht-Zuordenbarkeit von Pseudonym zu Basisidentität
B_UnbefDatenZuordnPseuPseu	2	1,39	2,78	SIMTD-62 Autorisierung für Zugang zur IRS SIMTD-61 Autorisierung für Zugang zur IVS SIMTD-45 Vertraulichkeit der Logging-Daten (gespeichert) SIMTD-42 Nicht-Zuordenbarkeit von Pseudonym zu Pseudonym SIMTD-20 Keine Rückverfolgbarkeit von Personen durch Positionsketten in DENM-Nachrichten SIMTD-18 Wechsel von Pseudonymen SIMTD-11 Anonymisierte Speicherung persönlicher Daten in der RSU
B_UnbefDatenMithrnVertrlKom	3	1,23	3,69	SIMTD-33 Vertraulichkeit von Informationen per Internetbasierte Dienste SIMTD-29 Vertraulichkeit individuell angefragter Standortinformationen SIMTD-10 Vertraulichkeit von persönlichen IVS Daten SIMTD-64 Absicherung der Verbindungen über "öffentliche" Netze

Tabelle 4.13: Risiken und resultierende Sicherheitsanforderungen aller Bedrohungen

4.4 IT-Sicherheitsanforderungen

Nach der Analyse des Schutzbedarfs, der potenziellen Bedrohungen und der tatsächlich in sim^{TD} existierenden Bedrohungen werden nun in diesem Abschnitt die daraus resultierenden Anforderungen an das IT-Sicherheitskonzept aufgelistet. Dazu wurde zunächst die bereits existierende Liste von IT-Sicherheitsanforderungen aus Deliverable D11.4 [10] herangezogen. Diese Liste wurde anhand des Sicherheitsbedarfs einzelner FETs erstellt und stellt nur einen groben Überblick über die Sicherheitsanforderungen in sim^{TD} dar. Auf Basis der nun

vorliegenden detaillierten IT-Sicherheitsanalyse wurde die Anforderungsliste überarbeitet, neue Anforderungen wurden hinzugefügt und Duplikate entfernt. Des Weiteren wurden die IT-Sicherheitsanforderungen anhand der jeweiligen Risiken nach „Relevanz“ priorisiert. Dazu wurde für jede Anforderung die Summe aller durch sie adressierten Risiken gewichtet. Die entsprechenden Summen sind in der nachfolgenden Tabelle aufgeführt, es ist jedoch wichtig zu betonen, dass diese Zahlen nur eine grobe Einordnung der Relevanz der IT-Sicherheits-anforderungen erlauben, da sie z.B. die Wirksamkeit der geforderten Maßnahmen außer Acht lassen. Eine hohe Relevanz kann sich beispielsweise auch für eine Anforderung ergeben, die viele Sicherheitsbedrohungen adressiert, jedoch nur von geringer Wirksamkeit ist. Aus den Relevanz-Werten lassen sich also keinesfalls Prioritäten für die Umsetzung der einzelnen Maßnahmen ableiten.

Einige der ursprünglichen Anforderungen blieben nach wie vor bestehen, werden jedoch im Rahmen des sim^{TD}-Versuchs nicht beachtet, da sie sich auf Punkte beziehen, die unter Abschnitt 1.3.1 „Vorleistungen“ aus dem IT-Sicherheitskonzept ausgeklammert wurden. Diese Anforderungen wurden nicht in die nachfolgende Tabelle übernommen.

Schlüssel	Zusammenfassung	Sicherheitsziel	Maßnahmen	Relevanz
SIMTD-62, SIMTD-61, SIMTD-63	**Autorisierung für Zugang zur IRS, ICS, IVS**	**Autorisierung, Integrität**	[M_ITS_VN] [M_ITS_VPN] [M_Fernzugriff_SSH]	**15,35**
	Zugang zur IRS, ICS, IVS insbesondere zu darin gespeicherten Daten und der installierten Software darf nur von autorisierten Personen erfolgen. Beispielsweise darf es unbefugten Personen nicht möglich sein, Software und Einstellungen der IRS, IVC, ICS zu ändern.			
SIMTD-57, SIMTD-58, SIMTD-53	**Authentizität von Messdaten**	**Authentizität (Daten), Integrität**	[M_IPSec_Mobil] [M_Cell_VN]	**14,74**
	Messdaten, Livedaten, Logging-Daten werden von allen Quellen (IVS, IRS, ICS) gesammelt und zur VsZ übertragen. Nach einer Auswertung werden sie dann zur Verfügung gestellt. Das Modifizieren dieser Messdaten muss verhindert werden. Andernfalls würde die Versuchauswertung verfälscht.			
SIMTD-45	**Vertraulichkeit der Logging-Daten (gespeichert)**	**Vertraulichkeit, Autorisierung**	[M_ICS_DB_R] [M_ICS_DB_RO]	**10,63**
	Logging-Daten, die an die Versuchszentrale gesendet wurden müssen vertraulich sein. Ansonsten können unbefugte Dritte die Daten auswerten und damit die Privatsphäre der Fahrer gefährden.			
SIMTD-64	**Absicherung der Verbindungen über „öffentliche“ Netze**	**Autorisierung, Authentizität**	[M_ITS_VN] [M_ITS_VPN] [M_IPSec_Mobil] [M_Cell_Sec] [M_Cell_VN] [M_ITS_CRYPTO]	**9,65**
	Absicherung der Kommunikationswege zwischen ICS, IRS und IVS			
SIMTD-28	**Plausibitätsprüfung von Nachrichten**	**Integrität**	[M_ITS_PLAUS]	**9,57**
	Zum Prüfen der Korrektheit der Nachrichten wird eine sehr grundlegende Prüfung durchgeführt, welche die Gültigkeitsbereiche der Mobilitätsdaten und wie Geschwindigkeit, Fahrtrichtung, Beschleunigung und dessen Zeitstempel beachtet. Eine erweiterte Prüfung beachtet die Nachrichtenplausibilität auf Anwendungsebene mit der das Verfolgen (Tracking) der Fahrzeuge realisiert wird. Mit Hilfe dieser erweiterten Prüfung können nicht plausible Fahrzeugbewegungen			

Schlüssel	Zusammenfassung	Sicherheitsziel	Maßnahmen	Relevanz
	detektiert und bewertet werden.			
SIMTD-30, SIMTD-31, SIMTD-36, SIMTD-38, SIMTD-32, SIMTD-39	**Integrität von Daten auf IVS, IRS, ICS**	**Integrität, Autorisierung**	[M_WVA_IS_LOGIN]	**8,64**
	Schutz von auf der ITS Vehicle Station gespeicherten Standortinformationen (z.B. Parkinformationen, Kommunalinformationen) Evtl. Nutzerprofile (serverseitig) die bei den Anfragen des Client berücksichtigt werden sollen. Nur der berechtigte Nutzer darf diese einsehen und ggf. verändern oder ergänzen.			
SIMTD-37	**Autorisierter Zugriff auf die Daten internetbasierter Dienste in ICS, IVS**	**Autorisierung**	[M_TLS_Sec]	**8,64**
	Die Daten über Verkehrsereignisse und Verkehrslage müssen vor unberechtigtem Lesen geschützt werden. Evtl. Nutzerprofile (serverseitig) die bei den Anfragen des Client berücksichtigt werden sollen. Nur der berechtigte Nutzer darf diese einsehen.			
SIMTD-60	**Integrität der verwendeten Software**	**Integrität**	[M_ITS_IRS_SW]	**5,75**
	Manipulation der Software auf IRS, IVS und ICS muss verhindert werden, um die Funktionalität aller Komponenten nicht zu gefährden.			
SIMTD-2, SIMTD-25, SIMTD-12, SIMTD-13, SIMTD-24, SIMTD-34, SIMTD-50	**Authentizität von C2X-Nachrichten**	**Authentizität (Daten), Integrität**	[M_ITS_SIGN] [M_ITS_VERIFIY]	**5,64**
	Das Einspielen falscher oder modifizierter Daten in die infrastrukturseitige oder fahrzeugseitige Datenerfassung muss verhindert werden. Andernfalls können darauf aufbauende Funktionen nicht korrekt ausgeführt werden.			
SIMTD-11	**Eingeschränkte Genauigkeit übertragener und gespeicherter persönlicher Daten**	**Anonymität / Pseudonymität**	Für die Umsetzung dieser Anforderung ist die jeweilige Funktion verantwortlich, die die persönlichen Daten verwaltet. Eine Umsetzung durch die sim^{TD}-IT-Sicherheitsarchitektur ist nicht möglich.	**5,56**
	Um nicht anhand von persönlichen Daten, die im Klartext übertragen oder gespeichert werden müssen auf Fahrer- und Persönlichkeitsprofile schließen zu können, sind diese Daten mit eingeschränkter Genauigkeit zu speichern. ("gesammelte Fahrzeugdaten müssen nach empfang anonymisiert werden. Reiseziele müssen anonymisiert werden")			
SIMTD-18	**Wechsel von Pseudonymen**	**Anonymität / Pseudonymität**	[M_IPSec_Mobil] [M_RND_Pref] [M_Cell_IP_Change] [M_ITS_PSDWM]	**5,56**
	Diverse Funktionen verschicken Positions- oder Routeninformationen per Broadcast. Durch das Abhören dieser Nachrichten darf ein Angreifer nicht auf die Identität des Fahrers oder des Fahrzeugs schließen können. Pseudonyme müssen daher gewechselt werden können.			
SIMTD-20	**Keine Rückverfolgbarkeit von Personen durch**	**Anonymität / Pseudonymität**	[M_ITS_PSDWM]	**5,56**

Schlüssel	Zusammenfassung	Sicherheitsziel	Maßnahmen	Relevanz
	Positionsketten in C2X-Nachrichten			
	Die Funktion 2.1.1 (Hinderniswarnung) sendet Positionsketten eines Fahrzeugs per Broadcast in C2X-Nachrichten. Da Positionsketten die Reiseroute und damit persönliche Daten repräsentieren darf es nicht möglich sein, diese Daten mit der Identität des Fahrzeugs oder des Fahrers zu verknüpfen da andernfalls die Privatsphäre des Fahrers verletzt würde.			
SIMTD-59	**Authentizität von ICS Steuerungsdaten**	**Authentizität (Daten), Integrität**	[M_IPSec_Mobil] [M_Cell_VN]	**4,78**
	Steuerungsdaten sind Daten, die für das Drehbuch, die Ad-Hoc Anweisungen, Versuchsanweisungen, Versuchsüberwachung und Defektmeldungen benutzt werden. Steuerungsdaten müssen authentisch sein, andernfalls würde die Versuchdurchführung gefährdet.			
SIMTD-47	**Rechtzeitigkeit von Fahrerinformationen**		Das rechtzeitige Ausliefern von Fahrerinformationen muss durch die entsprechenden Funktionen sichergestellt werden (Priorisierung auf HMI). Schutz gegen Manipulationen der Funktionen bietet Maßnahme [M_ITS_IVS_SW]	**4,68**
	Eine verzögerte Zustellung von Fahrerinformationen kann diese unter Umständen unbrauchbar machen, evtl. sogar schwerer wiegen als eine Nichtzustellung.			
SIMTD-48	**Rechtzeitigkeit von CAMs und DENMs**	**Integrität**	[M_ITS_PLAUS]	**4,47**
	Verzögerungen in der Zustellung von C2X Nachrichten oberhalb eines bestimmten Grenzwertes werden vom System erkannt und beachtet. Der Grenzwert wird so gewählt, dass entsprechend verzögerte Nachrichten keine Funktionsausfälle oder gravierende Beeinträchtigungen verursachen.			
SIMTD-44	**Vollständigkeit der Logging-Daten**	**Verbindlichkeit**	[M_ITS_Log_Sec	**4,17**
	Auch wenn die Integrität individueller Datensätze im Logging-Bestand gewährleistet werden kann, so kann doch die Gesamtheit des Datenbestands durch schlichtes Fehlen eines einzelnen Datums invalidiert sein oder werden.			
SIMTD-10, SIMTD-29, SIMTD-33	**Vertraulichkeit von persönlichen Daten**	**Vertraulichkeit**	[M_IPSec_Mobil] [M_Cell_VN] [M_ITS_CRYPTO] [M_ITS_DECRYPT]	**3,69**
	Lt. F_1.1.2-Template werden folgende persönliche Daten über Unicast versendet: Position des Fahrzeugs (incl. Richtung und Geschwindigkeit), aufgezeichnete Bewegung, gesammelte Fahrzeugdaten, Reiseziele. Diese müssen geschützt werden, so dass die Privatsphäre des Fahrers gewahrt bleibt. Absicherung von Anfragen von der IVS an den Server und der Antworten des Servers an die IVS (Client), Parkinformationen, Kommunalinformationen basierend auf TCP/IP. Anfragen an den Server können Daten über Identität des Nutzers, des Fahrzeugs, des Fahrtziels, die Position usw. enthalten. Diese Daten müssen sicher gegen Abhörversuche sein.			
SIMTD-26	**Authentizität des Nachrichtenerstellers**	**Authentizität (Akteure)**	[M_ITS_SIGN] [M_ITS_VERIFIY]	**3,48**
	Die Authentizität einer Nachricht impliziert nicht die Authentizität des Erstellers der Nachricht. Eine			

Schlüssel	Zusammenfassung	Sicherheitsziel	Maßnahmen	Relevanz
	nicht gefälschte oder nicht manipulierte Nachricht ist nicht implizit authentisch im Sinne des Erstellers. Also muss jeder Kommunikationsakteur der Herkunft der empfangenen Nachricht vertrauen können			
SIMTD-27	**Erkennung von Pseudonymmissbrauch**	**Verbindlichkeit, Authentizität (Akteure)**	[M_ITS_PLAUS] [M_W_ITS_PSDV]	**3,48**
	Ein Fahrer kann mit verschiedenen Nachrichten unter verschiedenen Identitäten (Pseudonymen) die Verkehrslage beeinflussen. Dies könnte fatale Folgen haben, je nachdem was der Fahrer in seinen Nachrichten weiterbreitet. Dies ist bekannt als Sybil Attacke.			
SIMTD-4	**Revokation von Pseudonymen**	**Authentizität (Daten), Authentizität (Akteure)**	[M_ITS_PSDV]	**3,48**
	Für den Fall, dass Pseudonyme kompromittiert wurden muss ein Revokationsmechanismus existieren. Andernfalls könnten Pseudonyme z.B. von Angreifern zur Einspielung falscher, aber authentischer Daten verwendet werden.			
SIMTD-43	**Autorisierung aller Teilnehmer (widerrufbar)**	**Autorisierung**	[M_ITS_PSDV]	**3,48**
	Um eine Verfälschung der Ergebnisse des Feldversuchs auszuschließen dürfen keine Nachrichten von Fahrern, die nicht an einem Versuch teilnehmen, weder vom System noch von den teilnehmenden Fahrzeugen beachtet werden.			
SIMTD-42	**Nicht-Zuordenbarkeit von Pseudonym zu Pseudonym**	**Anonymität / Pseudonymität**	[M_ITS_PSDWM]	**2,78**
	Um die Privatsphäre der Fahrer zu gewährleisten darf nach einem Wechsel des verwendeten Pseudonyms eine Zuordenbarkeit zum vorhergehenden Pseudonym nicht oder nur sehr schwer möglich sein.			
SIMTD-8	**Nicht-Zuordenbarkeit von Pseudonym zu Basisidentität**	**Anonymität / Pseudonymität**	[M_ITS_PSDV]	**2,78**
	Um die Privatsphäre der Fahrer zu gewährleisten darf eine Zuordenbarkeit von Pseudonym zu Basisidentität nur in der Versuchszentrale möglich sein.			
SIMTD-35	**Integrität der Informationen internetbasierter Dienste**	**Integrität**	[M_TLS_Sec]	**2,44**
	Absicherung von Anfragen von der CCU an den Server und der Antworten des Servers an die CCU (Client), Parkinformationen, Kommunalinformationen basierend auf TCP/IP. Anfragen an den Server können Daten über Identität des Nutzers, des Fahrzeugs, des Fahrtziels, die Position, Nutzerprofile usw. enthalten. Diese Daten müssen gegen Manipulationsversuche geschützt werden.			

Tabelle 4.14: IT-Sicherheitsanforderungen in sim^{TD}

5 IT-Sicherheitskonzept

Das IT-Sicherheitskonzept im vorliegenden Kapitel 5 ist in drei Teile untergliedert, um die Trennung zwischen der theoretischen IT-Sicherheitslösung und dem Sicherheitskonzept für sim^{TD} hervorzuheben. Die theoretische IT-Sicherheitslösung beschreibt ein optimales Sicherheitskonzept für ein Wirksystem wie es später für Deutschland bzw. Europa eingeführt werden könnte und nimmt keine Rücksicht auf sim^{TD}-spezifische Hardware- und Budget-Einschränkungen. Die sim^{TD}-spezifische Lösung hingegen berücksichtigt diese Aspekte, ist auf die in sim^{TD} zur Verfügung stehenden Ressourcen zugeschnitten und beachtet die zusätzlich vorhandenen Kommunikationswege.

Der Abschnitt 5.1 umfasst einleitend verschiedene Sicherheitstechniken, welche für die verschiedenen Funktionen innerhalb eines generischen Fahrzeugkommunikationssystems erforderlich sein können. In diesem ersten Abschnitt werden keine expliziten Lösungen vorgestellt sondern später verwendete Techniken, wie Protokolle und Systeme vorgestellt. In den folgenden Abschnitten 5.2 *IT-Sicherheitsarchitektur eines Wirksystems* und 5.3 *IT-Sicherheitsarchitektur für simTD* werden jeweils die IT-Sicherheitsarchitektur für ein späteres Wirksystem und die spezifische Sicherheitslösung für den Feldtest sim^{TD} beschrieben.

5.1 IT-Sicherheitstechniken eines ITS

Die grundlegende Problematik bei der Absicherung eines C2C- und C2I-Netzwerkes stellt sich wie folgt dar. Ein C2C-Netzwerk besteht aus gleichberechtigten, beweglichen Knoten, die über Funkverbindungen miteinander kommunizieren. Für die C2I-Kommunikation kommen weitere, i.d.R. ortsfeste Knoten hinzu, die über verschiedene Protokolle an die Fahrzeugkommunikation angebunden sind. Trotz der hohen Mobilität (d.h. kurze Verbindungszeiten) und beschränkten Ressourcen (d.h. keine aufwendige Kryptografie) müssen für dieses Netzwerk die IT Sicherheitsschutzziele (siehe Abschnitt 1.4.3) gelten. Durch die dezentrale Kommunikation zwischen den Teilnehmern über verschiedene Kommunikationstechniken, wie dem angepassten WLAN IEEE 802.11p beschrieben in Abschnitt 5.1.4, dem kommerziellen WLAN IEEE 802.11b/g beschrieben in Abschnitt 5.1.5 oder ITS IMT Public beschrieben in Abschnitt 5.1.6 müssen besondere IT-Sicherheitstechniken angewendet werden. Um dieses zu erreichen, kann im Wesentlichen auf die Herstellung geschlossener Benutzergruppen durch digitale Signaturen zurückgegriffen werden. Die für die Erstellung von digitalen Signaturen erforderliche Nutzung und Verwaltung digitaler Zertifikate wird daher in Abschnitt 5.1.1 für die Fahrzeuge, ITS Roadside Stations und Server in ITS Central Station erläutert.

Die Systeme und Kommunikationsverbindungen müssen darüber hinaus vor unautorisiertem Zugriff und dem Einspielen gefälschter Informationen geschützt werden. Durch die im Sicherheitskonzept festgelegten Maßnamen muss daher jede Nachricht eindeutig verifiziert und vertrauliche Kommunikation über öffentliche Netze verschlüsselt werden. Der Einsatz von sicheren Tunnelprotokollen, die diese Schutzziele erreichen, wird in Abschnitt 5.1.3 näher erläutert. Ein passiver Angreifer darf zwar verkehrssicherheitsrelevante Nachrichten mitlesen, da diese ohnehin öffentlich sind, darf jedoch keine eigenen Informationen in das System einbringen. Wie in der Bedrohungsanalyse oben gezeigt würde das Einspielen von gefälschten oder alten (ungültigen) Nachrichten die Funktionssicherheit des Gesamtsystems stören und muss somit verhindert werden. Jegliche vertrauliche Kommunikation über öffentliche Netzwerke wie dem Internet muss verschlüsselt übertragen werden, damit ein Angreifer den Inhalt der Nachricht nicht mitlesen kann.

Des Weiteren müssen Mechanismen zum Schutz der Privatsphäre adressiert werden, die das automatisierte Verfolgen eines Fahrzeuges verhindern. Hierzu werden Pseudonymisierungstechniken angewandt. Diese stehen in engem Zusammenhang mit der Verwaltung

von Zertifikaten für digitale Signaturen und werden daher ebenfalls in Abschnitt 5.1.1 betrachtet.

5.1.1 Identitäten und Pseudonyme

Alle Akteure im Kommunikationssystem, natürliche Personen wie Objekte, besitzen eine eindeutige, unveränderliche Identität. Zum Schutz dieser eindeutigen Identität können Pseudonyme verwendet werden. Frei wählbare Pseudonyme böten das höchste Maß an Anonymität, jedoch nicht die Möglichkeit kompromittierte Knoten von der Kommunikation auszuschließen. Wenn Pseudonyme jedoch von einer vertrauenswürdigen Instanz, der die Zuordnung zur eindeutigen Identität des Teilnehmers bekannt ist, ausgestellt werden kann damit das gleiche Maß an Sicherheit erreicht werden ohne auf die Möglichkeit, kompromittierte Knoten von der Kommunikation auszuschließen zu verzichten. Voraussetzung ist hierbei, dass der „vertrauenswürdigen Instanz“ von allen Teilnehmern vertraut wird, d.h. dass sich alle Teilnehmer darauf verlassen können, dass die Auflösung von Pseudonym zu eindeutiger Identität nur im (Ausnahme-) Fall eines kompromittierten Knotens angewandt wird.

Je nach Betrachtungsweise kann ein Pseudonym verschiedene Bedeutungen und Inhalte haben. Für die Verwendung im IT-Sicherheitskonzept gehen wir davon aus, dass ein Pseudonym aus der Menge von Merkmalen eines Netzwerkknotens besteht, welche in der Kommunikation benutzt werden und zur vorübergehenden Identifizierung eines Knotens verwendet werden können. Dies beinhaltet insbesondere, jedoch nicht ausschließlich, digitale Zertifikate und Netzwerkadressen (die exakte, in sim^{TD} verwendete Definition eines „Pseudonyms“ findet sich oben in Abschnitt 1.4).

Mit Hilfe dieser digitalen Pseudonyme ist es möglich abgehende Nachrichten des Kommunikationssystems digital zu signieren und zu verschlüsseln. Auf diese Weise können andere Teilnehmer überprüfen von welchem Pseudonym eine Nachricht erzeugt wurde und ob diese beim Transport unverändert geblieben ist. Durch die Zertifizierung können weitere Eigenschaften, wie Berechtigungen, an ein Pseudonym gebunden werden.

5.1.1.1 Digitale Zertifikate

Ein digitales Zertifikat besteht grundsätzlich aus Informationen über den Besitzer, Gültigkeitsdaten, Informationen über den Aussteller und dem öffentlichen Schlüssel des Besitzers. All diese Daten werden mit dem privaten Schlüssel des Ausstellers signiert und dem Zertifikat angehängt. Die verwendeten Schlüssel des Besitzers und des Ausstellers können unterschiedlich lang sein und hängen u.a. von der Gültigkeitsdauer des Zertifikates ab. So sollten Schlüssellängen so gewählt werden, dass ein Brechen des Schlüssels innerhalb der Gültigkeitsdauer des Zertifikates als sehr unwahrscheinlich erachtet wird. Als Richtwert für ein ITS sollten die empfohlenen Schlüssellängen verwendet werden wie sie von der Bundesnetzagentur[10] vorgeschlagen werden.

In einem ITS ist es sinnvoll zwei verschiedene Zertifikatstypen einzusetzen: Zum einen sollten standardisierte Absicherungsmechanismen verwendet werden, die überwiegend mit X.509v3-Zertifikaten arbeiten aber zum anderen sollten für die C2X Kommunikation auf die besonderen Anforderungen in C2X-Szenarien spezialisierte IEEE 1609.2-Zertifikate genutzt werden. Beide Zertifikatsformate werden im Folgenden für den Einsatz in einem ITS

[10] http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Algorithmen%5C_sw.html

beschrieben. Anschließend werden außerdem die unterschiedlichen Kontexte betrachtet, in denen die Zertifikate bei der ITS Kommunikation eingesetzt werden.

X.509 v3

X.509 ist der wichtigste Standard für digitale Zertifikate und wir daher in vielen Protokollen wie zum Beispiel SSL (engl. Secure Socket Layer) verwendet. Die aktuelle Version des Standards ist X.509 v3 und stellt im Gegensatz zu anderen Zertifikatsformaten eine flexible Struktur zur Verfügung mit der die Zertifikate dynamisch erweitert werden können. Beim Einsatz dieser Zertifikate wird eine strikte hierarchische PKI-Struktur vorausgesetzt, die aus vertrauenswürdigen Zertifizierungsstellen besteht.

Die Struktur eines X.509v3 Zertifikates wird im Folgenden dargestellt:

- Zertifikat
  - Version
  - Seriennummer
  - Algorithmus-ID
  - Aussteller
  - Gültigkeit
    - Von
    - Bis
  - Subject
  - Informationen zum Public Key
    - Public-Key-Algorithmus
    - Subject Public Key
  - Optionale ID des Ausstellers und des Inhabers
- Zertifikat-Signaturalgorithmus
- Zertifikat-Signatur

Wie bereits erwähnt können in der Version 3 von X.509 Erweiterungen ergänzt werden, auf die an dieser Stelle nicht weiter eingegangen werden soll. Die verwendeten Signaturalgorithmen sollten entsprechend der Vorgaben der Bundesnetzagentur verwendet werden.

IEEE 1609.2

Das für die C2X Kommunikation eingesetzte 1609.2-Zertifikatsformat (Wireless Access in Vehicular Environments, WAVE), ist in Abbildung 5.1 exemplarisch dargestellt.

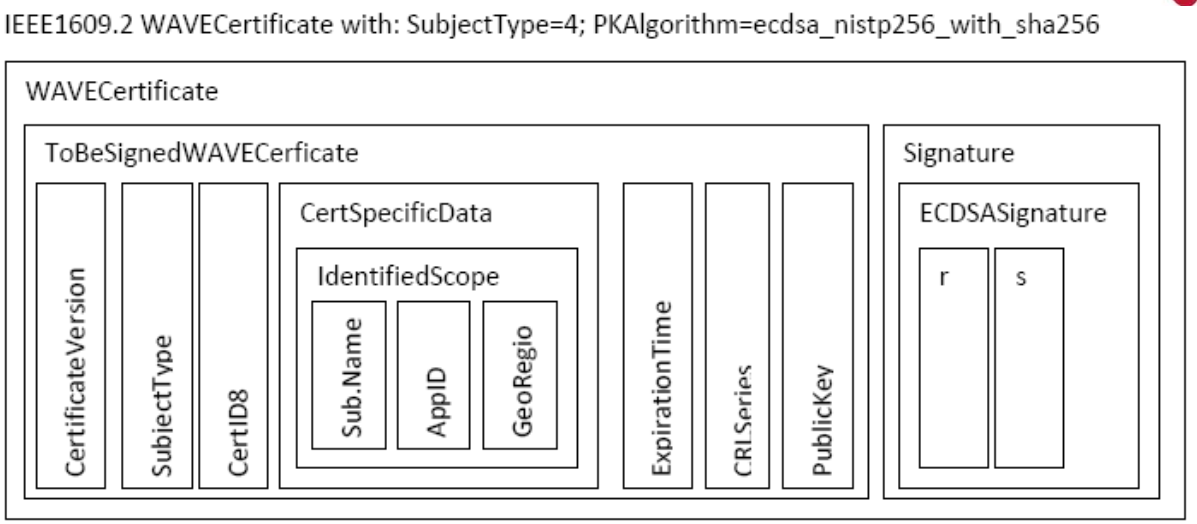

Abbildung 5.1: WAVE Zertifikatsformat (exemplarisch)

Für sim^{TD} sollen im Gegensatz zum IEEE 1609.2 Standard nicht nur ECDSA- sondern auch optional RSA-Signaturen in den Zertifikaten verwendet werden können, da RSA im Gegensatz zu ECDSA bei der Zertifikatsprüfung sehr viel weniger Berechnungen benötigt. Dies wiegt in einem System mit schwacher Rechenleistung den Nachteil der größeren Schlüssel von RSA wieder auf. In Tabelle 5.1 wird der ECDSA Algorithmus mit RSA verglichen. Für ein ITS ist primär die Verifikationszeit ausschlaggebend, da eine ITS Station nur ihre eigenen Nachrichten signieren muss, aber alle eingehenden Nachrichten der benachbarten ITS Stations verifiziert werden müssen. Aus diesem Grund ist die 3. Zeile (Verifizieren) in Tabelle 5.1 sehr viel stärker zu bewerten als die 2. Zeile. In der 4. Zeile wird eine Abschätzung für das Brechen der Schlüssel mit den jeweiligen Längen angegeben. Abhängig von diesen Informationen muss die Gültigkeitsdauer der Zertifikate angepasst werden. Die tatsächliche Dauer zum Brechen eines Schlüssels hängt jedoch stark von der verwendeten Hardware des Angreifers ab (was wiederum den Aufwand, den ein Angreifer betreibt, widerspiegelt). In der letzten Zeile wird der Security-Overhead dargestellt, um den sich die Größe einer ITS Nachricht aufgrund der Signatur erhöht. Die 200 Byte Security-Overhead beim Einsatz von ECDSA werden im ITS Umfeld als Referenz genommen, da dieser Algorithmus die kürzesten Zertifikate zur Verfügung stellt.

	ECDSA 256	**RSA 384 / 512**	**RSA 512**	**RSA 512 / 1024**
Signieren	24.276 ms 40 sign/s	3.332 ms 250 sign/s	4.852 ms 200 sign/s	22.668 ms 43 sign/s
Verifizieren	54.020 ms 18 verify/s	1.808 ms 500 verify/s	1.912 ms 500 verify/s	2.448 ms 400 verify/s
Gültigkeitsdauer	unbekannt	Stunden bis Tage	Jahre	unbekannt
Größe inkl. Zertifikat	~ 200 Byte	~ 214 Byte	~ 246 Byte	~ 310 Byte

Tabelle 5.1: Benchmarkwerte beim Einsatz von WAVE Zertifikaten mit 400 MHz CPU

Im Feld *CertSpecificData* können zudem Typinformationen für den Absender hinterlegt werden. Somit kann eine Unterteilung in folgende Typen gemacht werden:

- Aussteller (Certificate Authority, CA)
- ITS Vehicle Stations
- ITS Roadside Stations
- Einsatzfahrzeugen

Basisidentitäten

Ein 1609.2-Zertifikat kann als langlebige „Basisidentität“ eines Fahrzeuges verwendet werden (siehe Abschnitt 1.4.4 für eine genaue Definition von „Basisidentität“). Eine Basisidentität muss eine langfristige Gültigkeit haben. Die Gültigkeit wird durch das Feld *ExpirationTime* im Zertifikatsformat in Abbildung 5.1 festgelegt. Laut Spezifikation des WAVE Zertifikates kann auch eine unendliche Gültigkeit festgelegt werden, was für ein ITS jedoch nicht sinnvoll ist, da im Falle einer Revokation der Basisidentität das entsprechende Zertifikat für immer auf der Revokationsliste bleiben muss. Revokationslisten würden so im Laufe der Zeit beliebig umfangreich werden und damit der Skalierbarkeit des Systems im Wege stehen. Des Weiteren ist bei der Wahl der Gültigkeitsdauer einer Basisidentität zu beachten, dass es (aller Wahrscheinlichkeit nach) nicht möglich ist, den kryptografische Schlüssel innerhalb der Gültigkeit des Basiszertifikates zu brechen. Der Ablaufzeitpunkt des Zertifikates muss daher so gewählt werden, dass eine Basisidentität abgelaufen ist bevor ein Angreifer den privaten Schlüssel ermittelt haben kann. Generell muss davon ausgegangen werden, dass solche Angriffe mit Hilfe spezieller Hardwarebeschleunigung durchgeführt werden oder dass zu einem späteren Zeitpunkt (bis jetzt unbekannte) mathematische Methoden zur Verfügung stehen, die den Angriff beschleunigen. Entsprechend diesen Vorgaben muss eine geeignete Schlüssellänge für Basisidentitäten vorgesehen werden.

Pseudonyme

Zum Schutz der Privatsphäre sollen wechselnde Pseudonyme in der C2X Kommunikation eingesetzt werden (für eine Definition siehe Abschnitt 1.4.4.2). Die Pseudonymzertifikate können eine kürzere Schlüssellänge haben, da sie auch nur für einen kurzen Zeitraum gültig sind. Trotzdem sollte es vermieden werden, dass ein Fahrzeug nach längerer Standphase keine gültigen Pseudonyme zur Kommunikation mehr besitzt, da alle Ablaufzeitpunkte erreicht wurden. Generell ist es daher sinnvoll, dass ein Fahrzeug immer über einen ausreichend großen Vorrat an Pseudonymen verfügt.

Root-Zertifikat der PKI

Das Root-Zertifikat ist die Basis aller Fahrzeug-Zertifikate (Basisidentitäten und Pseudonyme). Dieses Zertifikat ist selbstsigniert und wird von allen Teilnehmern als vertrauenswürdig angesehen. In einer hierarchischen PKI können untergeordnete CA-Zertifikate mit Hilfe des Root-Zertifikats signiert werden. Bei einer flachen (nicht-hierarchischen) PKI-Struktur hingegen kann das Root-Zertifikat direkt zum Signieren der Fahrzeugzertifikate verwendet werden. Das Root-Zertifikat muss in allen ITS Stations verfügbar sein, so dass die Signaturen der ITS-Nachrichten korrekt verifiziert werden können.

Da das Root-Zertifikat der PKI für die lange Laufzeit Gültigkeit haben muss, ist eine entsprechend große Schlüssellänge dieses grundlegenden Zertifikates vorzusehen. Da mit diesem Zertifikat auch die Revokationsmechanismen abgesichert werden (d.h. eine Revokation eines kompromittierten Root-Zertifikates ist nicht mehr möglich) darf ein Angreifer auf keinen Fall den privaten Schlüssel innerhalb der Root-Zertifikatsgültigkeit aus dem öffentlichen Schlüssel berechnen können.

Der Zugriff auf den privaten Schlüssel des Root-Zertifikats benötigt zudem noch besondere Autorisierungsmechanismen in der PKI.

5.1.1.2 Signieren von C2X-Nachrichten

Die meisten Nachrichten in einer C2X-Kommunikation enthalten öffentliche Informationen, die über Broadcast oder Geocast übertragen werden. Da ein Großteil dieser Informationen nicht vertraulich ist, muss keine Verschlüsselung angewandt werden. Digitale Signaturen müssen jedoch auf jede ITS-Nachricht angewandt werden, um Manipulationen, Wiedereinspielungen oder Fälschungen von Nachrichten zu verhindern. Das Signieren und Verifizieren von Nachrichten ist daher eine der grundlegenden Aufgaben in der mobilen C2X-Kommunikation. Durch das Verifizieren der Signaturen kann der Empfänger die Authentizität des Absenders und die Integrität des Nachrichteninhaltes überprüfen.

Für das Signieren und Verifizieren einer Nachricht mir einem digitalen Zertifikat werden die folgenden Schritte unternommen.

1. Der Absender erstellt einen Hashwert der Nachricht und erstellt eine Signatur indem er seinen privaten asymmetrischen Schlüssel auf den Hashwert anwendet.
2. Der Absender der Nachricht hängt nun die Signatur und sein eigenes Zertifikat mit dem öffentlichen Schlüssel an die Nachricht.
3. Die Nachricht wird übertragen.
4. Der Empfänger erstellt wiederum von der Nachricht einen Hashwert mit dem gleichen Algorithmus wie ihn auch der Absender angewendet hat.
5. Mit dem öffentlichen Schlüssel aus dem Zertifikat entschlüsselt der Empfänger die Signatur.
6. Schließlich vergleicht der Empfänger den selbst erzeugten Hashwert der Nachricht mit dem entschlüsselten. Wenn beide Werte identisch sind, ist die Nachricht nicht verändert worden und eindeutig von dem Besitzer des Zertifikates abgesendet worden.
7. Das Zertifikat des Absenders ist signiert durch die CA und muss ebenfalls auf die gleiche Weise verifiziert werden wie die Nachricht selbst.

Eine Änderung des Nachrichteninhaltes nach dem Signieren kann zwar nicht verhindert werden, wird aber beim Verifizieren durch den Empfänger entdeckt. Jede Nachricht, die nicht korrekt verifiziert werden kann muss demnach verworfen werden. Neben der Integrität der Nachricht kann auch die Authentizität des Absenders festgestellt werden und mit Hilfe weiterer Argumente innerhalb des mitgelieferten Zertifikates kann eine Autorisierung erfolgen.

5.1.1.3 Verschlüsselung von C2X-Nachrichten

Die Verschlüsselung von Nachrichten ist für die C2X Kommunikation ein weiterer grundlegender Bestandteil, ist jedoch nicht so häufig erforderlich wie die Signatur. Vertrauenswürdige Informationen dürfen für Dritte nicht einsehbar sein. Funktionen, die vertrauliche Informationen übertragen oder Daten versenden, die dem Schutz der Privatsphäre unterliegen, müssen entsprechend geschützt werden.

Für die vertrauenswürdige Übertragung von Nachrichten werden überwiegend symmetrische Verschlüsselungsverfahren eingesetzt, da diese schneller und effizienter sind als die Verschlüsselung mit asymmetrischen Algorithmen. In Systemen, in denen jedoch nur asymmetrische Schlüssel zur Verfügung stehen wird das folgende hybride Verfahren eingesetzt.

1. Der Absender erstellt einen zufälligen symmetrischen Schlüssel.
2. Die Nachricht wird beim Absender mit dem gerade erstellten Schlüssel verschlüsselt.

3. Anschließend wird der symmetrische Schlüssel mit dem öffentlichen asymmetrischen Schlüssel des Empfängers verschlüsselt und an die Nachricht gehängt.
4. Die Nachricht wird vom Absender signiert. (optional)
5. Die Nachricht wird übertragen.
6. Der Empfänger überprüft die Signatur. (optional)
7. Der Empfänger entschlüsselt mit Hilfe seines privaten Schlüssels den symmetrischen Schlüssel.
8. Mit dem symmetrischen Schlüssel kann nun die Nachricht beim Empfänger entschlüsselt werden.

Mit Hilfe dieses Verfahrens kann zum einen die Authentizität des Absenders verifiziert werden (optional) und zum anderen werden die Nachrichteninhalte vor Manipulation und Einblick dritter geschützt.

5.1.2 Zentrale Pseudonymverwaltung

Der Einsatz wechselnder Pseudonyme im Automotive-Kontext ist sinnvoll, da durch sie der Schutz der Privatsphäre gewährleistet werden kann. Pseudonyme müssen durch eine vertrauenswürdige Instanz, die auch die spätere Rückauflösung von Pseudonymen zur Basisidentität übernehmen kann, (z.B. ein vertrauenswürdiges System in Form einer Public Key Infrastructure (PKI) in der Zentrale) signiert werden. Für die Verwaltung von Zertifikaten im Rahmen eines Fahrzeugkommunikationssystems sind jedoch neue Anforderungen zu erfüllen, die bisherige Lösungen aus dem Bereich Identitätsmanagement nur in angepasster Weise leisten können.

5.1.2.1 PKI

Eine PKI bietet die Möglichkeit, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Sie ist somit die Grundlage zum Schutz der Authentizität, Vertraulichkeit und Integrität von Daten.

Bei der Planung einer PKI gibt es folgende Vertrauensmodelle, die in der Praxis Anwendung finden:

- hierarchische PKI
- Cross-Zertifizierung
- Web of Trust

Im Folgenden wird ein kurzer Überblick über die verschiedenen Komponenten einer PKI, sowie über die verschiedenen Vertrauensmodelle gegeben.

PKI Komponenten

Eine Zertifizierungsinfrastruktur umfasst üblicherweise die vier folgenden Komponenten, die schematisch in Abbildung 5.2: Public Key Infrastruktur dargestellt sind.

- *Registrierungsstelle (RA, engl. Registration Authority)*
  Über die Registrierungsstelle werden Zertifikate beantragt und die Richtigkeit der Daten des Teilnehmers geprüft. Zur Ausführung dieser Aufgabe steht die RA im Kontakt mit der Zertifizierungsstelle.
- *Zertifizierungsstelle (CA, engl. Certificate Authority)*
  Diese Komponente ist die oberste und wichtigste Instanz der PKI, sie stellt CA-

Zertifikate bereit, verwahrt Schlüssel, generiert die Zertifikatsperrliste und stellt sie dem Validierungsdienst zur Verfügung.

- *Validierungsdienst (Validation Authority, VA)*
  Prüft unter Verwendung der Zertifikatsperrliste in Echtzeit die Gültigkeit und Echtheit eines Zertifikats.
- *Zertifikatsperrliste (Certificate Revocation List, CRL)*
  Mit Hilfe der Zertifikatsperrliste wird z.B. anhand von dem Gültigkeitszeitraum und der Seriennummer festgestellt, ob ein Zertifikat gesperrt ist. Ist das zu prüfende Zertifikat in der Liste nicht aufgeführt so ist es gültig.

Ablauf

Die Ausstellung eines Zertifikats läuft folgendermaßen ab:

1. Der Teilnehmer beantragt bei der Registrierungsstelle RA ein Zertifikat für eine digitale Signatur.
2. Die RA prüft die Identität des Teilnehmers und genehmigt den Zertifikatsantrag. Der Antragsteller muss im Voraus das Schlüsselpaar für das Zertifikat generiert haben, wobei der private Schlüssel niemals das Fahrzeug verlässt und auch dort vor externen Zugriff geschützt werden muss. Der öffentliche Schlüssel wird an die PKI übertragen.
3. Der öffentliche Schlüssel wird im Zertifikat integriert und mit dem privaten Schlüssel der CA signiert. Somit kann das Zertifikat nicht unbemerkt geändert bzw. verfälscht werden.

In der Praxis werden Zertifikate bei der VA abgefragt und mit Hilfe von CRLs geprüft, ob die Seriennummer des Zertifikats gesperrt wurde.

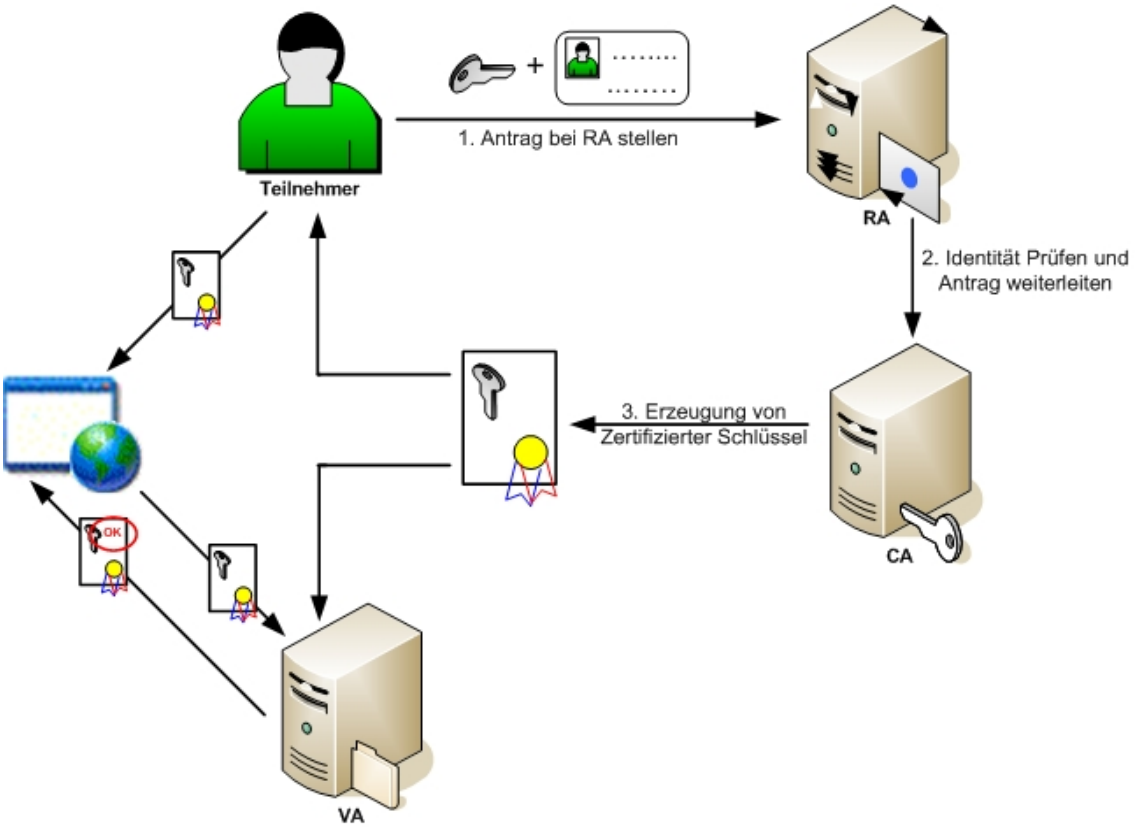

Abbildung 5.2: Public Key Infrastruktur

Vertrauensmodelle

Für ein ITS ist die hierarchische PKI-Lösung mit Cross-Zertifizierung am sinnvollsten, da hiermit die Aufgaben auf mehrere vertrauenswürdige Instanzen aufgeteilt werden können. Eine aktive Zertifizierung zwischen C2X-Teilnehmern ist schwierig, da eine Prüfung der Vertrauenswürdigkeit über das (unsichere) C2X-Netz mit großen Risiken behaftet ist.

Hierarchische PKI

Eine hierarchische PKI besteht aus einer einzigen Root-CA. In einer PKI sind zudem meist weitere Sub-CAs vorhanden, die in der Root-CA untergeordnet sind. Die Zertifikate der Sub-CAs werden hierzu durch die Root-CA signiert. In der hierarchischen PKI werden bei der Ausstellung von Zertifikaten das Schalenmodell (engl. Shell) und Kettenmodell (engl. Chain) für die Prüfung der Gültigkeitsdauer verwendet.

Cross-Zertifizierung

Cross-Zertifizierung ermöglicht Zertifikate über verschiedener Root-CAs hinweg auszustellen. Wenn zwei Zertifizierungsstellen (meist Root CAs) cross-zertifiziert sind, bedeutet dies, dass sie sich mit Hilfe ein sogenannten *Bridge-CA* gegenseitig anerkennen. Hier wird zwischen den beiden Zertifizierungsstellen (Root CA) eine Vertrauensbeziehung hergestellt, so dass sie gegenseitig Zertifikate prüfen können.

Web of Trust

Web of Trust ist ein Konzept, das bei den Verschlüsselungsanwendungen PGPdict, GnuPG und anderen OpenPGP-kompatiblen Systemen benutzt wird.

„Web of Trust" ist der Begriff für die Beschreibung des Vertrauens zwischen Teilnehmern einer Gruppe. Vertrauensbeziehungen können sowohl uni- als auch bidirektional sein. Das ideale „Web of Trust" ist eines, in dem jedes Web-of-Trust-Mitglied mit allen anderen über eine bidirektionale Vertrauensbeziehung verbunden ist z.B.:

- Bob signiert den Schlüssel von Alice.
- Alice signiert den Schlüssel von Linda.
- Bob vertraut dem Schlüssel von Linda.

Je mehr Zertifikate an einem Schlüssel hängen (d.h. je mehr Teilnehmer eine Vertrauensbeziehung zu dem Eigentümer dieses Schlüssels haben), desto sicherer kann man sein dass dieser Schlüssel tatsächlich zu seinem Eigentümer gehört. Die Umsetzung für ein ITS würde sich jedoch schwierig gestalten, da eine aktive Zertifizierung zwischen C2X Teilnehmern aufwendig ist und Probleme aufwirft. So könnte die Prüfung der Authentizität eines Fahrzeuges durch andere Teilnehmer nur sehr begrenzt erfolgen da entsprechende Vertrauensbeziehungen im Voraus bestehen müssten.

5.1.2.2 Zugriffsverwaltung auf Dienste der zentralen Pseudonymverwaltung

Der Zugriff auf zentrale Server und Dienste der Pseudonymverwaltung muss wie auch die C2X-Kommunikation abgesichert werden. Zum einen muss sich der PKI-Server gegenüber dem Nutzer authentifizieren und zum anderen muss der Benutzer autorisiert sein, den Dienst des PKI-Servers zu verwenden. Für die gegenseitige Authentifizierung können digitale Zertifikate (gewöhnlich X.509 v3) aber auch Benutzer, Passwortkombinationen verwendet werden.

Die einfachste Variante ist, dass sich der Server mit einem Zertifikat authentisiert und der Nutzer sich gegenüber dem Service mit einer Kombination aus Benutzername und Passwort authentifiziert. In Systemen mit komplexeren Autorisierungsregeln ist auch die clientseitige Authentisierung per Zertifikat sinnvoll, erfordert jedoch einen höheren Aufwand zur Ausstellung der entsprechenden Client-Zertifikate.

5.1.3 Absicherungsmöglichkeiten für IP-basierte Kommunikationsverbindungen

In diesem Abschnitt werden die grundsätzlichen Verfahren zur Absicherung von Datenübertragungen mithilfe von kryptografisch geschützten, IP-basierten Tunneln bzw. Fernverbindungen kurz dargestellt.

Die sichere Übertragung von Daten über ungesicherte Leitungen, Funkschnittstellen oder das generell als unsicher anzusehende Internet benötigt spezielle Sicherungsmaßnahmen, um Schutzziele[11] wie Vertraulichkeit, Integrität und Authentizität bei der Datenübertragung zu erreichen.

Bei einem ITS wird generell unterschieden zwischen den verkehrssicherheitsrelevanten Diensten, deren Nachrichten stets über IEEE 802.11p übertragen werden, und nicht unmittelbar die Verkehrssicherheit betreffende Funktionen, deren Nachrichten auch über andere Kommunikationsprotokolle übertragen werden können.

Es werden hier dementsprechend auch nur Verfahren zur Absicherung auf IP-Ebene bzw. oberhalb von ihr dargelegt.

Für die bei IEEE 802.11p verwendeten Datenübertragungen für C2X-Nachrichten sind die vorgestellten Sicherheitslösungen also nicht zuständig, diese werden über Verfahren abgesichert, welche den Standard IEEE 1609.2 umsetzen.

Grundsätzlich können für die Sicherung einer Verbindung unterschiedliche Technologien auf verschiedenen OSI[12] Sichten eingesetzt werden.

- Application Layer Security
- Session Layer Security
- Network Layer Security
- Data-Link Layer Security

Bevor die einzelnen Möglichkeiten vorgestellt werden, wird im Folgenden eine Übersicht über verschiedenen Arten der Verbindungssicherung gegeben.

Ende-zu-Ende: Bei einer Ende-zu-Ende-Absicherung erfolgt die Ver-/Entschlüsselung bzw. Signierung/Verifikation auf den jeweiligen Verbindungsendpunkten. Dies bedeutet, dass die Endpunkte selbst für Verschlüsselung/Signierung der gesendeten Nachrichten verantwortlich sind.

Netz-zu-Netz: Die Netz-zu-Netz-Absicherung stellt eine verschlüsselte Verbindung nur zwischen den einzelnen Netzen her. Die Kommunikation zwischen den Einheiten in diesen Netzten und den entsprechenden Gateways, die die Absicherung übernehmen, erfolgt ungesichert. Für die Einheiten erfolgt diese Art der Absicherung transparent. Eine darüber hinaus notwendige Ende-zu-Ende-Signierung muss allerdings von diesen selbst durchgeführt werden.

Application Layer Security: Bei dieser Art der Absicherung ist die Anwendung selbst verantwortlich für die Absicherung der Verbindung. Es handelt sich um eine Ende-zu-Ende Absicherung.

---

[11] s. a. Abschnitt 1.4.3 IT-Sicherheitsschutzziele.

[12] Open Systems Interconnection Reference Model

Session Layer Security: Ebenfalls eine Ende-zu-Ende Absicherung mit dem Unterschied, dass sich in der Regel nicht die Funktionen sondern das darunter liegende Framework um die Absicherung kümmert.

Network Layer Security: Dabei wird zwischen zwei Konzepten zu unterscheiden:

1. Die Absicherung erfolgt auf Network Layer Ende-zu-Ende oder
2. die Absicherung erfolgt Netz-zu-Netz.

Im ersten Fall ist die Endeinheit dafür verantwortlich eine entsprechende Absicherung durch den Aufbau eines Tunnels zur Verfügung zu stellen. Ein Beispiel hierfür wäre ein VPN Tunnel. Im zweiten Fall kann auch ein VPN Tunnel zum Einsatz kommen, allerdings würde dieser von einem Gateway zum entsprechenden Gegenstück hergestellt werden.

Es wird davon ausgegangen, dass nur Punkt-zu-Punkt Verbindungen auf IP-Ebene abgesichert werden sollen. Die Absicherung von Punkt-zu-Mehrpunkt Verbindungen, wie sie bei Broad- oder Multicast notwendig würde, wird hier nur im Rahmen der Darstellung der Vor- und Nachteile der Verfahren kurz erwähnt.

5.1.3.1 Virtuelle Netze (VN)

Eine Grundschutzmaßnahme für Datenübertragungen besteht darin, dass man die Datenübertragungen überhaupt nur zwischen einer festgelegten Menge von Start- und Endpunkten zulässt. Auf diese Weise realisierte Netze werden als virtuelle Netze[13] (VN) bezeichnet. Dies stellt das Standardvorgehen bei der Vernetzung von Liegenschaften eines Unternehmens zu einem gemeinsamen Unternehmensnetz dar.

Es gibt verschiedene Möglichkeiten virtuelle Netze aufzubauen. Bei größeren virtuellen (Fest-)Netzen werden von Telekommunikationsanbietern hauptsächlich Produkte auf Basis des MPLS-Protokolls (*Multiprotocol Label Switching*) und entsprechender MPLS-fähiger Komponenten (Zugangs- und Backbone-Router) eingesetzt.

MPLS ist ein Protokoll unterhalb von Layer 3, d.h. der IP-Ebene. Mithilfe von MPLS lassen sich (virtuelle) Netze unterschiedlicher Kunden sogar bei Nutzung gleicher (privater) IP-Adressen und Übertragungsstrecken dennoch von einander sauber separiert durch einen IP-Backbone schalten[14]. Man bezeichnet auf diese Weise realisierte virtuelle Netze auch als MPLS-Overlay-Netze.

Virtuelle Netze sorgen allerdings nur dafür, dass bei sicherer Konfiguration der entsprechenden Protokolle der Verkehr in diesen Netzen vom sonstigen (Backbone-) IP-Verkehr getrennt wird. Es existiert kein starker Schutz gegen das Mitlesen, böswilliges Injizieren oder Verfälschen von Nachrichten innerhalb der Übertragungsnetze, beispielsweise an Routern, sondern eben nur ein Grundschutz. Des Weiteren können Konfigurationsfehler oder Manipulationen auf Router-Ebenen dazu führen, dass Daten aus einem VN in andere Netze gelangen und umgekehrt.

---

[13] Wir folgen hier der konsistenten Benennung, wie sie z.B. vom BSI verwendet wird. Leider wird von vielen Praktikern und in der Werbeprosa von Netzanbietern ein virtuelles Netz häufig bereits als virtuelles privates Netz (VPN) bezeichnet. Wir verwenden VPN hier stets für ein virtuelles Netz, das zusätzlich auch noch kryptographisch abgesichert ist.

[14] Bei MPLS wird nicht mehr im eigentlichen Sinne geroutet, sondern mithilfe von so genannten Labeln, welche die IP-Pakete bereits am Zugangsrouter anhand ihrer Zieladresse bekommen, werden die MPLS/IP-Pakete direkt durch einen IP-Backbone geschaltet und bis zum Netzausgangspunkt transportiert, ohne dass zeitaufwändig die IP-Header durch Router ausgewertet werden müssten.

Aus den oben genannten Gründen ist es aus Sicherheitssicht nicht ausreichend, lediglich ein VN zu verwenden, sondern das VN muss noch durch geeignete kryptografische Verfahren zu einem virtuellen *privaten* Netz umgewandelt werden. IP-Pakete aus einem VPN sind aufgrund des zusätzlichen kryptografischen Schutzes auch dann noch geschützt, wenn ein Angreifer den Netzverkehr mitlesen kann bzw. die Pakete durch Konfigurationsfehler in andere Netze geroutet werden.

5.1.3.2 Virtuelle Private Netze (VPN)

Virtuelle private Netze sind virtuelle Netze, die mithilfe von kryptografischen Verfahren abgesichert werden, um die oben genannten Schutzziele zu erreichen. Hierbei müssen die zugrunde liegenden virtuellen Netze nicht notwendigerweise auf die in Abschnitt 5.1.3.1 beschriebene Weise realisiert sein. Bei festen IP-Adressen lässt sich ein virtuelles privates Netz auch allein mithilfe von IP-basierten Standardprotokollen realisieren, wobei sich auch Netzknoten mit dynamisch vergebener IP-Adresse über VPN-Gateways in das VPN einbinden lassen, wenn entsprechende Software eingesetzt wird. Aktuelle Betriebssysteme bringen die hierfür notwendigen Mechanismen häufig bereits mit bzw. sie lassen sich leicht entsprechend nachrüsten.

Ein VPN besteht aus meist räumlich entfernten, getrennten LANs, die über VPN-Gateways miteinander sicher über IP-Technik verbunden werden. Die IP-Adressen der VPN-Gateways sind hierbei i. Allg. statisch.

Mobile Rechner lassen sich in das VPN einbinden, indem sie über allgemeine IP-Zugänge von ISPs mit einem "Einwahl"-VPN-Gateway einen sicheren Tunnel aufbauen, über den alle Daten übertragen werden.

Die VPN-Software muss folgende Funktionalität bieten:

- *Aushandlung der Tunneleigenschaften zwischen Tunnelanfangspunkt und Tunnelendpunkt* (z.B. Schlüsselaustausch und sonstige Parameter). Damit sich Man-in-the-Middle-Angriffe beim Aushandeln der Tunneleigenschaften erkennen lassen, sollten hierbei asymmetrische Kryptoverfahren und Zertifikate (typ. X.509v3-Zertifikate) samt öffentlicher Schlüssel-Infrastruktur (PKI) eingesetzt werden.
- *Verschlüsselung und Integritätsschutz der Daten am Tunnelanfang* mit dem passenden Protokoll und Schlüssel
- *Entschlüsselung und Prüfung der Daten auf Veränderung am Tunnelendpunkt* mit dem entsprechenden Protokoll und Schlüssel

5.1.3.3 Realisierungsvarianten für ein VPN bzw. bei der Absicherung von Datenübertragungen

Im Folgenden werden mögliche Realisierungsvarianten für eine VPN-Lösung bzw. für eine Absicherung von Datenübertragungen dargestellt; da es sich hierbei um Standardverfahren handelt, wird nicht ausführlich auf die jeweilige Technik eingegangen, sondern es werden nur kurz die grundsätzlichen Vor- und Nachteile eines Einsatzes erläutert.

IPSec

Das Standardprotokoll zum Aufbau von virtuellen privaten Netzen ist IPSec, das sowohl für IPv4 als auch für IPv6 standardisiert ist. Damit eine Implementierung des IPv6-Standards als *vollständig* bezeichnet werden darf, muss auch IPSec bei ihr vorhanden sein.

Ein Entwurfskriterium bei IPSec war, dass es nicht nur zur Verschlüsselung, sondern auch rein zur Integritätssicherung und Authentifizierung ohne Verschlüsselung einsetzbar sein sollte.

IPSec stellt zwei unterschiedliche Absicherungsarten zur Verfügung:

- *Authentication Header* (AH), mit dem AH lässt sich verbindungslose Integrität, eine Authentifizierung des Daten-Ursprungs und ein Schutz von Wiedereinspielung gesendeter Daten für IP-Datagramme erreichen. Der AH schützt nur gegen Manipulation, die Vertraulichkeit wird nicht geschützt, da nicht verschlüsselt wird.
- *Encapsulating Security Payload* (ESP), bei Einsatz von ESP wird für die Nutzlast des IP-Datagramms die Authentizität, Integrität (samt Schutz vor Wiedereinspielung) und Vertraulichkeit gesichert, indem die Nutzlast verschlüsselt und authentifiziert wird. Der IP-Header des Datagramms wird allerdings nicht durch ESP geschützt.

Die oben genannten Absicherungsarten lassen sich nicht nur allein, sondern auch in Kombination einsetzen. Zusätzlich lässt sich IPSec in zwei unterschiedlichen Betriebsmodi verwenden:

- *im Transportmodus*, bei dem die ursprünglichen IP-Pakete direkt mithilfe von IPSec abgesichert werden. Allerdings führt beim Transportmodus mit AH die Authentifikation des IP-Headers dazu, dass Veränderungen des Headers und der Payload (z.B. durch NAT[15]) nicht mehr akzeptiert[16] werden. Der Transportmodus hat den Vorteil, dass kein zusätzlicher IP-Header zu den Paketen hinzukommt.
- *im Tunnelmodus*, bei dem die zu schützenden IP-Pakete verschlüsselt[17] als Nutzlast in ein IP-Paket umgepackt werden. Häufig wird dieser Modus verwendet, um mithilfe von VPN-Gateways einen sicheren Tunnel zwischen Liegenschaften oder auch einzelnen (mobilen) Rechnern und einem Firmennetz aufzubauen.

Typischerweise werden IPSec-VPNs meist im Tunnelmodus und mithilfe von VPN-Gateways (VPN-Appliances) bzw. IPSec-fähigen Routern aufgebaut. Auch wenn der Tunnelmodus aufgrund des zusätzlichen IP-Headers einen Overhead[18] mit sich bringt, so ist die Verschlüsselungsleistung von VPN-Gateways und Routern, die intern Hardware-Krypto-Beschleuniger verwenden, erheblich höher als die einfacher Server, die IPSec in Software realisieren. Zudem werden die einzelnen Rechner hierbei entlastet und sie müssen auch nicht für die Nutzung von IPSec konfiguriert werden, sondern eben nur das VPN-Gateway. Daher ist es i. Allg. effizienter, den Tunnelmodus zu verwenden. Hierbei ist der Verkehr hinter dem VPN-Gateway/Router im lokalen Netz natürlich nicht mehr durch IPSec geschützt, da der Tunnel am VPN-Gateway terminiert wird.

IPsec sieht verschiedene Möglichkeiten vor, an welche Entitäten man die notwendigen Schüsselinformationen und Verschlüsselungsparameter bindet. Häufig geschieht das auf Basis von IP-Adressen, aber es ist auch möglich eindeutig identifizierbare Bezeichner (*distinguished name*) zusammen mit X.509 Zertifikate zu verwenden.

Vorteile von IPSec sind:

- Es kann direkt alle Protokolle oberhalb der IP-Ebene absichern, also nicht nur TCP, sondern auch UDP, ICMP usw., so dass hier eine große Flexibilität besteht.

---

[15] Network Address Translation

[16] Eine ähnliche Problematik besteht auch beim Einsatz von ESP im Transportmodus; zwar kann hierbei der IP-Header ohne Probleme verändert werden, aber die Ports der höheren Protokollebenen eben nicht, da sich die Portangaben innerhalb der verschlüsselten und authentifizierten Nutzlast befinden.

[17] Man muss nicht unbedingt verschlüsseln, es gibt bei ESP auch die „Null-Encryption“ bei der nur authentifiziert wird, allerdings wird sie in der Praxis nur selten eingesetzt.

[18] Durch Einsatz von IP-Kompression (IPComp) *vor* der Verschlüsselung lässt sich der Overhead i.Allg. reduzieren.

- IPSec sichert alle über IP laufenden Protokolle transparent ab, d.h. es greift nicht in Port-Belegungen ein und es sind auch keine Veränderungen an der verwendeten Anwendungssoftware notwendig.
- Sind nur Integrität und Authentizität wichtig, kann auch auf Verschlüsselung verzichtet werden.
- Freie Implementierungen sind für viele Betriebssysteme verfügbar bzw. IPSec ist bereits Bestandteil des Betriebssystems.
- In IPSec-fähigen Routern bzw. VPN-Gateways werden die notwendigen kryptografischen Operationen meist schnell in Hardware ausgeführt.
- IPSec ist ein vom Standard vorgeschriebener Bestandteil einer vollständigen IPv6-Implementierung.

Nachteile von IPsec sind:

- Bei der anfänglichen Schlüsselaushandlung zwischen den Kommunikationsparteien muss bei einer großen Anzahl von Verbindungen mit einem großen Speicherbedarf an zentralen Knoten gerechnet werden.
- Herkömmliche IPSec-VPN-Gateways sind meist für eine nicht allzu große Anzahl von Tunneln vorgesehen. Selbst große VPN-Zugangsrouter werden i. Allg. nur tausende von Tunneln verwalten. Eine sehr große Anzahl von Tunneln kann hier zu Leistungsengpässen führen.
- Wenn zwischen den beiden Endpunkten, deren Kommunikation mit IPSec abgesichert werden soll, Netzkomponenten liegen, die eine Netzwerk Address Translation (NAT) vornehmen, lässt sich IPSec nicht in seiner einfachen Form einsetzen. Die NAT verwendenden Komponenten ändern nämlich i. Allg. sowohl die Absende-IP als auch die Absende-Ports der Protokolle der Transportschicht (TCP und UDP). Wenn ESP mit Verschlüsselung eingesetzt wird, ist ein Zugriff auf die nun verschlüsselten Ports nicht möglich; überdies würde durch NAT auch ohne Verschlüsselung, ähnlich wie beim Einsatz eines AH, der Wert der kryptografischen Prüfsumme verändert. Als Lösung dieses Problems sind von der IETF Standards verabschiedet worden, die beschreiben, wie sich bei Einsatz von ESP IPSec-Datagramme in UDP so kapseln lassen, dass eine IPSec-Verbindung auch bei NAT noch möglich ist, s. RFC 3947 und insbesondere RFC 3948.
- Wenn IPSec mit Zertifikaten eingesetzt wird, so sind dies X.509 Zertifikate, d.h. die im Rahmen von IEEE 1609.2 verwendete Zertifikatsstruktur kann nicht verwendet werden, so dass sich der Aufwand für die Zertifikatserstellung und -verwaltung (der Pseudonyme) verdoppelt.
- Bei Einsatz von Verschlüsselung (ESP), werden die Ports der höheren Protokollebenen (UDP/TCP) verschlüsselt, so dass Firewall-Filterregeln auf Port-Basis nicht mehr sinnvoll wirken können. Typischerweise ist dies aber kein Problem, da IPSec-Verkehr als vertrauenswürdig angesehen werden kann. Verwendet man den Tunnelmodus von IPSec und platziert die Firewall hinter dem IPSec-Gateway lassen sich die (nun entkapselten und entschlüsselten) IP-Pakete wieder von der Firewall untersuchen.
- Broad- und Multicast-Übertragung ist mithilfe von Standard-IPSec-Implementierungen nur mit Zusatzmaßnahmen (Modifikationen bei Schlüsselaustausch und Verwaltung der IPSec-internen Security Associations) möglich. Diese Modifikationen dürften bei Einsatz von herkömmlicher VPN-Gateway-Hardware allerdings nur sehr schwer realisierbar sein.
- Gerade bei der Kombination von IPv6 zusammen mit IPSec kann es noch zu Interoperabilitätsproblemen zwischen unterschiedlichen Implementierungen kommen.

Überdies wird IPv6 auch noch nicht von allen auf dem Markt befindlichen IPSec-VPN-Gateways unterstützt, so dass die Auswahl eingeschränkt wird.

- Bei Abbau eines alten und Aufbau eines neuen Tunnels, der bei einem Identitätswechsel[19] stets notwendig wird, werden natürlich alle bestehenden Verbindungen unterbrochen[20].

SSL/TLS

Secure Socket Layers (SSL) bzw. der offizielle IETF-Standard Transport Layer Security (TLS) ist ein Protokoll zum Absichern von TCP-Verbindungen. SSL/TLS wird in sehr großem Umfang für die Absicherung von Web-Diensten im Rahmen von https verwendet.

SSL/TLS kann sowohl zur Server-Authentifzierung als auch zur "Client"-Authentifizierung gegenüber dem Server verwendet werden. Daher lassen sich mithilfe von SSL/TLS abgesicherte Punkt-zu-Punkt-Verbindungen[21] realisieren.

Bei einem ITS ist SSL/TLS insbesondere interessant für die Anbindung externer Dienste, da SSL im WWW sehr weit verbreitet ist und häufig bereits ohnehin von Dienstleistern eingesetzt werden wird. Daher wird der zusätzliche Aufwand für die Anbindung der mobilen Knoten eines ITS verhältnismäßig gering sein.

Durch Vergabe von Zertifikaten einer ITS-CA an externe Anbieter ließe sich auch sicherstellen, dass nur vertrauenswürdige Services mit den Fahrzeugen kommunizieren können.

Vorteile von SSL/TLS:

- SSL ist sehr flexibel, insbesondere müssen sich nicht beide Seiten mit Zertifikaten authentisieren, häufig wird nur verlangt, dass der Server ein gültiges Zertifikat besitzt, das vom Client geprüft werden kann. Dies ist eine zur Wahrung der Anonymität interessante Option.
- SSL-Verbindungen haben gegenüber einer Absicherung mit IPSec den Vorteil, dass sie auch bei dazwischen liegenden Firewalls bzw. NAT verwendenden Komponenten, wie z.B. WLAN-Routern, dennoch leicht und ohne zusätzliche Konfiguration einen Tunnel aufbauen können.
- Durch Wahl der "Null-Encryption" kann auch auf Verschlüsselung verzichtet werden, dann wird nur authentifiziert und die Integrität gesichert bzw. geprüft.
- Freie Implementierungen sind für viele Betriebssysteme verfügbar.
- SSL/TLS arbeitet auf Basis von TCP-Segmenten, die wesentlich größer sein können als IP-Pakete, die i. Allg. durch die maximale Größe von Ethernet-Übertragungsrahmen beschränkt sind. Der Overhead für die Verschlüsselung ist daher (etwas) geringer als bei IPSec.
- SSL/TLS hat bei großen Webseiten mit hohem Verkehrsaufkommen seine Skalierbarkeit bewiesen. Da SSL/TLS Ports verwendet, deren Anzahl pro Server

---

[19] Bei dem auch gleichzeitig die IP-Adresse (bzw. das Präfix) gewechselt werden sollte.

[20] Das gilt auch für verbindungslose Protokolle wie UDP, deren Pakete nach Abbau des Tunnels nicht mehr entschlüsselt werden können.

[21] Mithilfe von SSL/TLS lassen sich auch sogenannte SSL-VPNs realisieren, bei denen SSL/TLS als Protokoll zum Tunneln von IP-Paketen verwendet wird. Typischerweise dienen SSL-VPNs zur sicheren Anbindung von mobilen Nutzern mithilfe entsprechender VPN-Gateways an Unternehmensnetze.

relativ beschränkt ist, muss hier aber mit Load-Balancern und mehreren Servern dahinter gearbeitet werden.

Nachteile von SSL/TLS:

- SSL/TLS-Zertifikate werden oft auf Domänennamen ausgestellt, in diesem Fall muss DNS verfügbar sein, was eine zusätzliche Ausfallmöglichkeit[22] darstellt. Verwendet man bei den Zertifikaten (innerhalb des ITS) nur eindeutige Identitätsbezeichner (distinguished names) ist dies aber nicht unbedingt notwendig. Für die Anbindung von externen Diensten und Webservices wird man allerdings DNS benötigen.
- Wenn Zertifikate Domänennamen verwenden, um die Schlüsselinformationen zu binden, kann mithilfe von Spoofing auf DNS-Ebene[23] im Prinzip ein Man-in-the-Middle-Angriff möglich sein, *wenn* das anfragende System auch selbst unterschriebene Zertifikate akzeptiert, was aber im Rahmen eines ITS ohnehin nicht passieren sollte.
- SSL verwendet X.509 Zertifikate, d.h. die im Rahmen von IEEE 1609.2 spezifiziert Zertifikatsstruktur kann nicht verwendet werden, so dass sich der Aufwand für die Zertifikatserstellung und -verwaltung (der Pseudonyme) verdoppelt, s.a. vorangehender Abschnitt zu IPSec.
- Mit Standard-Implementierungen von SSL/TLS können nur TCP-Verbindungen geschützt werden. Sollen z.B. Streaming-Daten geschützt versendet werden, müssen Varianten oder andere Protokolle wie z.B. Secure Real-Time Transport Protocol (SRTP) oder Datagram Transport Layer Security[24] (DTLS) für UDP eingesetzt werden.
- Der Verbindungsaufbau ist auf Serverseite relativ rechenintensiv, die genauen Auswirkungen (Server-Belastung, Verzögerung bis zur ersten Nutzdatenübertragung) müssten beim Einsatz von SSL daher im Rahmen des Feldversuchs getestet werden. Es gibt allerdings auch Hardware-Beschleuniger für SSL.
- Broad- und Multicast-Übertragung ist nicht effizient möglich, da zu jedem Rechner eine Verbindung aufgebaut werden muss.

5.1.3.4 Skalierungsfragen

Ein ITS muss in der Lage sein, eine sehr große Anzahl abgesicherter Verbindungen unterhalten zu können. Während die Anzahl der VPN-Verbindungen zwischen Liegenschaften überschaubar ist, wird insbesondere[25] die Anzahl der Tunnel von Fahrzeugen zu zentralen Systemen sehr hoch sein. Aus diesem Grund müssen auf der zentralen Seite Lastverteilungsmechanismen und eine Hardware-Beschleunigung der kryptografischen Algorithmen vorgesehen werden.

---

[22] Aufgrund der Wichtigkeit von DNS ist allerdings bereits im Standard „vorgeschrieben“, mindestens zwei DNS-Server für die Verwaltung der eigenen Domänennamen zu verwenden.

[23] Hierbei wird die DNS-Anfrage nach der IP-Adresse einer Domäne mitgelesen und vom Angreifer mit einer eigenen DNS-Meldung beantwortet, welche der Domäne eine falsche IP-Adresse zuweist.

[24] DTLS ist in RFC 4347 spezifiziert und in OpenSSL ist eine Referenzimplementierung verfügbar; allerdings wird DTLS nicht annähernd zu viel verwendet wie SSL/TLS, so dass die Implementierung noch nicht den gleichen Reifegrad besitzt wie bei SSL/TLS.

[25] Eine Anbindung von RSUs über Tunnel an zentrale Systeme kann natürlich auch zu einer großen Anzahl von Tunneln führen.

Sowohl IPSec als auch SSL lassen sich mithilfe entsprechender Hardware stark beschleunigen. In Zukunft ist auch davon auszugehen, dass die bereits in RFC 3686 und RFC 4309 bzw. RFC 4106 und RFC 4543 spezifizierten, gut parallelisierbaren Betriebsmodi Counter-Mode bzw. Galois-Counter-Mode samt passendem Authentifizierungsverfahren in Hochleistungsimplementierungen von IPSec verfügbar werden, so dass am IPSec-Gateway der Datendurchsatz erhöht und die Latenz minimiert werden kann.

Aktuell können allerdings selbst große VPN-Konzentratoren typischerweise „nur“ ca. 10.000 Tunnel gleichzeitig verwalten; bei Einsatz mehrerer Konzentratoren und ihren eingebauten Lastverteilungsmechanismen lässt sich das noch auf ca. 100.000 Tunnel steigern, wobei dies mit entsprechenden Kosten verbunden sein wird.

Abhängig davon, wie stark IP-Verbindungen zu zentralen Systemen vom Fahrzeug aus verwendet werden, kann bei einem ITS im Vergleich zu herkömmlichen VPNs die Anzahl gleichzeitig bestehender Tunnel allerdings um Größenordnungen höher sein!

Es muss daher davon ausgegangen werden, dass eine sehr große Anzahl von Tunneln ein nicht leicht lösbares Problem darstellt. Es empfiehlt sich für das Wirksystem dringend, Gespräche mit den großen Router- und VPN-Gateway-Herstellern zu führen.

Würden hingegen die Tunnel nur temporär und für kurze Zeit aufgebaut, z.B. rein für die Beschaffung von Pseudonym-Zertifkaten, wäre das Problem merklich kleiner. Auch der Einsatz einer eher dezentralen, hierarchischen Struktur bei den ICS könnte das Problem der Anzahl der Tunnel zu einem Punkt etwas lindern.

5.1.3.5 Pseudonymität bei IP-Verbindungen

Im Rahmen eines ITS kommt dem Datenschutz und der informationellen Selbstbestimmung eine große Rolle zu, s.a. Abschnitt 1.5. Insbesondere soll es weder für den Betreiber des ITS noch für Dritte möglich sein, ohne explizite Einwilligung des Nutzers Bewegungsprofile zu erstellen.

Aus diesem Grund werden auch wechselnde Pseudonym-Zertifikate für die Fahrzeuge verwendet und üblicherweise statische Kennungen, wie z.B. MAC-Adressen, werden zusammen mit dem Pseudonym gewechselt, damit sie nicht zur Identifikation verwendet werden können.

Während sich die oben genannten Informationen im Prinzip leicht durch das Fahrzeug selbst wechseln lassen, ist dies bei IP-Adressen aber nicht möglich, denn diese werden zwangsläufig von dem jeweiligen Betreiber des Zugangsnetzes vergeben, da sonst kein sinnvolles Routing möglich wäre.

Fahrzeug-Identifikation anhand der IP-Adresse

IP-Adressen lassen sich zur Identifikation[26] eines Fahrzeugs verwenden, wenn sie nicht hinreichend oft gewechselt werden (können). Besonders gravierend ist dies, wenn vom Fahrzeug noch Standort-Informationen über IP an eine Zentrale oder einen Dienst übermittelt werden, da man in diesem Fall die Route, welche das Fahrzeug mit der entsprechenden IP-Adresse genommen hat, nachverfolgen kann. Vermeiden ließe sich das nur, wenn die IP-Adresse häufig gewechselt würde *oder* sichergestellt wäre, dass keine Standort-Informationen über IP übertragen werden.

Man wird einwenden, dass eine entsprechende Ortung bereits im Mobilfunknetz gegeben ist, was natürlich auch stimmt. Allerdings benötigt man hierfür die entsprechenden Informationen aus dem Netzmanagement der Mobilfunkbetreiber, die typischerweise nicht identisch mit den ITS-Betreibern sein werden.

Besonders kritisch sind IP-Adressen auch deshalb, weil sie im Prinzip für eine „weltweite" Übertragung eingesetzt werden können und somit die Informationen leichter Netzgrenzen überwinden und auch von externen Diensten erfasst werden können.

Routenrekonstruktion trotz wechselnder IP-Adressen

Tatsächlich dürfte aber selbst ein Wechsel der IP-Adresse meist die Identifizierung nicht wirklich merklich erschweren. Zwar hätte man bei wechselnden IP-Adressen nur Kenntnisse über Teilabschnitte einer Strecke, die zu einer IP-Adresse gehören, aber selbst wenn sich die IP-Adresse eines Fahrzeugs änderte, ließen sich doch häufig anhand der räumlichen Nähe der Koordinaten noch die Teilstrecken einander zuordnen, die zu einem Fahrzeug gehören. Dies ist möglich, weil der Wechsel der IP-Adresse zusammen mit den anderen Pseudonym-Informationen stattfände und dies nicht bei allen Fahrzeugen zur gleichen Zeit passieren wird.

Die Wahrscheinlichkeit, dass zwei Fahrzeuge zur gleichen Zeit und in räumlicher Nähe die IP-Adresse wechseln, ist aber (insbesondere bei geringer Fahrzeugdichte) relativ klein, so dass man mit hoher Wahrscheinlichkeit die alte und die neue IP-Adresse dem gleichen Fahrzeug zuordnen kann und somit eben doch wieder in der Lage ist, die zurückgelegte Strecke zu rekonstruieren.

Letztendlich ist der beste Schutz vor der Routenrekonstruktion eine möglichst sparsame Übertragung von Positionsdaten via IP.

Dynamische Adressvergabe bei IPv4

Wenn die IP-Adresse hinreichend oft gewechselt wird, lässt sich die Routenrekonstruktion *etwas* erschweren. Aktuell lässt sich dies bei IPv4 dadurch erreichen, dass ein Verbindungsabbruch mit erneutem Verbindungsaufbau auf der Sicherungsschicht unterhalb von IP erfolgt. Typischerweise wird dann eine neue IP-Adresse aus einem Pool verfügbarer Adressen vergeben, i. Allg.[27] wird sich hierbei die IP-Adresse ändern.

---

[26] Streng genommen identifiziert man nicht direkt das Fahrzeug, sondern kann Informationen einem festen Marker zuordnen, den man wiederum mithilfe von Zusatzinformationen häufig einem Fahrzeug wird zuordnen können.

[27] Man kann sich natürlich nicht darauf verlassen, dass tatsächlich eine andere IP-Adresse vergeben wird als vorher, da die Vergabe vom jeweiligen Zugangsanbieter nach eigenem Ermessen erfolgt. Meist wird aber eine andere IP-Adresse vergeben, wobei allerdings nicht gesagt ist, dass diese nicht aufgrund des Vergabeverfahrens eben doch wieder der vorangehenden zuordnen lässt.

Bei dem für ein ITS besonders relevanten Fall des Mobilfunks kommt überdies noch hinzu, dass aufgrund der Adressknappheit der IPv4-Adressen, keine öffentlichen Adressen vergeben werden, sondern private IP-Adressen, die via NAT dann auf einen wesentlich kleineren Anteil von öffentlichen IP-Adressen abgebildet werden. In diesem Fall sieht also das ITS bzw. ein externer Dienst die tatsächlich vergebene (private) Adresse nicht, sondern nur eine kleine Zahl von IP-Adressen über welche sehr viel Verkehr von unterschiedlichen Absendeports läuft.

Bei Einsatz eines IPSec-Tunnels mit UDP-Verkapselung um NAT-Überwindung zu erlauben, wird allerdings die vergebenen IP-Adresse dem Empfänger doch wieder bekannt, da sie sich im originalen (IPSec-) Paket befindet, das als UDP-Payload verschickt wird.

Überdies wird vermutlich nach der mittelfristig auch im Mobilfunk zu erwartenden Umstellung auf IPv6 kein NAT mehr verwendet werden.

(Semi-) Dynamische Adressvergabe bei IPv6

Aktuell (Mitte 2009) ist IPv6 in Deutschland noch nicht für Endkunden im Mobilfunk verfügbar, allerdings ist die baldige Einführung geplant. Bei IPv6 wird der Kunde – zumindest im Festnetz – für die eigene Nutzung ein ganzes /64-Subnetz[28] (in IPv6-Terminologie: *Präfix*) vom Internet-Zugangsanbieter bereitgestellt bekommen.

Beim Entwurf von IPv6 sollte es durch die große Anzahl verfügbarer IP-Adressen wieder möglich werden, jeden Rechner mit einer öffentlichen IP-Adresse an das Internet anzubinden, über die er direkt kontaktiert werden kann, wie dies bereits einmal in den Anfangszeiten des Internets gegeben war. Auf diese Weise könnte z.B. jeder leicht Server-Dienste anbieten, ohne dass der Server unbedingt bei einem kommerziellen Hosting-Anbieter stehen müsste.

Zwischenzeitlich wurde aber auch klar, dass eine Vergabe statischer IPv6-Adressen (bzw. eines Präfixes) an Privatkunden orwellsch´ anmutende Möglichkeiten der Datensammlung erlaubten, welche dem Recht auf informationelle Selbstbestimmung quasi vollständig den Boden entzögen.

Daher wird heute von Internet-Zugangsanbietern für private Endkunden eine (semi-) dynamische IPv6-Adressvergabe geplant, bei der die beiden oben genannten, einander zuwiderlaufenden Aspekte miteinander in Einklang gebracht werden:

- IPv6-Präfixe werden für private Endkunden dynamisch vergeben.
- Bei Verbindungsaufbau zum gleichen Zugangsrouter nach einer nur kurzen verbindungslosen Phase (< ca. ½ Stunde) bekommt der Kunde wieder das vorher von ihm verwendete Präfix. Es besteht also eine quasi-statische Präfix-Vergabe wenn die Online-Verbindung dauerhaft aufrecht erhalten wird.
- Bei Verbindungsaufbau zum gleichen Zugangsrouter nach einer längeren Verbindungslosigkeit bekommt der Kunde ein anderes Präfix dynamisch zugewiesen. Durch Abschalten des heimischen DSL-Routers über Nacht würde also das Präfix bei der nächsten Einwahl anders ausfallen, so dass eine hinreichender Schutz gegen die Profilerstellung auf Basis von IP-Adressen[29] gegeben ist.

---

[28] Der Kunde verfügt also über ein Subnetz mit 2^{64} öffentlich routbaren IP-Adressen.

[29] Sofern für die IP-Adressen des Subnetzes die in RFC 3401 *Privacy Extensions for Stateless Address Autoconfiguration in IPv6* beschriebenen Mechanismen verwenden und nicht einfach „interne“ IP-Adressen auf Basis der Interface-MAC-Adresse bilden.

Zwar ist aktuell noch völlig unklar, wann und auf welche Weise IPv6 in Mobilfunknetzen verfügbar sein wird, aber es kann sehr gut sein, dass man zur Netzvereinheitlichung analog zum Festnetz vorgehen wird.

Für ein ITS bedeutet dies aber, dass das Standard-Vergabeverfahren für IPv6-Adressen/ Präfixe leider die Pseudonymität für länger andauernde IP-Konnektivität quasi aufhebt, da eine kurze Verbindungsunterbrechung mit nachfolgender Neueinwahl voraussichtlich wieder zur Vergabe der gleichen IP-Adresse führt.

In Abschnitt 5.2.3.8 wird dargelegt, welche Maßnahmen sich ergreifen lassen, um einen hinreichend häufigen, echten Wechsel der IPv6-Adresse zu erreichen.

5.1.3.6 Abgesicherter Fernzugriff auf Server via SSH

Im Rahmen jedes größeren IT-Systems ist man auf Fernzugriff auf Server angewiesen, der ebenfalls auf sichere Weise geschehen muss.

Secure Shell (SSH) ist ein sicherer Ersatz für Telnet und erlaubt den verschlüsselten und authentifizierten Zugriff auf einen Host-Rechner.

SSH lässt sich auch zum sogenannten Port-Forwarding verwenden, bei dem über eine SSH-Verbindung Zugriffe vom Clientsystem zum Server-System via SSH abgesichert getunnelt werden. Hiermit lassen sich leicht[30] alle Anwendungen und Protokolle tunneln, die TCP für den Datentransport verwenden.

SSH ist aufgrund seines primären Einsatzzwecks zum Aufbau von VPNs weniger gut geeignet, aber dafür stellt es eine einfache und flexible Lösung für den sicheren Zugriff via Internet auf Systeme in einer geschützten Umgebung dar.

Typischerweise wird man zusätzlich zu den SSH-eigenen Absicherungsmechanismen noch den Zugriff auf die Systeme durch eine Firewall einschränken, die SSH-Zugriffe nur von einer beschränkten Anzahl berechtigter IP-Adressen zulässt.

Für SSH existiert mit OpenSSH auch eine Open-Source-Implementierungen, die für eine große Zahl von Betriebssystemen und Plattformen verfügbar ist.

5.1.3.7 Quality of Service

Neben der Absicherung der Verbindung ist auch eine Priorisierung der Daten von hoher Wichtigkeit. Hierfür sind verschiedenen Quality of Service (QoS) Mechanismen nutzbar. Es stehen folgende Techniken zur Verfügung:

- IEEE 802.1P (OSI Layer 2, Class of Service im IEEE 802.1Q Header)
  - sieben Prioritätsstufen
- Quality of Service (OSI Layer 3, 8-bit Differentiated Services [ehemals ToS])
  - 6 bit Differentiated Services Code Point (Priorität)
  - 2 bit Explicit Congestion Notification (IP Staumeldung)

Mit Hilfe dieser Mechanismen ist es möglich Anwendungs- und Managementdaten bzw. auch Anwendungsdaten untereinander entsprechend ihrer Anforderungen zu behandeln d.h. zu priorisieren.

---

[30] Auch UDP lässt sich bei Bedarf tunneln, aber hierfür muss auf dem Server noch ein zusätzliches TCP-to-UDP-Forwarding auf Betriebssystemebene konfiguriert werden.

5.1.4 ITS G5A

ITS G5A, d.h. funkbasierte Kommunikation basierend auf IEEE 802.11p, stellt ein Kommunikationsmedium für sicherheits- und verkehrsrelevante Informationen dar. Dieser WLAN-Standard ist speziell auf die Bedürfnisse der automobilen Kommunikation angepasst. Er bietet verbesserte Datenübertragung bei hohen relativen Geschwindigkeiten und über größere Entfernungen als die bekannten kommerziellen WLAN-Standards.

ITS-G5A	(European Profile) 5.875 GHz - 5.905 GHz
ITS-G5B	(European Profile) 5.855 GHz - 5.875 GHz
ITS-G5C	(European Profile) WLAN 5.4 GHz Bereich

Tabelle 5.2: IEEE 802.11p Profile

Die Tabelle 5.2 stellt die verschiedenen in der Standardisierung befindlichen Ad-Hoc-Komunikationswege gegenüber. In Tabelle 5.3 sind charakteristische Merkmale des Draft-Standards IEEE 802.11p im Vergleich zum IEEE 802.11a aufgeführt. Da 802.11p noch im Draft Status ist und in Deutschland das European Profile angewendet wird, sind die Daten nur als grobe Abschätzung für die Spezifikation des Sicherheitssystems zu verstehen. In sim^{TD} wird ITS G5A mit 3 Kanälen à 10MHz verwendet werden

	802.11p	**802.11a**
Kanal Bandbreite	10 MHz	20 MHz
Datenrate	3 – 27 Mbps (brutto)	6 – 54 Mbps (brutto)
SlotTime	16 µs	9 µs
SIFSTime	32 µs	16 µs
CHSwitchTime	≤ 2048 µs	-
AirPropagationTime	< 4 µs	<< 1 µs
PreambleLenght	32 µs	20 µs
PLCPHeaderLenght	8 µs	4 µs
CW_{min}	15	15
CW_{max}	1023	1023

Tabelle 5.3: IEEE 802.11p Merkmale

ITS Vehicle Stations und ITS Roadside Stations bilden ein hochdynamisches Ad-hoc-Netzwerk, in dem die Bandbreite und die eingeschränkte Konnektivität der Partner eine entscheidende Rolle spielen. Der Informationsaustausch basiert im Wesentlichen auf verbindungsloser, paketorientierter Kommunikation. Über den IEEE 802.11p Kanal sind ausschließlich verkehrssicherheitsrelevante Informationen auszutauschen, die in diesem Dokument als C2X-Nachrichten bezeichnet werden. Andere Daten wie lokale Mehrwertinformationen zum Beispiel Parkraumdaten oder Multimediadaten müssen über andere Kommunikationskanäle ausgetauscht werden.

Ad-Hoc ITS-Funktionen per IEEE 802.11p stehen im Zentrum eines Fahrzeugkommunikationssystems. Da es sich bei diesem Kommunikationsweg um einen relativ jungen Dienst handelt gibt, es im Vergleich zu den etablierten Kommunikationstechnologien wie WLAN oder ITS IMT Public nur wenige Standards, die angewendet werden können. Technologisch

eng verwandt mit Ad-Hoc Sensornetzwerken sind jedoch zusätzlich die besonderen Anforderungen dieser „hypermobilen“ Kommunikation zu berücksichtigen. Wie im Kapitel 2 zusammengefasst dargestellt, können auf die Erfahrungen in den vorangehenden Projekten, insbesondere dem Standard IEEE 1609.2 [11], zurückgegriffen werden.

5.1.5 WLAN IEEE 802.11 b/g

Es bestehen grundsätzlich mehrere Möglichkeiten die Kommunikation über 802.11 b/g abzusichern. Auf der einen Seite ist es sinnvoll, eine Absicherung auf OSI-Layer 1 und 2, sprich Physical- und Link-Layer („Sicherungsschicht“) durchzuführen, andererseits kann aber auch eine Absicherung auf höheren OSI-Layern sinnvoll sein. Die jeweilige Absicherungsvariante ist von der Anwendung sowie den eingesetzten Techniken abhängig. Im Folgenden werden beide Varianten erläutert.

5.1.5.1 Absicherung auf Sicherungsschicht durch IEEE 802.11i

Die Authentifizierung und Autorisierung von Teilnehmern, sowie eine Verschlüsselung von Datenpaketen in Funknetzen nach IEEE 802.11b/g ist unter Zuhilfenahme von Verfahren des Sicherheitsstandards IEEE 802.11i direkt auf Layer 2 möglich. Das in kommerziellen IEEE-802.11 b/g-fähigen Geräten umgesetzte WiFi Protected Access 2 (WPA2) Profil umfasst alle als Basisfunktionalität ausgewiesenen Funktionen dieses Standards. IEEE 802.11i ermöglicht den Einsatz von modernen symmetrischen Verschlüsselungsverfahren, z.B. auf Basis von AES mit einer Blocklänge von 128 Bit. Zur Authentifizierung und Autorisierung von Endgeräten sind in IEEE 802.11i zwei prinzipielle Verfahren vorgesehen:

- Im "Personal Mode" wird ein statischer, beiden Parteien vorab bekannter Schlüssel (PSK, Pre-Shared Key) eingesetzt.
- Im "Enterprise Mode" findet die Anmeldung mithilfe des Extensible Authentication Protocol (EAP) [RFC 5247] statt, das eine flexible Aushandlung des einzusetzenden Mechanismus', etwa EAP-TLS [RFC 5216] oder EAP-PEAP von Cisco, Microsoft und RSA erlaubt. Um eine Speicherung von Berechtigungsnachweisen wie zum Beispiel Schlüssel auf der Gegenstelle, dem Access-Point (AP), zu vermeiden, kann bei der Anmeldung, wie im RADIUS-Protokoll spezifiziert, ein zentraler Authentication Server (AS) eingesetzt werden, sodass der AP nur noch in Vermittlerrolle auftritt.

Diese Absicherungsvariante ist sehr weit verbreitet und kann als Standard angesehen werden. Der größte Vorteil liegt darin, dass die Absicherung auf einer sehr niedrigen Ebene der Verbindung durchgeführt wird und sie für alle darüberliegenden Protokolle unsichtbar ist. Speziell für gewöhnliche TCP/IP-Verbindungen ist eine solche Absicherung am sinnvollsten.

5.1.5.2 Absicherung auf Anwendungsschicht durch IEEE 1609.2

Wenn zum Beispiel C2X-Nachrichten mit C-WLAN als Broadcast verbreiten werden sollen, ist es eventuell sinnvoll, die gleichen Sicherungsmechanismen anzuwenden wie sie nach IEEE 1609.2 spezifiziert sind. Das heißt alle Protokolle wie zum Beispiel Ethernet, IP oder UDP auf den OSI-Layern unterhalb der Anwendungsschicht können ohne Anpassungen verwendet werden. Auf Layer 7 des OSI-Schichtenmodells wird die Nachrichtenabsicherung durchgeführt.

5.1.6 ITS IMT Public

Im Rahmen eines ITS sind Mobilfunkverbindungen für folgende Kommunikationsverbindungen vorgesehen:

- **[K_C2I_VsZ_cell]**, Kommunikation zwischen Fahrzeug und (Versuchs-) Zentrale
- **[K_I2I_IRS_VsZ_cell]**, Kommunikation zwischen RSU und (Versuchs-) Zentrale
- **[K_C2I_ExtServ_cell]**, Kommunikation zwischen Fahrzeug und externen Diensten Dritter

Für die Kommunikation mit externen Diensten wird man keine VPN-Lösung verwenden, sondern SSL/TLS zusammen mit Zertifikaten einsetzen, da dies weiter verbreitet und flexibler zu handhaben ist, siehe auch Abschnitt 5.1.3.3.

Generell ist neben der Absicherung durch die Mobilfunkstandards keine zusätzliche Absicherung auf Layer 1 und Layer 2 vorgesehen, da dies innerhalb der hoch standardisierten Mobilfunknetze ohnehin nicht betreiberübergreifend möglich ist. Eine Ende-zu-Ende-Absicherung zwischen Teilnehmern ist somit auf dieser Ebene nicht möglich. Dies ist aber unkritisch, da der Mobilfunk nur als Übertragungstechnik für IP verwendet wird und somit eine Ende-zu-Ende-Absicherung stets mithilfe von IP-basierten Verfahren möglich ist.

In den folgenden Abschnitten erfolgt eine kurze Auflistung der Sicherheitsmechanismen, die bei Mobilfunknetzen für deren Absicherung eingesetzt werden. Die Auflistung dient nur als (sehr) knapper Überblick, für detaillierte Darstellungen wird auf die einschlägige Literatur verwiesen.

5.1.6.1 Datendienste im Mobilfunk

Aus Sicherheitssicht ist EDGE eine Methode zur Bündelung von GPRS-Verbindungen auf GSM-Ebene. Der GSM-Datendienst GPRS besitzt keine eigenen Methoden der Authentisierung oder Verschlüsselung. Ähnlich verhält es sich mit UMTS in Relation zu HSDPA und HSUPA (HSPA). Auch das sind unterschiedliche Übertragungsdienste für UMTS-Netze ohne eigene Sicherheitsmechanismen. Deshalb werden in der nachfolgenden Auflistung von Sicherheitsmechanismen nur GSM bzw. UTMS betrachtet.

5.1.6.2 Auflistung der IT-Sicherheitsmechanismen in GSM-Netzen

Generell ist zu beachten, dass bei den Mobilfunkstandards in der Regel eine Abwärtskompatibilität bis hin zum GSM-Standard realisiert ist.

Folgende Sicherheitsmechanismen gibt es in GSM-Netzen

- Authentisierung des Funknetzteilnehmers durch den Funknetzbetreiber A3-Algorithmus. Eine Authentisierung des Funknetzes durch den Funknetzteilnehmer ist hingegen nicht möglich, so dass hier natürlich potenziell eine Angriffsmöglichkeit (Man-in-the-Middle) besteht.
- Verschlüsselung erfolgt mit einem Verschlüsselungsalgorithmus aus der Gruppe „A5“ in verschiedenen Ausprägungen. Sonderfall: A5/0-keine Verschlüsselung. A5/1 und A5/2 gelten als kryptografisch gebrochen und somit als unsicher. A5/3 ist der in UMTS verwendete KASUMI, allerdings aus GSM-internen Gründen nur mit halber effektiver Schlüssellänge, d.h. 64 Bit. Zudem muss noch bedacht werden, dass die Verschlüsselung durch Funknetzteilnehmer nicht beeinflussbar ist, sondern von der Basisstation bestimmt werden kann.
- Schutz der Privatsphäre durch Anwendung einer zufällig generierten „Temporary Mobile Subscriber Identity“ TMSI. Zum Verbindungsaufbau wird jedoch immer die

eindeutig zuordenbare „International Mobile Subscriber Identity“ (IMSI) unverschlüsselt übertragen. Außerdem kann ihre Übertragung zu Synchronisationszwecken für die Identifikation erzwungen werden. Tracking mit Hilfe der Mobiltelefon-Ortung ist auch ohne TMSI möglich.

- Die aufgelisteten IT-Sicherheitsmechanismen beziehen sich nur auf die Luftschnittstelle. (Verschlüsselung zwischen Mobile Station (MS) und Base Station (BS)).
- Die Absicherung der anderen Verbindungen im GSM- bzw. GPRS-Netz liegt in der Verantwortung der Netzbetreiber. Hierbei muss man sich darüber im Klaren sein, dass die Sicherheit in diesen Netzen auch nicht höher als im herkömmlichen Telefonnetz ist, d.h. es handelt sich um eine Übertragung von Klartext-Daten.

5.1.6.3 Auflistung der IT-Sicherheitsmechanismen in UMTS-Netzen

- Gegenseitige Authentisierung des Funknetzteilnehmers und des Funknetzbetreibers durch Challenge-Response-Verfahren. Damit wird eine Verbesserung gegenüber GSM erreicht. Allerdings ist eine Abwärtskompatibilität zu GSM eingebaut.
- Verschlüsselung beruht wie auch der GSM-Verschlüsselungsalgorithmus A5/3, auf einem kryptografisch starken Blockchiffrieralgorithmus mit 128 Bit Schlüssellänge, hier dem KASUMI. Die Verschlüsselung in UMTS-Netzen ist zwingend. Allerdings ist auch hier die Abwärtskompatibilität zu berücksichtigen.
- Schutz der Privatsphäre durch Anwendung einer verschlüsselten „Extended Encrypted Mobile Subscriber Identity“ (XEMSI). Tracking mit Hilfe der Mobiltelefon-Ortung ist gegenüber GSM deutlich erschwert.
- Die aufgelisteten IT-Sicherheitsmechanismen beziehen sich nur auf die Luftschnittstelle. (Verschlüsselung zwischen MS und BS). Zusätzlich erfolgt eine Verschlüsselung zwischen MS und Radio Network Controller (RNC).
- Die Absicherung der anderen Verbindungen liegt in der Verantwortung der Netzbetreiber.

5.1.6.4 C2X via Mobilfunk

Neben der Übertragung von C2X-Nachrichten per Ad hoc Kommunikation sollen verkehrssicherheitsrelevante Informationen über das Mobilfunknetz übertragen werden, sodass auch entfernte Teilnehmer frühzeitig informiert werden können. Es ist beabsichtigt, dass ein zentraler Geo-Server die aktuelle Position jedes Fahrzeuges zu der aktuellen IP-Adresse zuordnen kann. Dazu melden sich die Fahrzeuge in regelmäßigen Abständen bei dem Geo-Server und übermitteln die eigene IP-Adresse und Position. Anschließend können Fahrzeuge oder eine ITS Central Station C2X-Nachrichten mit einem Zielgebiet an den Geo-Server schicken, der die Nachricht an alle Knoten des geografischen Gebietes spiegelt.

5.1.7 Ausfallsicherheit

In einem ITS werden wichtige Systemkomponenten, wie im Abschnitt 4.1 Schutzbedarfsanalyse ausgeführt, eine hohe Verfügbarkeit haben müssen. Die sich durch einen Ausfall ergebenden Risiken sind in Abschnitt 4.3 beschrieben.

Generell kann man ein komplexes System in verschiedene Komponenten zerlegen, deren multiplizierten Einzelverfügbarkeiten die Gesamtverfügbarkeit des Systems bestimmen. Deswegen sollten die Auswirkungen der Ausfälle einzelner Komponenten möglichst reduziert werden. Zum Beispiel können Arbeitsspeicher, Massenspeicher sowie die Netzwerkkompo-

nenten aufgrund von Defekten bei ihren elektronischen Bauteilen ausfallen. Neben technischen gibt es auch nicht technische Faktoren, die die Ausfallsicherheit eines Systems beeinflussen können. Der wichtigste Faktor ist dabei der Mensch. Er kann durch inadäquate Bedienung der Software und unsachgemäße Handhabung der Hardware für verschiedenste Ausfälle verantwortlich sein.

Die nachfolgende Abbildung zeigt eine Übersicht der beteiligten Ebenen:

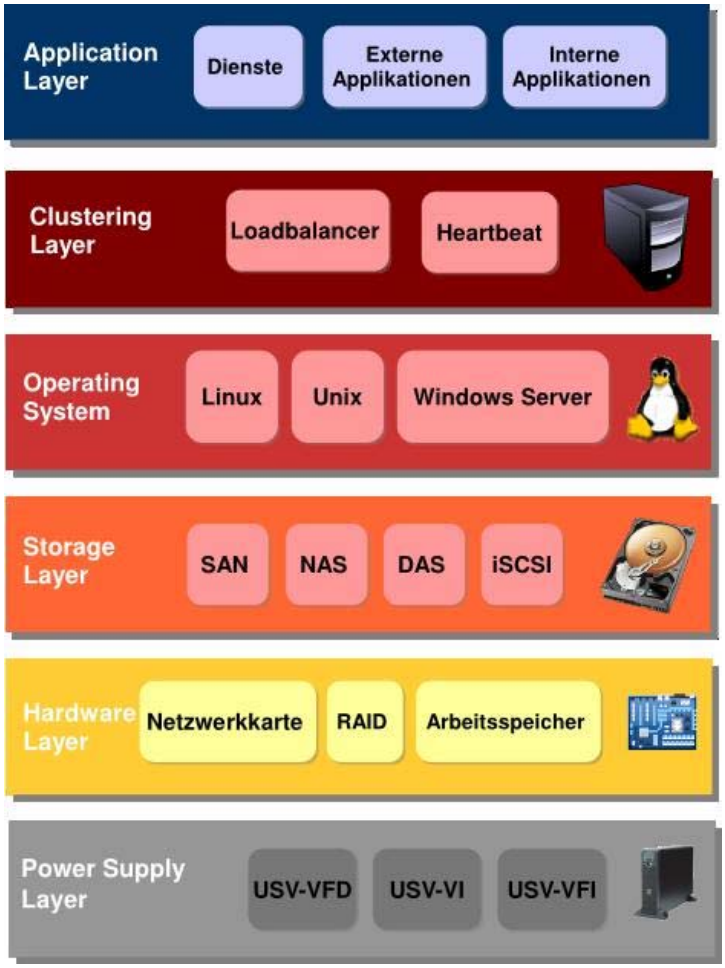

Abbildung 5.3: Ebenen der Ausfallsicherheit

Die nachfolgenden Unterabschnitte erläutern diese Ebenen sowie deren Funktionen.

5.1.7.1 [M_ITS_AS_AL] Application Layer

Die Dienstverfügbarkeit ist das wichtigste Kriterium auf der Anwendungsebene. Hier hat nicht die Erreichbarkeit des Rechners selbst Priorität, sondern die Dienste und Ressourcen, die den Anwendern zur Verfügung gestellt werden. Demzufolge ist es notwendig, die Verfügbarkeit von Anwendungen bzw. Diensten zu überwachen, um im Fehlerfall sofort Maßnahmen ergreifen zu können.

Zur Überwachung muss eine entsprechende Anwendung implementiert oder eine externe Anwendung integriert werden. Fällt eine überwachte Anwendung aus, muss anhand eines vorher definierten Ablaufs die Wiederherstellung der Anwendung bzw. des Dienstes einschließlich aller Eskalationsstufen eingeleitet werden.

5.1.7.2 [M_ITS_AS_CL] Clustering Layer

Ein Computercluster bezeichnet eine Menge von vernetzten Computern, die zur parallelen Abarbeitung von einer oder mehreren Aufgabe oder Teilaufgaben zur Verfügung steht. Es gibt verschiedene, skalierbare Möglichkeiten die Daten oder Dienste auf Cluster-Nodes zu verteilen. Die dabei eingesetzten Techniken sind z.B. Heartbeat (zur Überwachung des Cluster Nodes), Load-Balancer (zur gleichmäßigen Verteilung der Anfragen auf die Nodes) oder beide gleichzeitig. Diesen Techniken können auch über Standorte hinweg eingesetzt werden.

5.1.7.3 [M_ITS_AS_OS] Betriebssystem

Laut einer aktuellen Studie der Yankee Group [12] zur Zuverlässigkeit von Serverbetriebssystemen im vergangenen Jahr, haben sich die durchschnittlichen Ausfallzeiten von Linux und Unix-Betriebssystemen im Vergleich zum Vorjahr reduziert, wohingegen sich die Ausfallzeiten der Windows-Servern sogar leicht erhöht haben. Das zuverlässigste Betriebssystem hatte dabei eine Verfügbarkeit von 99,99 %.

Als Schlussfolgerung daraus muss für die Auswahl eines geeigneten Betriebssystems nicht nur dasjenige Betriebsystem ausgewählt werden, welches am besten zu den inhaltlichen Anforderungen passt, sondern auch das welches die Anforderungen bzgl. Verfügbarkeit am besten erfüllt. Die Höhe der notwendigen Verfügbarkeit hängt dabei individuell vom konkreten Einsatzzweck des Betriebssystems ab.

Wenn ein den Anforderungen am nächsten kommendes Betriebsystem ausgewählt ist, sollten Maßnahmen zu seinem „Schutz“ eingeleitet werden: die Härtung des Betriebssystems (OS-hardening). Hierbei sollten folgende Schritte durchgeführt werden:

- Installation aller Sicherheitsupdates (Anwendungen und Betriebssystem)
- Deaktivierung aller nicht benötigter Dienste und Anwendungen
- Installation nur der wirklich benötigten Anwendungen
- Deaktivierung der nicht benötigten Benutzerkonten und Beschneiden der Rechte von Benutzern auf das unbedingt Nötige (Prinzip der minimalen Rechte)

5.1.7.4 [M_ITS_AS_MS] Massenspeicher

Speichermedien lassen sich vielfältig vernetzen und in die Infrastruktur einbinden. Derzeit existieren drei grundsätzliche Speichermodelle:

- DAS **D**irect **A**ttached **S**torage: DAS ist eine Datenträger, der an den lokalen Bus eines Servers angeschlossen ist.
- NAS **N**etwork **A**ttached **S**torage: NAS Server sind der einfache und kosteneffiziente Weg einem Netzwerk Speicherplatz hinzuzufügen. Dabei wird Speicherplatz über standardisierte Freigabemethoden zur Verfügung gestellt.
- SAN oder iSCSI **S**torage **A**rea **N**etwork oder **i**nternet **S**mall **C**omputer **S**ystem **I**nterface: Ein SAN ist eine Architektur, die dazu bestimmt ist, den Bedarf an Netzwerkdatenspeicher für Server bereit zu stellen. Hauptzweck eines SAN ist der Transfer von Daten zwischen Computersystemen und Speicherelementen und zwischen den Speicherelementen selbst. Über eine iSCSI genannte Technik können Server auf diesen Speicher so zugreifen, als ob er direkt angeschlossen wäre.

5.1.7.5 [M_ITS_AS_HL] Hardware Layer

Netzwerkkarte

Durch eine redundante Nutzung von Netzwerkarten auf Servern nimmt die Ausfallsicherheit zu. Die Netzwerkkarte liefert Datenverkehrslastausgleich und redundanten Betrieb, wenn eine Netzwerkverbindung ausfällt. Zusätzlich sollten verschiedenen Netzwerkkarten auch mit verschiedenen Netzwerkkomponenten verbunden werden.

Hauptspeicher

Als weitere Stufe des Sicherheitskonzeptes werden Server mit abgesichertem Arbeitsspeicher ausgestattet, so genanntem ECC-Memory (Error-Correcting Code Memory). Dieser erkennt Fehler bei der Speicherung und Übertragung von Daten und korrigiert sie, wenn möglich. ECC operiert bei der Korrektur von Daten mit 90-prozentiger Erfolgsquote. Darüber hinaus kann der Hauptspeicher redundant ausgelegt werden. Hierbei werden die gleichen Techniken wie für Festplatten eingesetzt (siehe auch folgenden Abschnitt).

Redundant Array of Independent Disks (RAID)

Unter dem Begriff RAID versteht man die redundante Anordnung unabhängiger Festplatten. Damit werden Daten über mehrere Platten verteilt gespeichert, d.h. die Daten werden mehrmals oder mehrteilig auf physisch unterschiedlichen Platten gelagert. Beim Einsatz bestimmter RAID ist es möglich, falls eine Festplatte ausfällt, die benötigten Daten auf anderen, nicht ausgefallenen Festplatten immer noch zur Verfügung zu haben.

Zur Nutzung von RAID gibt es eine Vielzahl von verschiedenen sogenannten RAID Levels, die für unterschiedliche Einsatzzwecke (sicheres oder schnelles Schreibe bzw. Lesen) bzw. Sicherheitsniveaus (Ausfall von ein, zwei oder mehr Festplatten) entwickelt wurden.

Weitverbreitet und häufig benutzten sind die folgenden RAID-Level:

- RAID 0 (Striping - Beschleunigung ohne Redundanz)
- RAID 1 (Mirroring - Spiegelung) [Ausfall einer Platte ohne Datenverlust möglich]
- RAID 5 (Leistung + Parität) [Ausfall einer Platte ohne Datenverlust möglich]
- RAID 6 (Sicherheit + doppelte Parität) [Ausfall zweier Platten ohne Datenverlust möglich]
- RAID 60 (RAID 0 über zwei RAID 6) [Ausfall zweier Platten ohne Datenverlust möglich]

5.1.7.6 [M_ITS_AS_USV] Unterbrechungsfreie Stromversorgung (USV)

Eine unterbrechungsfreie Stromversorgung (USV), wird für kritische IT-Infrastrukturen eingesetzt, um bei Störungen oder Spannungsschwankungen im Stromnetz die Versorgung von wichtigen Anlagen oder Geräten sicherzustellen. Dank der USV werden alle Server bei einem Stromausfall ordnungsgemäß heruntergefahren. In der höchsten Ausbaustufe wird die Funktion einer USV von einem Notstromgerät unterstützt oder sogar ganz ersetzt. Damit ist es möglich, ein Rechenzentrum – abhängig von der Kapazität des Notstromaggregats – teilweise tagelang mit Strom für den weiteren Betrieb zu versorgen.

5.1.8 Wartung, Verwaltung und Aktualisierung der ITS Stations

Software und Hardware sind in einer IT-Infrastruktur die beiden großen Blöcke, die sich im Zusammenspiel zu einem System vereinen. Die Wartung, Verwaltung und Aktualisierung der

Komponenten in einem solchen System erfordert ein spezialisiertes Wissen über das jeweilige Teilsystem.

Im folgenden Abschnitt werden die grundlegenden Techniken zur Wartung von Hardware beschrieben. Die Überwachung der Hardware soll dabei – wenn möglich – remote realisiert werden. Die eigentliche (Hardware-)Wartung muss dann vor Ort erfolgen.

Neben der Wartung der Hardware wird im Folgenden auch die Verwaltung und Aktualisierung der Software beschrieben. Die Verwaltung der Software muss dabei sowohl über remote als auch lokal möglich sein.

Aus der IT-Sicherheitssicht sind folgende Aspekte sowohl für Hardware als auch für Software zu betrachten:

- [M_WVA_SW_CERT] CERT[31] Modell: Es ist sehr wichtig, eine Richtlinie auszuarbeiten, wie in Falle eines Sicherheitsvorfalls vorzugehen ist. Diese Richtlinie sollte die vier folgenden Aktionspunkte umfassen:
  1. Ausführen von Gegenmaßnahmen bzw. Begrenzung des Schadens
  2. Untersuchung und Dokumentation des Vorfalls (wie weit ist der Angreifer eingedrungen, welche Systeme, Schlüssel, Daten usw. wurden möglicherweise kompromittiert)
  3. Wiederherstellung des Ursprungszustandes unter Berücksichtigung einer möglicherweise durch den Angriff aufgezeigten Schwachstelle
  4. Meldung der Vorfalls an eine verantwortliche Stelle

- [M_WVA_SW_SU] Sicheres Update: Ein automatischer Austausch von Softwarekomponenten im Betrieb erfordert mehrere Sicherheitsmaßnahmen, um einen Missbrauch zu verhindern. Der Zugang zu dem Aktualisierungsdienst muss beschränkt sein auf autorisierte Benutzer, die eventuell nur berechtigt sind, bestimmte Softwarekomponenten auszutauschen. Zudem muss vor der Installation der aktualisierten Softwarekomponente die Integrität sowie die Herkunft geprüft werden (Prüfung der kryptografischen Signatur). Darüber hinaus muss bei Austausch von Hardware Komponenten möglich sein, unerlaubte Manipulationen zu erkennen. Hierfür existieren verschiedene Authentisierungsmechanismen. Darüber hinaus existieren neue Technologien wie „Physical Unclonable functions“, die zusätzliche Hardware Sicherheitsmaßnahmen anbieten. Ein anderes sehr wichtiges Schutzziel bei Update ist der Schutz des Know-Hows. Es darf bei der Aktualisierung nicht möglich sein, wichtige Softwarekomponenten auszulesen, um sie z.B. zu analysieren, um sich fremdes Know-How anzueignen.
- [M_WVA_IS_LOGIN] Sicheres Login auf den ITS Stations: Zur Absicherung der Benutzeranmeldung auf den ITS Stations existieren eine Reihe von Methoden zur Verteidigung gegen „Brute-Force“ Angriffe. Die folgende Auflistung gibt einen Überblick, welche Methoden umgesetzt werden können.
  1. *Komplexe Passwörter:* Durch Nutzung der Initialen der Wörter eines Satzes lassen sich auf einfache Weise starke und merkbare Passwörter erzeugen. Zusätzlich können noch Sonderzeichen hinzugenommen werden, um die Komplexität zu erhöhen.

[31] CERT: Computer Emergency Response Team

2. *Public-Key-Authentifizierung:* Diese Authentifizierungsmethode basiert auf einem Paar von für diesen Zweck generierten kryptografischen Schlüsseln (privaten und öffentlichen Schlüssel), die zwischen dem Server und dem Benutzer aufgeteilt werden. Der Vorteil ist, dass die Authentifikation auf dem Besitz des passenden Schlüssels basiert, und deshalb die sichere Verbindung ohne Eingabe eines Passwortes aufgebaut werden kann.
3. *IPTables:* Mit Hilfe des integrierten Netzwerkfilters IPTables kann man den Adressraum der möglichen Angreifer einschränken: Es können beispielsweise nur vertrauenswürdige IP-Adressen zugelassen werden.
4. *SSHD:* Durch die Überwachung der Syslog–Einträge auf fehlgeschlagenen Anmeldungen können die IP-Adressen von möglichen Angreifern ermittelt werden und automatisch für eine gewisse Zeit blockiert werden. Es existieren mehrere Programme, die nach diesem Mechanismus arbeiten (z.B.: ssdfilter, Fail2Ban, DenyHosts, etc.).

5.1.8.1 Software

Die Software in einem Verbund von Systemen sollte sich auf einen einheitlichen Standard zurückführen lassen, d.h. im prinzipiellen Aufbau und der technischen – nicht inhaltlichen – Systematik sollten sie sich nicht grundlegend unterscheiden. Dabei ist es aber möglich, dass sich die Plattformen (d.h. die Betriebssysteme) auf denen sie läuft unterscheiden. Wobei grundsätzlich zwischen zwei verschiedenen Arten von Software unterschieden werden muss. Auf der einen Seite ist die eigentliche Anwendung, auf der anderen Seite die Verwaltungs-software und das Framework für die Anwendungen.

Die Anwendungen sollten sich dabei über einen einheitlichen Mechanismus aktualisieren lassen. Dabei können prinzipiell unterschiedliche Verfahren um Einsatz kommen:

- Update/Installation über Betriebssystemmechanismen (bei Linux-basierten Systemen z.B. aptitude oder rpm)
    - Vorteil: Der Updatemechanismus und die verwendeten Technologien sind bereits vorhanden und müssen nur genutzt werden.
    - Nachteil: Dieser Mechanismus ist von Betriebssystem zu Betriebssystem unterschiedlich, so dass immer eine individuelle Prozedur notwendig ist. Nicht bei allen Betriebssystemen ist eine einfache Möglichkeit vorgesehen, um eigene Anwendungen über die Updatemechanismen des Betriebssystems zu installieren.
- Update/Installation über das Anwendungsframework
    - Vorteil: Das Anwendungsframework stellt eine abstrahierende Sicht gegenüber dem Betriebssystem dar. Dadurch kann sichergestellt werden, dass (unter der momentan sich abzeichnenden Prämisse, dass Anwendungen durch ein pattformunabhängige Laufzeitumgebung, z.B. Java repräsentiert werden) unabhängig von Betriebssystem der gleiche Mechanismus und die gleichen Executables genutzt werden können. Im Fall, dass die Prämisse nicht zutrifft, müssen die Executables für jedes im Verbund vorhandene Betriebssystem vorgehalten werden.
    - Nachteil: Das Anwendungsframework muss über Wartungsfunktionalitäten verfügen, die das Framework deutlich vergrößern, dadurch kann sich, abhängig von der verwendeten Technologie, eine Abhängigkeit vom Anbieter des Frameworks ergeben.
- Update/Installation durch eine eigene Systemkomponente

- Vorteil: Durch die Nutzung einer eigenen Komponente zur Wartung der Software können Mechanismen unabhängig vom zugrunde liegende System und dem Anwendungsframework entwickelt werden, dadurch kann eine Form von Freiheit gegenüber diesen Komponenten erreicht werden, d.h. es besteht keine direkte Abhängigkeit von den Anbietern der andern Komponenten.
- Nachteil: Es muss eine zusätzliche Komponente in das System integriert werden. Diese Komponente selbst generiert wieder Wartungsaufwand.

- Update/Installation von Hand
  - Vorteil: Die Installation kann sehr individuell ablaufen und es kann auf alle Bedürfnisse der jeweiligen Anwendung Rücksicht genommen werden.
  - Nachteil: Es existiert kein standardisierter Prozess zur Installation, das bedeutet, dass der Installations- und Updateprozess für jede Anwendung ausführlich beschrieben werden muss und dieser Prozess durch die händische Arbeit deutlich mehr Zeit und Ressourcen in Anspruch nimmt.

Die Systemkomponenten teilen sich wiederum in zwei Bereiche auf. Die Verwaltungssoftware und das Anwendungsframework bilden dabei die nutzergenerierten Komponenten und die dem Betriebssystem eigenen Funktionen bilden den systeminhärenten Teil von Komponenten. Die dem Betriebssystem eigenen Komponenten sollten auch nur in der vom Betriebssystem vorgesehen Prozedur installiert und verwaltet werden, damit es zu keinen Instabilitäten bzw. Inkonsistenzen kommt.

Die nutzergenerierten Komponenten können durch ähnliche Verfahren installiert werden, wie die Anwendungen.

- Betriebssystemmechanismen (Vor- und Nachteile siehe Anwendungen)
- Eigene Systemkomponente (Vor- und Nachteile siehe Anwendungen)
- Per Hand (Vor- und Nachteile siehe Anwendungen)

Die Mechanismen sind näher am eigentlichen Betriebssystem orientiert und können sich je nach Kontext und Betriebssystem deutlich unterscheiden.

Für alle oben genannten Mechanismen muss es eine Möglichkeit geben diese sowohl lokal auf dem System als durch Fernwartung über eine wie auch immer geartete Verbindung durchführen zu können.

Eine Beschreibung von Software Lebenszyklen kann unter „ISO 10007:2004 Qualitätsmanagement – Leitfaden für Konfigurationsmanagement“ gefunden werden.

5.1.8.2 Hardware

Die Wartung der Hardware kann in zwei Teile aufgeteilt werden. Die Überwachung der Hardware ist dabei dafür zuständig, Fehler zu erkennen, während die eigentliche Wartung der Fehlerbehebung dient.

Die Überwachung der Hardware kann dabei über hardwareseitige Sensoren (z.B. Watchdog, Temperatursensor) erfolgen. Die Daten der Sensoren können genutzt werden, um die Hardware zu schützen und – über geeignete Kommunikationswege – eine Zentrale über Probleme zu informieren.

Die Wartung der Hardware eines Systems kann zyklisch, d.h. nach einem bestimmten Zeitintervall, oder bei Bedarf im Falle einer Fehlfunktion durchgeführt werden. Für die Hardware sollten auch entsprechende Wartungsverträge mit den jeweiligen Lieferanten abgeschlossen

werden, so dass eine zeitnahe und kompetente Lösung hardwaretechnischer Maßnahmen schnellstmöglich durchgeführt werden können.

5.2 IT-Sicherheitsarchitektur eines Wirksystems

In diesem Abschnitt wird die grobe IT-Sicherheitsarchitektur eines zukünftigen Wirksystems vorgestellt, welche basierend auf Abbildung 5.4 die Komponenten zur Absicherung der Kommunikation beschreibt. In diesem Abschnitt werden Absicherungsmaßnahmen vorgeschlagen, die für ein umfangreiches C2X-Kommunikationsnetz Anwendung finden könnten. Einerseits wird im Gegensatz zu Abschnitt 5.3 wird nicht von der Existenz eines Versuchssystems ausgegangen. Das heißt, die Übertragung von Logdaten und Fahreranweisungen werden in diesem Abschnitt nicht betrachtet. Andererseits muss davon ausgegangen werden dass die eingesetzten Schlüssel für einen langen Zeitraum gültig sein müssen und dass spezielle Hardware (TPM, Hardware zur Kryptografiebeschleunigung) zum Schutz der internen Fahrzeugkommunikation eingesetzt wird.

Die Empfehlungen für die Absicherung eines Wirksystems beruhen auf Annahmen, die derzeit für ein wahrscheinliches ITS vorliegen. Diese können in den folgenden Abschnitten eventuell von den Vorstellungen des Lesers oder verschiedener beteiligter Parteien leicht abweichen.

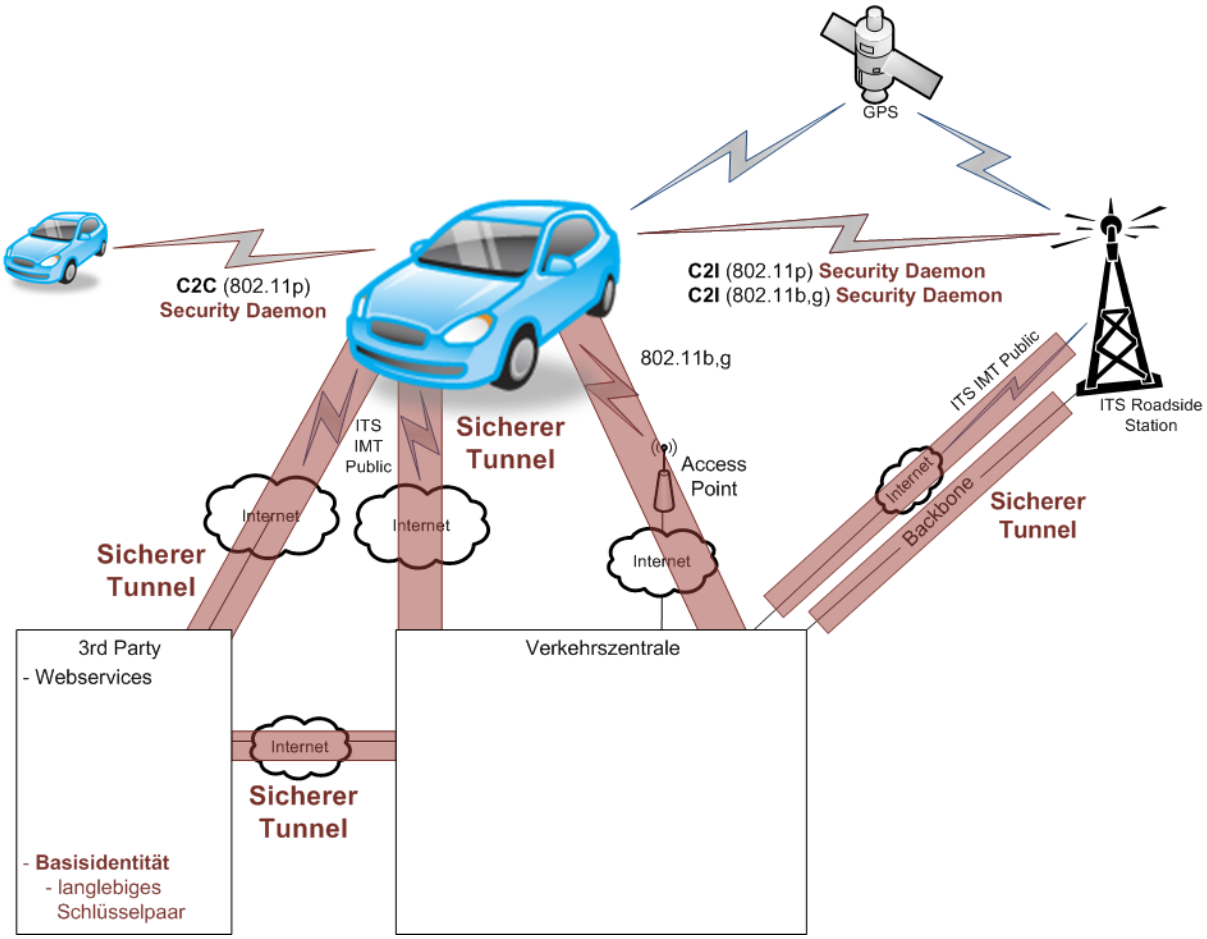

Abbildung 5.4: Übersicht der ITS Absicherung eines Wirksystems

Abbildung 5.4 zeigt eine grobe Übersicht aller wichtigen Komponenten, die miteinander kommunizieren. Hierbei lassen sich verschiedene Arten von Kommunikationskanälen identifizieren, die IT-sicherheitstechnisch relevant sind. Eine Übersicht der Kommunikationskanäle

für ein ITS IT-Sicherheitskonzept bietet die Tabelle 5.4, in der auch die verwendeten Protokolle und die Absicherungsverfahren aufgelistet sind.

Kommunikationskanäle	Kommunikations-technologie	IT-Sicherheitsmechanismen
Vehicle CCU – Vehicle CCU **[K_C2C_11p]**	IEEE 802.11p	IEEE 1609.2 (Authentisierung) Plausibilitätschecks
Vehicle CCU – Roadside CCU **[K_C2I_11p]** **[K_C2I_11bg]**	IEEE 802.11p	IEEE 1609.2 (Authentisierung) Plausibilitätschecks
	IEEE 802.11 b/g (C-WLAN)	Absicherung durch IEEE 1609.2 Anwendungsebene
Vehicle CCU – Verkehrszentrale **[K_C2I_VsZ_cell]** **[K_C2I_11bg]**	ITS IMT Public (UMTS, GPRS)	Sicherer Tunnel **[M_ITS_VN] [M_ITS_VPN]** (Verschlüsselung + Authentisierung)
	IEEE 802.11 b/g (C-WLAN)	WLAN Absicherung auf Layer 2 über die Luftschnittstelle, danach sicherer Tunnel bzw. proprietäre Verbindung
Vehicle CCU – Third Party **[K_C2I_ExtServ_cell]**	ITS IMT Public (UMTS, GPRS)	Sicherer Tunnel **[M_ITS_VPN] [M_TLS_Sec]** (Verschlüsselung + Authentisierung) Autorisierung
Roadside AU – Verkehrszentrale bei sim^{TD} repräsentiert durch: ***[K_I2I_IRS_IGLZ]*** **[K_I2I_IRS_VsZ_cell]**	Proprietärer Backbone / Ethernet, TCP/IP	Sicherer Tunnel **[M_ITS_VPN] [M_TLS_Sec]** (Verschlüsselung + Authentisierung)
	ITS IMT Public (UMTS, GPRS)	Sicherer Tunnel **[M_ITS_VPN] [M_IPSec_Mobil]** (Verschlüsselung + Authentisierung)
3rd Party – Verkehrszentrale **[K_ExtServ_VsZ]**	Internet	Sicherer Tunnel **[M_ITS_VPN] [M_TLS_Sec]** (Verschlüsselung + Authentisierung + Autorisierung)

Tabelle 5.4: Absicherung der Kommunikationskanäle im ITS eines Wirksystems

ITS Sicherheitsdienst

Wie in Abbildung 5.5 dargestellt, muss ein Sicherheitsdienst für ITS Funktionen eine Schnittstelle zum Signieren und/oder Verschlüsseln bzw. Verifizieren und/oder Entschlüsseln von Datenpaketen (I-S1, I-S2) bieten. Das Signieren erfolgt mit Hilfe von lokal vorhandenen Zertifikaten und Schlüsseln und entsprechender Signaturalgorithmen.

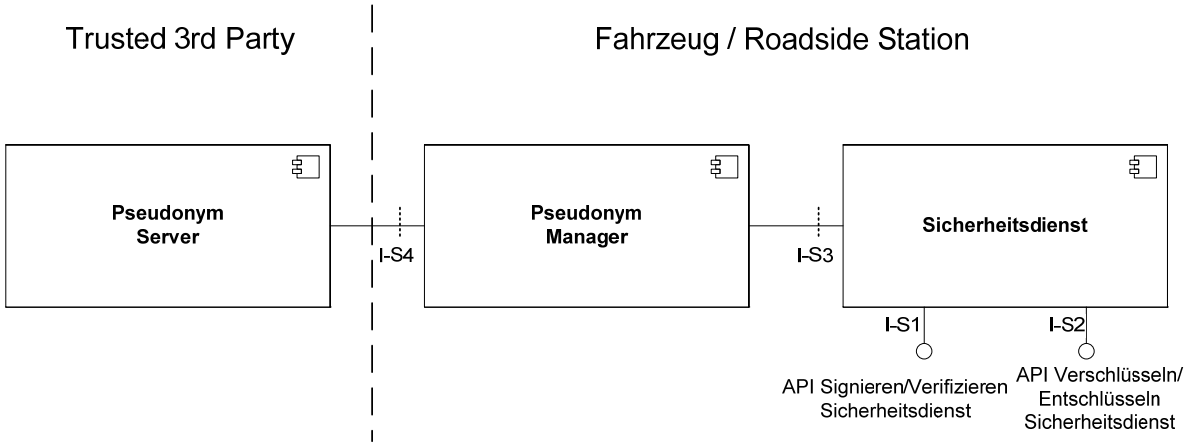

Abbildung 5.5: Komponenten des Sicherheitsdienstes für Ad-Hoc ITS-Sicherheitsfunktionen

Eine lokale Instanz auf dem Fahrzeug muss verschiedene Zertifikate und Pseudonyme verwalten, die zentral von einem Pseudonymserver einer vertrauenswürdigen dritten Instanz zugewiesen worden sind. Schnittstellen zwischen diesen Komponenten sind I-S3 für die interne Versorgung mit korrekten Schlüsseln und Zertifikaten bzw. I-S4 für die Versorgung mit neuen Schlüsseln und Zertifikaten vom Pseudonymserver.

Aufgaben eines IT-Sicherheitsdienstes im ITS sind:

- Verifizieren von Signaturen und Zertifikaten
- Signieren von Nachrichten
- Verschlüsseln von Nachrichten
- Entschlüsseln von Nachrichten
- Steuerung eines Pseudonymwechsels in allen Kommunikationskomponenten
- Plausibilitätsprüfung der Nachrichteninhalte
- Konfigurationsprüfung des Fahrzeugsystems

In den folgenden Unterkapiteln werden die einzelnen Aufgaben des ITS-Sicherheitsdienstes genauer betrachtet und diskutiert. In 5.2.1 wird die Verwaltung und der Einsatz digitaler Zertifikate und dessen Schlüssel betrachtet die für die Kommunikationsabsicherung von der Zentrale bereitgestellt werden. Die zentrale Verwaltung und die Übertragung der digitalen Pseudonyme wird in Abschnitt 5.2.2 diskutiert. Wie bereits erwähnt müssen Kommunikationskanäle über unsichere Netze durch einen Tunnel gesichert werden, wie in Abschnitt 5.2.3 näher erläutert wird. Die drahtlosen Kommunikationskanäle über IEEE 802.11p, IEEE 802.11b/g und ITS IMT Public werden in den Abschnitten 5.2.4, 5.2.5 und 5.1.6 in Hinblick auf deren Absicherung betrachtet. Da die Zentrale alle infrastrukturseitigen Systeme steuert und die meisten zentralen Aufgaben übernimmt, werden in Abschnitt 5.2.10 die Schnittstellen aus Sicht der IT-Sicherheit genauer betrachtet. Ein weiterer wichtiger Punkt ist die Ausfallsicherheit der zentralen und infrastrukturseitigen Systeme, welche in Abschnitt 5.2.7 behandelt wird. Abschnitt 5.2.8 befasst sich mit den organisatorischen und rechtlichen Maßnahmen in Bezug auf IT-Sicherheit, da diese in einem generischen Fahrzeugkommunikationssystems eine wichtige Rolle spielen. Schließlich werden in Abschnitt 5.2.9 IT-Sicherheitsrelevante Maßnahmen in Bezug auf die Wartung, Verwaltung und Aktualisierung von Hardware und Software betrachtet.

5.2.1 Identitäten und Pseudonyme

Die fahrzeugseitige Pseudonymverwaltung muss gewährleisten, dass Schlüsselmaterial nicht missbräuchlich benutzt werden kann. Hierfür sind entsprechende sichere Hardwarelösungen anzustreben. Jedes Fahrzeug muss mit einem langlebigen Schlüsselpaar (der Basisidentität) ausgestattet werden. Dabei ist wichtig, dass der private Schlüssel der langlebigen Basisidentität auf dem Fahrzeug generiert wird und auch immer auf dem Fahrzeug bleibt. Diese Forderung ist äußerst wichtig, da ansonsten Basisidentitäten inklusive der zugehörigen privaten Schlüssel aus einem Fahrzeug exportiert werden könnten. Durch Verwenden mehrerer solcher exportierter Basisidentitäten kann ein Angreifer mehrere Fahrzeuge gleichzeitig simulieren und dadurch besondere Verkehrssituationen wie Staus oder Unfälle (virtuell) erzeugen. Die Folgen eines solchen *Sybil*-Angriffes können die Verkehrssicherheit wesentlich gefährden und müssen daher auf jeden Fall vermieden werden. Daher muss durch spezielle Hardware (z.B. Tamper Proof Device, TPD) sichergestellt werden, dass private Schlüssel der Basisidentität nicht aus einem Fahrzeug exportiert werden können. Darüber hinaus darf ein Fahrzeug niemals mehr als eine gültige Basisidentität erhalten. Zur Aktualisierung der Basiszertifikate wird daher ein halbautomatischer Vorgang vorgeschlagen, bei dem im Zuge eines Serviceintervalls neue Basisidentitäten automatisch erzeugt werden, ihre Zertifizierung jedoch durch einen Administrator bestätigt werden muss. Es muss dabei sichergestellt werden, dass sobald ein Fahrzeug eine neue Basisidentität erhält, die alte Basisidentität ungültig wird, bzw. für den verbleibenden Gültigkeitszeitraum auf die Revokationsliste gesetzt wird.

Die Verwendung von wechselnden Pseudonymen anstelle von unveränderlichen eindeutigen Identitäten erfordert ein entsprechendes Management der Pseudonyme. Von grundsätzlicher Bedeutung ist es hierbei, einen Vorrat an Pseudonymen anzulegen, zertifizieren zu lassen und ein Schema für das Wechseln von Pseudonymen zu verwalten. Um eine Verknüpfung zwischen Pseudonymen untereinander und zwischen Pseudonymen und der eindeutigen Identität zu erschweren muss ein gleichzeitiger Wechsel aller Pseudonymbestandteile gewährleistet werden. Des Weiteren darf der private Schlüssel eines Pseudonyms das Fahrzeug nicht verlassen – aus den gleichen Gründen, wie sie auch für die Basisidentität im vorigen Absatz erläutert wurden. Nach der Erzeugung eines neuen Schlüsselpaares wird der öffentliche Teil des Schlüssels vom Fahrzeug an die Pseudonymverwaltung in der ITS Central Station geleitet um dort signiert zu werden. Der signierte öffentliche Schlüssel bildet mit weiteren Attributen, wie zum Beispiel Typ und Gültigkeit, ein Zertifikat, das wiederum zusammen mit dem privaten Schlüssel das Pseudonym bildet. Alle Nachrichten, die vom Inhaber des Pseudonyms abgesendet werden, müssen mit dem privaten Schlüssel des Pseudonyms unterschrieben werden. Außerdem muss das Zertifikat mit dem öffentlichen Schlüssel an die Nachricht angehängt werden. Mit dem öffentlichen Schlüssel des Pseudonyms können symmetrische Schlüssel für verschlüsselte Kommunikation verschlüsselt werden, die nur dem Besitzer des privaten Schlüssels bekannt werden.

Der Wechsel zwischen verschiedenen Pseudonymen kann nach unterschiedlichen Strategien erfolgen. Die einfachste Variante führt einen regelmäßigen oder zufälligen Wechsel zwischen den Pseudonymen durch. Mit diesem Ansatz kann eine Basis für den Privatsphärenschutz gelegt werden. In Situationen in denen sich nur sehr wenige Fahrzeuge in einem bestimmten Gebiet befinden kann ein unkoordinierter Wechsel sehr einfach durch externe passive Teilnehmer entdeckt werden, die die Kommunikation mithören. Für die konzeptuelle IT-Sicherheitslösung müssen intelligente, kooperative Mechanismen zum gemeinsamen Wechsel von Pseudonymen vorgesehen werden um vor allem im Anfangsstadium von C2X-Kommunikationsnetzwerken einen erhöhten Schutz der Privatsphäre zu gewährleisten.

5.2.2 Pseudonymverwaltung

Wir gehen davon aus, dass im Wirksystem eine hierarchische PKI existiert, da die Vergabe von Pseudonymen für die ITS Kommunikation wahrscheinlich föderal aufgebaut wird und beim Eintreten in ein anderes Bundesland Pseudonyme durch die CA des jeweiligen Landes vergeben werden. Durch dieses Vorgehen ergeben sich verschiedene Vorteile. Zum einen reduziert sich für die CA der Aufwand für die Verwaltung von Pseudonymen auf die im jeweiligen Hoheitsbereich vorhandenen Fahrzeuge, zusätzlich wird die Privatsphäre der Benutzer besser geschützt, da Fahrzeuge nicht anhand ihrer Herkunft identifiziert werden können. Dazu wird in jedem Hoheitsbereich ein zentrales ITS Sicherheitssystem aufgebaut, welches für die Verwaltung und Ausgabe von digitalen Zertifikaten (Pseudonymen) zuständig ist. Die eingesetzten PKI-Komponenten werden im Folgenden erläutert.

5.2.2.1 [M_W_ITS_PSDV] Verteilung der Pseudonyme

Für die Absicherung der C2C- und C2I-Kommunikation muss gewährleistet sein, dass die Absender von Nachrichten authentisch sind, d.h. die Angabe des Absenders nicht gefälscht und die Daten nicht manipuliert wurden. Dazu wird eine vertrauenswürdige Instanz (CA) benötigt, der alle Fahrzeuge und Systeme „vertrauen“. Diese ordnet jedem Fahrzeug und System ein oder mehrere Pseudonyme zu. Die Zuordnung erfolgt in Form eines Zertifikats, das durch die CA signiert ist.

Eine zentrale PKI im ITS Umfeld soll alle verwendeten Zertifikatsformate ausstellen können und Mechanismen zum Verteilen bereitstellen wie in Abschnitt 5.2.2.2 beschrieben.

Jeder Teilnehmer im Wirksystem wird mit einer Basisidentität ausgestattet. Diese Basisidentität kann initial nur lokal durch einen Servicetechniker installiert werden. Eine automatische Verteilung über ein Fernwartungssystem ist nicht zu realisieren, da sich der Teilnehmer nicht gegenüber der PKI authentisieren kann, solange er noch keine Basisidentität besitzt. Spätere Aktualisierungen der Basisidentität können dann – wie oben beschrieben – in einem halbautomatisierten Prozess vonstatten gehen, bei der ein Servicetechniker die Ausstellung einer neuen Basisidentität bestätigt. Mit Hilfe dieser Basisidentität kann sich nun anschließend die ITS Vehicle Station oder ITS Roadside Station mit weiteren Pseudonymen ausstatten, die zur aktiven C2X-Kommunikationsabsicherung eingesetzt werden. ITS Vehicle Stations müssen ständig über einen Vorrat an Pseudonymen verfügen, um damit die C2X-Kommunikation signieren zu können ohne Rückschlüsse auf ihre Identität zuzulassen. Durch einen regelmäßigen Wechsel der Pseudonyme kann der Schutz der Privatsphäre für den Fahrer erhöht werden. ITS Roadside Stations werden jedoch nur mit einer Basisidentität oder einem nicht wechselnden Pseudonym ausgestattet, da diese im Allgemeinen ortsfest sind und Pseudonymwechsel keinen anonymisierenden Effekt haben.

Bei der automatischen Verteilung von neuen Pseudonymen ist es wichtig, dass die neuen Schlüsselpaare für die Pseudonyme auf dem Fahrzeug selbstständig und in hoher Qualität generiert werden. Der öffentliche Schlüssel wird anschließend in eine Zertifikatsanforderung (*Certificate Request*) eingefügt und zur zentralen PKI zum Signieren versendet. Die Kommunikation mit der PKI muss in diesem Fall mit dem öffentlichen Schlüssel der PKI verschlüsselt werden um die Daten geheim zu halten und dadurch eine Zuordnung der angefragten Basisidentität zu aktuell verwendeten Pseudonymen zu verhindern. Des Weiteren wird die Zertifikatsanforderung mit der Basisidentität des Fahrzeuges signiert, so dass die PKI die Authentizität der Anfrage verifizieren und eine Autorisierung vornehmen kann.

In einem Wirksystem ist der Schutz des Schlüsselmaterials essentiell für die Sicherheit und Vertrauenswürdigkeit des Gesamtsystems. Wie schon erwähnt müssen alle Schlüsselpaare auf dem Fahrzeug in einem besonders geschützten Bereich erstellt und abgespeichert werden. Hierzu können evtl. Tamper Proof Devices (TPDs) verwendet werden. Der private Schlüssel darf dieses TPD niemals verlassen und es muss gewährleistet sein, dass ein

unerlaubter Zugriff den privaten Schlüssel zerstört oder unbrauchbar macht. Außerdem muss die unerlaubte oder fehlerhafte Benutzung von Schlüsseln zu einer Revokation desselben führen wie in Abschnitt 5.2.2.3 weiter erläutert. Des Weiteren muss in einem Wirksystem dafür gesorgt werden, dass pro Fahrzeug immer nur ein Pseudonym gleichzeitig eingesetzt werden kann. Sybil-Angriffe, in denen sich ein Fahrzeug gleichzeitig mit mehreren Pseudonymen authentifiziert und damit imaginäre Fahrzeuge simuliert, müssen verhindert werden. Die Erkennung von Fehlverhalten des eigenen Systems kann in einem Wirksystem mit nur einer Plausibilitätsprüfung oder einem Intrusion Detection System (IDS) realisiert werden, welches nicht nur die empfangen Daten prüft, sondern auch die eigenen ausgesendeten Daten bewertet. Diese Erkennung ist jedoch – je nach Situation – mit unterschiedlich starker Unsicherheit behaftet, so dass sie im Einzelfall auch überhaupt keinen Schutz bieten kann.

5.2.2.2 Verwaltung und Auflösung der Pseudonyme

In besonderen Fällen muss die Kommunikation einem bestimmten Fahrzeug jederzeit zugeordnet werden können um Unfälle oder Diebstähle aufklären zu können. Für ein generisches Fahrzeugkommunikationssystem ist es daher wichtig, dass die verwendeten und ausgestellten Zertifikate durch eine vertrauenswürdige Instanz in einem geschützten Bereich mit Zuordnung zur langfristigen Basisidentität des Fahrzeuges gespeichert werden. Um dies gewährleisten zu können muss eine Datenbank angelegt werden, in der alle Zertifikate für einen gewissen Zeitraum gespeichert werden. Wie in Abschnitt 5.2.2.1 beschrieben, werden die öffentlichen Schlüssel eines Pseudonyms in einem Zertifikat mit weiteren Informationen zusammengefasst und durch eine CA unterschrieben, damit sie in der C2X-Kommunikation eingesetzt werden können. Bei jeder Zertifizierung ist es nun Aufgabe des Sicherheitsservers der ITS Central Station, die Verknüpfung zwischen Zertifikat und Basisidentität des anfragenden Teilnehmers zu speichern. Im Notfall kann nun im Nachhinein durch Auflösung des Pseudonyms zu dem dazugehörigen Basiszertifikat eine eindeutige Identifizierung des Netzwerkteilnehmers erfolgen. Da diese Zuordnung nur im Sonderfall möglich sein soll, muss der Zugriff auf diese Funktion besonders geschützt werden und durch besondere Autorisierungsmaßnahmen umgesetzt werden.

5.2.2.3 Revokation von Pseudonymen

ITS-Komponenten können angegriffen oder gestohlen werden. In solchen Situationen muss von einer Kompromittierung der auf der Komponente gespeicherten Schlüssel ausgegangen werden. Bei einer Kompromittierung des Schlüsselmaterials müssen die betroffenen Zertifikate so schnell wie möglich im gesamten System revoziert werden.

Die Revokation von Basisidentitäten und ggf. auch von wechselnden Pseudonymen wird durch die PKI der ITS Central Station sichergestellt. Information über die gesperrten Pseudonyme werden automatisiert allen Teilnehmern schnellstmöglich zur Verfügung gestellt.

5.2.2.4 Hard- und Softwarevalidierung der Fahrzeugsysteme

Bei jeder Anfrage nach neuen Pseudonymen durch eine ITS Vehicle Station muss der PKI das Basiszertifikat zur Authentifizierung vorgelegt werden. Zusätzlich übermittelt werden Validierungswerte aus einer Analyse des Fahrzeugsystems. Aufgrund dieser Werte kann mit Hilfe einer zentralen Datenbank überprüft werden, ob die verwendeten Hard- und Softwarekomponenten auf dem Fahrzeug korrekt sind. Nur bei einer erfolgreichen Authentisierung und Autorisierung durch das Testergebnis werden dem Fahrzeug die signierten Pseudonyme zurückgeliefert. Die Vergabe von Basisidentitäten sollte ebenfalls an eine erfolgreiche Validierung der verwendeten Hard- und Softwarekomponenten gebunden sein.

Diese Validierung kann in zwei Ausprägungen geschehen. Einerseits eine Selbstdiagnose mit Hilfe einer sicheren Hardwareplattform und andererseits eine Diagnose, die im Rahmen der erstmaligen und regelmäßigen technischen Überprüfung des Fahrzeugs durchgeführt wird.

Mit diesem Vorgehen wird den Zertifikaten nicht nur die Autorisierung zugrundegelegt, sondern auch die Verfassung des Fahrzeugs, d.h. die Zusammensetzung der Hard- und Softwareausstattung. Auf diese Weise kann sichergestellt werden, dass nur ein als betriebssicher eingestuftes Fahrzeug eingesetzt wird. Bekannte kompromittierte Komponenten können so aus dem Verkehr gezogen werden. Es ist jedoch zu beachten, dass die Zusammensetzung der Fahrzeugsysteme nur in größeren Abständen geprüft werden kann, da die Anfrage nach neuen Pseudonymen auch nur in größeren Abständen sinnvoll ist.

5.2.3 Absicherung der IP-basierten Kommunikationsverbindungen

Im diesem Abschnitt wird dargelegt, welche der in Abschnitt 5.1.3 dargelegten Verfahren für Absicherung von IP-Verbindungen im Rahmen eines ITS eingesetzt werden.

Im Wirksystem werden die vorgeschlagenen Verfahren neben der Anbindung der stationären Knoten auch noch für die Ende-zu-Ende-Absicherung der IP-Kommunikation der vielen mobilen Knoten verwendet. Allerdings werden die mobilen Knoten im ITS nur in sehr eingeschränkter Form IP-Verbindungen verwenden, nämlich

- bei der Kommunikation über Mobilfunk, sei es zur Zentrale oder zu externen Diensten und
- gegebenenfalls noch bei der Kommunikation über kommerzielles WLAN nach IEEE 802.11b/g, dies aber aller Voraussicht nach nur in einem quasi-statischen Szenario, man denke z.B. an einen Hot-Spot auf einer Raststätte.

Hierbei wird zwar eine dynamisch vergebene IP-Adresse verwendet, allerdings bleibt diese über einen hinreichend langen Zeitraum konstant, so dass die (abgesicherten) Verbindungen nicht übermäßig von Abbrüchen durch IP-Adresswechsel betroffen sein werden.

Im Fokus dieses Abschnittes steht die Mobilfunk-Verbindung, da diese auch im Wirksystem aller Voraussicht zumindest temporär notwendig sein wird. Die Übertragung der lokal generierten Zertifikate zum zentralen Signaturdienst und wieder zurück muss nämlich über eine hinreichend stabile IP-Verbindung erfolgen. Allerdings ist es hierfür nicht notwendig eine IP-Verbindung dauerhaft aufrecht zu erhalten, sondern es ist reicht, wenn dies nur sporadisch geschieht.

5.2.3.1 [M_ITS_VN] Virtuelles IP-Netz zwischen stationären Knoten des ITS

Alle Zentralen und andere (größeren) stationäre Elemente eines ITS sind durch ein virtuelles IP-Netz verbunden. Zur Erhöhung der Ausfallsicherheit ist auf eine entsprechende Vermaschung mit Mehrwege-Führung zu achten. Bei der Anbindung ausfallkritischer Systeme ist auch eine Zwei-Wege-Anbindung der Liegenschaft notwendig, z.B. durch Metro-Ringe. Die vorgeschlagenen Teilmaßnahmen stellen die bewährte Praxis beim Aufbau ausfallsicherer Unternehmensnetze dar, so dass Anbieter von Telekommunkationsinfrastrukturanbindung diese Maßnahmen standardmäßig umsetzen können.

5.2.3.2 [M_ITS_Anti_DDos] Anti-DDoS-Absicherung der Übergänge ins Internet

Das virtuelle IP-Netz wird nur an einer kleinen Anzahl räumlich getrennter Punkte[32] Übergänge zu externen Netzen via Internet vorsehen. Diese Übergänge sind gegen DDoS-Angriff zu sichern.
Gegebenenfalls kann es sinnvoll sein, einen Teil der Übergänge bevorzugt für Internet-Verkehr mit bekannten Partner-Netzen zu reservieren, z.B. für externe Dienste und insbesondere für die Kommunikation mit anderen europäischen ITS. Durch diese einschränkende Maßnahme lassen sich DDoS-Angriffe leichter bekämpfen und die Ausfallsicherheit der Kommunikation mit wichtigen Partnernetzen erhöhen.

5.2.3.3 [M_ITS_VPN] Kryptografische Absicherung des virtuellen Netzes

Die Verbindungen zwischen statischen Knoten des virtuellen IP-Netzes sind mit Hilfe von VPN-Gateways zusätzlich kryptografisch zu sichern. Hierbei werden bewährte Standardprodukte eingesetzt, die IPSec verwenden.

5.2.3.4 [M_TLS_Sec] SSL/TLS-Absicherung der Datenübertragung zwischen mobilen Knoten und externen Diensten

Für die Kommunikation mobiler Knoten mit ITS-externen Diensten wird eine Ende-zu-Ende-Absicherung der Kommunikation auf Basis von SSL/TLS realisiert.

Auf beiden Seiten werden X.509v3 Zertifikate existieren, so dass eine wechselseitige Authentifizierung möglich ist. Zur Separation der ITS-spezifischen Zertifikate der externen Dienste von den übrigen wird empfohlen, dass die ITS-spezifischen Zertifikate der Dienste ebenfalls von PKI des ITS signiert werden sollten. Hierdurch muss nicht einer großen Zahl externer CAs vertraut werden und überdies stellt es eine weitere Schranke des Zugangs zur Kommunikation mit den Fahrzeugen dar. Wie in Abschnitt 5.1.3.3 erwähnt, ist die Struktur der X.509v3 Zertifikate anders als bei den Zertifikaten für IEEE 1609, so dass leider jeweils zwei Zertifikate verwaltet werden müssen. Für das Basiszertifikat wird allerdings ein X.509v3 Zertifikat verwendet, so dass Interoperabilität gegeben sein sollte.

Die Zertifikate der zentralen Systeme bzw. von externen Diensten sind hierbei langlebig und die Zertifikate der Fahrzeuge „relativ“ kurzlebig, da sie zur Gewährleistung einer hinreichenden Anonymität bzw. Pseudonymität häufig gewechselt werden.
Im Rahmen der anfänglichen Authentisierung beim Aufbau einer SSL/TLS-Verbindungen kann es durchaus wünschenswert sein, auf eine Client-Authentisierung zu verzichten, um die Anonymität zu erhöhen. Insbesondere wenn am Internet-Übergang zwischen ITS (bzw. Mobilfunknetz) und externem Dienst NAT eingesetzt wird, lässt sich hiermit ein hoher Grad an Anonymität[33] gegenüber dem externen Dienst erreichen.

SSL/TLS setzt auf TCP auf und ist daher verbindungsorientiert, so dass beim Wechsel der IP-Adresse die Verbindung zwangsläufig abreißt, daher darf die IP-Adresse nicht zu häufig gewechselt werden.

---

[32] Zur Erhöhung der Ausfallsicherheit sind mindestens zwei Übergangspunkte vorzusehen, andererseits solle die Anzahl aber auch nicht zu groß gewählt werden.

[33] Im Fall des Mobilfunknetzes könnte eine wechselseitige Authentisierung allerdings notwendig werden, nämlich dann, wenn der externe Dienst sicher sein muss, dass er tatsächlich mit einem Fahrzeug kommuniziert.

5.2.3.5 [M_Fernzugriff_SSH] SSH-Absicherung von Fernzugriffen

Falls für die Zentrale(n) eines Wirksystems Fernzugriffsmöglichkeiten vorgesehen werden, z.B. für Wartungsarbeiten, muss der Fernzugang mithilfe von SSH abgesichert werden. SSH ist hierbei so zu konfigurieren, das asymmetrische Krypto-Verfahren für die Authentisierung verwendet werden.

Im Wirksystem empfiehlt es sich, keinen direkten Zugriff auf Systeme zuzulassen, sondern mit einem sogenannten „Jump-Host“ zu arbeiten, auf dem die SSH-Verbindungen terminiert werden und von dem sich weiter zu den internen Systemen verbunden wird. Der Jump-Host kann stärker gehärtet werden und durch den Einsatz von Logging-Shells und Syslog-Verfahren können alle abgesetzten Kommandos revisionssicher auf Logservern gesichert werden.

5.2.3.6 [M_Firewall] Einsatz von Firewalls zur Einschränkungen der Zugriffe auf festgelegte IP-Adressbereiche

In der Vergangenheit sind schon mehrfach Sicherheitslücken bei SSH- oder SSL/TLS-Implementierungen aufgetreten, die sich für entfernte Angriffe ausnutzen ließen, falls der Angreifer in der Lage war eine TCP-Verbindung zum entsprechenden (Server-)System aufbauen zu können. Auch in Zukunft muss damit gerechnet werden, dass wieder neue Schwachstellen in der Software gefunden werden.

Beschränkt man mithilfe einer Firewall die Quell-IP-Adressen, von denen aus Verbindungen aufgebaut werden können, auf festgelegte IP-Adressen (spez. bei SSH-Fernzugriff) bzw. IP-Adressbereiche (bei SSL), lässt sich das Risiko solch eines Angriffs minimieren, da Angreifer nur noch von Adressen aus diesen Bereichen aus angreifen können und nicht vom ganzen Internet aus. Deshalb sind zentrale Systeme mithilfe von Firewalls zu schützen.

5.2.3.7 [M_IPSec_Mobil] IPSec zur Absicherung der IP-basierten Kommunikation zwischen Fahrzeugen und zentralen ITS-Stations

Die zentralen Systeme[34] eines ITS werden in Zukunft mit öffentlichen IPv6-Adressen arbeiten und somit kann im Prinzip eine direkte IPv6-Kommunikation zwischen dem Fahrzeug und zentralen Servern erfolgen. Wir gehen überdies davon aus, dass sich im Fahrzeug ein Netzwerk befinden kann, über das verschiedene IT-Komponenten jeweils über eigene öffentliche IPv6 Adressen mit dem ITS und externen Diensten über einen Zugangsrouter kommunizieren können.

Es wird also hier von einer IPv6-Architektur für das ITS ausgegangen, auch wenn mittelfristig aufgrund der noch verwendeten reinen IPv4-Netze für den Transport IPv4-Tunnel verwendet werden sollten.

Zur Absicherung der Kommunikation innerhalb[35] des ITS wird IPSec vorgeschlagen, da dies maximale Flexibilität und Protokolltransparenz erlaubt. Da die eigentliche Identität an das Fahrzeug gebunden ist, erfolgen alle kryptografischen Operationen in seinem Zugangsrouter, was auch die Wartung und den kostengünstigen Einsatz von Kryptohardware vereinfacht.

---

[34] Für die Fahrzeuge selbst ist aufgrund der potenziell großen Anzahl gleichzeitig kommunizierender Fahrzeuge IPv6 ohnehin vorgesehen.

[35] Für abgesicherte Verbindungen zu externen Diensten im Web wird eher SSL/TLS vorgeschlagen, da dies für den Diensteanbieter einfacher ist. Allerdings kann im Prinzip auch hierfür IPSec verwendet werden.

Solange Transportnetze noch auf Basis von IPv4 arbeiten, muss man allerdings davon ausgehen, dass für IP-Verbindungen über Mobilfunktechnik aufgrund der IPv4-Adressenknappheit NAT eingesetzt wird. Daher muss die bereits in Abschnitt 5.1.3.3 erwähnte Kapselung der IPSec-Datagramme in UDP-Pakete eingesetzt werden, s. RFC 3947 und insbesondere RFC 3948. Diese Kapselung in UDP-Pakete führt lediglich zu einem kleinen Overhead von 8 Byte für den zusätzlichen UDP-Header, der in die IPv4-IPsec-Pakete zwischen äußerem IP-Header und ESP-Header eingeschoben wird.

IPSec wird folgendermaßen für die Absicherung verwendet:

- Es werden temporäre X.509v3-Zertifikate verwendet, bei denen die Schlüssel an eindeutige Identitätsbezeichner (distinguished names) gebunden werden. Diese Bezeichner (und die X.509v3-Zertifkate) werden z.B. auf Basis der ebenfalls variablen MACs und gleichzeitig mit der Erstellung der Pseudonym-Zertifikate für 1609.2 generiert, es empfiehlt sich zur Komplexitätsreduktion möglichst analog vorzugehen. Die Bezeichner müssen allerdings lang genug gewählt werden, um die Wahrscheinlichkeit von Kollisionen[36] hinreichend klein zu halten. *Zudem darf es nicht möglich sein aus den Bezeichnern auf die MAC-Adressen und umgekehrt zu schließen.*
- Die verschiedenen Zertifikate dürfen sich gleichfalls nicht (extern) zuordnen lassen, da sich sonst beim Tunnelaufbau mit zusätzlichen Informationen von einer ITS Roadside Station das Fahrzeug initial orten und anschließend mithilfe der Informationen weiterer ITS Roadside Stations verfolgen ließe. Aus diesem Grund müssen die entsprechenden Zertifikate auch jeweils unterschiedliche öffentliche Schlüssel enthalten, da sich sonst der Schlüssel also Zuordnungsinformation verwenden ließe. Dies führt leider dazu, dass sich der Aufwand für die Schlüsselgenerierung und Zertifikatserstellung bzw. –verwaltung verdoppelt.
- Der für den Aufbau einer sicheren Kommunikation notwendige Schlüsselaustausch verwendet anschließend diese temporären X.509v3-Zertifikate anhand derer das IPSec-Gateway bzw. der IPSec-fähige Router entscheiden kann, ob es sich um einen legitimen Endpunkt handelt, indem er mithilfe des gespeicherten CA-Zertifikats die Echtheit des X.509v3-Pseudonym-Zertifikats prüft.
- Es wird nur ESP (Encapsulated Security Payload) ohne AH (Authentication Header) verwendet, da es ausreicht die Nutzlast zu sichern und NAT-bedingte Änderungen des IP-Headers möglicherweise notwendig werden könnten.
- Wenn auf der Übertragungsstrecke NAT eingesetzt wird, müssen die IPSec-Datagramme in UDP-Pakete gepackt versendet werden, s. Abschnitt 5.1.3.3.
- Wenn das unterliegende Transportnetz nur IPv4 anbietet, muss IPv6 über IPv4 getunnelt werden. Hierbei wird IPSec im Tunnelmodus auf IPv4-Ebene eingesetzt, d.h. wir tunneln ein IPv6 Paket im IPv4-IPSec-Tunnelmodus, wobei die IPv4-IPSec-Pakete bei NAT auf der Strecke noch zusätzlich in UDP verpackt werden müssen. Überdies kann es zu Problemen beim Auspacken der IPv6-Pakete kommen, da nach der IPSec-Schnittstelle das IPv6-Paket weitergeroutet werden muss. Für IPSec und IPv6-fähige Router sollte dies kein Problem sein, für herkömmliche VPN-Konzentratoren könnte dies aber Problem darstellen.

[36] Anders als bei den generierten MACs ist hier die Kollisionswahrscheinlichkeit höher, da die Bezeichner im gesamten ITS (temporär) eindeutig sein sollten.

Verwendete Algorithmen

Falls in der IPSec-Implementierung verfügbar, sollten die in RFC 3686 und RFC 4309 bzw. RFC 4106 und RFC 4543 spezifizierten, gut parallelisierbaren Betriebsmodi Counter-Mode bzw. Galois-Counter-Mode samt passendem Authentifizierungsverfahren verwendet werden.

In RFC 4835 werden die für eine IPSec-Implementierung erforderlichen und wünschenswerten kryptografischen Algorithmen festgelegt. Sind die oben genannten Verfahren nicht verfügbar, sollten die als obligatorisch für IPSec vorgeschriebenen Verfahren AES-CBC mit 128-Bit Schüssel für die Verschlüsselung und HMAC-SHA1-96 zur Authentifizierung verwendet werden.

MTU-Anpassung

Aufgrund der gegebenenfalls notwendigen mehrfachen Kapselung der Nutzdaten in IP-Paketen muss die Maximum Transmission Unit (MTU) auf den „lokalen" Netzen (Fahrzeug bzw. Zentrale) so angepasst (erhöht) werden, dass nicht unnötig häufig IP-Pakete fragmentiert werden müssen.

Skalierungsfragen

Wie bereits in Abschnitt 5.1.3.4 ausgeführt, muss darauf geachtet werden, dass die Anzahl der gleichzeitig gehaltenen Tunnel an zentralen Punkten nicht zu groß wird. Neben dem Einsatz von Lastverteilungsmechanismen an den Tunnelendpunkten an zentralen Systemen, empfiehlt es sich auch, durch dezentrale Strukturen die Last noch weiter zu verteilen.

Lokale IPv6-Präfixe bei Einsatz eines IPv4-Transportnetzes

Wenn das Transport-Netz nur IPv4-fähig ist, aber dennoch eine Kommunikation zwischen Komponenten (AU) im Fahrzeug und zentralen Systemen über IPv6 erfolgen soll, muss jedem Fahrzeug ein IPv6-Präfix zugewiesen werden, da sonst keine IPv6-Kommunikation möglich ist.

Es muss also im Rahmen des ITS ein IPv6-Präfix-Vergabe-Mechanismus vorgesehen werden, der den Fahrzeugen „interne" IPv6-Adressen zuweist. Dies kann im Prinzip mit Radius/ Diameter-Protokoll geschehen, wobei in der IVS CCU dann auch ein entsprechender Client vorhanden sein muss, siehe zu einer ähnlichen Fragestellung auch Abschnitt 5.2.3.8.

5.2.3.8 [M_RND_Pref] Nicht vorhersehbarer IPv6-Präfixwechsel

Wie bereits in Abschnitt 5.1.3.5 erläutert, wird es bei IPv6 nicht notwendigerweise so sein, dass stets andere IP-Adressen (bzw. Subnetz-Präfixe) bei einem Verbindungsaufbau vergeben werden.

Allerdings bieten Mobilfunkanbieter bereits heute die Möglichkeit an, für geschlossene Benutzergruppen, identifiziert durch die SIM-Karten, (VPN-) Übergänge zu einem Firmennetz auch mit einer kundeneigenen IP-Adressvergabe zu realisieren. Es ist daher davon auszugehen, dass es entsprechende Produkte auch bei der Einführung von IPv6 geben wird.

Die Lösung für eine zufällige IPv6-Präfix-Vergabe[37] bei einem ITS ließe sich dann folgendermaßen erreichen:

- Die im Rahmen eines ITS ausgegebenen SIM-Karten der verschiedenen Mobilfunkanbieter bilden jeweils eine geschlossene Nutzergruppe in den Netzen der Anbieter.
- Es wird ein hinreichend großer IPv6-Adressraum für das ITS reserviert, aus dem dann Präfixe via Radius/Diameter vergeben werden können.
- Es wird jeweils eine entsprechende Mobilfunklösung bei den relevanten Mobilfunkanbietern eingekauft und über IPSec-Tunnel werden die Radius/Diameter-Server[38] an die IP-Plattformen der Mobilfunkanbieter angebunden.
- Die IP-Adress/Präfix-Vergabe erfolgt dann jeweils bei der Neueinwahl über die eigenen Radius/Diameter-Server, so dass eine Vergabe stets unterschiedlicher Präfixe sichergestellt werden kann.

Eigentlich muss nur der Verkehr von und zu dem Radius-Server über den dedizierten Weg geleitet werden, der restliche Verkehr könnte, wenn öffentlichen Adressen verwendet werden, auch über andere Wege übertragen werden.

Die Radius/Diameter-Server sollten, ähnlich wie die PKI, getrennt von den übrigen IT- und Organisations-Strukturen des ITS sein, bevorzugt auch unter Kontrolle eines externen Datenschutzbeauftragten.

Feste lokale IP-Adressen trotz IPv6-Präfixwechsel

IPv6 wurde unter anderem auch deswegen entwickelt, damit jeder Rechner wieder mit einer eigenen, global eindeutigen Adresse im Internet sein kann. Insbesondere entfällt die Notwendigkeit NAT einzusetzen, das ursprünglich primär als Übergangslösung für die Knappheit der IPv4-Adressen vorgesehen war.

Die global eindeutigen IPv6 Adressen bringen allerdings in unserem Szenario mit Präfix-Wechsel folgendes Problem mit sich:

Beim Wechsel des IPv6-Präfixes eines Fahrzeug (-netzes) werden nicht nur die Verbindungen nach außen unterbrochen[39], sondern auch alle IP-Verbindungen im Fahrzeug, da jeder LAN-Knoten eine IP-Adresse in dem Subnetz besitzt, das durch das IPv6-Präfix vorgegeben ist.

Ohne Präfix-Wechsel würde dieses Problem natürlich nicht auftauchen, da sich dann die IPv6-Adressen des Fahrzeug-LAN auch nicht ändern würden.

Will man einen Präfix-Wechsel ohne Unterbrechung der fahrzeuginternen IP-Verbindungen, muss man leider wieder zwischen global sichtbaren und (festen) internen Adressen trennen.

In den Standards zu IPv6 ist dies eigentlich nicht vorgesehen, bedeutet es doch letztendlich, dass wieder NAT eingesetzt wird. Anders als beim üblicherweise eingesetzten NAT ist es allerdings nur eines auf Basis von IP-Adressen, d.h. Ports müssen nicht verändert werden.

---

[37] Sollte die IPv4-Adressvergabe bei der Mobilfunk-Einwahl ebenfalls nicht die IP-Adresse hinreichend wechseln, könnten auch für IPv4 ähnlich vorgegangen werden, dies könnte möglicherweise als Test der Funktionalität interessant sein.

[38] Zur Erhöhung der Verfügbarkeit muss es sich um mindestens zwei räumlich getrennte Server handeln. Jeder der Server wird an jede der Mobilfunkplattformen angebunden.

[39] Das ist bei einem Wechsel grundsätzlich nicht zu vermeiden.

Hierbei würde der Router zusätzlich noch als NAT-Gerät fungieren, das die internen IPv6-Adressen auf externe IPv6-Adressen im Subnetz des aktuellen Präfixes umsetzt. Im Prinzip könnte man eine sehr einfache, 1-zu-1 Umsetzung verwenden, die das interne Präfix wegschneidet und durch das externe Präfix ersetzt.

Auch wenn hier lediglich NAT auf Basis der IP-Adressen verwendet wird, so kann dies natürlich trotzdem zu den allgemein bekannten Problem des NAT führen: Protokolle, die auf höheren Protokoll-Ebenen die IP-Adresse als Information an die Gegenstelle der Kommunikation übertragen, werden hier natürlich die nicht global routbare, interne IP-Adresse übermitteln. Beispielsweise überträgt das im Rahmen von VoIP verwendete SDP (Session Description Protocol) die IP-Adresse auf höherer Ebene.

Solche für NAT typischen Probleme lassen sich (leider) nur mit Hilfe von Proxy-Mechanismen beheben. Glücklicherweise sind viele wichtige Protokolle (z.B. HTTP) von diesem Problem nicht betroffen.

5.2.4 ITS G5A

Wie in diesem Deliverable beschrieben, wird die C2X Kommunikationsabsicherung per IEEE 802.11p auf Vermittlungsschicht (OSI-Layer 3) durchgeführt. Dieses Vorgehen hat mehrere Gründe und bietet verschiedene Vorteile.

- Mobilitätsdaten wie zum Beispiel Position, Fahrtrichtung und Geschwindigkeit werden auf Vermittlungsschicht im Netzwerkprotokoll integriert und übertragen. Da diese Daten ein wesentlicher Bestandteil der C2X Kommunikation darstellen, muss die Integrität diese Informationen durch die Kommunikationsabsicherung gewährleistet werden.
- Jede auszusendende und empfangene Nachricht muss durch die Kommunikationsabsicherung signiert bzw. verifiziert werden. Auf Wunsch kann auch die Nachricht bei einer Unicast-Kommunikation verschlüsselt werden. Der Großteil der Kommunikation im ITS findet jedoch per Broadcast statt, was eine Verschlüsslung, unmöglich macht, da es beabsichtigt ist, dass alle Nachbarknoten diese Informationen lesen können.
- Für die Anwendungen auf OSI-Layer 7 sind die Absicherungsmechanismen in der C2X Kommunikation über IEEE 802.11p transparent, da sie auf Vermittlungsschicht statt findet. Zusätzlich zur Signierung kann die Anwendung bei der Unicast Kommunikation den Wunsch nach Verschlüsselung äußern. In diesem Fall wird die Information von der Anwendung bis zur Kommunikationsabsicherung heruntergereicht. Die Ergebnisse der Verifikationsprüfung wird im Gegenzug von der Kommunikationsabsicherung zu den Anwendungen hochgereicht.
- Neben den Informationen der Anwendungen müssen auch die Mobilitätsdaten und die Informationen zum Routing auf Vermittlungsebene geschützt werden. Ein Angreifer könnte versuchen die *Hop-Count* Informationen verfälschen und dadurch einen DoS Angriff provozieren. Bei der Weiterleitung von C2X Nachrichten über mehrere Hops ist es daher notwendig, dass die veränderbaren Elemente im Netzwerkpaket von jedem Zwischenknoten in der Weiterleitungskette signiert und beim nächsten Knoten verifiziert werden. Bei einer Platzierung der Kommunikationsabsicherung auf Vermittlungsschicht muss die Nachricht nicht auf höhere Schichten hochgereicht werden, um die Hop-zu-Hop Absicherung der Routinginformationen zugewährleisten.

5.2.5 WLAN IEEE 802.11 b/g

Innerhalb eines Wirksystems kann C-WLAN auf verschiedene Weise angewendet werden. Neben der eigentlichen C2C- und C2I-Kommunikation besteht eine sicherlich denkbare Möglichkeit darin, dass öffentliche oder private Access Points für anwendungsspezifische Datenübertragungen genutzt werden. Ein denkbarer Fall ist sicherlich, dass Daten über das eigene private WLAN in das Fahrzeug übertragen werden. Diese Übertragungen müssen natürlich ebenfalls abgesichert werden. Weiterhin besteht die Möglichkeit öffentliche Access Points für z.B. 3rd Party Dienste zu nutzen.

Hierfür sind ebenfalls Sicherungsmaßnahmen zu ergreifen. Neben der Absicherung von C2C und C2I-Kommunikation analog zur Absicherung über IEEE 802.11p können für die genannten Spezialfälle Maßnahmen über 802.11i ergriffen werden.

5.2.6 ITS IMT Public

Neben den in 0 dargestellten Standardmechanismen des Mobilfunks werden für die Absicherung der IP-Kommunikation über Mobilfunknetze noch zusätzliche ITS-eigene Maßnahmen eingesetzt, um eine durchgängige Ende-zu-Ende-Sicherheit gewährleisten zu können.

5.2.6.1 [M_Cell_Sec] Ende-zu-Ende-Absicherung der IP-Kommunikation via Mobilfunk

Jegliche Art der Kommunikation über das Mobilfunknetz muss über eine entsprechende kryptografische Absicherung erfolgen, die jedoch auf Layer 3 (IP-Ebene) oder höher angesiedelt wird. Dieses Vorgehen hat folgende Vorteile:

- Die Absicherung geschieht unabhängig von der unterhalb von Layer 3 verwendeten Übertragungstechnik und kann sich somit auch über Layer-2-Schnittstellen zwischen verschiedener Übertragungstechnik erstrecken.
- Ein Wechsel des Mobilfunknetzes bzw. –übertragungsverfahrens ist (aus Sicherheitssicht) unproblematisch[40], solange IP-Pakete übertragen werden können. Dies ist auch aus regulatorischer und politischer Sicht wichtig, da spezifische Lösungen eines Mobilfunkanbieters nicht von den zuständigen Behörden befürwortet würden.

Für eine Darstellung der verschiedenen Möglichkeiten der Ende-zu-Ende-Absicherung wird auf Abschnitt 5.1.3 verwiesen, die bevorzugte Lösung für ein ITS wird in Abschnitt 5.2.3 dargelegt und für sim^{TD} spezifische Details in Abschnitt 5.3.

5.2.6.2 [M_Cell_IP_Change] Zufälliger Wechsel der IP-Adressen

Zu Wahrung der Pseudonymität muss sichergestellt sein, dass keine Informationen, die statisch oder leicht vorhersagbar sind, an eine zentrale Instanz oder gar Dritte gelangen und so zu einer Identifizierung des Nutzers dienen können.

---

[40] Beim Wechsel der dynamischen IP-Adresse, wenn z.B. das verwendete Netz gewechselt wird, erfolgt allerdings zwangsläufig ein Abbruch der abgesicherten Verbindung. Bei TCP-basierter Kommunikation passiert dies allerdings ohnehin.

Man muss sich allerdings darüber im Klaren sein, dass innerhalb des Mobilfunknetzes grundsätzlich jedes Fahrzeug leicht verfolgbar wäre, so wie dies heute bereits für Handy-Nutzer gilt.

Anders als beim Handy, dessen Nutzung im Prinzip freiwillig ist, wird bei einem ITS mittelfristig davon auszugehen sein, dass die notwendigen Komponenten standardmäßig in Neuwagen integriert werden und langfristig ihre Aktivierung gesetzlich vorgeschrieben werden könnte. Daher ist hier die Frage der Pseudonymität besonders kritisch.

Die vorgeschlagenen Maßnahme ändert auch nichts an der oben beschriebenen mobilfunkinternen Problematik, sondern bezieht sich nur darauf, wie sich verhindern lässt, dass ein Nutzer auch von außerhalb des Netzes (indirekt) identifiziert werden kann. Würde die IP-Adresse, die auch außerhalb des Mobilfunknetzes sichtbar ist, nicht gewechselt, könnte man nämlich möglicherweise eine *indirekte* Nachverfolgung der Route eines Fahrzeugs anhand der IP-Adresse durchführen.

Aus diesem Grund muss die IP-Adresse hinreichend häufig gewechselt werden, wobei sich die neue IP-Adresse nicht anhand der alten IP-Adresse vorhersagen lassen sollte.

Bei einer neuen Einwahl in Mobilfunk-Netze wird i. Allg. eine neue (private) IP-Adresse vergeben, so dass sich durch einen Verbindungsabbau und eine erneute Einwahl die IP-Adresse im Prinzip wechseln lassen sollte, sofern tatsächlich jeweils eine neue IP-Adresse vergeben wird. Da die genauen Vergaberichtlinien von IP-Adressen im Mobilfunknetz kein Teil der Standardisierung sind, kann allerdings jeder Mobilfunk-Betreiber anders vorgehen, daher kann man sich man sich nicht darauf verlassen, dass sich die IP-Adresse bei Neueinwahl auch tatsächlich ändert; zu dieser grundsätzlichen Problematik siehe auch Abschnitt 5.1.3.5.

Wird am Gateway des Mobilfunknetzes zum Internet NAT verwendet, wie aktuell aufgrund der IPv4-Adressknappheit der Fall, erschwert dies die indirekte Nachverfolgung noch weiter, da nun alle Verbindungen von einem kleinen Pool von IP-Adressen kommen werden.

Bei länger bestehenden Verbindungen wird man allerdings auch hier noch eine indirekte Zuordnung erreichen, da die Absende-Ports sich nicht ändern. Bei dem oben erwähnten IP-Wechsel durch eine neue Einwahl wäre im Zusammenspiel mit NAT die kontinuierliche Zuordnung zu anderen Informationen bereits merklich erschwert.

Ein ähnlicher Effekt würde sich durch die Verwendung von Mobile IP ergeben, vorausgesetzt die statischen primären IP-Adressen der Fahrzeuge wären nur einem *Home Agent* innerhalb des Mobilfunknetzes bekannt, der die Fahrzeuge nach außen hin durch wechselnde *Care-Of-Adressen* repräsentieren würde. In diesem Fall wäre eine Identifizierung von Fahrzeugen und Verknüpfung von Pseudonymen anhand der IP-Adressen nur innerhalb des Mobilfunknetzes möglich, so dass lediglich der Zugang zum Mobilfunk-IP-Netz kontrolliert werden müsste.

Für weitergehende Fragen, auch im Zusammenhang mit IPv6, sei auf Abschnitte 5.1.3.5 ff. und 5.2.3.7 ff verwiesen.

5.2.6.3 C2X via Mobilfunk

Zur Absicherung der Übertragung von C2X-Nachrichten via Mobilfunk müssen die gleichen Absicherungsmaßnahmen in Anspruch genommen werden, wie sie auch in der Ad-hoc-Kommunikation Anwendung finden. Für das Fahrzeugsystem muss der Übertragungsweg völlig transparent sein. Daher darf es für die Kommunikationsabsicherung auch keine Unterscheide zwischen einer Multihop-Übertragung per IEEE 802.11p und C2X via Mobilfunk geben.

5.2.7 Ausfallsicherheit

Für die Gesamtarchitektur sollten die folgende Systemstruktur bei der Implementierung diese Vorteile bieten:

- Höchstmögliche Skalierbarkeit
- Höchstmögliche Verfügbarkeit
- Vermeidung von Single-Point-of-Failures

Bei den im Folgenden aufgeführten Verfahren handelt es sich um Standardmaßnahmen, die in allen typischen Rechenzentren und den darin enthaltenen Serversystemen üblich sind.

5.2.7.1 [M_ITS_AS_AL] Application Layer

Für Komponenten sollte eine Anwendung implementiert werden, die zur Überwachung der anderen Komponenten dient. Unter dem Begriff 'Überwachung' versteht man folgende Aufgaben:

- das Sicherstellen der Funktionsfähigkeit der Module,
- bei Bedarf ein Neustart der Module,
- Überwachung der Komponenten und
- in bestimmten Situation (Fehlfunktion, kritische Zustände, etc.) Auslösen von Eskalationsmechanismen.

5.2.7.2 [M_ITS_AS_CL] Einsatz von Load-Balancern

Durch den Einsatz von Load-Balancern kann ein Optimum an Ausfallsicherheit, Betriebskosten und einfacher Skalierbarkeit erreicht werden. Die Architektur im Backend auf Basis eines erweiterbaren Serverclusters hat den Vorteil, dass bei einem Komponentenausfall nicht das komplette System zum Erliegen kommt.

5.2.7.3 [M_ITS_AS_OS] Auswahl des Betriebssystems

Die Entscheidung des Betriebssystems muss nach verschiedenen Kriterien – abhängig von den eigenen Anforderungen – getroffen werden. Dabei können die folgenden Aspekte maßgeblich zur Entscheidung beitragen:

- Support (Qualität, Aktualität, Zuverlässigkeit)
- Betriebs- und Wartungskosten (Total Cost of Ownership: Gesamtbetriebskosten)
- Zuverlässigkeit (bezogen auf die Verfügbarkeit)

Verfügbarkeit von Anwendung (z.B. Datenbank Software)

5.2.7.4 [M_ITS_AS_MS] Backup Server

Bei der Planung und Bereitstellung der Systemarchitektur wird ein einfacher und effektiver Mechanismus zur langfristigen Sicherung von Daten benutzt. Dabei einzusetzende Technik wird mit vollen und inkrementellen Backups arbeiten. Dabei wird in einem festgelegten Rhythmus ein volles Backup durchgeführt und in dem dazwischen liegenden Zeitraum nur die Differenz gesichert. Dabei sind zwei unterschiedliche Techniken möglich: zum einen kann immer die Differenz zum letzten vollen Backup und zum anderen die Differenz zum letzten inkrementellen Backup gespeichert werden.

Das Backup sollte sowohl lokal als auch eine physikalisch anderen Ort gespeichert werden, um bei einer Beschädigung eines Backups (Z.B: durch Brand oder Diebstahl) eine zweites Backup zu besitzen.
Darüber hinaus sollte das Backup auf dem jeweiligen Backupmedium (Hard Disk, Magnetic Tape, ...) nur verschlüsselt abgelegt werden, damit die Daten im Falle eines Diebstahl nicht missbraucht werden können sind.

5.2.7.5 [M_ITS_AS_USV] Unterbrechungsfreie Stromversorgung (USV)

Zum Erreichen eines hohen Grades an Verfügbarkeit wird für die aktiven Netzwerkkomponenten und die zentralen Server eine unterbrechungsfreie Stromversorgung installiert. Anhand der Nutzleistung aller installierten Server wird eine oder mehrere USV benötigt.

5.2.8 Organisatorische und rechtliche Maßnahmen

Aus den Inhalten des Abschnitts 1.5 „Rechtlich regulatorische Rahmenbedingungen“ ergeben sich für das spätere Wirksystem eine Reihe notwendiger Maßnahmen. Vor Abschluss der „Studie zu rechtlich regulatorischen Rahmenbedingungen“ (Deliverable D5.2) kann dazu noch keine abschließende Aussage getroffen werden, die folgenden Anforderungen scheinen aber wahrscheinlich:

- Die Zustimmung zur aktiven, also sendenden Teilnahme am System darf unter keinen Umständen Voraussetzung zum Führen eines Fahrzeugs sein.
- Die Zustimmung muss personenbezogen erfolgen und im Fahrzeug protokolliert werden.
- Kann eine personenbezogene Zustimmung nicht eindeutig eingeholt werden, muss der Fahrzeughalter dafür verantwortlich gemacht werden, die Zustimmung zur Teilnahme am System von anderen Nutzern einzuholen (Analogie „Einzelverbindungsnachweis beim Telefon“).
- Die aktive Teilnahme am System muss für den Nutzer eines Fahrzeugs jederzeit ersichtlich sein.
- Der Nutzer muss in der Lage sein, das System für das von ihm geführte Fahrzeug jederzeit zu deaktivieren.
- Zur Verhinderung passiver Nutznießer, also reine Empfänger, sollte das System so ausgelegt sein, dass es nur nutzbar ist, sollte sich der Fahrzeugführer für die aktive Teilnahme entscheiden.
- Aufgrund der Zustimmung der Betroffenen erscheint eine Vorabkontrolle nicht nötig.
- Das Verständnis der Komplexität eines ITS ist dem Betroffenen nicht zuzumuten. Daher ist die Einrichtung einer zentralen Stelle zur Klärung datenschutzrelevanter Fragen nötig.
- Die Übermittlung von Daten an eine öffentliche Stelle ist zulässig, wenn es für die Aufgabenerfüllung dieser Stelle notwendig ist (z.B. Übermittlung von Klarnamen an die Exekutive zur Aufklärung von Straftaten).
- Die Übermittlung von Daten ein eine nicht-öffentliche Stelle ist hingegen nicht zulässig. Das begründete Interesse einer nicht-öffentlichen Stelle ist über die Einschaltung einer öffentlichen Stelle nachzuweisen.
- Der Datenaustausch mit außer-europäischen Stellen ist gesondert zu regeln.

5.2.9 Wartung, Verwaltung und Aktualisierung der ITS Stations

Bei der Betrachtung der Komponenten wird zwischen zwei großen Blöcken unterschieden: den Fahrzeugen und der Infrastruktur. Diese Aufteilung wurde gewählt, da für diese beiden Teile sehr unterschiedliche Rahmenbedingungen vorherrschen. Die Komponenten der Infrastruktur stehen in ständigen Kontakt zu einer kontrollierenden Zentrale. So kann ein Fehlerfall schnell erkannt und eine Anwendung schnell installiert bzw. aktualisiert werden. Die Fahrzeuge verfügen in breiter Masse noch nicht über eine solche Kontrollinstanz: Ausnahmen sind bestimmte Luxusklassen von Herstellern, die sich über UMTS mit Service Center verbinden können. Es ist aber vorstellbar, dass man eine breitere Anwendung von Kontrollinstanzen mit der Einführung von Car2X Anwendungen erlebt. Dementsprechend wird in diesem Abschnitt davon ausgegangen, dass auch für IVS remote Wartung und Aktualisierung möglich ist.

Da alle hier genanten Komponenten zwar in einem Wirksystem vorhanden sein werden, aber deren genauer Aufbau und die genaue Arbeitsweise und Systemspezifikationen nicht bekannt sind, können in diesem Abschnitt nur sehr allgemeine Sachverhalte dargestellt werden.

Zur Absicherung sollten die Maßnahmen [M_WVA_SW_CERT], [M_WVA_SW_SU] und M_WVA_IS_LOGIN aus Abschnitt 5.1.8 Anwendung finden.

5.2.9.1 Komponenten IVS

Die Komponenten der IVS werden sowohl kabelgebunden als auch über Remotetechnologien verwaltet werden. Für die jeweilige Art von Kommunikation erfolgt die Wartung und Aktualisierung durch dedizierte Werkstätten. Dabei werden üblicherweise die Hardwarefehlerspeicher ausgelesen und abhängig der daraus gewonnenen Informationen Aktualisierungen durchgeführt.

Um die Maßnahmen [M_WVA_SW_CERT] und [M_WVA_SW_SU] erfolgreich umsetzen zu können, ist hier ein Authentisierungs- / Autorisierungskonzept für die verschiedenen Hersteller/Zulieferer/Behörden nötig. Weil aber die Punkte „Wartung, Aktualisierung“ unternehmensspezifisch sind, werden wir zwar die IT-Sicherheitspunkte erwähnen aber keine konkrete Lösung vorgeben.

Dabei sind folgende Punkte zu betrachten:

- Es muss für die IVS-Komponenten möglich sein, die Identität der Wartungs- und Aktualisierungskomponenten zu überprüfen. Ebenso muss es für die Werkstatt möglich sein, die IVS-Komponenten auf Authentizität zu prüfen, um beispielweise mögliche Garantieverletzungen, wie z.B. Komponentenmanipulationen entdecken zu können. Das dafür notwendige Zugriffskontrollmodell basiert auf den Authentisierungsprotokollen. Verschiedene Zugriffskontrollmodelle sind u.a. in „IT-Sicherheit“ von Prof. Eckert [2] aufgeführt.
- Mechanismen zur Signaturerzeugung und -verifikation und im Fall einer Softwareaktualisierung auch zur Verschlüsselung/Entschlüsselung werden benötigt. Dies erfordert wiederum ein Konzept zur Verwaltung der Zertifikate und der dazugehörigen kryptografischen Schlüssel, das vollständig und nahtlos in die „Werkstatt-Infrastruktur“ integriert sein muss. Wir empfehlen eigenständige Zertifikate zu verwenden, die nur für diesen Zweck eingesetzt werden dürfen.
- Die eingesetzten kryptografischen Algorithmen sollten dem Stand der Technik entsprechen. Empfehlungen diesbezüglich werden jährlich durch das Bundesamt für Sicherheit in der Informationstechnik BSI [13] sowie internationalen Organisationen wie dem NIST [14] herausgegeben.

5.2.9.2 Komponenten IRS und ICS

Die Wartung der Komponenten der ICS können über die standardisierten Prozeduren durchgeführt werden, die auch in „normalen“ Rechenzentren Anwendung finden.

In Fall der IRS kann über die Verbindung zu einer Verwaltungszentrale jederzeit der Zustand der IRS ermittelt werden und somit entsprechende Maßnahmen initiiert werden. Zur Aktualisierung von Software können unterschiedliche Verfahren für unterschiedliche Software eingesetzt werden. Es ist dabei aber darauf zu achten, dass für die Wartung und Aktualisierung genutzten Ressourcen in dieser Zeit nicht für andere Anwendung zur Verfügung stehen.

5.2.10 Hierarchisch strukturierte ITS Central Stations

Die ICS wird, wie schon unter 1.1 beschrieben, durch eine Reihe von Systemen und Kommunikationsschnittstellen repräsentiert. Die Systeme werden dabei von verschiedenen anderen Unterkapiteln von Abschnitt 5.2 abgedeckt, so dass in diesem Abschnitt nur noch die Kommunikationsschnittstellen und nicht vorher behandelte Komponenten beschrieben werden. Die ITS Central Station ist durch eine Firewall [M_Firewall] gegen Gefahren von außen zu schützen. Für alle folgenden Komponenten gelten die Anforderungen an einen authentifizierten und autorisierten Zugriff und an eine Härtung des entsprechenden Betriebssystems. Als zentrale Forderung gilt die Erreichbarkeit aller Komponenten und Schnittstellen; hierbei sind die Maßnahmen aus den Abschnitten 5.2.3.2 und 5.1.7 durchzuführen.

5.2.10.1 Komponenten

Die zu schützenden Komponenten ergeben sich sinngemäß aus den in Abschnitt 4.1.2.2 aufgeführten Sicherheitsanforderungen.

- IRS Management System
  - Das IRS Management System (IRSMC) sollte durch eine Firewall getrennt vom übrigen System aufgebaut werden. Unter Umständen ist das IRS Management System sogar als eigene ICS zu deklarieren, für die dann die gleichen Sicherheitsmaßnahmen greifen wie für eine „normale“ ICS-ICS Kommunikation.
- Software-Systeme der ICS, z.B. für Anwendungen
  - Die Software muss gegen Zugriff von Dritten durch geeignete Maßnahmen (z.B. autorisierten Zugriff) geschützt werden. Dabei ist auch auf Sachverhalte wie z.B. geistiges Eigentum zu achten.
- Datenbank zur Speicherung der verschiedenen Anwendungsdaten.
  - Die Datenbank muss sicherstellen, dass die abgespeicherten Daten gegen jedwede unbefugte Änderung abgesichert werden. Dafür sind folgende Maßnahmen zu treffen:
    - **[M_ICS_DB_R]** Der Zugriff auf die Datenbank muss durch ein rollenbasiertes Nutzerkonzept abgesichert werden. Dabei erhält ein Nutzer immer nur so viel Rechte, wie er zur Bearbeitung seiner Aufgabe unbedingt benötigt.
    - **[M_ICS_DB_RO]** Daten, die nach der Speicherung nicht mehr geändert werden dürfen, sollten in einer read-only Tabelle bzw. Datenbank gespeichert werden.

- PKI-Server
  - Der PKI-Server wird in einem Wirksystem nicht am gleichen Ort wie eine ICS vorhanden sein. Sie sollte besonders geschützt werden und sich auf einer anderen Liegenschaft befinden. Darüber hinaus sind die Maßnahmen wie unter Abschnitt 5.1.2 beschrieben strikt anzuwenden.
- DNS-Server
  - Für Zertifikate, die auf Domänennamen basieren, muss sichergestellt sein, dass entsprechende DNS-Server erreichbar sind.

5.2.10.2 Schnittstellen

Im Folgenden werden die Schnittstellen beschrieben, die im Zusammenhang mit der ITS Central Station vorhanden sind:

- ITS Central Station und ITS Central Station
  - Die Kommunikation zwischen ITS Central Stations muss über geeignete Protokolle (z.B. DATEX2[41]) realisiert werden. Die Absicherung der Verbindung sollte dabei über Virtuelle Netze [M_ITS_VN] bzw. VPN [M_ITS_VPN] erfolgen.
- ITS Central Station und Internet
  - Hier sind verschiedene Techniken denkbar: VPN, SSH, TLS (siehe Abschnitt 5.2.3)
- ITS Central Station und ITS Roadside Stations
  - Welche Art der unter Abschnitt 5.2.3 beschriebenen Absicherungen die passende für die Kommunikation zwischen einer IRS und ICS ist, hängt stark von der Beurteilung und den Anforderungen an die Kommunikation innerhalb einer ITS Station ab. Generell muss eine Ende-zu-Ende-Absicherung als notwendig erachtet werden.
  - Die Priorisierung der Daten kann auf zwei Ebenen durchgeführt:
    - Die Managementdaten werden gegenüber den Anwendungsdaten auf IP-Ebene bevorzugt behandelt, da sie für den sicheren und zuverlässigen Betrieb und die Nachvollziehbarkeit von IRS Aktionen wichtig sind.
    - Innerhalb der Anwendungsdaten wird ebenfalls priorisiert, da es unterschiedliche zeitliche und sicherheitsrelevante Anforderungen an die Anwendungen gibt.
- ITS Central Station und PKI
  - Die Schnittstelle zwischen der ICS und der PKI, die in einem Wirksystem räumlich getrennt voneinander untergebracht sein werden, muss über eine gesicherten Verbindung (siehe Abschnitt 5.2.3) realisiert werden. Gleichzeitig müssen eine Authentifizierung und eine Autorisierung gewährleistet werden. Entsprechende Techniken sind in den Abschnitten 5.1.2 und 5.2.2 beschrieben.

[41] Mehr Information unter: http://www.datex2.eu/

Aufgrund der noch andauernden Konzeptionsphase der Schnittstellen

- ITS Central Station - ITS Vehicle Station,
- ITS Central Station - 3rd Party Services

können keine Aussagen über Sicherheitsmechanismen für ein späteres Wirksystem getroffen werden.

5.3 IT-Sicherheitsarchitektur für sim^{TD}

In diesem Abschnitt werden die IT-Sicherheitsmechanismen und Komponenten beschrieben, die für die Kommunikationsabsicherung des sim^{TD} Feldtests notwendig sind. Im Gegensatz zu einer IT-Sicherheitsarchitektur eines Wirksystems wie in Abschnitt 5.2 beschrieben, können in einer Feldtestabsicherung nicht alle Anforderungen vollständig erfüllt werden und es müssen Fall-Back-Maßnahmen definiert werden. Auf der einen Seite soll die sim^{TD} Absicherung so weit wie möglich an einer späteren Wirksystemumsetzung orientiert werden. Auf der anderen Seite müssen jedoch spezielle Komponenten und Protokolle berücksichtigt werden, die es in einem Wirksystem nicht mehr geben wird. Darüber hinaus muss die begrenzte Ausstattung der Systeme in sim^{TD} beachtet werden. Da die meisten Bestandteile des sim^{TD} Feldtests neu entwickelt werden beziehungsweise noch nie zusammen in einem System integriert wurden, kann für das genaue Systemverhalten in der Konzeptphase nur eine begrenzte Aussage getroffen werden. Es muss also in dieser Architektur dafür gesorgt werden, dass auch die Kommunikation durch IT-Sicherheitsmaßnahmen geschützt ist, auch wenn nur wenig CPU-Ressourcen oder wenig Netzwerkbandbreite zur Verfügung steht.

Eine Übersicht über das IT-Sicherheitskonzept bietet Abbildung 5.6. Alle dargestellten Bestandteile in der sim^{TD} spezifischen Umsetzung mit roter Schrift, rotem Hintergrund oder roten Umrandungen werden durch das IT-Sicherheitskonzept abgesichert. Grüne Beschriftungen weisen darauf hin, dass eine Absicherung durch sim^{TD} nicht notwendig ist, da externe Regulatorien alle Sicherheitsbelange regeln.

Alle Funktionen, die *Ad-hoc ITS Kommunikation* über IEEE 802.11p nutzen, werden durch einen speziell für diese Kommunikationsart entworfenen Sicherheitsdienst abgesichert. In der sim^{TD} Umsetzung wird der Sicherheitsdienst vom *Security-Daemon* (siehe Abschnitt 5.3.4) implementiert, welcher bereits in anderen Projekten eingesetzt wurde. Die Kommunikation findet zwischen ITS Vehicle Stations (C2C), ITS Vehicle Stations und ITS Roadside Stations (C2I) statt. Beim normalen Austausch von Nachrichten im Kontext von C2X werden alle Informationen über eigene Protokolle (C2X Paket) ausgetauscht. Da auf Vermittlungsebene zusätzlich zu den C2X-Nachrichten Mobilitätsdaten übertragen werden, muss auch die Absicherung auf dieser Ebene stattfinden. IEEE 1609.2 stellt einen existierenden Standard zur Absicherung der *Ad-hoc ITS Kommunikation* über IEEE 802.11p dar. Der Security Daemon nutzt diesen Standard jedoch nur in einer angepassten Variante, da in sim^{TD} Daten auf der Vermittlungsschicht abgesichert werden und nicht wie im IEEE 1609.2 Standard festgelegt auf Anwendungsschicht. Daten, die auf Vermittlungsschicht geschützt werden, sind in Abbildung 5.6 mit der Bezeichnung *Security Daemon* gekennzeichnet. Die Kommunikationskomponente auf Vermittlungsschicht trägt in sim^{TD} den Namen SIM-NET und ist verantwortlich für den Aufruf des Security Daemons. SIM-NET ist zuständig für die Kommunikation per IEEE 802.11p, IEEE 802.11b/g sowie für die ITS IMT Public Kommunikation auf Layer 3 des OSI Modells. Des Weiteren werden durch SIM-NET die CAM Nachrichten erzeugt und die Mobilitätsdaten in jede Nachricht integriert.

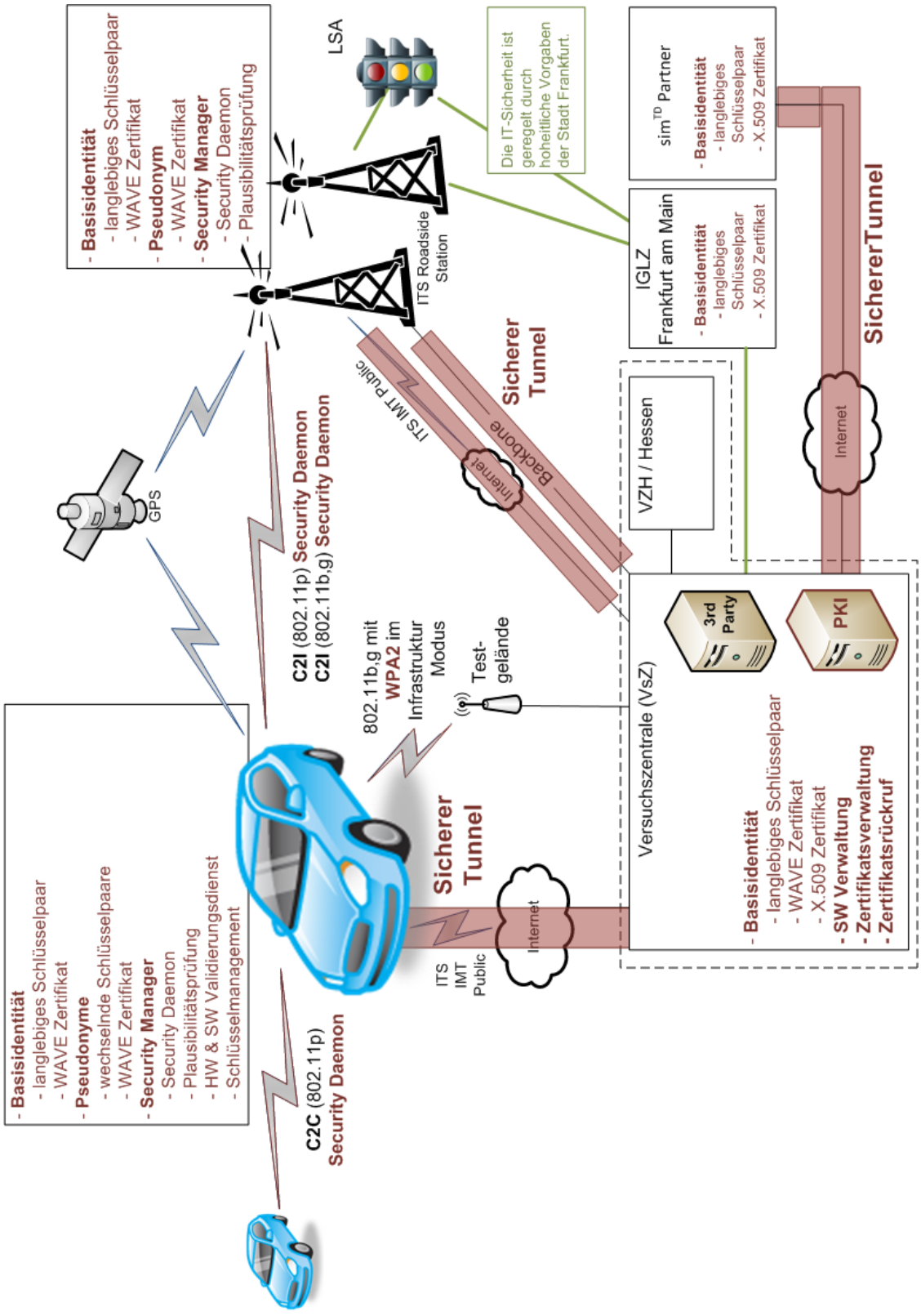

Abbildung 5.6: IT-Sicherheitsarchitektur in sim^TD

Neben der drahtlosen Kommunikation per IEEE 802.11p, über die nur ausschließlich verkehrssicherheitsrelevante Nachrichten ausgetauscht werden, wird eine drahtlose Kommunikation über das kommerzielle WLAN (IEEE 802.11b und IEEE 802.11g) eingesetzt, also für Daten die nicht primär die Verkehrssicherheit oder Optimierung betreffen. Für den Einsatz von kommerziellem WLAN (C-WLAN) sind zwei Einsatzszenarien zu unterscheiden:

1. Anwendungsspezifische Datenübertragung per UDP/IP zwischen ITS Roadside Station und Fahrzeug (C2I). In diesem Fall wird eine Ad-Hoc Verbindung zwischen der ITS Roadside Station und den ITS Vehicle Stations aufgebaut.
2. Für die Übertragung großer Datenmengen ist eine Kommunikationsverbindung zu einer WLAN-Basisstation auf dem Testgelände oder anderen sim^{TD}-internen Standorten vorgesehen.

Die Absicherung dieser C-WLAN Kommunikation ist in Abschnitt 5.3.5 beschrieben.

Alle Verbindungen über öffentliche Netze und dem Internet müssen mit entsprechenden Sicherheitsdiensten gesichert werden (siehe Abschnitt 5.1.3). Weiterhin werden aber auch die Verbindungen der ITS Roadside und Vehicle Stations zu den Zentralen mit Hilfe von Tunneln abgesichert. Dieses betrifft die drahtlose Verbindung per UMTS von den Fahrzeugen und den ITS Roadside Stations, zu den 3rd Parties und der Versuchszentrale. In Abbildung 5.6 sind all diese Verbindungen mit der Beschriftung „Sicherer Tunnel“ gekennzeichnet. Die Kommunikationsabsicherung durch die Tunnel wird in Abschnitt 5.1.3 bzw. 5.2.3 und 5.3.3 näher beschrieben.

Zu den nicht abgesicherten Verbindungen gehört der Empfang von GPS-Signalen auf Fahrzeugen und ITS Roadside Stations. Schließlich ist auch die Verbindung zwischen den ITS Roadside Stations und den LSAs eingezeichnet, welche über einen internen drahtgebundenen Anschluss realisiert wird und somit keiner besonderen Absicherung bedarf.

Eine Übersicht aller Kommunikationskanäle in sim^{TD} bietet die Tabelle 5.5. Über das Kommunikationssystem werden die unterschiedlichsten C2C, C2I und I2C-Nachrichten versendet. Je nach Art der übertragenen Daten und des Übertragungstyps (Unicast, Multicast, Broadcast) müssen andere Schutzmaßnahmen angewendet werden.

Kommunikationskanäle	Kommunikations-technologie	IT-Sicherheitsmechanismen
Vehicle AU – Vehicle CCU	Ethernet	keine
Vehicle CCU – Vehicle CCU **[K_C2C_11p]**	IEEE 802.11p	IEEE 1609.2 (Authentisierung) Plausibilitätschecks
Vehicle CCU – Roadside CCU **[K_C2I_11p]** **[K_C2I_11bg]**	IEEE 802.11p	IEEE 1609.2 (Authentisierung) Plausibilitätschecks
	IEEE 802.11 b/g (C-WLAN)	WPA2 / 802.11i auf Layer 2 oder Absicherung durch IEEE 1609.2 auf Anwendungsebene
Vehicle CCU – VsZ **[K_C2I_VsZ_cell]** **[K_C2I_11bg]**	ITS IMT Public (UMTS, GPRS)	Sicherer Tunnel **[M_IPSec_Mobil] [M_ITS_VPN]** (Verschlüsselung + Authentisierung)
Vehicle CCU – Third Party	ITS IMT Public (UMTS,	Sicherer Tunnel

Kommunikationskanäle	Kommunikations-technologie	IT-Sicherheitsmechanismen
[K_C2I_ExtServ_cell]	GPRS)	**[M_IPSec_Mobil] [M_ITS_VPN]** (Verschlüsselung + Authentisierung) Autorisierung
Roadside AU – VsZ **[K_I2I_IRS_VsZ_cell]**	Proprietärer Backbone / Ethernet, TCP/IP	Sicherer Tunnel **[M_TLS_Sec] [M_IPSec_Mobil] [M_ITS_VPN]** (Verschlüsselung + Authentisierung)
	ITS IMT Public (UMTS, GPRS)	Sicherer Tunnel **[M_IPSec_Mobil] [M_ITS_VPN]** (Verschlüsselung + Authentisierung)
Roadside CCU – IGLZ ***[K_I2I_IRS_IGLZ]***	Proprietärer Backbone / Ethernet, TCP/IP	Die IT-Sicherheit ist geregelt durch hoheitliche Vorgaben der Stadt Frankfurt.
Roadside AU – LSA	Drahtgebunden	Keine Absicherung erforderlich da kein externer Zugriff möglich ist. Physikalischer Schutz, s. a. Abschnitt 1.3.1.
Roadside AU – VBA	Drahtgebunden	Keine Absicherung erforderlich da kein externer Zugriff möglich ist. Physikalischer Schutz, s. a. Abschnitt 1.3.1.
IGLZ – VsZ **[K_I2I_IGLZ_VsZ]**	Internet	Sicherer Tunnel **[M_ITS_VPN]** (Verschlüsselung + Authentisierung), s. a. Abschnitt 1.3.1.
VZH – VsZ	internes Ethernet, TCP/IP	Keine Absicherung notwendig da interne Verbindung, s. a. Abschnitt 1.3.1.
sim^{TD} Partner **[K_SimPart_VsZ]**	Internet	Sicherer Tunnel (SCP, SSH, HTTPS) **[M_ITS_VPN] [M_Fernzugriff_SSH]** (Verschlüsselung + Authentisierung)
3rd Party – VsZ **[K_ExtServ_VsZ]**	Internet	Sicherer Tunnel **[M_ITS_VPN]** (Verschlüsselung + Authentisierung)

Tabelle 5.5: Absicherung der Kommunikationskanäle in sim^{TD}

Die Pseudonymverwaltung bzw. PKI-Zentrale ist in der Versuchszentrale untergebracht, zu der alle Teilnehmer des sim^{TD}-Versuchssystems Zugriff haben. Mit Hilfe dieser PKI werden

unter anderem langlebigen Schlüsselpaare ausgegeben, die von allen Teilnehmern des Systems zur Authentifizierung genutzt werden können.

Das HLSV strebt für das Forschungsprojekt sim^{TD} eine Lösung an, in der zumindest Basisfunktionalitäten einer PKI demonstriert werden. Da das Versuchsgebiet geografisch nicht allzu groß ist, genügt eine „flache“ Hierarchie, d.h. eine einzige CA. Für einen späteren Wirkbetrieb und das Ausrollen von sim^{TD} auf größere Gebietshoheiten wäre eine hierarchisch gegliederte PKI die geeignetere Variante.

Der Verzicht auf eine PKI-Lösung im Forschungsprojekt sim^{TD} gefährdet nach Ansicht des HLSV die Akzeptanz von sim^{TD}, die insbesondere in der Bewertung (TP5) Gegenstand umfangreicher Untersuchungen sein wird. Ferner wären alle Ergebnisse in den von TP4 durchzuführenden Versuchen anfechtbar, da die Einspeisung von Nachrichten und Messdaten aus fremden Quellen nicht ausgeschlossen werden könnte.

5.3.1 Einsatz von Pseudonymen

Digitale Identitäten bieten folgende für den Feldtest nützliche Eigenschaften:

- Zertifizierung und Zulassung von Konfigurationen bzw. Versionen zu Tests
- Manipulationssicherheit von versendeten Daten
- Sicheres Audit versendeter Daten (Nichtabstreitbarkeit)

Versendete digital signierte Daten können daraufhin vom Empfänger auf Manipulation überprüft werden. So kann – bei entsprechender Filterung – vermieden werden, dass manipulierte Daten die Testergebnisse beeinflussen und damit den Feldtest gefährden. Nicht zuletzt können digital signierte Daten eindeutig einem Absender zugeordnet werden. Damit können Fahrzeuge und Anwendungen mit unzulässigem Verhalten zuverlässig identifiziert und aus dem Verkehr gezogen werden.

Die oben genannten Eigenschaften werden erkauft durch einen höheren Aufwand zur Verteilung und Zuweisung von digitalen Identitäten bzw. dem Rechenaufwand auf den im Feldtest befindlichen Plattformen. Die zur Verwaltung von Identitäten notwendigen Komponenten werden in den folgenden Abschnitten kurz erläutert.

Abbildung 5.7 stellt die Kommunikationsabsicherungskomponenten der CCU in sim^{TD} dar, welche die benötigten Subkomponenten für die Pseudonymverwaltung enthält. Neben der *Identity Database*, die alle Zertifikate speichert, ist der *Pseudonym Change Manager* für das gleichzeitige Ändern aller Identifizierer auf allen Kommunikationsebenen zuständig. Für die Absicherung von Nachrichten auf der Anwendungsebene ist ein Client Bundle (*Security Daemon Client*) auf der AU vorgesehen mit der die Nachrichten durch den Security Daemon auf der CCU angesprochen werden kann. Pseudonyme werden auf der IRS auf die gleiche Weise wie auf der IVS eingesetzt. Grund hierfür ist nicht die Pseudonymisierung, die bei ortsfesten IRS keinen Effekt erzielt, sondern die Tatsache, dass Pseudonyme eine kurze Schlüssellänge haben und damit eine wesentlich effizientere Signierung und Verifizierung erlauben. Die Häufigkeit des Pseudonymwechsels kann sich bei IRS von der Wechselrate der IVS unterscheiden.

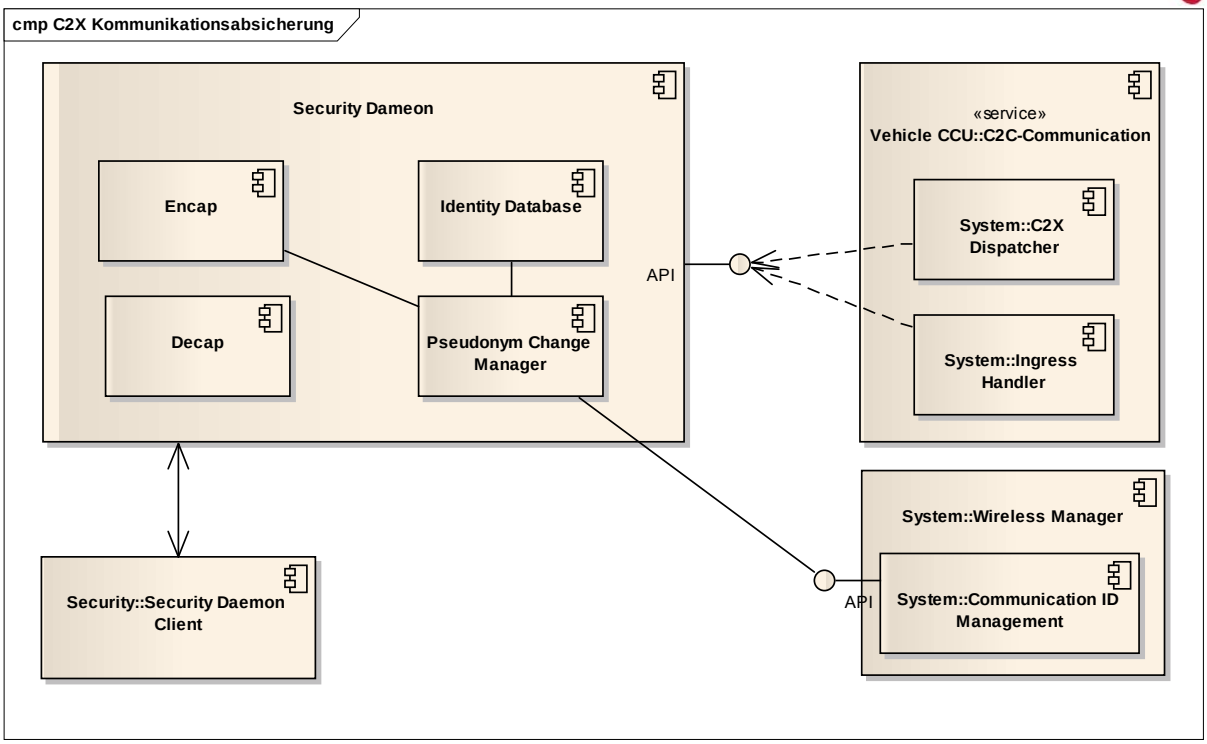

Abbildung 5.7: Kommunikationsabsicherung auf der CCU

Abbildung 5.8 stellt die Komponenten der AU mit ihren Subkomponenten und den Schnittstellen dar. Die Funktionen F_5.1.1 *Verteilung individueller Sicherheitsparameter*, die von der zentralen Komponente eine Signierung neuer Pseudonyme anfordert, sowie der *Verteildienst für allgemeine Sicherheitsparameter (F_5.1.2)* werden als Anwendungen realisiert. Die Komponente für die Verteilung individueller Sicherheitsparameter beinhaltet wiederum die Subkomponente *Configuration Check*, mit der die aktuell installierten Bundleversionen auf der AU zur Prüfung an die Versuchszentrale übertragen werden. Die Zertifizierung und damit die Zulassung von bestimmten Konfigurationen zu verschiedenen Tests ermöglicht eine strenge Kontrolle der Systeme, die sich innerhalb des Testsystems bewegen. Das ist sinnvoll um zu vermeiden, dass veraltete Software sich im System befindet oder ein Fahrzeug bestimmte Funktionen nicht (korrekt) bietet und so das Ergebnis des Tests verfälschen. Deshalb bietet es sich an, die Zertifikatsvergabe an die Ergebnisse aus dem Prüfstand zu koppeln, um nur Fahrzeuge mit zulässiger Konfiguration innerhalb des Feldtests zu verwenden. In diesem Zusammenhang kann die Erfüllung der Qualitätskriterien nach AP 1212 Grundlage zur Zertifizierung von Systemen sein. Die Funktion *Verteildienst für allgemeine Sicherheitsparameter* unter anderem für die Erstellung und Abfrage von Revokationslisten zuständig. Im Gegensatz zur optimalen IT-Sicherheitslösung für ein späteres Wirksystem wird in sim^{TD} nur eine Revokation von Pseudonymen, nicht jedoch von Basisidentitäten vorgesehen. Da in sim^{TD} nur eine einzige CA existieren wird, kann bei Kompromittierung einer Basisidentität (z.B. bei Diebstahl des Fahrzeugs) die entsprechende Basisidentität einfach innerhalb der CA als „revoziert“ markiert werden und muss nicht über Revokationslisten verbreitet werden. Spätere Pseudonymanforderungen dieser Basisidentität werden dann abgelehnt und das Fahrzeug somit von der sim^{TD}-Kommunikation ausgeschlossen.

Die Subkomponenten Encap und Decap werden vom *Security Daemon Client* aufgerufen, um Nachrichten auf Anwendungsschicht durch andere Bundles signieren, verifizieren bzw. verschlüsseln und entschlüsseln zu lassen. Wenn der Security Daemon auf der CCU von dem Client von der AU verwendet wird, werden sichere Nachrichten nach IEEE 1609.2 genutzt.

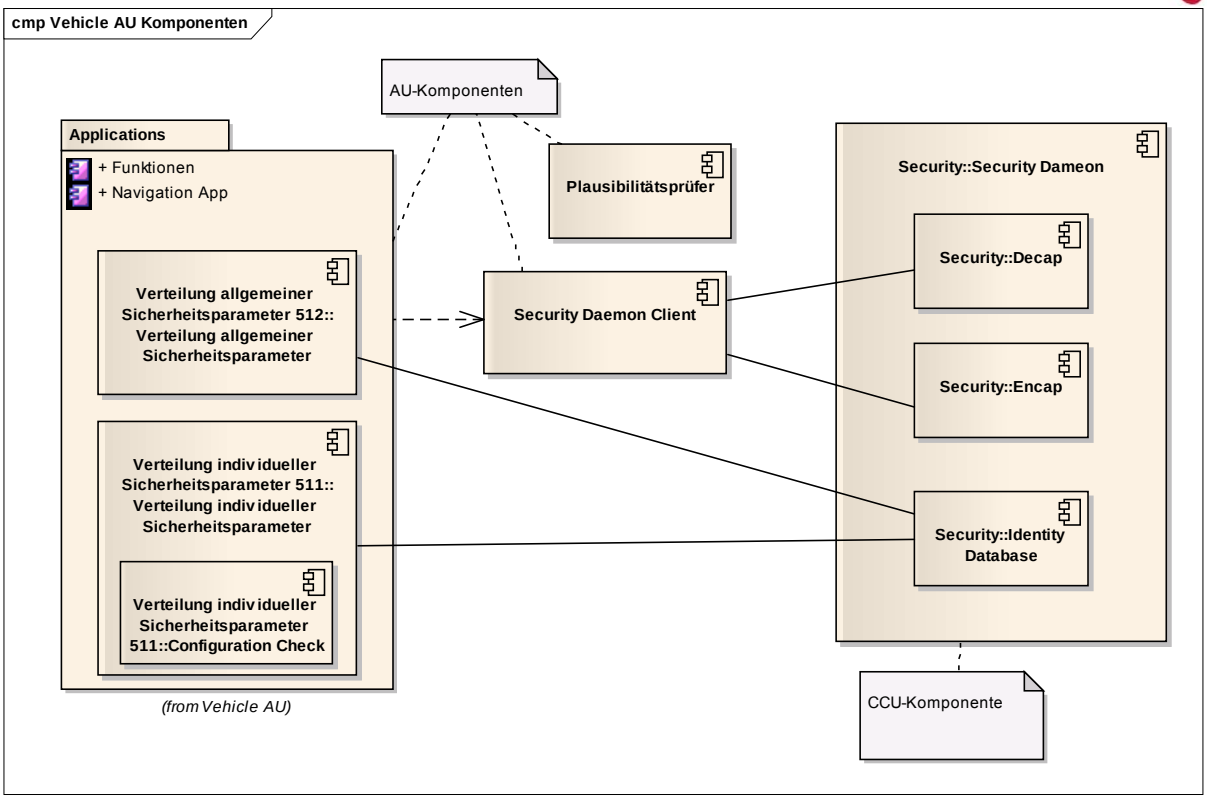

Abbildung 5.8: Verteildienst für individuelle Sicherheitsparameter

Im Folgenden wird auf die einzelnen Komponenten eingegangen, die für den Einsatz von digitalen Pseudonymen zuständig sind.

5.3.1.1 Pseudonymvorrat

Der Pseudonymvorrat ist als Komponente *Identity Database* im Security Daemon eingebettet. In dieser Komponente werden alle digitalen Zertifikate und Identitäten des Fahrzeuges gespeichert. In sim^{TD} wird zwischen den folgenden Identitäten beziehungsweise Pseudonymen unterschieden:

- Basisidentität
- Wechselnde Pseudonyme
- Root-Zertifikat der PKI
- Zertifikate aller Teilnehmer im Kommunikationsradius

Grundsätzlich wird mit der Funktion F_5.1.1 dafür gesorgt, dass immer genug Pseudonyme auf dem Fahrzeug im Pseudonymvorrat zur Verfügung stehen. Eine Basisidentität ist dem Fahrzeug fest zugeordnet und muss über die Dauer des gesamten sim^{TD} Feldtests gültig sein. Die Basisidentität dient zur Authentifizierung gegenüber der zentralen PKI, die mit Hilfe der Komponente *Verteildienst für individuelle Sicherheitsparameter* vom Fahrzeug erstellte Pseudonyme signiert. In sim^{TD} ist es auch vorgesehen, dass das Zertifikat der Basisidentität auf die IVS bzw. IRS transportiert wird. Da der private Schlüssel niemals das eigene System verlassen darf, muss das asymmetrische Schlüsselpaar auf dem Fahrzeug bzw. der IRS erzeugt werden und anschließend mit Hilfe einer Zertifikatsanforderung (Certification Request) an die PKI zum Signieren übertragen werden. Die Vorgehensweise zum Übertragen der Basisidentität wird im Folgenden näher beschrieben.

1. In der Versuchszentrale werden mehrere Zertifikate generiert, die für den Austausch der Basisidentitäten verwendet werden und im folgenden Token genannt werden.
2. Mit einem USB Stick wird ein initiales Token auf das Zielsystem (IVC, IRS) übertragen und dort gespeichert.
3. Beim Start des Security Daemons wird geprüft, ob ein Initialisierungstoken vorliegt und falls das der Fall ist ein neues Schlüsselpaar für die Basisidentität erzeugt. Der private Schlüssel wird in der lokalen Datenbank (*Identity Database*) abgespeichert.
4. Der öffentliche Schlüssel wird mit dem Initialisierungstoken verschlüsselt an die zentrale Komponente des Verteildienstes für individuelle Sicherheitsparameter übertragen.
5. Die PKI erstellt ein Zertifikat für die Basisidentität des Anforderers und schickt das signierte Zertifikat zurück. Das verwendete Initialisierungstoken wird anschließend zerstört bzw. als ungültig erklärt, damit er nicht ein zweites Mal verwendet werden kann.
6. Sobald der Anforderer eine neue gültige Basisidentität erhalten hat, wird diese in der Datenbank abgespeichert. Falls eine alte Basisidentität vorhanden war, wird diese überschrieben.

Die wechselnden Pseudonyme werden auch in sim^{TD} auf dem Fahrzeug erstellt und anschließend per Verteildienst für individuelle Sicherheitsparameter zur PKI in der Versuchszentrale übertragen, wo sie mit dem Root-Zertifikat signiert werden. Da in sim^{TD} aus Performancegründen RSA statt ECDSA eingesetzt wird, kann der Zertifikatsstandard von IEEE 1609.2 nicht vollständig eingehalten werden. Zusätzlich zu dem öffentlichen Schlüssel überträgt der Verteildienst für individuelle Sicherheitsparameter Informationen, die in dem Pseudonym-Zertifikat enthalten sein sollen. Die PKI prüft beim Empfang die Daten, erstellt das Zertifikat mit den entsprechenden Fahrzeugdaten und Ablaufzeitpunkten und signiert es schließlich mit dem eigenen Root-Zertifikat.

Die wechselnden Pseudonyme werden in einer größeren Menge vorgehalten, so dass ein Teilnehmer auch über mehrere Wochen aktiv an der C2I Kommunikation teilnehmen kann ohne mit der PKI in Kontakt zu treten, um neue Pseudonyme anzufordern. Bei der Anforderung neuer Pseudonyme muss darauf geachtet werden, dass für die Zukunft zu jedem Zeitpunkt genug gültige Pseudonyme vorliegen, diese aber jeweils nur eine beschränkte Gültigkeitsdauer haben. Es werden zum Beispiel vom Verteildienst für individuelle Sicherheitsparameter Pseudonyme für die nächsten Tage oder Wochen beantragt. Der Security Daemon muss in diesem Fall darauf achten, dass jedes Pseudonym nicht länger als 24 Stunden gültig ist, da bei einer längeren Gültigkeit ein Angreifer die privaten Schlüssel innerhalb der Gültigkeitsdauer des Zertifikats berechnen könnte. Die Pseudonyme müssen also als 24-Stundenpaket gebündelt und von der PKI verifiziert werden. Der Security Daemon kann durchaus Pseudonyme für die Zukunft beantragen, da die Angreifbarkeit der privaten Schlüssel erst beachtet werden muss sobald ein Pseudonym zum ersten Mal durch die C2X-Kommunikation veröffentlicht wurde.

In sim^{TD} sollte der erstellte Pseudonymvorrat für jedes Fahrzeug so viele Pseudonyme enthalten, dass eine durchgängige sichere Kommunikation über einen langen Zeitraum des Versuchs garantiert werden kann. So wird verhindert, dass mögliche Ausfälle der PKI oder der UMTS-Verbindung zur CA dazu führen, dass Fahrzeuge keine benötigten Pseudonyme mehr erhalten. Sollte es in sim^{TD} nicht mehr möglich sein, neue Pseudonyme über UMTS zu erhalten, so würde dies unter Umständen den Grad der Pseudonymisierung einschränken, da Fahrzeuge nicht mehr beliebig häufige Pseudonymwechsel durchführen können, jedoch wird dies als das deutlich geringere Problem angesehen, verglichen mit einem kompletten Ausfall der sicheren Kommunikation. In sim^{TD} ist vorgesehen, dass ein Fahrzeug mit einer Grundausstattung für mindestens 30 Tage im Voraus ausgestattet wird. Das würde bedeuten

dass jedes Fahrzeug 30 Pseudonyme für den folgenden Monat als Grundausstattung vorhält, wobei jedes Pseudonym nur maximal 24 Stunden gültig ist. Zusätzlich zu diesem Grundstock beantragt das Fahrzeug regelmäßig für die zukünftigen 24 Stunden 48 Pseudonyme bei der PKI. Da jedes Pseudonym maximal 200 Byte groß ist, fällt der Aufwand für die Speicherung und Übertragung sehr gering aus.

Das Root-Zertifikat der zentralen PKI wird einmalig manuell auf das Fahrzeug aufgespielt und dort in der *Identity Database* gespeichert. Mit Hilfe dieses Zertifikates müssen alle empfangenen Nachrichten verifiziert werden.

Damit der Security Daemon eine Nachricht verschlüsseln kann, muss das Pseudonym des Empfängers beim Absender vorliegen. Da jeder Teilnehmer all seine Nachricht signiert und das eigene Zertifikat des Pseudonyms anhängt, kann im Security Daemon bei jedem Verifikationsprozess geprüft werden ob das jeweilige Pseudonym in der internen Datenbank vorliegt. Falls es noch nicht vorhanden ist, muss ein entsprechender Eintrag, indiziert durch die MAC-Adresse des Absenders angelegt werden. Mit diesem Zertifikat kann zu einem späteren Zeitpunkt eine Nachricht mit dem öffentlichen Schlüssel des Ziels verschlüsselt werden. Die Speicherung der Pseudonyme ist nur so lange notwendig wie sich der C2I Teilnehmer im Empfangsradius befindet und das empfangene Zertifikat gültig ist. Für sim^{TD} empfehlen wir daher der Einfachheit halber, gespeicherte Schlüssel nach einem festen Timeout von einigen wenigen Minuten wieder aus der internen Datenbank zu entfernen.

5.3.1.2 Verteildienst für individuelle Sicherheitsparameter

Der Verteildienst für individuelle Sicherheitsparameter wird vom Security Daemon getriggert sobald erkannt wird, dass nicht genug Pseudonyme für den aktuellen Zeitabschnitt vorhanden sind oder wenn für zukünftige Zeitabschnitte keine Pseudonyme vorliegen. Die genaue Spezifikation der Verteildienste für individuelle und allgemeine Sicherheitsparameter werden in den Funktionen F_5.1.1 und F_5.1.2 spezifiziert.

5.3.1.3 [M_ITS_PSDWM] Pseudonymwechselmanager

In sim^{TD} kann der Wechsel der Pseudonyme vom Pseudonymwechselmanager (Pseudonym Change Manager) anhand verschiedener Algorithmen getriggert werden:

- Zufällig
- Im festgelegten Zeitintervall
- Zu bestimmten festgelegten Zeitpunkten

Weitere Algorithmen die einen kooperativen Wechsel zwischen allen benachbarten Fahrzeugen organisieren, werden in sim^{TD} nicht beachtet, da diese einen zu großen Aufwand mit sich bringen. Es soll jedoch für ein Wirksystem die Möglichkeit offengehalten werden, weitere intelligentere Algorithmen einsetzen zu können.

Sobald der *Pseudonymwechselmanager* des Security Daemons getriggert wurde, liefert er dem SIM-NET eine neue ID (6 Byte des Fingerprints des neuen Zertifikats). Dieser Fingerprint wird in SIM-NET als MAC-Adresse und Node-ID genutzt, wobei die Node-ID noch um zwei feststehende Bytes ergänzt wird. Der Pseudonymwechsel wird von SIM-NET an eine unkritische Nachricht, zum Beispiel an eine CAM gebunden. Es ist wichtig, dass mit dieser ausgewählten Nachricht auf allen Kommunikationsebenen synchron die IDs gewechselt werden. Ohne die Kopplung des Wechsels an eine Nachricht könnte es zu einem „Zwischenzustand“ kommen, bei dem einige Kommunikationsebenen noch die alte und einige schon die neue ID verwenden. Dies würde zu einem Bruch des Privatsphärenschutzes führen und zum anderen zu Fehlern bei den Empfängern.

Um die Funktionalität der Anwendungen auf der AU wird in sim^{TD} jedoch ein Pseudonymwechsel in kritischen Situationen nicht durchgeführt. Da das Situationswissen bei den Funktionen auf der AU vorliegt, wird bei dem Security Daemon Client eine Schnittstelle angeboten, bei der jede Hauptfunktion eine kritische Situation melden kann. Sobald eine Funktion eine kritische Situation registriert hat, wird die Information zum *Pseudonymwechselmanager* auf die CCU übertragen. Vor jedem Pseudonymwechsel wird nun geprüft ob eine unkritische Situation vorliegt und nur wenn das der Fall ist, wird der Wechsel angestoßen. Falls ein Wechsel nicht möglich war, wird der Zeitintervall für den nächsten Wechsel herunter gesetzt, so dass ein Pseudonymwechsel so schnell wie möglich durchgeführt werden kann.

Grundsätzlich besteht das Problem, dass der Pseudonymwechsel durchgeführt wird sobald das eigene System die aktuelle Situation als unkritisch betrachtet. Es ist jedoch möglich dass für das eigene System die Situation unkritisch ist, jedoch für benachbarte Teilnehmer ein kritischer Moment vorliegt. In sim^{TD} wird davon ausgegangen, dass die kritischen Situationen überwiegend ortsgebunden sind und dadurch bei benachbarten Teilnehmern eine sehr ähnliche Situation vorherrscht. Eine Erweiterung des Kommunikationsprotokolls zum kooperativen Steuern des Pseudonymwechsels wird in sim^{TD} deshalb nicht vorgesehen.

5.3.2 Pseudonymverwaltung in der Versuchszentrale

Abbildung 5.9 zeigt eine Übersicht des PKI-Konzeptes in sim^{TD}. In diesem Abschnitt wird die Maßnahme [M_ITS_PSDV] diskutiert. Die zentrale Komponente des Konzeptes ist der PKI-Dienst, der für die Ausstellung von Basisidentitäten und Pseudonymen nach dem IEEE 1609.2 Trial-Use Standard verantwortlich ist. Hierzu verwendet der PKI-Dienst die Pseudonymverwaltung, die alle Pseudonyme sowie die Zuordnungen zu deren Basisidentitäten in einer Datenbank bereithält. Weiterhin existieren zwei Registration Authorities (RA), die für die der Zertifikatsausstellung vorgeschaltete Autorisierung verantwortlich sind. Die RA ist für die Ausstellung der Pseudonyme zuständig, welche über die Funktion F_5.1.1 geliefert werden und ist daher in Abbildung 5.9 durch den Block *Verteildienst* dargestellt.

Der Verteildienst F_5.1.2 ist für die Verbreitung von Revokationslisten zuständig. Die Listen werden manuell erstellt und automatisch an alle C2X-Teilnehmer verbreitet. Da die IVS und IRS physikalisch angreifbar sind ist es wichtig, dass Pseudonyme revoziert werden können. Basisidentitäten können ebenfalls revoziert werden, müssen in sim^{TD} aber nicht über Revokationslisten verteilt werden. Da sie nur zur Kommunikation mit der CA verwendet werden und es – im Gegensatz zu einem Wirksystem – in sim^{TD} nur eine CA geben wird, reicht es aus, kompromittierte Basisidentitäten innerhalb der CA als „revoziert“ zu markieren und die weitere Auslieferung neuer Pseudonyme für diese Basisidentitäten zu verweigern. Der genaue Mechanismus zum Revozieren von Zertifikaten wird in F_5.1.2 beschrieben.

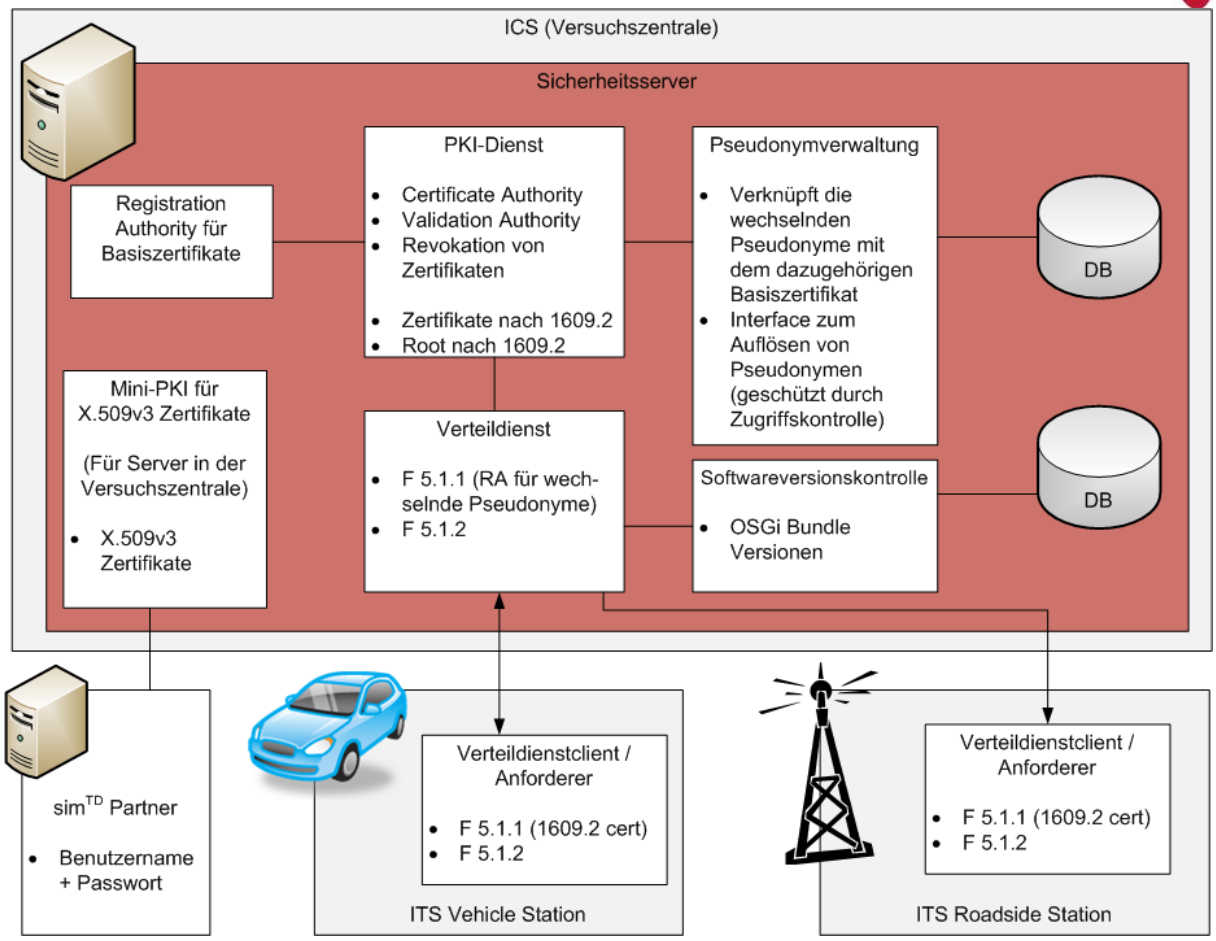

Abbildung 5.9: PKI-Konzept in sim^{TD}

Die Erweiterbarkeit der PKI sollte beachtet werden, so dass in einem späteren Wirksystem evtl. eine verteilte Lösung genutzt werden kann. Die Bildung von Hierarchien ist in sim^{TD} nicht erforderlich. Um trotzdem das Konzept des Security Servers soweit wie möglich in einem späteren Wirksystem wiederverwenden zu können, sollten die Softwarekomponenten unter einer Open-Source-Lizenz verfügbar sein, so dass für spätere Anpassungen der Quellcode verfügbar ist.

5.3.2.1 Registration Authority für Basiszertifikate

Die RA ist für die Autorisierung zur Beantragung von Basisidentitäten zuständig. Nur mit Hilfe der Basisidentität ist es den C2X-Teilnehmern möglich wechselnde Pseudonyme anzufordern. Der Einfachheit halber werden in sim^{TD} die Schlüsselpaare für die Basisidentität auf dem Security Server erzeugt und anschließend durch die Certification Authority (CA) signiert. Die Registrierung neuer Basisidentitäten durch die RA wird durch eine lokale Authentifikation über Benutzername und Passwort am Securityserver umgesetzt. Für die Registierung werden die Zertifikats-Parameter abgefragt:

- Identifikator (Name)
- Typ (normales Fahrzeug, ITS Roadside Station, Einsatzfahrzeug, …)
- Gültigkeitsdauer

Mit diesen Informationen und dem dazugehörigen öffentlichen Schlüssel des Fahrzeugs wird ein Basiszertifikat erzeugt und von der CA signiert. Das Zertifikat wird zusammen in einer PKCS#12 abgespeichert. In dieser Form kann das Basiszertifikat z.B. via USB-Stick manuell

in das betreffende Fahrzeug übertragen werden. Der genaue Prozess zur Schlüsselverteilung wird in F_5.1.1 spezifiziert.

5.3.2.2 Registration Authority für wechselnde Pseudonyme

Die RA zur Beantragung der wechselnden Pseudonyme übernimmt der Dienst der Funktion F_5.1.1, der ebenfalls auf dem Securityserver läuft. Nach erfolgreicher Authentifizierung und Autorisierung wird die Anfrage mit den öffentlichen Schlüsseln an die Certification Authority (CA) der PKI weitergeben.

5.3.2.3 Certification Authority

Die Certification Authority erzeugt und signiert die IEEE 1609.2 Zertifikate mit Hilfe des privaten Schlüssels der PKI und bestätigt damit die Authentizität des Zertifikates. Der für die Validierung des Zertifikates öffentliche Schlüssel der PKI wird als Root-Zertifikat manuell (z.B. zusammen mit der Software) auf die Fahrzeuge verteilt.

5.3.2.4 Pseudonymverwaltung

Bei jeder Anfrage nach neuen Pseudonymen wird protokolliert, welche Pseudonyme zu welcher Komponente (Fahrzeug, IRS,…) gehören. Dazu in der Datenbank der Pseudonymverwaltung jedes ausgegebene Pseudonym seinem Basiszertifikat zugeordnet. Dies erlaubt die „Depseudomisierung“ für die Versuchsauswertung. Zugriffe auf diese Datenbank dürfen nur über eine spezielle Schnittstelle möglich sein, deren Nutzung auf bestimmte autorisierte Nutzer und Dienste beschränkt ist (Authentifikation und Autorisation).

Bei der Anfrage neuer Pseudonyme erzeugen die C2X-Teilnehmer selbstständig die Schlüsselpaare (privater und öffentlicher Schlüssel) die zu einem Pseudonym gehören und senden eine Zertifikatsanforderung zur zentralen PKI über F_5.1.1 Die in der Zertifikatsanforderung enthaltenen öffentlichen Schlüssel, der Fahrzeugdaten und der Fahrzeugsoftwarekonfiguration werden mit der Basisidentität signiert und mit dem öffentlichen Schlüssel der PKI verschlüsselt. Bevor die PKI die Zertifikatanforderung erhält, muss durch die Softwareversionskontrolle bestätigt werden, dass sich das Fahrzeug in einem gültigen Zustand befindet. In sim^{TD} wird der Zustand des Fahrzeugs alleine durch die Versionsnummern der aktiven OSGi-Bundles beschrieben; in einem Wirksystem würden an dieser Stelle jedoch weitergehende Fahrzeugparameter wie z.B. durch einen TPM erzeugte *Platform Attestations* verwendet werden. Wenn die Prüfung erfolgreich war, bekommt die PKI die Zertifikatsanforderung zugestellt und erzeugt für jeden öffentlichen Schlüssel ein Pseudonym in Form eines IEEE 1609.2-ähnlichen Zertifikates. Danach wird das Zertifikat mit dem privaten Schlüssel der PKI unterschrieben. Da laut IEEE 1609.2 nur ECDSA eingesetzt werden darf, in sim^{TD} aber aus Performancegründen RSA eingesetzt wird, muss an dieser Stelle vom Standard leicht abgewichen werden. Anschließend wird das gültige Zertifikat mit dem öffentlichen Schlüssel der Fahrzeug-Basisidentität verschlüsselt und zum Fahrzeug zurückgesendet. Der private Schlüssel des Pseudonyms verlässt also niemals das Fahrzeug.

Wie in Abbildung 5.9 dargestellt, hat auch die IRS einen Zugriff per F_5.1.1 und F_5.1.2 auf den Verteildienstserver in der VsZ. Revokationslisten werden per F_5.1.2 an die IRS geliefert, damit diese wiederum per Broadcast an die Fahrzeuge verteilt werden können.

5.3.2.5 Authentifizierung und Autorisierung beim Zugriff auf die VsZ

Die externen sim^{TD}-Partner, die auf die Versuchszentrale zugreifen, werden mit Benutzernamen und Passwörtern ausgestattet, um autorisierten Zugriff auf die Server in der Versuchszentrale zu gewährleisten. Die Server der Versuchszentrale werden sich im Gegen-

satz zur C2X-Kommunikation mit X.509v3 Zertifikaten authentifizieren. Die Zertifikate werden auf einer eigenen *Mini-PKI* generiert und selbst signiert. Eine Revokation dieser Serverzertifikate ist für den Feldtest in sim^{TD} nicht vorgesehen. Die Schlüssellängen für die Serverzertifikate sollten entsprechend groß gewählt werden.

5.3.3 Absicherung der IP-basierten Kommunikationsverbindungen

Im Testaufbau von sim^{TD} sind die Sicherheitsanforderungen gegenüber einem Wirksystem stellenweise merklich entschärft; insbesondere ist die Anzahl der zu verbindenden Liegenschaften erheblich kleiner als dies bei einem nationalen oder internationalen ITS der Fall wäre.

Hinzu kommt noch, dass einige der Kommunikationswege zwischen den Liegenschaften über proprietäre, dedizierte Übertragungsleitungen geführt werden, so dass hier keine zusätzliche Absicherung im Rahmen des Tests notwendig ist. Zudem obliegt die Anbindung der weitaus größten Zahl von ITS Roadside Stations dem Land Hessen bzw. der Stadt Frankfurt am Main, siehe auch Abschnitt 1.3.1.

Nur für die folgenden Verbindungen ist im Rahmen des Feldversuchs eine Absicherung auf IP-Ebene überhaupt sinnvoll:

- **[K_C2I_VsZ_cell]**: direkte Kommunikation zwischen Vehicle CCU und der (Versuchs-) Zentrale, skizziert in Abbildung 5.10 via ITS IMT Public (UMTS/GPRS): z.B. für den Upload von Testprotokollen; im Rahmen von sim^{TD} wird voraussichtlich die im Wirksystem vorhandene Kommunikationsbeziehung zwischen dem Fahrzeug und den externen Diensten hiermit ebenfalls abgedeckt, da die externen Dienste von Drittanbietern durch einen Server in der Versuchszentrale emuliert werden.
- **[K_I2I_IRS_VsZ_cell]**: Kommunikation zwischen Roadside CCU und Versuchszentrale skizziert in Abbildung 5.11. Diese verwendet ITS IMT Public (UMTS bzw. GPRS) für mobile ITS Roadside Stations.
- **[K_C2I_ExtServ_11bg]**: Kommunikation zwischen Vehicle CCU und externen Diensten/Mehrwertdiensten via Consumer-WLAN (IEEE 802.11 b/g), zur Absicherung s. Abschnitt 5.3.5.
- **[K_C2I_ExtServ_cell]**: Kommunikation zwischen Vehicle CCU und externen Diensten/Mehrwertdiensten via ITS IMT Public (UMTS bzw. GSM). Da in sim^{TD} Mehrwertdienste aller Voraussicht nach direkt in der Versuchszentrale gehostet werden, wird diese Verbindung mit **[K_C2I_VsZ_cell]** zusammenfallen.
- **[K_SimPart_VsZ]**: Kommunikation zwischen den sim^{TD}-Partnern und der Versuchszentrale – diese Kommunikation wird über das öffentliche Internet laufen.
- **[*K_ExtServ_VsZ*]**: Kommunikation zwischen externen Diensteanbietern und der (Versuchs-) Zentrale, diese Verbindung existiert bei sim^{TD} nach aktuellem Kenntnisstand nicht, da externe Dienste durch einen Server in der Versuchszentrale emuliert werden. Sollte hier dennoch ein externer Dienst angebunden werden, so wird eine Absicherung im Prinzip wieder aktuell und kann z.B. mit VPN-Technik erfolgen.

In Abbildung 5.10 sind die direkten Verbindungen des Fahrzeugs zur Versuchszentrale grafisch dargestellt und in Abbildung 5.11 die Verbindungen der IRSs zur Versuchszentrale. Allerdings ist ein großer Teil der IRSs über proprietäre Verbindungen zu den Verkehrszentralen angebunden, deren Anbindung an die Versuchszentrale im vorliegenden IT-Sicherheitskonzept nicht betrachtet wird, siehe auch Abschnitt 1.3.1.

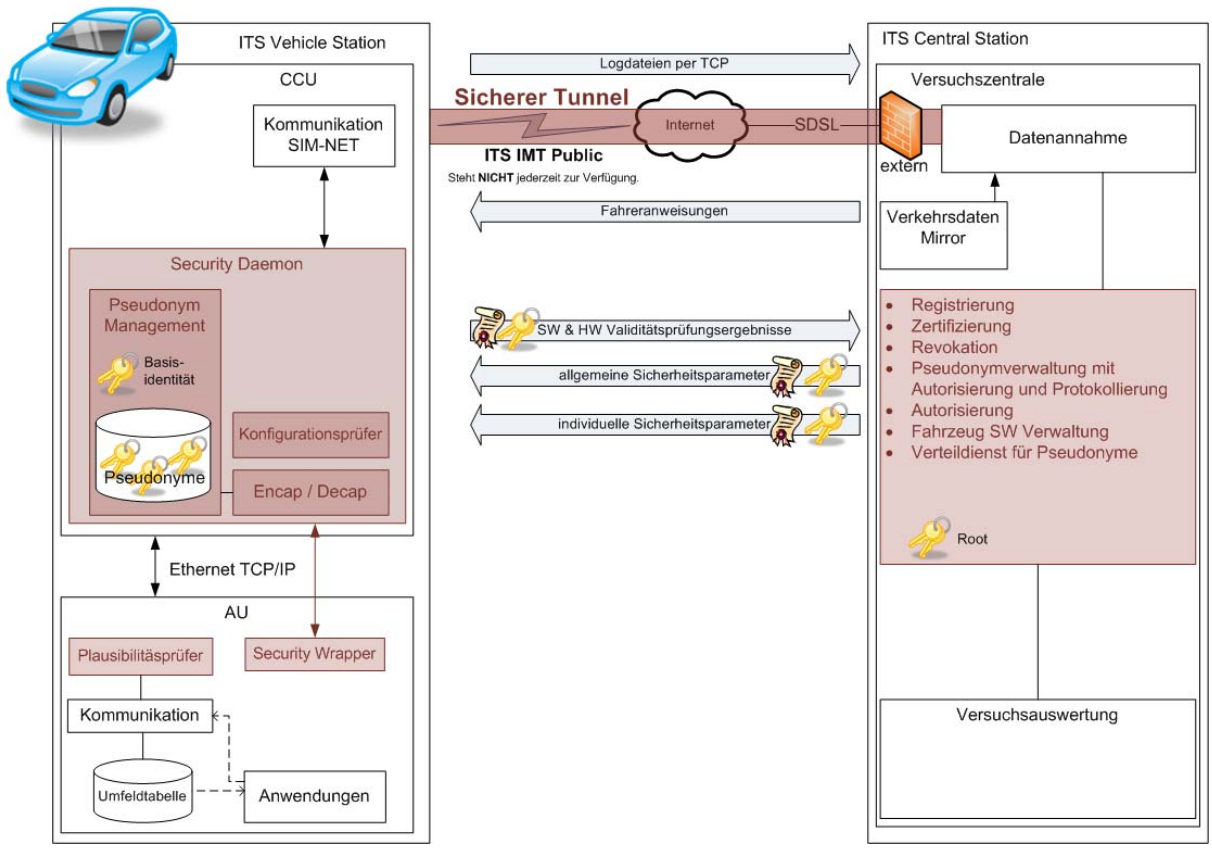

Abbildung 5.10: ITS IMT Public Kommunikation zwischen Fahrzeugen und Versuchszentrale

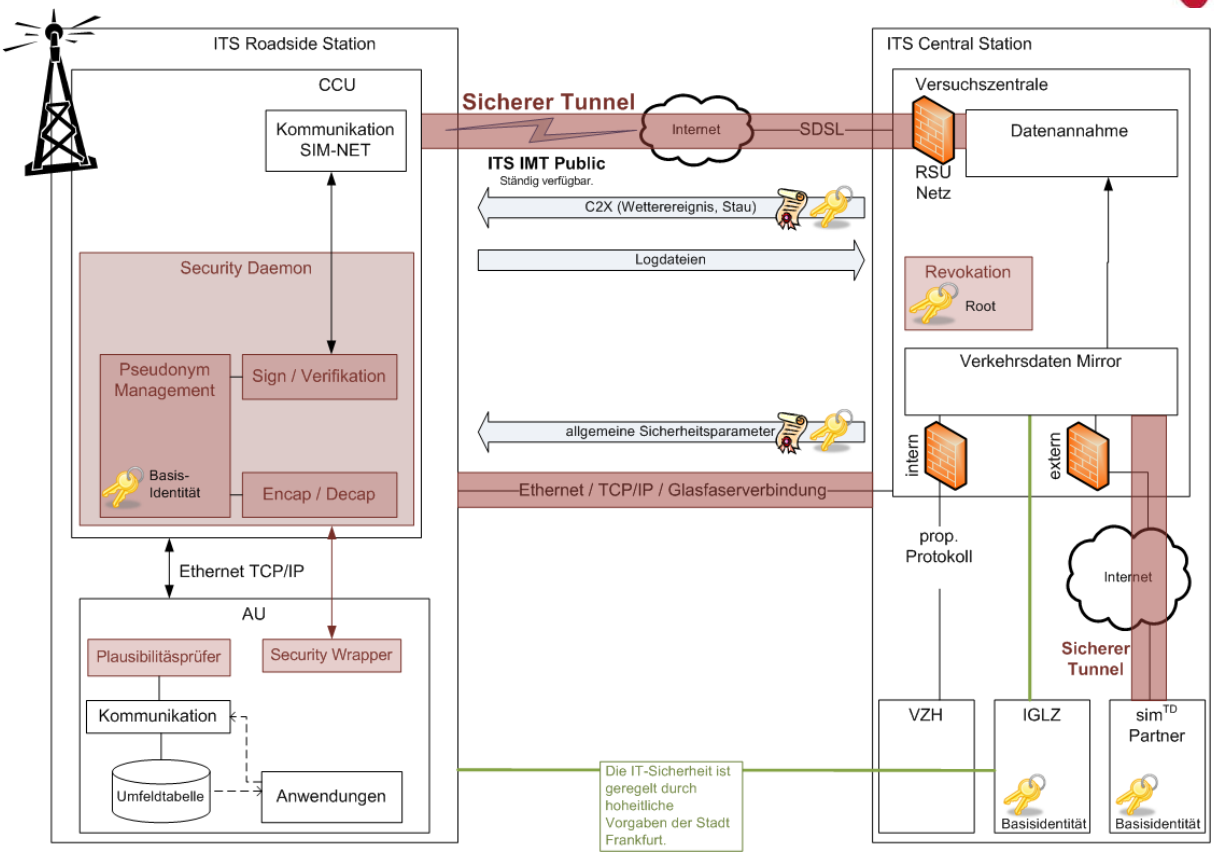

Abbildung 5.11: ITS IMT Public Kommunikation zwischen Roadside Station und Versuchszentrale

In den folgenden Unterabschnitten werden die in Abschnitt 5.2.3 bereits für das Wirksystem beschriebenen Maßnahmen auf ihre Notwendigkeit im Rahmen von sim^{TD} beurteilt.

5.3.3.1 [M_ITS_VN] Virtuelles IP-Netz zwischen stationären Knoten des ITS

Für sim^{TD} ist diese Maßnahme aufgrund der oben genannten Gründe nicht relevant.

5.3.3.2 [M_ITS_Ext_Sec] Anti-DDoS-Absicherung der Übergänge ins Internet

Für einen Feldtest ist diese Maßnahme nicht wirtschaftlich darstellbar; da große Netzbetreiber ohnehin über das entsprechende Wissen für eine Anti-DDoS-Absicherung verfügen, erscheint ein Test auch nicht notwendig.

5.3.3.3 [M_ITS_VPN] Kryptografische Absicherung des virtuellen Netzes

Bei sim^{TD} gibt es zwar kein virtuelles Netz zwischen den Liegenschaften wie beim späteren ITS, aber es ist dennoch notwendig, die über öffentliche Netze laufende Verbindung **[K_I2I_VsZ_TestgInd]** zwischen Versuchszentrale und Testgelände abzusichern. Hier sollte die in Abschnitt 5.2.3.1 vorgeschlagene gleichnamige Maßnahme umgesetzt werden.

Dies gilt optional auch für die sim^{TD}-Projektpartner, wenn sie einen umfassenderen Zugriff brauchen, als allein mit SSH-Zugriff zu erreichen wäre. Die Absicherung des Zugriffs auf die jeweils relevanten Server müsste dann jeweils auf Betriebssystem-Ebenen erfolgen.

5.3.3.4 [M_TLS_Sec] SSL/TLS-Absicherung der Datenübertragung zwischen mobilen Knoten und externen Diensten

Auch falls für die primär betroffene Absicherung der Mobilfunkstrecke bei sim^{TD} eine Mobile VPN Lösung eingesetzt wird, siehe Maßnahme [M_Cell_VN] in Abschnitt 5.3.6.3, und überdies die externen Dienste nur in der Versuchszentrale emuliert werden, so sollte SSL/TLS eingesetzt werden, damit getestet werden kann, wie leistungsfähig dies ist und wie sich dies auf das ITS auswirkt.

5.3.3.5 [M_Fernzugriff_SSH] SSH-Absicherung von Fernzugriffen

Die Absicherung der Verbindung der sim^{TD}-Projektpartner an die Versuchszentrale geschieht mithilfe dieser Maßnahme oder mit der oben genannten VPN-Anbindung.

5.3.3.6 [M_Firewall] Einsatz von Firewalls zur Einschränkungen der Zugriffe auf festgelegte IP-Adressbereiche

Diese Maßnahme muss auch bei sim^{TD} umgesetzt werden.

5.3.3.7 [M_IPSec_Mobil] IPSec zur Absicherung der IP-basierten Kommunikation zwischen Fahrzeugen und zentralen ITS-Stations

Auch falls für die primär betroffene Absicherung der Mobilfunkstrecke bei sim^{TD} *Mobile IP VPN basic* von T-Mobile eingesetzt wird, ist es dennoch für den Aufbau eines späteren ITS interessant, hier zusätzlich zu testen, ob es Probleme beim Zusammenspiel der verschiedenen Komponenten gibt und wie leistungsfähig eine Ende-zu-Ende-IPSec-Absicherung ist.

Im Rahmen der Tests wird noch kein IPv6-fähiges Transportnetz zur Verfügung stehen, so dass auf jeden Fall IPv6 über IPv4 getunnelt werden muss. Zum Zeitpunkt der Erstellung dieses Dokumentes stand eine abschließende Klärung der verwendeten IP-Protokollversionen und –varianten jedoch noch aus.

Je nachdem welche Mobilfunk-Lösung eingesetzt wird, müssen unterschiedliche Randbedingungen berücksichtigt werden:

- Bei der herkömmlichen IP-Verbindung im Mobilfunk wird NAT am Gateway zwischen Mobilfunknetz und Internet eingesetzt, so dass man die IPSec-Pakete zusätzliche in UDP einpacken muss, vgl. Abschnitt 5.1.3.3.
- Wird *Mobile IP VPN basic* von T-Mobile eingesetzt, können die IP-Adressen selbst vergeben werden und NAT kann vermieden werden. Allerdings muss man beachten, dass die Kommunikation zwischen dem Mobilfunknetz und der Versuchszentrale ebenfalls durch einen separaten IP-Tunnel geschützt wird. Dies führt zu einem zusätzlichen Overhead (äußerer IP-Header, ESP-Header und ESP-Trailer) pro IP-Paket, der verlangt, dass die MTU auf den lokalen Schnittstellen noch weiter reduziert wird, damit nicht zu oft fragmentiert werden muss. Es kann hier allerdings nicht ausgeschlossen werden, dass diese doppelte Tunneln zu Problemen am VPN-Gateway/Router der Versuchszentrale führt, da hier zwei ineinandergeschachtelte IPSec-Tunnel terminiert werden müssten.

5.3.4 ITS G5A

In diesem Abschnitt wird die sim^{TD}-spezifische Absicherung der C2X-Kommunikation per IEEE 802.11p beschrieben. In der C2C-Kommunikation sind beide Kommunikationspartner ITS Vehicle Stations wie in Abbildung 5.12 gezeigt.

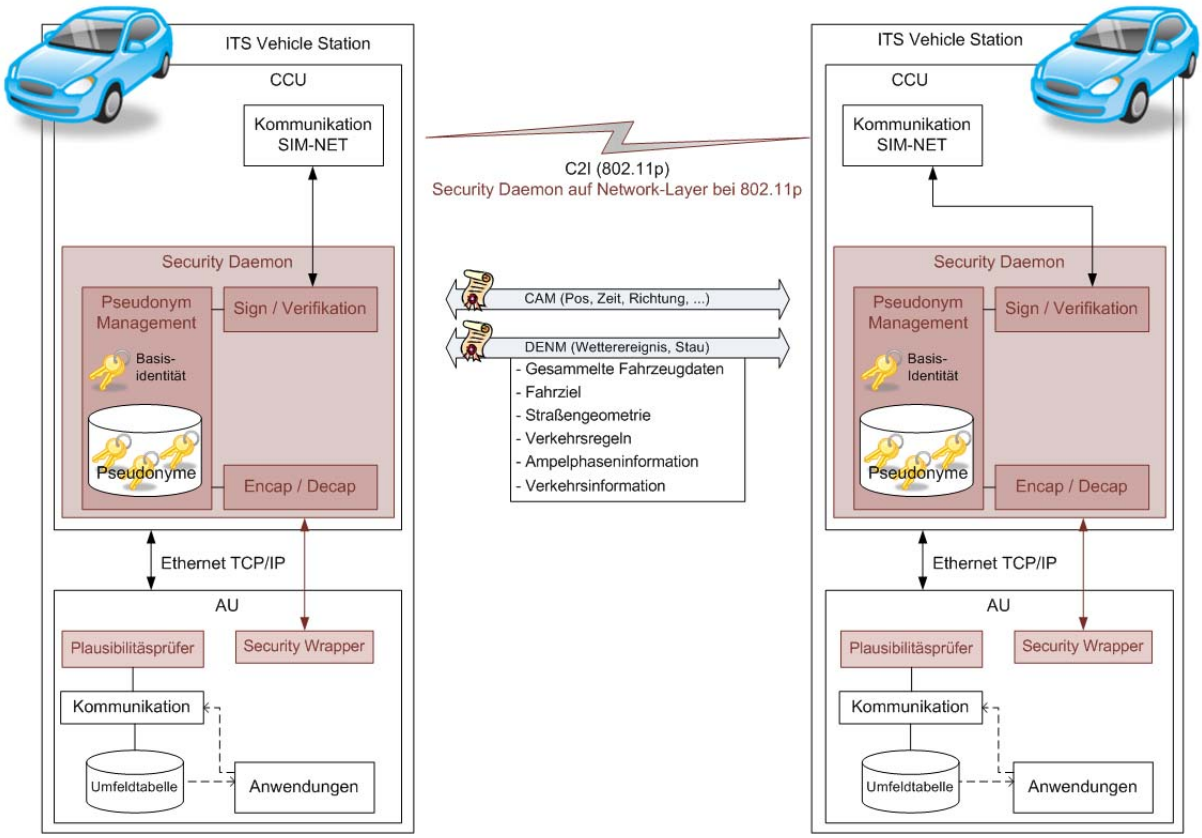

Abbildung 5.12: Ad-Hoc Kommunikation zwischen Fahrzeugen

Die Absicherung der ITS-G5A-Kommunikation wird vom Sicherheitsdienst „Security Daemon“ übernommen. Dieser wird auf der CCU platziert. Die Platzierung der Sicherheitskomponenten auf der CCU hat mehrere Gründe: Da zu schützende Informationen wie Position, Geschwindigkeit und Fahrtrichtung auf Netzwerkebene in die Pakete integriert werden, muss die Kommunikationsabsicherung (Security Daemon) diese Daten genauso schützen wie auch die Informationen in den Paketen der Anwendungsebene. Das sim^{TD}-spezifische Netzwerkpaket (C2X Packet) wird durch den Security Daemon abgesichert. Die Funktionen „Sign“ und „Verifikation“ stehen stellvertretend für die Signierung beim Versand und für die Verifikation beim Empfang von Nachrichten. Der Security Daemon entscheidet, welche Sicherheitsparameter, (z.B. Schüssel und Zertifikat) und Algorithmen verwendet werden. Es soll weiter untersucht werden, ob Sicherheitsoptionen beim Versand von Nachrichten von der Anwendungsebene bis auf die Netzwerkebene im System durchgereicht werden sollen, damit der Security Daemon entscheiden kann, welche Aktion durchgeführt werden soll.

In sim^{TD} wird die Komponente, die unter anderem den IEEE 802.11p Kommunikationsstack implementiert, als „SIM-NET“ bezeichnet. Bei der Aussendung wird SIM-NET die Funktion „Sign“ mit dem C2X Packet als Bytearray aufrufen und bekommt vom Security Daemon den „Security Header“ als Bytearray zurück. Mit dem Bytearray baut SIM-NET das C2X Packet anschließend auf. Je nach Übertragungstyp (Single-hop, Multi-hop) kann SIM-NET einmal oder zweimal „Sign“ beim Security Daemon aufrufen um Hop-by-Hop oder End-to-End Datenfelder zu signieren. Eingehende Nachrichten werden nach dem Empfang von SIM-NET an den Security Daemon geleitet um die Sicherheitsfunktion „Verifikation“ durchzuführen. SIM-NET wird die Funktion „Verifikation“ mit C2X Packet als Bytearray aufrufen und bekommen vom Security Daemon das Ergebnis (Verifikation erfolgreich oder fehlgeschlagen) zurück. Je nach Übertragungstyp (Single-hop, Multi-hop) kann das SIM-NET einmal

oder zweimal „Verifikation“ vom Security Daemon aufrufen um Hop-by-Hop oder End-to-End Datenfelder zu verifizieren.

In der C2I-Kommunikation über IEEE 802.11p sind Kommunikationspartner ITS Vehicle Stations und ITS Roadside Stations wie in Abbildung 5.13 dargestellt.

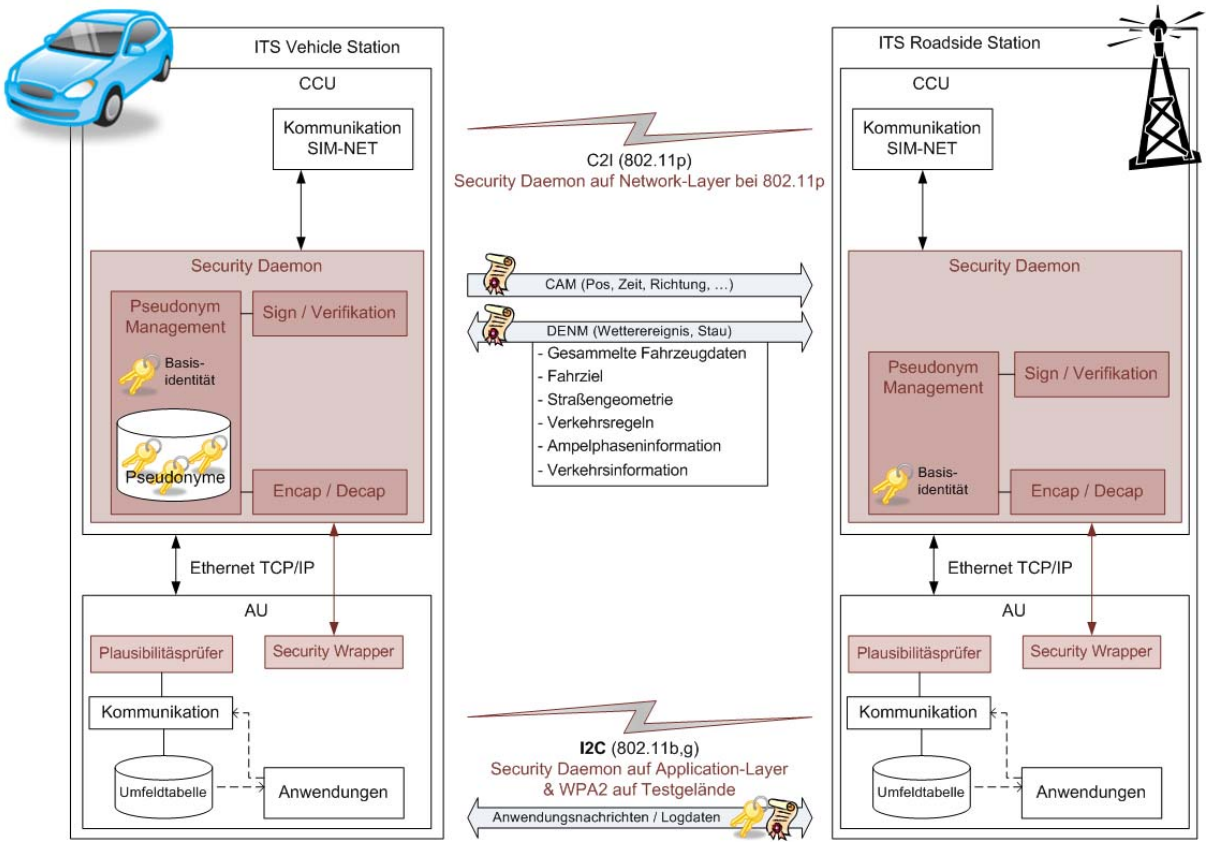

Abbildung 5.13: Ad-Hoc-Kommunikation zwischen Fahrzeugen und Roadside Stations

Die soeben beschriebenen Mechanismen zur Kommunikationsabsicherung werden sowohl auf IVS als auch auf IVS gleichermaßen angewandt. Im Gegensatz zur C2C-Kommunikation ist der Schutz der Privatsphäre ist bei den ITS Roadside Stations nicht notwendig, da diese öffentlichen Infrastrukturkommunikationseinheiten ohnehin ortsfest sind. Für den Fall, dass kurze Schlüssellängen zum Einsatz kommen, werden Pseudonyme jedoch ebenso wie auf der IVS gewechselt werden müssen, da kurze Schlüssel nur eine kurze Haltbarkeit aufwiesen und daher regelmäßig ausgetauscht werden müssen.

5.3.4.1 [M_ITS_SIGN] Signierung

Für die Signierung ausgehender Nachrichten werden die folgenden Daten als Bytearray an den Security Daemon geleitet:

- Zu signierende Nachricht als Bytearray
- Parameter von SIM-NET wie zum Beispiel Nachrichtentyp oder Absicherungsanweisungen

Rückgabewerte des Security Daemons sind:

- Security Header als Bytearray mit variabler Länge

Der Security Daemon entscheidet selbstständig mit Hilfe des internen Pseudonymwechselmanagers welches Zertifikat für die Signierung verwendet wird. Der Security Daemon ist außerdem dafür zuständig, dass jeweils nur ein Zertifikat gleichzeitig für die Signierung verwendet werden darf.

Die Schritte zum Signieren einer ausgehenden Nachricht in sim^{TD} sehen wie folgt aus:

1. SIM-NET erstellt das Netzwerk-Paket.
2. SIM-NET liefert dem Security Daemon das komplette Paket, bestehend aus Network Header und Payload, wobei alle veränderbaren Felder auf null gesetzt sind.
3. Der Security Daemon sendet den Ende-zu-Ende Security Header zurück zu SIM-NET.
4. SIM-NET fügt dem in Schritt 1 erstellten Netzwerk-Paket den Security Header hinzu.
5. SIM-NET übergibt das in Schritt 4 zusammengestellte Netzwerk-Paket komplett an den Security Daemon.
6. Der Security Daemon gibt den Hop-zu-Hop Security Header zurück an SIM-NET.
7. SIM-NET fügt den gerade erhaltenen Security Header dem Netzwerk-Paket hinzu. Die Nachricht beinhaltet nun: Netzwerk Header, (Hop-zu-Hop) Security Header, (Ende-zu-Ende) Security Header, Payload
8. SIM-NET versendet das Paket.

Die Schritte 5 bis 7 sind in sim^{TD} optional. Wahrscheinlich ist der erzeugte Zusatzaufwand bei der Nutzung einer Ende-zu-Ende- und Hop-zu-Hop-Absicherung in diesem Projekt zu hoch.

Außerdem muss in sim^{TD} je nach vorhandener CPU-Leistung und eingesetztem kryptografischen Algorithmus eine Optimierungsstrategie durchgeführt werden. Als Beispiel könnte eine probabilistische Verifikation durchgeführt werden oder es wird beispielsweise nur das Zertifikat validiert, wenn der Knoten vorher unbekannt war.

Die Eingliederung der C2X-Kommunikationsabsicherung in dem sim^{TD} Gesamtsystem wird in dem Sequenzdiagramm in Abbildung 5.14 dargestellt.

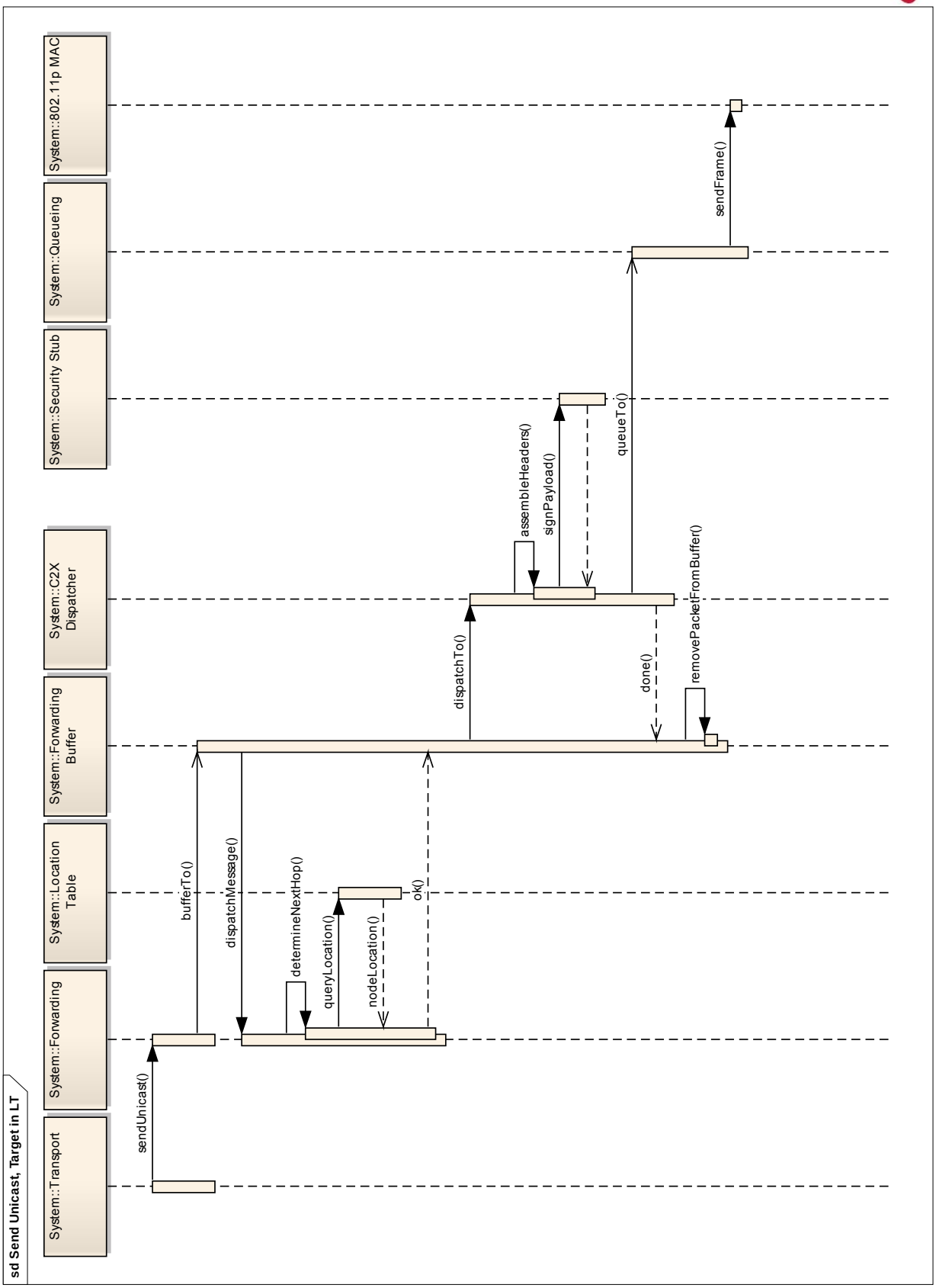

Abbildung 5.14: Sequenzdiagramm: Absicherung der C2X-Nachrichten beim Aussenden

5.3.4.2 [M_ITS_VERIFIY] Verifizierung

Für die Verifizierung eingehender Nachrichten werden dem Security Daemon folgende Daten durch SIM-NET geliefert:

- Nachricht ohne Signatur als Bytearray
- Security Header als Bytearray

Rückgabewerte des Security Daemons sind:

- Ergebnis der Verifizierung (Erfolg, Grund für einen Fehler)

Die Schritte zum Verifizieren einer empfangenen Nachricht sehen wie folgt aus:

1. SIM-NET empfängt Nachricht
2. SIM-NET sendet dem Security Daemon zum einen das eigentliche Paket ohne Hop-zu-Hop Security Header und zum anderen den entsprechenden Hop-zu-Hop Security Header.
3. Security Daemon antwortet mit dem Verifikationsergebnis bzw. mit dem Grund eines Fehlschlags.
4. SIM-NET sendet dem Security Daemon zum einen das eigentliche Paket ohne Security Header und zum Anderen den entsprechenden Ende-zu-Ende Security Header.
5. Security Daemon sendet das Verifikationsergebnis bzw. mit dem Grund eines Fehlschlags bei der Verifikation des Ende-zu-Ende Teils an SIM-NET zurück.
6. SIM-NET leitet das Paket für die weitere Verarbeitung an den Network & Transport-Layer weiter.

Für die Weiterleitung empfangener Nachrichten an direkte Nachbarn sind Schritte 4 und 5 nicht notwendig. Für die endgültige Verarbeitung einer empfangenen Nachricht können Schritt 2 und 3 ausgelassen werden, da diese nur bei einer Multihopkommunikation notwendig sind. In sim^{TD} ist eine Umsetzung der Hop-zu-Hop-Absicherung unwahrscheinlich, da die Ressourcen der eingesetzten Systeme nur eine Ende-zu-Ende-Absicherung zulassen.

Die Eingliederung der C2X-Kommunikationsabsicherung in das sim^{TD}-Gesamtsystem wird in dem Sequenzdiagramm in Abbildung 5.15 dargestellt.

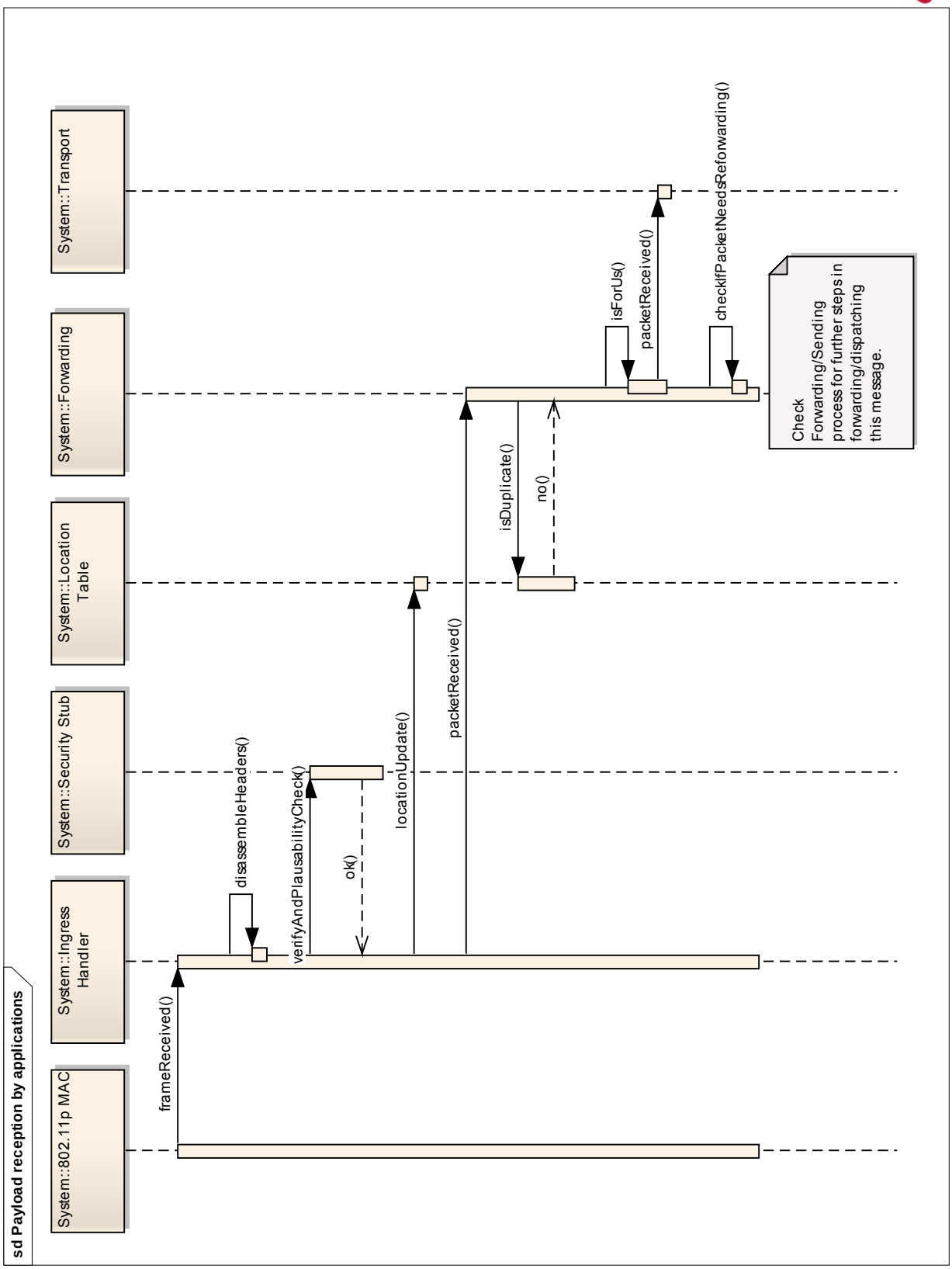

Abbildung 5.15: Sequenzdiagramm: IT-Sicherheitsprüfung beim Empfang von C2X Nachrichten

Wenn die Verifikation der Nachricht durch den Security Daemon (*Security Stub*) fehlschlägt, wird die Nachricht als ungültig makiert und trotzdem durch den C2X-Kommunikationsstack weiterverarbeitet. Die Information der Fehlgeschlagenen Verifikation wird den Anwendungen auf der AU zur Verfügung gestellt.

5.3.4.3 [M_ITS_CRYPTO] Verschlüsselung

Für verschiedene Funktionen ist es notwendig, dass die Daten der C2X-Nachrichten verschlüsselt übertragen werden. Wie bereits in Abschnitt 5.3.1 beschrieben, muss für die Verschlüsselung der öffentliche Schlüssel des Empfängers bekannt sein. Durch die wechselnden Pseudonyme in sim^{TD} kann jedoch nicht garantiert werden, dass der Empfänger immer noch das gleiche Pseudonym verwendet wie der Absender zum Verschlüsseln verwendet hatte. Der Empfänger könnte beispielsweise sein Pseudonym genau in dem Moment wechseln, in dem der Absender das Paket mit dem alten Pseudonym verschlüsselt und aussendet. Die neuen öffentlichen Schlüssel werden erst nach einem Pseudonymwechsel mit allen ausgehenden Nachrichten verteilt.

Für sim^{TD} wurde entschieden, dass keine besonderen Maßnahmen beim Absender getroffen werden, um den richtigen Schlüssel auszuwählen. Der Empfänger kann jedoch versuchen, direkt nach einem Pseudonymwechsel zusätzlich mit dem Vorgängerschlüssel zu entschlüsseln. Ein Konzept zum synchronisierten Wechsel der Pseudonyme erscheint in diesem Feldtest nicht sinnvoll, da der Absender in der Lage sein muss, dynamisch zu entscheiden, wann ein Pseudonymwechsel durchgeführt werden muss. In kritischen Situationen soll ein Pseudonymwechsel vermieden werden, um die Funktionalität der Anwendungen auf der AU nicht zu gefährden.

Für die Verschlüsselung ausgehender Nachrichten werden die folgenden Daten an den Security Daemon geleitet:

- Zu verschlüsselnde Nachricht als Bytearray
- Sicherheitsnachrichtentyp als Parameter von SIM-NET, womit der Security Daemon die vorher definierten Absicherungsanweisungen zuordnen kann.
- Empfängerinformation

Rückgabewerte des Security Daemons sind:

- Verschlüsselter Payload
- Security Header
- Information über Bearbeitungserfolg (Erfolg, Fehler)

Für die Verschlüsselung des Payloads wird ein symmetrischer Schlüssel verwendet der eine schnellere Abarbeitung garantiert als eine Verschlüsslung mit dem asymmetrischen Schlüssel. Die notwendigen Schritte zum Verschlüsseln einer ausgehenden Nachricht sehen wie folgt aus:

1. SIM-NET erstellt das Netzwerk-Paket.
2. SIM-NET liefert dem Security Daemon den Payload als Byte Array im Klartext sowie den Sicherheitsnachrichtentyp und die Empfängerinformationen
3. Der Security Daemon erzeugt einen neuen symmetrischen Schlüssel und verschlüsselt anschließend den Payload damit. Dieser symmetrische Schlüssel wird nun mit dem öffentlichen Schlüssel des Zielknotens verschlüsselt und zusammen mit dem Ende-zu-Ende Security Header und dem verschlüsselten Payload zurück zu SIM-NET geschickt.
4. SIM-NET fügt dem in Schritt 1 erstellten Netzwerkpaket, den Security Header hinzu und tauscht den originalen, unverschlüsselten Payload gegen den verschlüsselten Payload aus, der vom Security Daemon zurückgegeben wurde. Die Nachricht beinhaltet nun: Netzwerk Header, (Ende-zu-Ende) Security Header, verschlüsselten Payload
5. SIM-NET versendet das Paket.

5.3.4.4 [M_ITS_DECRYPT] Entschlüsselung

Für die Entschlüsselung eingehender Nachrichten werden die folgenden Daten an den Security Daemon geleitet:

- Verschlüsselter Payload als Bytearray
- Security Header als Bytearray

Rückgabewerte des Security Daemons sind:

- Entschlüsselter Payload im Klartext
- Ergebnis der Verifikation (Erfolg, Grund für einen Fehler)

Die Schritte zum Entschlüsseln einer empfangenen Nachricht sehen wie folgt aus:

1. SIM-NET empfängt Nachricht
2. SIM-NET sendet dem Security Daemon den verschlüsselten Payload den entsprechenden Ende-zu-Ende Security Header.
3. Der Security Daemon extrahiert den verschlüsselten symmetrischen Schlüssel aus dem Security Header und entschlüsselt ihn mit dem privaten Schlüssel des eigenen Pseudonyms. Anschließend wird der Payload mit dem symmetrischen Schlüssel entschlüsselt und zusammen mit dem Verifikationsergebnis bzw. dem Grund eines Fehlschlags an SIM-NET zurück gegeben.
4. Falls kein Fehler aufgetreten ist, leitet SIM-NET das Paket für die weitere Verarbeitung an den Network & Transport Layer weiter.

5.3.4.5 [M_ITS_PLAUS] Plausibilitätsprüfung

Die Plausibilitätsprüfung in sim^{TD} ist auf der AU in dem Sicherheitsbundle „Plausibilitätsprüfer“ untergebracht. Das Bundle ist in dem Kommunikationsweg aller C2X-Nachrichten integriert und kann somit die Inhalte, primär die Mobilitätsdaten, bewerten. Durch die Plausibilitätsprüfung werden die folgenden Bedrohungen adressiert:

- Von einem authentischen Akteur wird eine authentische Nachricht erzeugt, deren Inhalt jedoch fehlerhaft ist.
    - Fehlerhafte Hardwaresensoren oder fehlerhafte Software können dazu führen, dass falsche Signale von authentischen Teilnehmern unbemerkt versendet werden.
    - Da das Schlüsselmaterial in sim^{TD} nicht durch Hardware (TPD) geschützt wird, können die privaten Schlüssel von Angreifern ohne großen Aufwand missbraucht werden um falsche Informationen zu versenden.
- In sim^{TD} können evtl. nicht jederzeit alle Nachrichten verifiziert werden, da keine hardwarebeschleunigte Kryptografie zur Verfügung steht. Daher kann eine effiziente Plausibilitätsprüfung einen Hinweis auf einen Angriff geben.

Sobald eine nicht-plausible Nachricht entdeckt wurde, wird diese als nicht-vertrauenswürdig markiert. Die Anwendungen können daraufhin entsprechend mit den Nachrichten verfahren. Es kann evtl. sinnvoll sein, die nicht-plausible Nachricht mit geringer Gewichtung zu verwenden und anschließend auf weitere vertrauenswürdige Nachrichten mit dem gleichen Inhalt zu warten.

Eine grundlegende Prüfung der Wertebereiche der Mobilitätsdaten stellt die Basis der Plausibilitätsprüfung dar. Mit Hilfe dieser Prüfung können zum Beispiel Replay-Attacken erkannt werden, bei denen veraltete Nachrichten erneut in das System eingespielt werden.

Anhand des Timestamps kann festgestellt werden, ob die Nachricht aktuell oder veraltet ist und nicht weiter beachtet werden darf. Für die Prüfung ist dabei jedoch immer die Nachricht im Kontext der Absenderposition zu bewerten. Bei einer Nachricht die aus einem entfernten Gebiet abgesendet wurde und per Multihop- oder Store-and-Forward-Übertragung empfangen wurde, sind andere Bewertungskriterien zu wählen als bei Nachrichten aus dem direkten Empfangsgebiet. Die folgenden Werte aus den C2X-Nachrichten werden für die Prüfung einbezogen:

- Station ID
- Timestamp
- Position (Longitude, Latitude)
- Geschwindigkeit
- Fahrtrichtung
- Beschleunigung
- Genauigkeitswerte zur Position, Geschwindigkeit und Richtung
- Informationen der Transportschicht (Packet Type, Content Type, Content Subtype)
- Fahrzeugabmessungen
- Sendefrequenz von C2X-Nachrichten

Die Prüfung der Sendefrequenz dient dazu, DoS-Angriffe zu erkennen. Da der Plausibilitätsprüfer keine eigene Filterung von Nachrichten vornimmt, können die Angriffe nicht verhindert werden. Durch eine Erkennung eines Fehlverhaltens kann jedoch die Quelle identifiziert und im Nachhinein revoziert werden. Außerdem werden nicht-plausible Nachrichten als erstes aus der Umfeldtabelle gelöscht, wenn eine Überfüllung droht. Ein DoS-Angriff kann somit nicht mit einer Flutung der Umfeldtabelle die Kommunikation behindern.

Neben der Prüfung der Wertebereiche können die Mobilitätsdaten der Nachrichten zu einer Verfolgung (*Tracking*) aller benachbarten Fahrzeuge im direkten Empfangsbereich genutzt werden. Mit dieser Prüfung kann festgestellt werden, ob das Verhalten des Absenders plausibel ist oder er durch nicht-plausibles Auftreten bösartig oder ungewollt falsche bzw. störende Informationen verbreitet. Eine zentrale Plausibilitätsprüfung kann die Positionen aller C2X-Nachrichten zu einem Bewegungsmodell umsetzen und somit zum Einen fehlerhafte Daten identifizieren und zum Anderen nicht plausible Absender entdecken. Sybil-Attacken, bei denen ein Absender gleichzeitig mehrere Pseudonyme verwendet, um das Verkehrsbild zu beeinflussen, können von der Plausibilitätsprüfung in einigen Fällen erkannt werden. Dabei ist zwischen bösartigen Angreifern zu unterscheiden, die mit externen Kommunikationsmitteln (z.B. Laptop) Nachrichten einspielen und manipulierten Fahrzeugen. Durch den mangelnden Schutz des Schlüsselmaterials auf dem Fahrzeug im sim^{TD} Feldtest ist die Erkennung solcher Fehl- oder Angriffsverhalten sehr wichtig. Die Plausibilitätsprüfung verfolgt die Fahrzeuge in der direkten Nachbarschaft und ist somit auch in der Lage, über einen Pseudonymwechsel hinaus ein Fahrzeug zu identifizieren. Da die Daten aber nur innerhalb des Fahrzeuges verwendet werden und auch nur Fahrzeuge im Empfangsradius getrackt werden können, wird der Schutz der Privatsphäre nicht gefährdet. Dieses Tracking der C2X-Teilnehmer wird weiterhin für eine fahrzeuginterne Identifizierung der benachbarten Teilnehmer verwendet. Da jede eingehende Nachricht durch den Plausibilitätsprüfer geleitet wird, kann dieser eine eigene ID in die C2X-Nachricht schreiben um Fahrzeuge über einen Pseudonymwechsel hinaus zu identifizieren.

Alle Anwendungen der Vehicle AU können auf die Daten der Plausibilitätsprüfung zugreifen, um eine Entscheidungshilfe für deren eigene interne Prüfungen zu bekommen. Für die Funktionen ist es nur sinnvoll, die inhaltlichen Daten der C2X-Nachrichten (Verkehrslage, Ampel-

phasen, Wetter, etc.) zu prüfen, aber nicht die Bewegungsinformationen der Absender, die in allen Nachrichten enthalten sind. Die Ergebnisse der Plausibilitätsprüfung werden mit dem Resultat der Verifikation in den C2X-Message-Objekten in der Umfeldtabelle abgelegt. Des Weiteren wird für jeden C2X-Teilnehmer im Empfangsbereich eine eindeutige ID vergeben, die das Fahrzeug auch über einen Pseudonymwechsel hinaus identifiziert. Diese Zuordnung wird lediglich innerhalb des Fahrzeugs bzw. der Roadside Station durchgeführt und nicht mit externen Quellen abgeglichen. Die Anwendungen auf der AU basieren teilweise auf konstanten IDs die den Teilnehmer zugeordnet sind. Ein Pseudonymwechsel würde diese Zuordnung zerstören und die Funktionalität der Anwendungen beeinträchtigen. Deshalb wird das Tracking des Plausibilitätsprüfers genutzt um eine konstante ID zu vergeben.

Der Plausibilitätsprüfer kann zusätzlich auch für eine CAM-Prädikation genutzt werden. Das heißt mit Hilfe des Trackings kann die Mobilität eines Fahrzeuges vorausberechnet werden. Bei Bedarf kann die zukünftige Position eines Teilnehmers in die C2X-Nachricht geschrieben werden und in der Umfeldtabelle zur Verfügung gestellt werden.

Wie in Abbildung 5.16 dargestellt, hat der Plausibilitätsprüfer eine Schnittstelle mit dem Communication Client der AU. Da die Plausibilitätsprüfung in sim^{TD} essentiell für die interne Identifizierung der benachbarten Teilnehmer ist, darf diese nicht von der grundlegenden Kommunikation abgekoppelt werden.

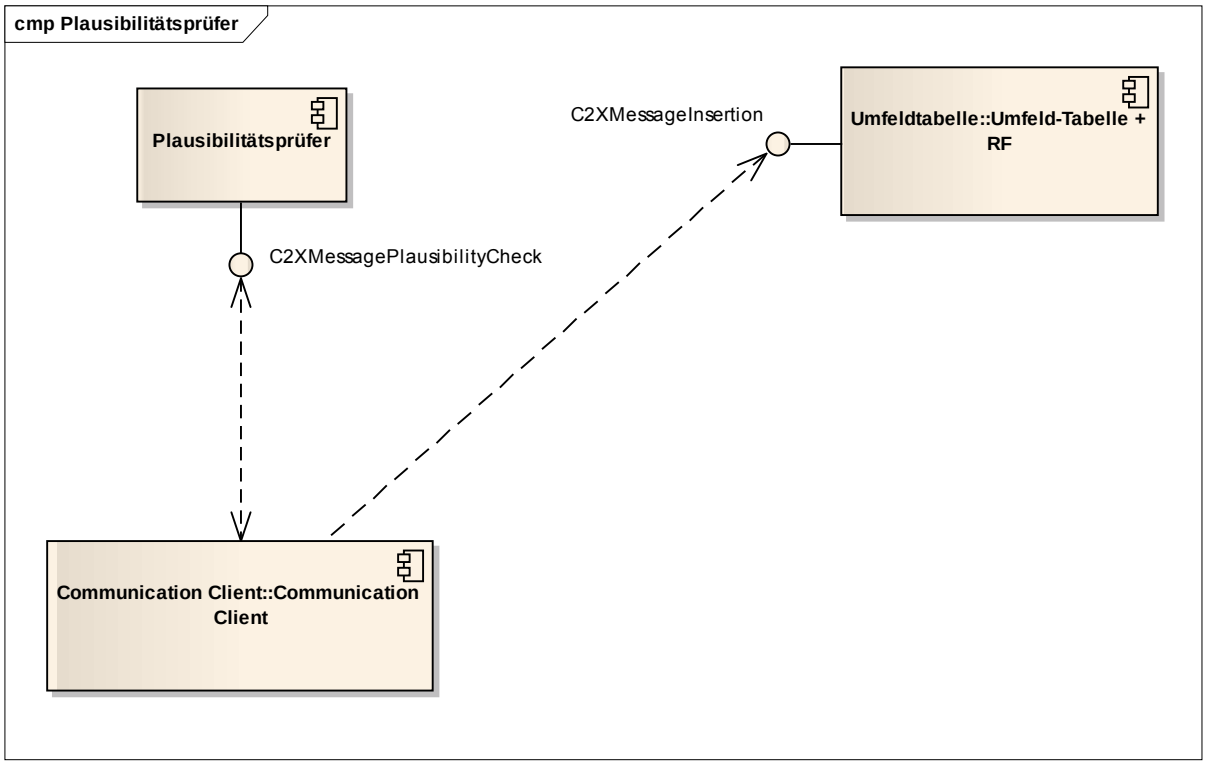

Abbildung 5.16: Schnittstellen des Plausibilitätsprüfers

Der Communication Client prüft beim Start durch einen OSGi Service Tracker, ob der Service des Plausibilitätsprüfers zur Verfügung steht. Wenn das der Fall ist, wird der Service beziehungsweise die Schnittstelle „C2XMessagePlausibilityCheck“ genutzt und bei jeder eingehenden C2X-Nachricht werden folgende Schritte abgearbeitet:

1. Der Communication Client übergibt das C2X-Nachrichtenobjekt dem Plausibiltitäsprüfer.
2. Das Ergebnis der Prüfung und eine intern eindeutige Knoten ID wird direkt in das Nachrichtenobjekt geschrieben.

3. Das gleiche C2X Nachrichtenobjekt mit den erweiterten Security-Informationen wird an den Communication Client zurückgegeben.
4. Der Communication Client leitet die C2X-Nachricht über die Schnittstelle „C2XMessageInsertion“ an die Umfeldtabelle weiter.

Wenn das OSGi-Bundle des Plausibilitätsprüfers deaktiviert ist, steht dem Communication Client der entsprechende Service nicht zur Verfügung. In diesem Fall werden alle Nachrichten ohne eine Plausibilititätsprüfung an die Umfeldtabelle gegeben. Abbildung 5.17 stellt den Aufruf der Plausibilitätsprüfung auf der AU als Sequenzdiagramm dar.

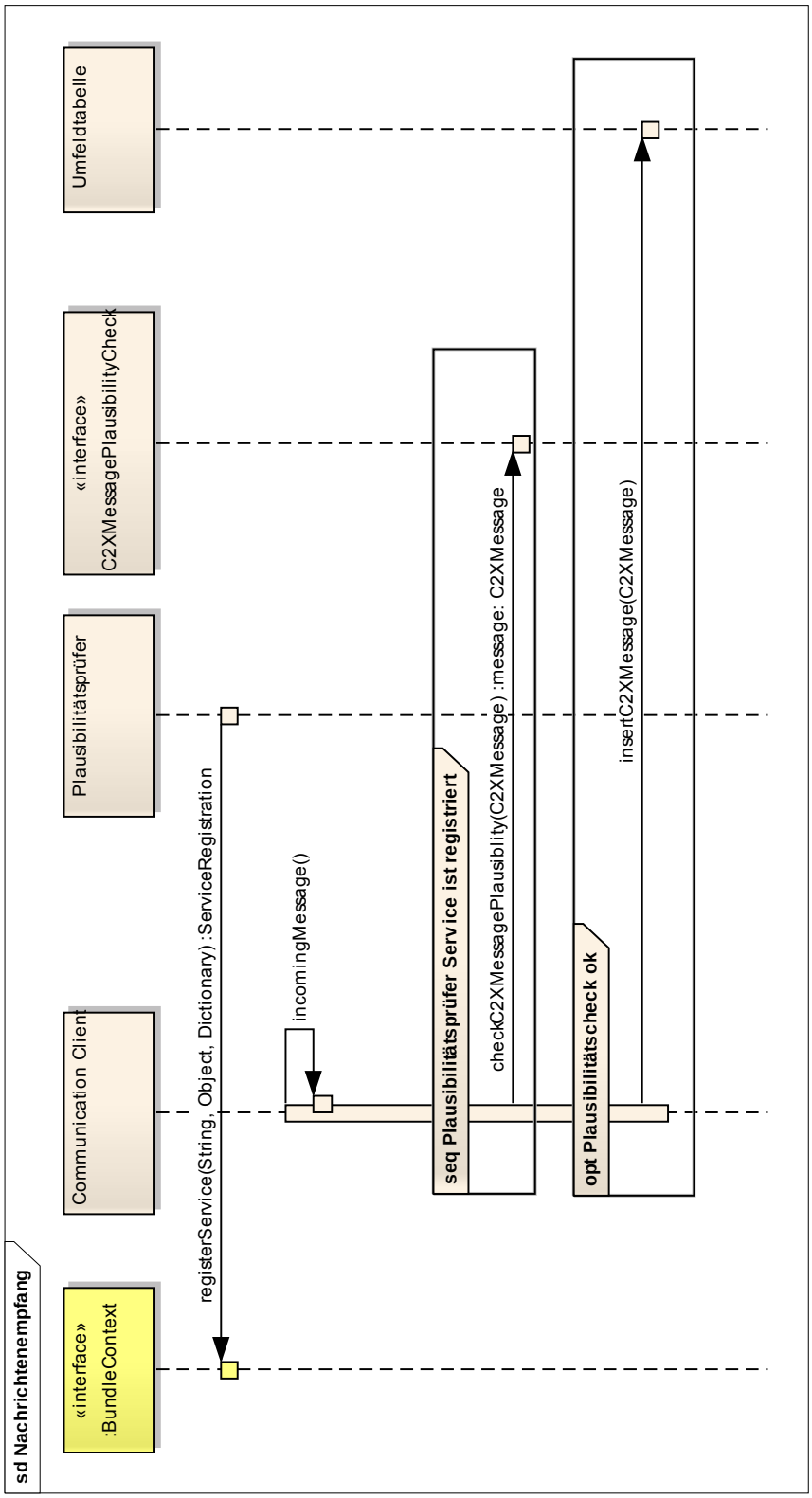

Abbildung 5.17: Sequenzdiagramm: Plausibilititätsprüfung auf der AU

5.3.5 WLAN 802.11 b/g

Es werden hier grundsätzlich drei verschiedene Anwendungsfälle für die Datenübertragung über Consumer-WLAN unterschieden. Dies beinhaltet zum einen die Übertragung im Infra-

strukturmodus, welche auf dem Testgelände und auf Parkplätzen möglich ist, zum zweiten die Ad-Hoc-Verbindung zwischen Fahrzeug und IRS bzw. zwischen Fahrzeugen und die dritte Möglichkeit ist die Übertragung von anwendungsspezifischen Daten. In Abbildung 5.18 wird eine Übersicht, der für die C-WLAN-Kommunikation genutzten Verbindungen dargestellt. Komponenten für die Kommunikationsabsicherung sind in rot dargestellt und werden in den folgenden Abschnitten näher erläutert.

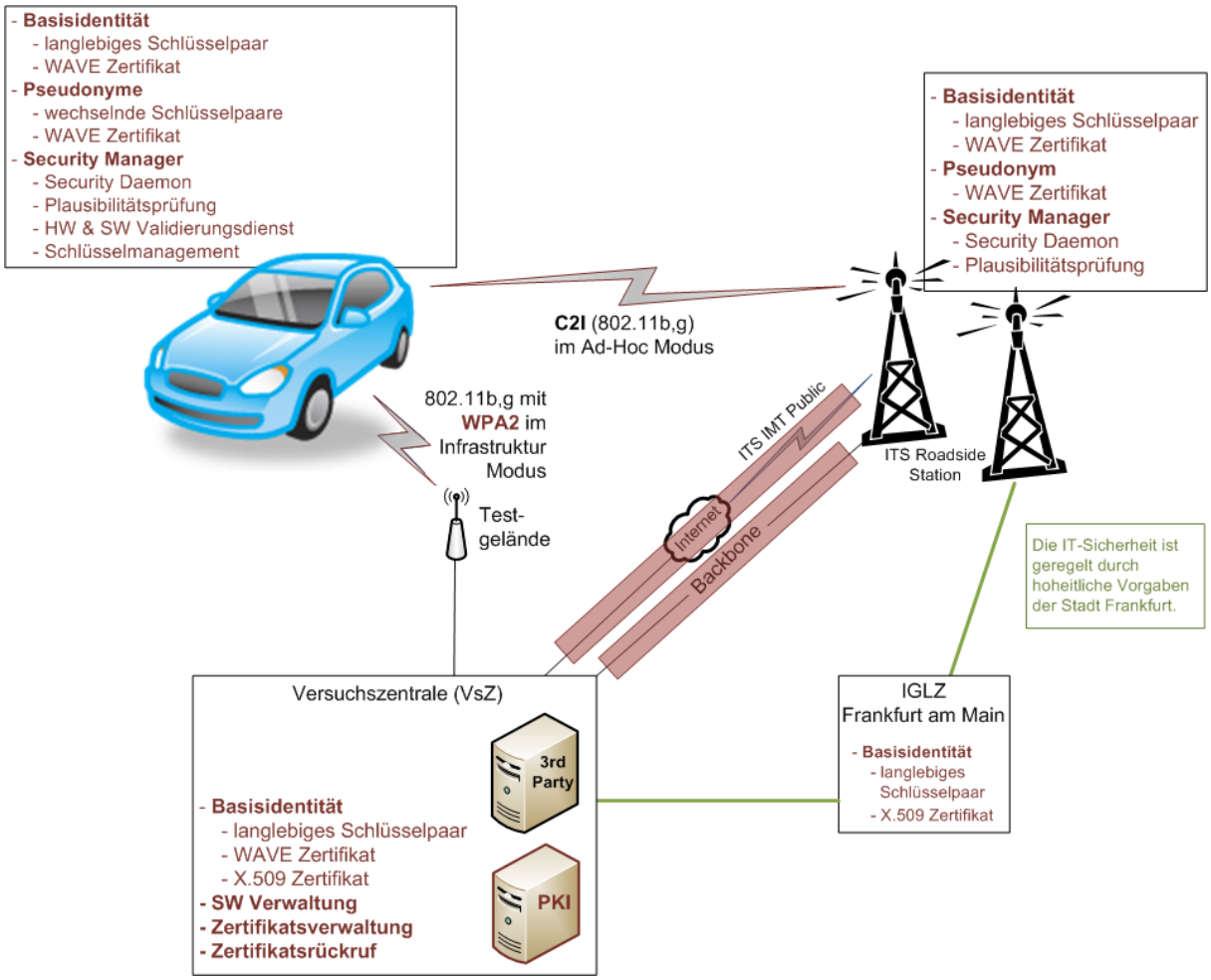

Abbildung 5.18: Einsatz von kommerziellen WLAN IEEE 802.11 b/g

5.3.5.1 Infrastrukturmodus

Bei der Kommunikation über den Infrastrukturmodus verbindet sich das Fahrzeug über aufgestellte Access Points mit der Versuchszentrale, wie in Abbildung 5.19 dargestellt. Es werden bei sim^{TD} keine öffentlichen Access Points eingesetzt. So kommen diese nur an ausgewählten Stellen zum Einsatz, wie z.B. auf dem Testgelände. Nur über diese Access Points ist eine TCP-Verbindung zur Versuchszentrale möglich. Aufgrund dieser nicht öffentlichen Ausrichtung erfolgt die Absicherung der Kommunikation im Infrastrukturmodus über die C-WLAN eigene Absicherung WPA2 mit Pre-Shared-Keys. Falls die WPA2 Schlüssel kompromittiert werden, muss ein manueller Austausch in allen Fahrzeugen erfolgen. Da nur sim^{TD} interne Access Points verwendet werden, brauchen keine automatisierten Verteildienste genutzt werden.

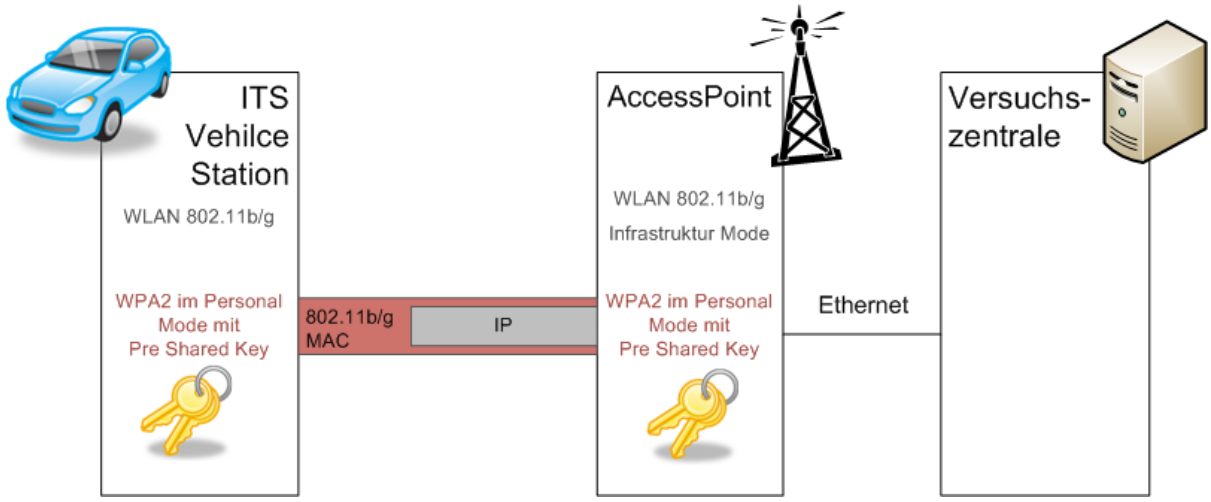

Abbildung 5.19: Absicherung der C-WLAN-Kommunikation im Infrastrukturmodus

5.3.5.2 IEEE 802.11b/g als IEEE 802.11p Ersatz

Bei der Ad-Hoc-Verbindung mit der IRS bzw. mit anderen Fahrzeugen soll ein Vergleich von IEEE 802.11p und IEEE 802.11b/g WLAN möglich werden. Des Weiteren wird dies eingesetzt, um eine möglichst frühzeitige Testung der C2C-Protokoll-Stacks in sim^{TD} sicherstellen zu können. Diese Kommunikation kann analog zu der Absicherung von WLAN über 802.11p mit dem Security Deamon (Abschnitt 5.3.4) abgesichert werden. Die Absicherung erfolgt über Layer 3 Mechanismen. Hierbei sind dann keine weiteren Maßnahmen notwendig.

5.3.5.3 Ad-Hoc-Modus für anwendungsspezifische Datenübertragung

Weiterhin besteht die Möglichkeit bei sim^{TD} noch weitere anwendungsspezifische Daten zu übertragen. Je nach Anwendung müssen diese Daten signiert und/oder verschlüsselt übertragen werden. Hierdurch können Authentizität, Integrität und gegebenenfalls Vertraulichkeit (nur bei Unicast-Nachrichten möglich) sichergestellt werden. Für die Absicherung kann der Security-Daemon verwendet werden. Dieser muss jedoch von der Anwendung selbst aufgerufen werden, damit die Daten entsprechend abgesichert werden. Abbildung 5.20 stellt die Absicherung der anwendungsspezifischen Kommunikation dar.

Die ITS Roadside Station stellt ein offenes Ad-hoc WLAN-Netzwerk zur Verfügung, zu dem sich jedes Fahrzeug und prinzipiell auch jeder Computer verbinden kann. Die WLAN Kommunikationseinheit in der ITS Vehicle Station und ITS Roadside Station muss also dementsprechend stabil sein, so dass nur anwendungsspezifische Nachrichten mit einer korrekten Absicherung der Nachrichteninhalte akzeptiert und weiterverarbeitet werden.

Der Security-Overhead der anwendungsspezifischen Daten muss bei der zu übertragenden Nachricht berücksichtigt werden. Soll eine Nachricht z.B. signiert werden, so ist hierfür mit bis zu 310 zusätzlichen Bytes zu rechnen. Es sollte darauf geachtet werden, dass die maximale MTU der Schnittstellen nicht überschritten wird, damit die Nachricht ohne Fragmentierung übertragen wird. Eine Fragmentierung würde das Risiko für Übertragungsfehler erhöhen und evtl. eine manuelle Mehrfachübertragung erfordern, da das verbindungslose UDP Protokoll verwendet wird.

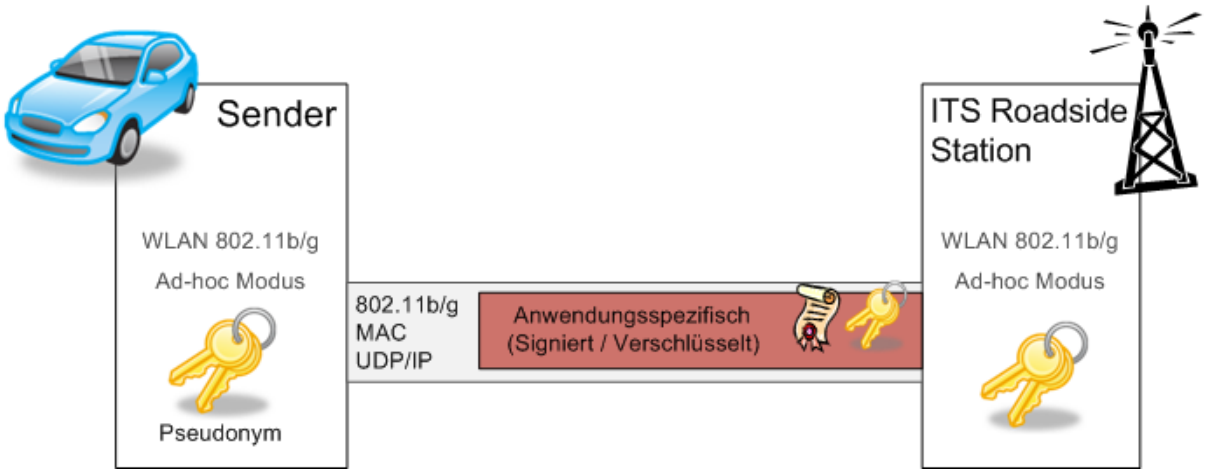

Abbildung 5.20: Absicherung der C-WLAN-Kommunikation im Ad-hoc-Modus

Das Sequenzdiagramm in Abbildung 5.21 stellt die Vorgehensweise beim Versenden von anwendungsspezifischen Nachrichten dar.

1. Die Anwendung ruft das OSGi-Bundle der Kommunikationsabsicherung auf und übergibt die Nachricht als Bytearray, sowie Parameter, die bestimmen ob die Nachricht nur signiert oder zusätzlich verschlüsselt werden muss. Bei der Verschlüsselung muss außerdem die MAC-Adresse des Ziels angeben werden. Die Kodierung der Nachricht innerhalb der Anwendung spielt für die Kommunikationsabsicherung keine Rolle.
2. Das Bundle der Kommunikationsabsicherung auf der AU baut eine Socketverbindung zur Kommunikationsabsicherung der CCU (Security Daemon) auf und übergibt die Nachricht als Bytearray sowie die Parameter zur Absicherung.
3. Der Security Daemon erstellt eine sichere Nachricht nach IEEE 1609.2 und signiert bzw. verschlüsselt die Daten entsprechend. Die sichere Nachricht wird nun als Bytearray an das OSGi-Bundle der Kommunikationsabsicherung auf der AU zurück geschickt.
4. Der Kommunikationsabsicherungsclient (Security Daemon Client) gibt die sichere Nachricht an die Anwendung zurück.
5. Die Anwendung sendet die Daten per UDP/IP an das OSGi-Bundle *Java TCP/IP* und legt einen bestimmten Port fest, über die die Anwendung erreichbar ist. Die IP Nachricht wird anschließend über das Ad-Hoc Netzwerk per C-WLAN übertragen.

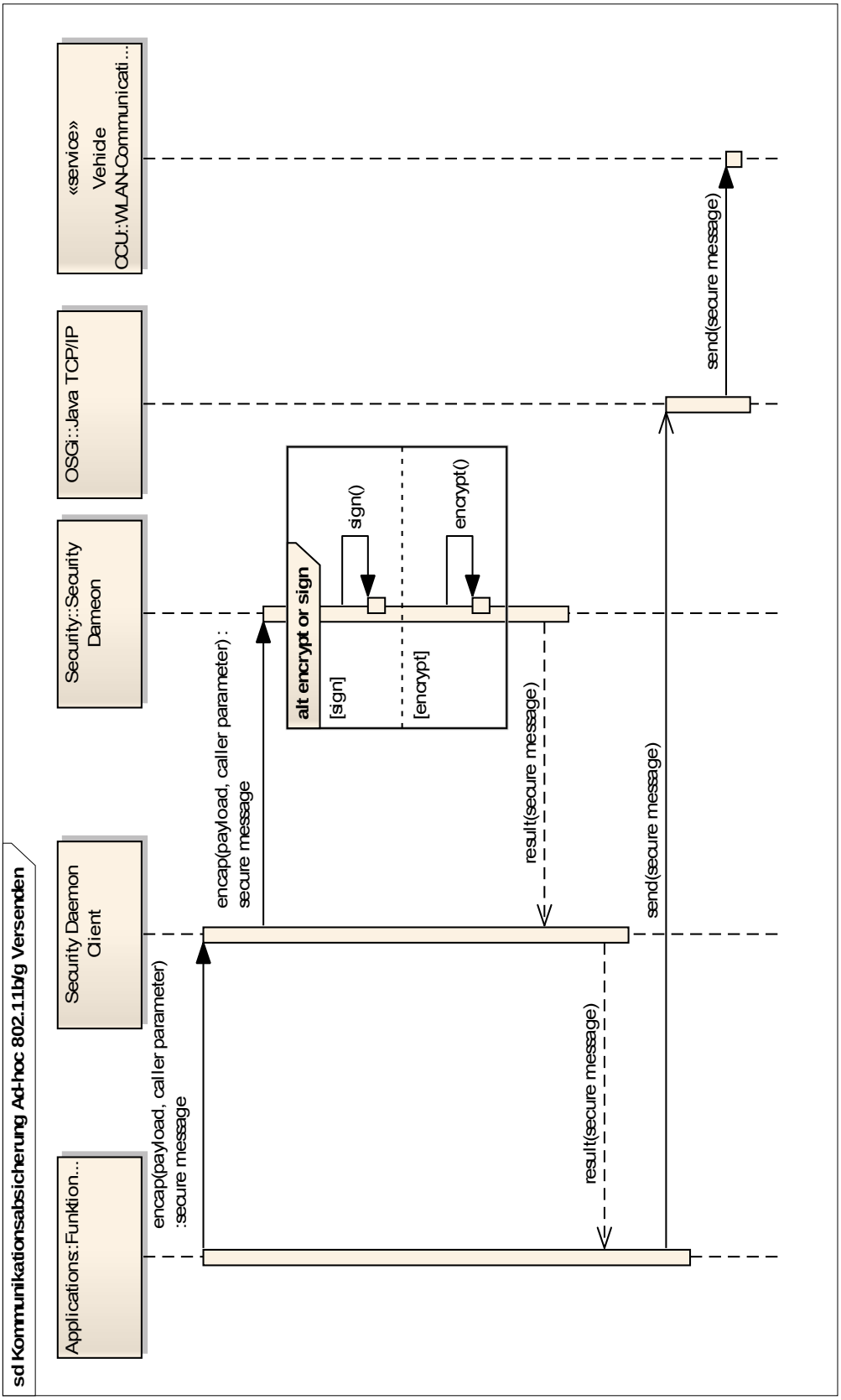

Abbildung 5.21: Sequenzdiagramm: Versand von anwendungsspezifischen Nachrichten über Ad-Hoc C-WLAN

Der Empfang von anwendungsspezifischen Nachrichten per Ad-Hoc C-WLAN wird in Abbildung 5.22 illustriert und im Folgenden beschrieben.

1. Die CCU-WLAN-Komponente hat mit einer ITS Roadside Station eine Ad-hoc-Verbindung aufgebaut und bekommt von dieser eine UDP/IP Nachricht mit einer bestimmten Portnummer.
2. Anhand dieser Portnummer wird das Paket von der OSGi Java TCP/IP Komponente an die entsprechende Anwendung geleitet.
3. Die Anwendung ruft das OSGi Bundle der Kommunikationsabsicherung und übergibt die sichere Nachricht als Bytearray.
4. Das Bundle der Kommunikationsabsicherung auf der AU baut einen Socket zur Kommunikationsabsicherung der CCU (Security Daemon) auf und übergibt die Nachricht als Bytearray.
5. Der Security Daemon entschlüsselt bzw. verifiziert die sicherer Nachricht und gibt den Payload als Bytearray zurück zur eigenen OSGi Komponente, von wo aus es an die Anwendung durchgereicht wird.

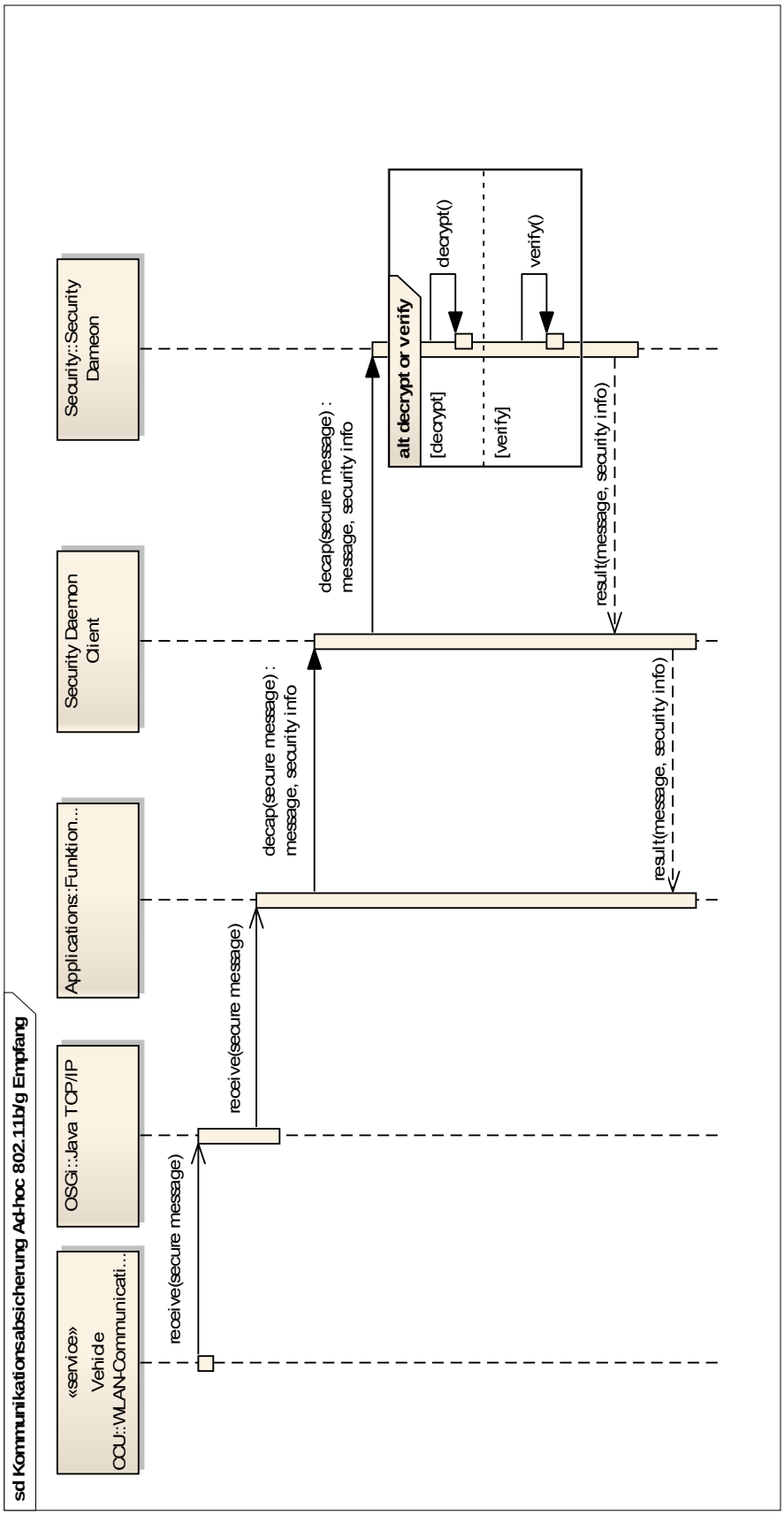

Abbildung 5.22: Sequenzdiagramm: Empfang von anwendungsspezifischen Nachrichten über Ad-Hoc C-WLAN

5.3.6 ITS IMT Public

Im Rahmen von sim^{TD} sind die Sicherheitsanforderungen im Vergleich zum Wirksystem geringer, aber für einen realistischen Test der IT-Sicherheitsfunktionen sollte dennoch versucht werden, möglichst nahe an die voraussichtlichen Sicherheitsarchitektur eines Wirksystems heranzukommen.

5.3.6.1 [M_Cell_Sec] Ende-zu-Ende-Absicherung der IP-Kommunikation via Mobilfunk

Für realistische und aussagekräftige Tests ist es generell sehr wünschenswert, die Maßnahme auch im Rahmen von sim^{TD} zu erproben. Sollte es aber beim Einsatz zu massiven Problemen kommen, wie z.B. zu hoher Last auf der CCU, wäre im Rahmen von sim^{TD} auch die optionale Sicherheitsmaßnahme [M_Cell_VN] alleine tragbar, bei der auf eine eigene Absicherung der Kommunikation verzichtet wird und Lösungen des Mobilfunkbetreibers eingesetzt werden.

5.3.6.2 [M_Cell_IP_Change] Zufälliger Wechsel der IP-Adressen

Es wäre sehr wünschenswert, die in Abschnitt 5.2.6.2 beschriebene Maßnahme auch bei sim^{TD} umzusetzen und zu testen, allein damit man erkennt, ob IP-Adressen hinreichend zufällig zugewiesen werden.

Die Verwendung von Mobile IP mit statischen primären Adressen oder IPv4 mit statischen Adressen in sim^{TD} ist möglich. Da allerdings über statische IP-Adressen Pseudonyme miteinander verknüpft und Fahrzeuge identifiziert werden können, ist in jedem Fall dafür zu sorgen, dass die Kommunikation über ITS IMT Public unterhalb der IP-Schicht verschlüsselt und außerdem der Zugang zum Mobilfunk-IP-Subnetz nicht öffentlich ist. Ersteres wird in sim^{TD} durch die UMTS-Verschlüsselung auf der Luftschnittstelle erreicht, während letzteres durch Verwendung eines sim^{TD}-spezifischen APN im Rahmen der T-Mobile Mobile IP VPN Lösung (siehe Anhang A) umgesetzt wird.

5.3.6.3 [M_Cell_VN] Virtuelles Netz für die Mobilfunkkommunikation

Bei dieser Maßnahme wird der gesamte IP-Verkehr, der via Mobilfunk übertragen wird, direkt vom Mobilfunknetz an einen zentralen Übergabepunkt geleitet, so dass der Verkehr nicht über das öffentliche Internet laufen muss.

Sieht man das standardmäßige Sicherheitsniveau in Mobilfunknetzen und die Verschlüsselung der Funkschnittstelle als ausreichend an, siehe auch Abschnitt 5.1.6, ist somit ein hinreichender Schutz der Datenübertragungen via Mobilfunk im Rahmen des sim^{TD} Feldversuchs gegeben. Für die Umsetzung dieser Maßnahme muss der im Rahmen der Tests eingebundene Mobilfunkbetreiber die Möglichkeit bieten, ein virtuelles IP-Netz via Mobilfunk aufzubauen, das sich hinreichend umfassend administrieren lässt. Im 0 findet sich eine kurze Beschreibung eines entsprechenden Produktes von T-Mobile: *Mobile IP VPN basic.*

Bei einem so aufgebauten virtuellen Netz wird der der Datenverkehr für eine geschlossene Benutzergruppe im Mobilfunknetz zu einem Übergabepunkt geleitet, von dem aus ein IPSec-Tunnel über das (öffentliche) Internet zu einem IPSec-fähigen Eingangsrouter führt, s.a. Maßnahme [M_ITS_VPN] in Abschnitt 5.2.3.3. Das Sicherheitsniveau der Luftschnittstelle entspricht in diesem Fall der im Mobilfunknetz üblichen Sicherheit, s. Abschnitt 5.1.6; im Festnetz-Anteil des Mobilfunknetzes werden die Daten allerdings unverschlüsselt transportiert.

5.3.6.4 C2X via Mobilfunk

Für die Übertragung von C2X-Nachrichten zwischen Fahrzeugen und von der Versuchszentrale zu Fahrzeugen wird ein Geo-Server eingesetzt der eingehende Nachrichten per ITS IMT Public an Fahrzeuge in einem bestimmten geografischen Gebiet spiegelt. Damit dieser Server stets die IP-Adressen aller Fahrzeuge zu einem geografischen Gebiet zuordnen kann, müssen regelmäßige Nachrichten (Beacons) von den Fahrzeugen zum Geo-Server übertragen werden. Jedes Beacon wird als CAM Nachricht durch den Security Daemon auf der CCU signiert und anschließend per ITS IMT Public versendet. Auch die Absicherung der C2X-Nachrichten wird wie bei der IEEE 802.11p Kommunikation durch den Security Daemon signiert. Eine verschlüsselte Übertragung von C2X-Nachrichten per Unicast ist in sim^{TD} nicht vorgesehen.

5.3.7 Ausfallsicherheit

Der in diesem Abschnitt behandelte Inhalt ist aus den Ergebnissen des Kapitels 5.1.7 abgeleitet. Diese liefern wertvolle Aspekte für den Einsatz im Projekt sim^{TD}. Dabei muss zwischen drei Systemen unterschieden werden, deren Hard- und Softwarearchitektur für den effizienten Gesamtbetrieb ausgelegt sind:

- IVS
- IRS, ICS (AU)
- ICS (IRSMC)

5.3.7.1 [M_ITS_AS_OS] Auswahl des Betriebssystems

Sowohl auf den Servern des IRS Management Centers [ICS (IRSMC)] (64bit), als auch auf die Roadside Application Unit (RAU) (32bit) wird Ubuntu 8.04 LTS Server Edition (Long Time Support bis 2013) als Betriebssystem eingesetzt. Der Ubuntu Server basiert auf dem als soliden und als zuverlässig bekannten Betriebssystem von Debian GNU/Linux. Auf der VAU kommt WindowsXP Embedded zum Einsatz und auf ICS (AU) Solaris 10.

Die Auswahl des Betriebssystems oblag dabei den jeweiligen verantwortlichen Partnern. Diese führten die Auswahl unhängig voneinander nach ihren eigenen Bedürfnissen und Ressourcen durch.

5.3.7.2 [M_ITS_AS_ICS_M] Sicherheitsarchitektur der ICS (IRSMC)

Auf den Servern des IRS Management Centers werden virtuelle Maschinen als Grundlage für die Load-Balancer, IRS-Management-Server (IRSMS) und Datenbank-Server eingesetzt. Es können dabei auch mehrere gleichartige Instanzen einer Serverart zur gleichen Zeit koexistieren.

Im Zentrum des IRSMC steht der IRSMS. Er bearbeitet auf mehreren Instanzen lastverteilt alle Anfragen und notwendigen Prozesse. Die Verteilung der Anfragen findet vor den IRSMS statt. Hier kommen die Anfragen der IRS an und werden von den Load-Balancer gleichmäßig auf die vorhandenen IRSMS verteilt.

Aufgrund der Arbeitsbelastung eines Load-Balancers (LB) sind im Testfeld zwei Instanzen geplant. Die eingesetzte Struktur der vorgesetzten Load-Balancer ist eine Master-Slave-Topologie. Bei dieser Betriebsart übernimmt einer der Server (der Master) alle Anfragen. Dieser ist via Heartbeat mit dem zweiten Server (Slave) verbunden. Fällt der Master aus oder ist nicht mehr erreichbar, so übernimmt der Slave die Funktion der Lastverteilung. Für Anfragen von außen bleibt die IP-Adresse des IRSMC immer die gleiche. Dies wird durch

eine virtuelle Netzwerkadresse erreicht. Kommt es zu einem Ausfall, so nimmt der Slave die IP-Adresse des Masters an.

Die Daten und virtualisierten Maschinen werden dabei entweder auf lokalen Servern oder einem SAN vorgehalten. Das notwendige Backup soll entweder auf dem SAN oder einem externen Backup erfolgen.

Alle Server sind durch eine unterbrechungsfreie Stromversorgung (USV) gegen Stromausfälle abgesichert.

5.3.7.3 [M_ITS_AS_IRS] Sicherheitsarchitektur der IRS

Im Folgenden sind die geplanten Bestandteile der IRS AU (RAU) vorgestellt, in deren Mittelpunkt das RAU Fallback and Recovery System steht:

- Hardware-Watchdog
- Rettungssystem bestehend aus Notfallsystem und Reparatursystem
- Notfallsystem mit minimaler IRS-Funktionalität (basierend auf einer RAM-Disk)
- Reparatursystem mit Fault-Management-Client
- Standardbetriebssystem eingebettet in mehrschichtiges Dateisystem auf der Basis von AUFS (Another Union File System)

5.3.7.4 [M_ITS_AS_IVS] Sicherheitsarchitektur des IVS

Auf der IVS AU (VAU) sind keine Maßnahmen zur Ausfallsicherheit des Systems geplant.

5.3.7.5 [M_ITS_AS_CCU] Sicherheitsarchitektur der CCU

Auf der CCU sind keine Maßnahmen zur Ausfallsicherheit des Systems geplant.

5.3.7.6 [M_ITS_AS_ICS_A] Sicherheitsarchitektur der ICS

Die Server sind redundant ausgelegt. Die anfallenden Daten werden auf einem SAN-System redundant gespeichert.

Alle Funktions- und PKI-Server werden durch eine unterbrechungsfreie Stromversorgung (USV) gegen Stromausfälle abgesichert.

5.3.8 Organisatorische und rechtliche Maßnahmen

Vom Wirksystem unterscheidet sich das sim^{TD} System vor allem durch die Tatsache, dass das System zur Durchführung von Fahrversuchen verwendet werden soll. Damit liegt der Verwendungszweck persönlicher Daten im Bereich der Forschung und nicht der kommerziellen Verwertung. Darüber hinaus kann von den Fahrern der Versuche ein Maß an Kooperation bei der Verarbeitung personenbezogener Daten vorausgesetzt werden, wie dies im Wirksystem nicht der Fall sein dürfte. Dennoch ergeben sich gerade für das sim^{TD} System eine Reihe von Maßnahmen, die für das Gelingen der Versuche und ein positives Bild in der Öffentlichkeit unerlässlich sind:

- Im Rahmen von AP53 ist zu prüfen, ob ein Datenschutzbeauftragter für simTD erforderlich ist.

- Die Aufhebung der implementierten Sicherheitsmaßnahmen z.B. aufgrund technischer Schwierigkeiten im Versuch ist durch die Gesamtprojektleitung zu veranlassen und zu verantworten.
- Die Versuchsauswertung muss auf pseudonymisierten Daten stattfinden. Wechselnde Pseudonyme sind jedoch für die Versuchsauswertung jederzeit zu einer Basisidentität auflösbar.
- Fahrer müssen im Vorfeld darüber informiert werden, dass ihre Pseudonyme durch die Versuchszentrale aufgelöst werden können und es dadurch möglich ist, Bewegungsprofile von Fahrern zu erstellen.
- Es sind nur die zur Vertragsgestaltung unbedingt notwendigen Daten personalisiert zu erheben.
- Sollten über die Vertragsgestaltung hinaus Daten zur Versuchsplanung, -durchführung und -auswertung erhoben werden müssen, sind diese pseudonymisiert zu speichern (z.B. Einschätzung der eigenen Leistungsfähigkeit als Fahrer).
- Der Zweck der Datenerhebung muss den Versuchsfahrern deutlich gemacht werden.

Aufgrund der Zustimmung der Betroffenen erscheint eine Vorabkontrolle nicht nötig.

5.3.9 Wartung, Verwaltung und Aktualisierung der ITS Stations

In sim^{TD} werden verschiedene Partner für die Integration von CCU, VAU, RAU, CAU verantwortlich sein. Diese Partner entwickeln für ihre jeweilige Komponente eigene Management- und Wartungsfunktionalitäten, die unabhängig von den jeweilig anderen koexistieren, d.h. welche Konzepte (remote oder lokal) für Hard- bzw. Software umgesetzt werden liegt allein in der Verantwortlichkeit des jeweiligen Partners.

5.3.9.1 [M_ITS_WVA_CCU] CCU

Ein initiales System für die CCU wird von Continental als Plattform geliefert. Die Installation, Wartung und Aktualisierung der Anwendungen auf der VCCU erfolgt dabei datenbankgesteuert mit Hilfe eines Update-Clients sowie für das Betriebssystem über die Debian Paketverwaltung. Dazu baut der Update-Client eine SSL-verschlüsselte und zertifizierte Datenverbindung über UMTS zu einem Update-Server auf und ermittelt anhand einer eindeutigen Kennung, ob Updates zur Verfügung stehen. Diese werden dann über die bestehende Verbindung vom Update-Server geladen und nach Verifikation skriptgesteuert auf der VCCU installiert. Betriebssystem-Updates werden skriptgesteuert über die Debian-Paketverwaltung installiert.

5.3.9.2 [M_ITS_WVA_IVS] IVS

a) Software

Ein initiales System wird von Bosch als Plattform geliefert. Die Installation, Wartung und Aktualisierung der Anwendung auf der CAU erfolgt mit Hilfe des mPRM (mPower Remote Management) von ProSyst. Mit diesem System ist es möglich, OSGi Anwendungen (Bundles) zu installieren aber auch zu starten und zu stoppen. Zusätzlich können diese Anwendungen überwacht und bei einem eventuellen Fehlverhalten eingegriffen werden.

[M_ITS_IVS_SW] Für eine sichere Installation, Überwachung und Aktualisierung der Anwendungen auf der CAU bietet das mPRM bietet folgende Sicherheitsmechanismen an:

- Network-level security: Hierzu unterstützt ProSyst TLS 1.0, SSL 3.0 und HTTPS.

- Benutzer-Authentisierung und -Autorisation: einfache bis starke Authentisierung ist möglich. Für letzteres wird die Anwendung von X.509v3-Zertifikaten (auch im Zusammenhang mit zusätzlicher Hardware wie Smartcard) unterstützt. Die Autorisation erfolgt über rollenbasierte Zugriffsmodelle.
- Zertifikatsmanagement System: Verwaltung von Zertifikaten, Signierung und Verifikation von Softwarepaketen, etc.

b) Hardware

Die allgemeinen Anforderungen an die Hardware (genannt CarPC in sim^{TD}) sind im Deliverable D11.4 [10] beschrieben. Die Vorgehensweise beim Ausfall der Hardware wird erst in AP 42 beschrieben.

5.3.9.3 [M_ITS_WVA_IRS] IRS

Die IRS in sim^{TD} wird über ein unfassendes Managementsystem verwaltet und administriert werden. Durch dieses System sollen sowohl Hardwareprobleme entdeckt als auch Software installiert und verwaltet werden können.

a) Software

Ein initiales System wird von der HTW als Plattform geliefert. Die Installation und Aktualisierung der Anwendungen auf der RAU erfolgt mit Hilfe des Debian Paketverwaltungssystems. Alle Pakete – nicht nur die OSGi Bundles – werden über diesen Mechanismus installiert, d.h. sowohl Betriebssystempaket und -updates, eigene Systemdienste und Bundles (eigene und von Partnern) fallen hierunter. Der Installationsprozess (secure-apt) selber läuft dabei skriptgesteuert über https und verlangt signierte Pakete. Es können also nur Pakete installiert werden, deren Echtheit anhand ihrer Signatur verifiziert werden konnte.

Die installierte Software wird dabei von einem Systemdienst überwacht und bei Ausfällen und Fehlverhalten entsprechende Benachrichtigungen an das Management Center geleitet. Für „von Hand“ korrigierte Fehler werden – soweit möglich – in der Zentrale Strategien zur Problemlösung erstellt. Diese können dann, falls die gleichen Fehler nochmals auftreten, automatisiert angewendet und so Probleme schnell und effizient gelöst werden.

[M_ITS_IRS_SW] Neue Versionen der Funktionen werden von dem IRS-Integrator in das zentrale Repository eingepflegt. Von dort werden die Funktionen automatisch der Konfiguration entsprechend auf die IRS verteilt und installiert. Während des gesamten Ablaufes werden dabei automatisch Protokollinformationen in die Datenbank geschrieben. Hierdurch lässt sich jeder Zeit eindeutig feststellen, welche Version einer Funktion zu einem bestimmten Zeitpunkt auf einer IRS installiert bzw. aktiv war.

b) Hardware

Die Anforderungen an die Hardware der IRS sind durch die Ausschreibung so definiert, dass ein 24/7 Betrieb von Seiten der Hardware garantiert werden soll. Eine auf der RAU vorhandene Softwarekomponente überwacht die jeweilige Hardware und informiert bei einem Fehler die ICS (IRSMC). Falls die gesamte IRS ausfällt oder die Kommunikation zwischen IRS und ICS gestört ist, erkennt dies die IRSMC-Komponente, welche die Verbindungen zwischen den IRS und der ICS überwacht. Diese Überwachung ist möglich, da zwischen allen IRS und der ICS ein ständiger Kontakt (über FOC, ITS IMT Public, xDSL, …) besteht.

Als Konsequenz auf einen Ausfall einer Hardwarekomponente muss eine entsprechende Maßnahme ergriffen werden. Für die Kommunikationsstrecke wird eine entsprechende Information an die jeweils verantwortlichen Netzprovider eskaliert. Sollte es sich dabei um einen Defekt handeln, muss der entsprechende Service bzw. Support des

Hardwareherstellers der RAU informiert werden und der entsprechende Prozess angestoßen werden.

5.3.9.4 [M_ITS_WVA_ICS] ICS

Die ICS teilt sich in zwei Teilsysteme auf die von unterschiedlichen Verantwortlichen beschafft und administriert werden.

Anwendungsserver

In der sim^{TD}-Versuchszentrale sind fünf SPARC Server der Modellreihe T5410 bereits aufgestellt. Es handelt sich um einen DB-Server und einen Application Server, die jeweils redundant ausgelegt sind, sowie um einen DB-Historienserver (keine Redundanz). Die Application Server führen alle Anwendungen aus, die von verkehrlicher Relevanz sind (Ermittlung der aktuellen Verkehrslage einschließlich der Fusion der aus den IVS stammenden Daten, Bereitstellung aller erforderlichen aktuellen verkehrlichen Daten an IRS und ggf. IVS sowie Abarbeiten von Anforderungen aus IRS und ggf. IVS). Der Datenbank-Server enthält die Datenbank, in der die aktuellen Verkehrsdaten abgelegt sind. Es wird auch ein Datenverteiler implementiert, an dem sich „Kunden“ (Programme und Institutionen) registrieren und aus ihm entsprechend den vereinbarten Abonnements und Vereinbarungen Daten beziehen. Der Datenbank-Historienserver nimmt alle verkehrlichen Daten auf, die nicht mehr aktuell sind und für die Ermittlung der Verkehrslage nicht mehr benötigt werden. Dadurch entlastet er den oben erwähnten Datenbank-Server, dessen Suchanfragen sich auf kleinere, aber stets aktuelle Datenbestände beziehen.

Ob zusätzliche Hardware in der ICS-Versuchszentrale installiert wird, hängt von einigen sim^{TD}-Partnern ab, aber auch vom noch zur Verfügung stehenden freien Platz im ICS. Verbindlich für alle in der ICS-Versuchszentrale installierte Hardware gilt: sie ist nur über VPNs von außerhalb zu erreichen.

IRS Management Center

a) Software

Die Software im IRS Management Center wird auf die gleiche Weise überwacht, installiert und gewartet, wie die Software auf der IRS.

b) Hardware

Die Verwaltung der Hardware der Server und Komponenten erfolgt nach dem gleichen Muster wie bei anderen produktiven Servern (Abschnitt 5.2.9). Zum einen existiert eine Instanz die die Server überwacht und im Fehlerfall eine Benachrichtigung an den Administrator sendet. Im Fall des IRS Management Center ist hierfür ein EAG (Emergency Alarm Gateway) geplant, das den Administrator per Mail oder SMS über ein Fehlverhalten informiert. Zum anderen werden für Server Supportverträge mit entsprechenden Reaktionszeiten abgeschlossen.

5.3.10 Versuchszentrale

Die Versuchszentrale in sim^{TD} ist gegenüber einer Verkehrszentrale, wie man sie in einem ITS erwarten würde, um verschiedene versuchs- und testspezifische Komponenten und Schnittstellen ergänzt. Die folgende Abbildung 5.23 gibt einen Überblick über die einzelnen Schnittstellen der ICS (VsZ). Die darin enthaltenden Komponenten wurden in den vorherigen Abschnitten unter 5.3.2 und 5.3.7 bereits beschrieben.

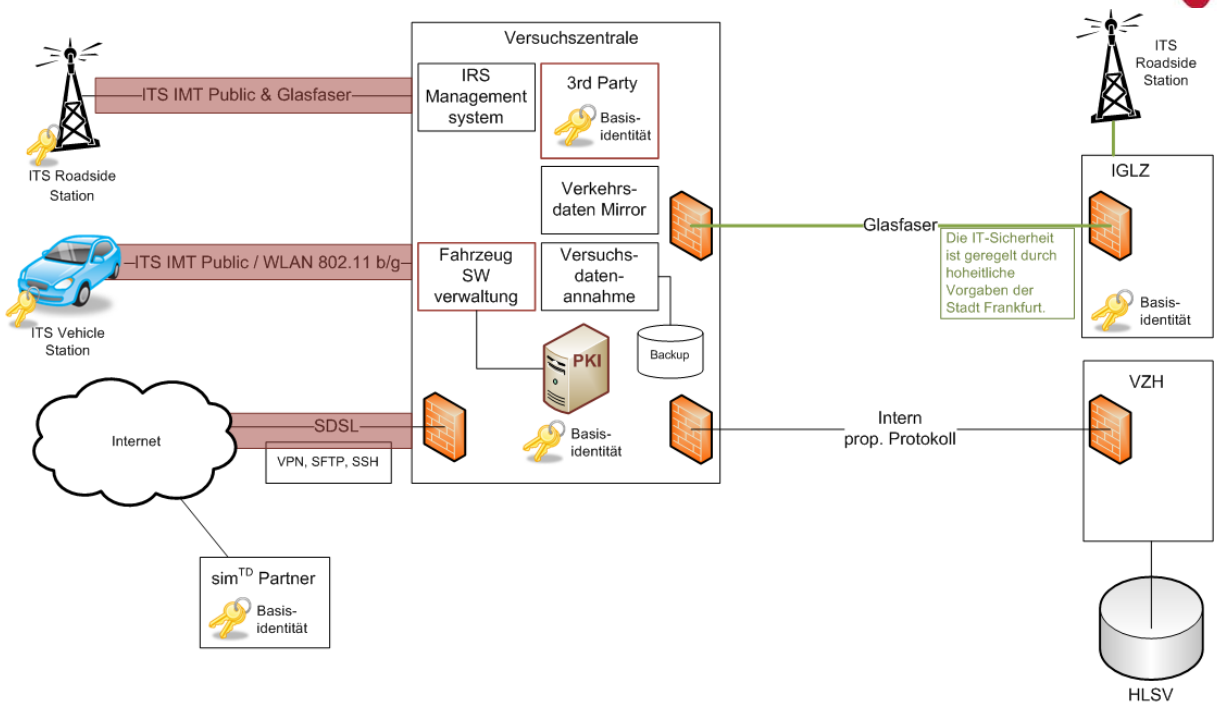

Abbildung 5.23: Schnittstellen und Sicherheitskomponenten der Versuchszentrale

5.3.10.1 Komponenten

Die zu schützenden Komponenten ergeben sich aus der Sicherheitsanforderungen in Abschnitt 4.1.2.2.

- **[S_ICS_VsZ_IRS_Man]**, IRS Management System
  - Die Absicherung des IRS Management Systems sollte analog der Beschreibung im Abschnitt 5.2.10.1 erfolgen. Für die Konkrete Umsetzung der Maßnahmen ist der zuständige Projektpartner verantwortlich.
- **[S_ICS_VsZ_AU],** weitere Software-Systeme der Versuchszentrale, z.B. für die Fahrzeugverwaltung
  - Die Software selbst und die damit verbundenen Daten, sofern diese nicht in der Datenbank abgespeichert werden, müssen gegen Änderungen gesichert werden. Es sollte eine Unabstreitbarkeit für die Version der laufenden Software vorhanden sein, damit eine sinnvolle Versuchsauswertung gewährleistet wird.
- **[S_ICS_VsZ_DB],** Datenbank zur Speicherung der verschiedenen Versuchsdaten.
  - Die Datenbank unterliegt in sim^{TD} den gleichen Schutzzielen, wie sie auch in einem Wirksystem vorhanden sind, d.h. die gleichen Maßnahmen wie unter Abschnitt 5.2.10.1 angegeben müssen Anwendung finden.
- **[S_ICS_VsZ_PKI]**, Server auf dem die PKI-Software läuft.
  - Die PKI wird in sim^{TD} in der VsZ unterbracht werden, dabei finden die im Abschnitt 5.3.2 beschriebenen Maßnahmen Beachtung und sollten umgesetzt werden. Die völlige Anonymisierung, wie sie im Wirksystem unabdingbar ist, wird für sim^{TD} aufgebrochen werden, da es zur Versuchsauswertung unumgänglich ist die vorhandnen Pseudonyme realen Fahrzeugen zuordnen zu können.
- **[S_ICS_VsZ_DNS]**, DNS-Server

- Die Zertifikate in sim^{TD} werden höchstwahrscheinlich auf DNS-Namen basieren; daher ist es essentiell, dass eine DNS-Server sowohl erreichbar, als auch gesichert ist. Wobei in sim^{TD} weder die DoS Problematik noch eine physikalische Ausfallsicherheit im Zusammenhang mit diesem Dokument beachtet werden.

5.3.10.2 Schnittstellen

Im Folgenden werden die Schnittstellen beschrieben, die im Zusammenhang mit der ITS Central Station vorhanden sind.

Schnittstellen zwischen ITS Central Station und VZH

Die Hardware der sim^{TD}-Versuchszentrale ist in den Räumlichkeiten des HLSV untergebracht, ebenso de Hardware des aktiven Systems VZH. Zwischen der ICS und der VZH wird eine LAN-Verbindung geschaltet, die über eine Firewall abgesichert ist.

Die Verbindung zwischen VZH und ICS ist notwendig, weil die ICS laufend auf die aktuellen Datenbestände des in der VZH installierten Info-Verteilers zugreifen muss. In der ICS wird die Verkehrslage berechnet (wie im VZH-System), zusätzlich erfolgt in diesem Zusammenhang eine Aggregation der aus den Fahrzeugen gewonnenen verkehrlich relevanten Daten, so dass die in der ICS erstellte Verkehrslage feingranularer ist als diejenige der VZH. Die Ergebnisse der verfeinerten Verkehrslage werden als Klartext dem Bedienpersonal der VZH zur Verfügung gestellt. Es gleicht die gewonnen Erkenntnisse mit der tatsächlichen Verkehrslage ab und ermöglicht auf diese Weise die Verbesserungen in der Anwendung „Erweiterte Verkehrslage“.

Neben dem Zugriff auf das VZH-System ist aus Gründen der Zeitsynchronisation der lesende Zugriff von der ICS auf den NTP-Server erforderlich, der auf GPS-Zeit ausgerichtet ist.

ITS Central Station und Internet

Damit die ICS von außen durch sim^{TD}-Partner erreichbar ist, ist sie an das Internet angebunden. Wegen der damit verbundenen Gefahren in Bezug auf IT-Sicherheit ist diese Internet-Anbindung aus Sicht der ICS über eine Firewall abgesichert, die sowohl auf Grundlage der Paketfilterung (*packet filter*) als auch auf Anwendungsebene (*stateful inspection*) konfiguriert ist.
Die Erreichbarkeit der ICS von außen ist seitens der sim^{TD}-Partner gefordert, die von ihren Standorten aus auf die ICS zugreifen möchten, ohne im Einzelfall vor Ort in der sim^{TD}-Versuchszentrale präsent zu sein. Das Testgelände (genauer Standort steht zurzeit noch nicht fest) bedarf ebenfalls einer Anbindung, ebenso wie das „Versuchs-Center“, in welchem sich die Fahrer der Fahrzeugflotte(n) treffen, um Anweisungen vom Versuchsregisseur entgegenzunehmen.

ITS Central Station und ITS Roadside Stations

In sim^{TD} bildet die Versuchszentrale (VsZ) die ICS mit den Funktionsservern und dem IRS Management. Die Kommunikation zwischen dieser VsZ und den IRS läuft auf unterschiedlichen physikalischen Wegen ab, siehe Abschnitt 1.1. Um die Kommunikation unabhängig von der zugrunde liegenden Technik zu machen wurde entschieden, eine verbindungsorientierte Kommunikation auf Grundlage von TLS zu nutzen. Die Authentifizierung erfolgt dabei mit Hilfe von X509v3-Zertifikaten, die von der zentralen PKI zur Verfügung gestellt werden.

Dabei werden verschiedene Tunnel für Funktionen (Anwendungen) und Management zur Verfügung gestellt, so dass eine strikte Trennung von Anwendung- und Managementdaten möglich ist. Darüber hinaus kann auf diese Weise auch IRS-seitig zwischen den einzelnen

Quellen priorisiert werden. Im Einzelnen bedeutet dies, dass für das Management eine bestimmte Mindestbandbreite zur Verfügung gestellt wird und dass Funktionen untereinander auf Anwendungsebene priorisiert werden.

Als weiterer Punkt werden Konzepte entwickelt, um die Kommunikation der Management- und der Funktionsserver aus der VsZ zu den IRS – obwohl sie unterschiedliche TLS-Tunnel benutzen und auf unterschiedlichen Servern aufgeführt werden – zu priorisieren und gegebenenfalls sogar an die zur Verfügung stehenden Bandbreite anzupassen.

ITS Central Station und ITS Vehicle Stations

Im Rahmen von sim^{TD} gibt es zwischen den ITS Vehicle Stations und der ITS Central Station, keine direkten Schnittstellen, sondern nur IP-basierte Datenübertragungen, die über mehrere Abschnitte mit unterschiedlichen Übertragungstechniken laufen:

- Die Verbindung zwischen der Central Station und dem Fahrzeug, die vom Fahrzeug via UMTS in das Netz des Mobilfunk-Anbieters reicht und anschließend über einen IPSec-Tunnel von einem Übergabepunkte des Mobilfunk-Anbieters zur Versuchszentrale.
- Verbindungen bei denen Nachrichten zwischen Fahrzeug und Versuchszentrale via IEEE 802.11p zur IRS und anschließend über den proprietären Backbone der VZH zur Versuchszentrale übertragen werden.
- Die Verbindung von Fahrzeugen auf dem Testgelände zur Versuchszentrale via C-WLAN im Ad-hoc-Modus und anschließender Übertragung von der IT-Infrastruktur des Testgeländes via IPSec-Tunnel in die Versuchszentrale.

ITS Central Station und 3rd-Party-Dienste

Im Rahmen des Projekts sim^{TD} erfolgt eine Einbindung von 3rd-Party-Diensten nur über die Versuchszentrale. Aus diesem Grund wird während der Projektlaufzeit von sim^{TD} ein Server für diese 3rd-Party-Dienste in der Versuchszentrale zur Verfügung gestellt. Hierauf werden die Dienste verarbeitet. Der Server befindet sich physisch in der VsZ und ist über geeignete Sicherheitsmaßnahmen von außen erreichbar. Der Server wird von extern mit Daten gespeist. Dies geschieht z.B. über eine SSH-Verbindung. Geeignete Maßnahmen sind in Abschnitt 5.3.3 beschrieben.

ITS Central Station und PKI

Hier wird keine Schnittstelle zwischen ICS und PKI geben, weil sich die PKI direkt in der Zentrale befindet.

5.3.10.3 [M_ITS_Log_Sec] Absicherung der Logdaten/Messdaten

Neben der Absicherung der einzelnen Komponenten und Schnittstellen ist in sim^{TD} auch explizit die Absicherung von in der VZH gespeicherten Logdaten und Messdaten gefordert. Unter dieser Maßnahme werden eine Reihe von Einzelmaßnahmen aufgelistet, die dazu dienen sollen die folgenden Sicherheitsziele für die Logdaten/Messdaten zu erreichen:

- *Vollständigkeit*, d.h. es muss auch noch im Nachhinein möglich sein zu überprüfen, ob Datensätze in den Daten fehlen,
- *Integrität*, d.h. es sollte erkennbar sein, wenn Daten verfälscht wurden und die Daten sollten nach der Speicherung in einer Datei bzw. Datenbank möglichst nicht mehr einfach zu verändern sein.

Verwendung von Sequenznummern

Jedem Lodaten-Eintrag wird eine hinreichend lange Sequenznummer vorangestellt, die bei jedem Eintrag um Eins inkrementiert wird. Der Stand der Sequenznummer wird beim Deaktivieren der sim^{TD}-Hardware in deren Dateisystem gespeichert, damit bei nachfolgender Aktivierung lückenlos weitergezählt werden kann. Die Speicherung muss hierbei manipulationssicher erfolgen.

Auf diese Weise lässt sich später in der Datenbank mithilfe von DB-Skripten leicht feststellen, ob die Logdaten der entsprechenden sim^{TD}-Einheit Lücken aufweisen oder nicht.

Rein-Anhängendes-Schreiben von Logdateien

Logdaten sollten stets nur rein anhängend in Dateien geschrieben werden, damit keine Daten überschrieben werden können.

Zu den Fragen der nicht mehr veränderbaren Speicherung in der Datenbank, siehe Maßnahme **[M_ICS_DB_RO]**.

Signieren von Logdaten

Natürlich bestünde die optimale Methode der Integritäts- und Authentizitätssicherung darin, die Daten digital zu signieren. Aufgrund der hierfür notwendigen Prozessor-Ressourcen ist dies ohne zusätzliche Hardwarebeschleunigung für Kryptografie im Rahmen von sim^{TD} allerdings zumindest nicht für einzelne Einträge effizient realisierbar.

Werden Logdaten/Messdaten nicht in Form einzelner Einträge, sondern in Form ganzer Dateien – und daher auch weniger häufig – versendet, ließen sich digitale Signaturen im Prinzip wieder einsetzen, da in diesem Fall der rechenaufwändige Anteil der asymmetrischen, kryptografischen Verfahren im Vergleich zum recht schnellen Berechnen des Hashwertes der Logdaten-Datei nicht mehr stark ins Gewicht fiele.

Für die reine Absicherung auf der Übertragungsstrecke sind allerdings die in Abschnitt 5.3.3 beschriebenen Tunnelverfahren völlig ausreichend; zwar sichern sie nur bis zum Tunnelendpunkt in der ITC ab und nicht in der ITC selbst, aber für einen Testbetrieb erscheint dies durchaus ausreichend, zumal der Zugriff auf die Daten über ein Rollenkonzept beschränkt wird.

6 Ergebnisse und Ausblick

In diesem Deliverable wurde die Sicherheitsarchitektur für sim^{TD} sowie für ein späteres Wirksystem erarbeitet. Dieses Kapitel fasst die wichtigsten Ergebnisse zusammen und hebt kritische Punkte hervor, an denen aus verschiedenen Gründen Abstriche aus IT-Sicherheitssicht gemacht werden mussten. Abschließend wird ein Ausblick auf die Umsetzung des hier erarbeiteten Konzepts gegeben.

Zusammenfassung

Zunächst wurden relevante Vorprojekte und Standards identifiziert. Die drei Projekte Network on *Wheels*, *SeVeCom* und das *Fraunhofer Innovationscluster Sichere Identität Berlin-Brandenburg* sowie der IEEE-Standard 1609 wurden als sehr relevant für die Entwicklung der IT-Sicherheit in sim^{TD} erachtet. Sie werden weiterhin beobachtet und ihre Ergebnisse werden die IT-Sicherheitslösung in sim^{TD} beeinflussen. Weitere vier Projekte und Standardisierungsgremien wurden als *mittel* oder *wenig* relevant eingestuft.

Im folgenden Kapitel 3 wurden mögliche Angriffsmotivationen in sim^{TD} und einem späteren Wirksystem erarbeitet. Sie dienen als Grundlage für die anschließende IT-Sicherheitsanalyse in Kapitel 4.

Die IT-Sicherheitsanalyse beginnt mit der Ermittlung des Schutzbedarfs in sim^{TD}, bzw. dem späteren Wirksystem. Hierzu wurden 20 verschiedene Datenkategorien, sechs funktionale Güter, 15 Kommunikationsverbindungen und zehn Komponentenkategorien identifiziert sowie ihr Schutzbedarf – jeweils für ein Wirksystem und für sim^{TD} – bewertet. Da der Funktionsumfang und die Architektur eines späteren Wirksystems jedoch nicht bekannt ist, sind die Schutzbedarfsbewertungen für das Wirksystem nur Schätzwerte. Der Schutzbedarf eines tatsächlichen Wirksystems kann daher gegebenenfalls erheblich von den in Abschnitt 4.1.3 genannten Werten abweichen. Im Folgenden wurden sechs „Mächtigkeitskategorien“ von möglichen Angreifern aufgestellt, d.h. Angreifer können anhand dieses Schemas aufgrund ihres Know-hows und ihrer finanziellen Möglichkeiten klassifiziert werden. Auf Basis dieses Angreifermodells sowie der vorigen Analyse von Angriffsmotiviationen wurden dann mögliche Bedrohungen für sim^{TD} ermittelt. Bedrohungen für ein späteres Wirksystem abzuschätzen war nicht möglich und sinnvoll, da keine Details über dieses Wirksystem bekannt sind. Aus den Bedrohungen und dem zuvor aufgestellten Schutzbedarf konnten dann Risiken für das IT-System in sim^{TD} abgeleitet werden. Aus diesen Risiken, sowie dem konkreten IT-Sicherheitsbedarf der sim^{TD}-Funktionen, der zuvor per IT-Sicherheits-Template abgefragt wurde, konnte dann eine Liste von konkreten IT-Sicherheitsanforderungen, die in sim^{TD} erfüllt sein müssen abgeleitet werden. Ziel der Definition der IT-Sicherheitslösung war es, jede der so ermittelten Anforderungen durch geeignete IT-Sicherheitsmaßnahmen abzudecken. Wie Tabelle 4.14 zeigt, ist dies größtenteils gelungen. An einigen Stellen mussten jedoch aufgrund verschiedener Bedingungen in sim^{TD} die IT-Sicherheitsmaßnahmen erheblich beschnitten werden. Diese Einschränkungen der IT-Sicherheitslösung werden weiter unten in diesem Abschnitt genauer beschrieben.

An die ausführliche IT-Sicherheitsanalyse schließt sich in Kapitel 5 die Beschreibung der konkreten IT-Sicherheitsarchitektur an. Im ersten Unterkapitel werden grundsätzliche Techniken vorgestellt, die in einem ITS zur Anwendung kommen können. Das zweite Unterkapitel stellt die IT-Sicherheitsmaßnahmen dar, welche in einem späteren Wirksystem, das nicht wie sim^{TD} verschiedenen Einschränkungen unterliegt, anwendet werden sollten um einen optimalen Schutz zu erreichen. Dies beinhaltet Maßnahmen zur Anonymität und Pseudonymität, zur Absicherung der verschiedenen Kommunikationskanäle gegen Manipulation und Abhören, Maßnahmen für die Ausfallsicherheit verschiedener Komponenten sowie rechtliche und regulatorische Maßnahmen. Im anschließenden Unterkapitel 5.3 werden dann die IT-Sicherheitsmaßnahmen vorgestellt, die einen Mindestschutz für das sim^{TD}-System herstellen sollen, teilweise jedoch sehr stark von den optimalen Schutzmaßnahmen abweichen.

Konkret wird eine Pseudonymisierung vorgesehen, die dem Schutz der Privatsphäre der Fahrer und der Einhaltung datenschutzrechtlicher Bestimmungen dient. Technisch wird diese Pseudonymisierung durch wechselnde asymmetrische Schlüssel, sowie Mechanismen zum Wechsel aller persistenter Identifizierer wie MAC- und IP-Adressen realisiert. Die asymmetrischen Schlüssel werden für die Signierung von Car2X-Nachrichten eingesetzt, wodurch die Authentizität und Integrität dieser Nachrichten sichergestellt wird. In einigen Fällen von Punkt-zu-Punkt-Kommunikation können Nachrichten überdies verschlüsselt und damit vor Abhören geschützt werden.

Aufgrund der in sim^{TD} stark beschränkten Hardwareressourcen und fehlenden TPMs (Hardwarebeschleunigung für Kryptografie) können nur sehr kurze Schlüssellängen verwendet werden. Dies hat zur Folge, dass das Brechen eines Schlüssels und damit der Missbrauch des Schlüssels (z.B. zum Manipulieren von Nachrichten sowie zum unberechtigten Entschlüsseln von Nachrichten) nicht ausgeschlossen werden kann. Daher müssen Schlüssel – auch in sim^{TD} – in regelmäßigen Abständen ausgetauscht werden. Das Erzeugen und Verteilen der Schlüssel wird durch eine Publik-Key-Infrastruktur (PKI) sowie die Funktion F_5.1.1 umgesetzt. Die PKI hat überdies die Aufgabe, kompromittierte Schlüssel (z.B. im Falle eines Diebstahls) zurückzurufen (revozieren) – die entsprechenden Protokolle und Komponenten werden im Rahmen der Funktion F_5.1.2 spezifiziert und implementiert.

Neben den Pseudonymschlüsseln (für die das 1610.2-Format angewandt wird), werden auch X509v3-Zertifikate für die Verbindung zu 3rd-Party-Diensten sowie für die Zugriffe der sim^{TD} -Partner auf die Versuchszentrale eingesetzt. Für die Verwaltung und Verteilung dieser Zertifikate existiert keine sim^{TD}-Funktion. Daher wird hierfür eine Minimallösung vorgesehen, die über keine automatische Revokationsmechanismen verfügt. Des Weiteren geben wir Empfehlung zur Ausfallsicherheit verschiedener kritischer Komponenten und zu erforderlichen Autorisierungskonzepten, etwa für den Zugriff auf die PKI.

Bewertung

Dieses Deliverable bietet mit der Analyse relevanter Vorprojekte und der ausführlichen IT-Sicherheitsanalyse eine umfangreiche Grundlage, auf deren Basis eine IT-Sicherheitsarchitektur für ein Wirksystem und für sim^{TD} entwickelt werden kann. Mit dem Sicherheitskonzept für sim^{TD} konnten die meisten IT-Sicherheitsanforderungen zumindest teilweise adressiert werden. Es ist gelungen, eine Sicherheitsarchitektur für sim^{TD} zu entwickeln, die folgende Punkte (zumindest teilweise) erfüllt und damit die größten Risiken in sim^{TD} weitgehend abgedeckt:

- Pseudonymität der Fahrer
- Authentizität und Integrität von verkehrsrelevanten Daten
- Vertraulichkeit bei der Übertragung von persönlichen Daten
- Zugriffskontrolle für persönliche Daten und kritische Komponenten

Die für sim^{TD} vorgeschlagene Lösung unterliegt jedoch starken Einschränkungen und kann daher keineswegs ein optimales IT-Sicherheitsniveau erreichen. Die Gründe für diese Einschränkungen sind im Wesentlichen:

- In sim^{TD} ist keine Hardwarebeschleunigung für Kryptografie (z.B. TPMs) verfügbar. Es können daher nur kryptografische Schlüssel verwendet werden, die deutlich unter den z.B. vom BSI als ausreichend sicher eingestuften Schlüssellängen liegen.
- Die Hardwareressourcen in sim^{TD} sind fest vorgegeben und stark begrenzt.
- Die in sim^{TD} für IT-Sicherheit zur Verfügung stehenden Ressourcen sind zum gegenwärtigen Zeitpunkt noch nicht bekannt. Falls das Design der Sicherheitsarchitektur sich später als zu anspruchsvoll herausgestellt hätte, wäre die Umsetzung

aller IT-Sicherheitsmaßnahmen in sim^{TD} in Gefahr gewesen. Daher mussten Minimallösungen angestrebt werden, was zur Folge hatte, dass auf einige zum Teil erforderliche Sicherheitsmaßnahmen verzichtet werden musste.

- In sim^{TD} werden im Gegensatz zum einem späteren Wirksystem teilweise andere Protokolle verwendet (z.B. IEEE 802.11 b/g, ITS IMT Public statt IEEE 802.11p für nicht-verkehrsrelevante Daten oder IPv4 statt IPv6). Da die Sicherheitsmaßnahmen einerseits für sim^{TD} geeignet sein sollen, andererseits aber auch in einem Wirksystem wiederverwendet werden können sollen, mussten hier Kompromisse eingegangen werden, die keineswegs optimal sind (Verwendung der UMTS-Sicherheit, Verwendung dedizierter Lösungen eines einzelnen Telekommunikationsanbieters, Pre-Shared-Keys für C-WLAN, usw.)
- Die Berücksichtigung von In-Car-Security wurde in sim^{TD} ausgeschlossen. Es existieren daher keine Schutzmaßnahmen gegen Angriffe auf das Schlüsselmaterial oder die Software in den Fahrzeugen und ITS Roadside Stations.

Die für das spätere Wirksystem vorgeschlagene Lösung versucht hingegen „optimalen“ Schutz zu realisieren und lässt die o.g. Einschränkungen außer Acht. Allerdings ist das Design des Wirksystems noch nicht bekannt, so dass für die IT-Sicherheitslösung Annahmen getroffenen wurden, die u.U. nicht erfüllt sein werden: In einem späteren Wirksystem werden andere IT-Sicherheitsanforderungen gelten, da das System komplexer sein wird, umfangreicheren rechtlichen Bestimmungen unterliegen und auf Basis noch nicht verabschiedeter Standards arbeiten wird.
Zum Teil konnten die zukünftigen Sicherheitsanforderungen in der Schutzbedarfsanalyse schon abgeschätzt werden. Da jedoch die Details eines solchen Systems nicht bekannt sind, können weitere, in diesem Deliverable nicht identifizierte Risiken auftreten. Für den Fall, dass jedoch die für das Wirksystem getroffenen Annahmen gelten, wird das hier vorgestellte Sicherheitskonzept optimalen Schutz gegen Nachrichtenmanipulation, Abhören, Verletzungen der Privatsphäre sowie unbefugte Zugriffe bieten.

Ausblick

Basierend auf der Grobbeschreibung der IT-Sicherheitsarchitektur dieses Deliverables, wird sich eine Feinspezifikation der Sicherheitskomponenten anschließen. Diese wird zum einen in AP22 erarbeitet und in Deliverable D22.3 *Fahrzeugseitiges IT-Sicherheitssystem* veröffentlicht werden. Neben der fahrzeugseitigen Feinspezifikation ist auch eine infrastrukturseitige Feinspezifikation der IT-Sicherheitslösung erforderlich, jedoch ist hierfür gemäß der Vorhabensbeschreibung bis jetzt kein eigenes Deliverable vorgesehen.

Darüber hinaus werden Teile der PKI im Rahmen der Funktionsentwicklung der Funktionen F_5.1.1 Verteildienst individueller Sicherheitsparameter und F_5.1.2 Verteildienst allgemeiner Sicherheitsparameter spezifiziert und entwickelt werden. Darunter werden insbesondere die Protokolle zur Verteilung von Pseudonymen, die Erstellung der Basisidentitäten sowie die Auslieferung von Revokationslisten fallen. Inwieweit auch die „internen“ Komponenten der PKI wie Schlüsseldatenbank, Management-Interface, etc. durch diese Funktionen abgedeckt werden, wird sich erst im Laufe des Spezifikationsprozesses herausstellen.

Anhang A: T-Mobile Mobile IP VPN basic: Sicherer mobiler Zugriff auf private Unternehmensnetze

T-Mobile bietet mit *Mobile IP VPN basic* eine kostengünstige VPN-Lösung an, bei der die Daten mobiler Rechner durch das Mobilfunknetz zu einem privaten APN[42] geleitet werden und anschließend über einen IPSec-Tunnel via (öffentlichem) Internet zu einem IPSec-fähigen Router (mit statischer IP-Adresse) des Kunden.

Über die Luftschnittstelle wird der Datenverkehr mit den Standard-Mechanismen des Mobilfunks verschlüsselt; im Mobilfunknetz selbst liegen die Daten im Klartext vor, allerdings ist die Benutzergruppe geschlossen. Vom APN zum Kunden sind die Daten wieder über den IPSec-Tunnel geschützt. Es handelt sich somit nicht um eine VPN-Lösung mit Ende-zu-Ende-Sicherheit, sondern es muss dem Mobilfunk-Anbieter vertraut werden.

Es folgt hier eine kurze Beschreibung Produktes *Mobile IP VPN basic* von T-Mobile[43], siehe auch www.t-mobile.de/business/mobile_business für weitere Informationen:

Mobile IP VPN basic ist ein kostengünstiges Standardangebot für Geschäftskunden, das die sichere Einwahl auf private Unternehmensnetze per Mobilfunk ermöglicht.

Eine geschlossene Benutzergruppe innerhalb des Mobilfunknetzes und die per IPSec gesicherte Datenübertragung bis zum Kundennetz stellen sicher, dass der Zugriff nur für berechtigte Nutzer möglich ist und die Daten über die gesamte Übertragungsstrecke geschützt sind.

Als Übertragungsweg zum Kundennetz nutzt Mobile IP VPN basic das Internet, die einzige Voraussetzung auf Kundenseite ist eine Internet-Anbindung mit statischer IP-Adresse und ein IPSec-fähiger Router. Eine ideale Ergänzung für diese Internet-Anbindung und den Router stellen die Business LAN-Produkte der T-Systems dar.

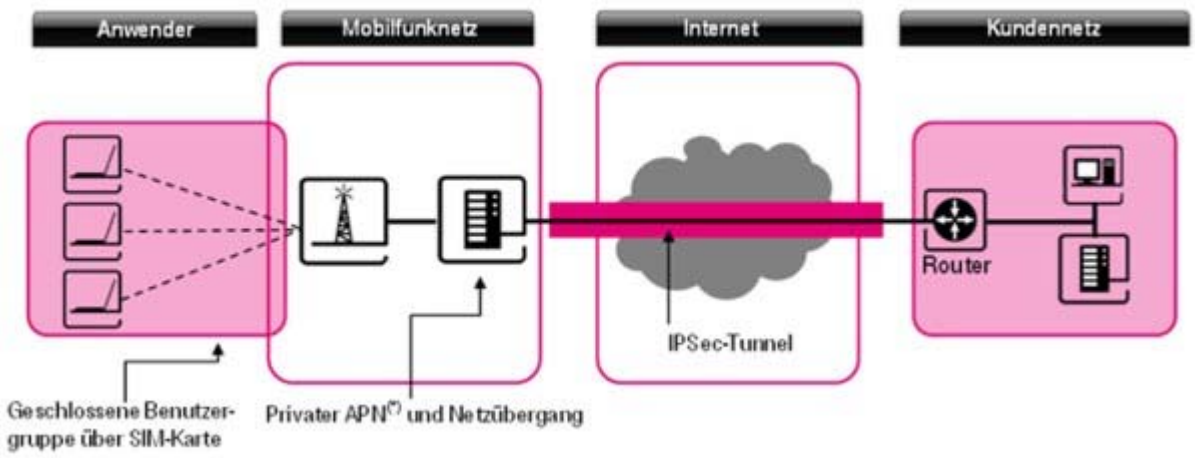

Abbildung 6.1: Architektur von T-Mobiles Mobile IP VPN basics

Aufgrund der integrierten, netz-internen Sicherheit, der optionalen Erweiterungsmöglich-keiten um z.B. Redundanzbausteine und des speziellen technischen Services bietet Mobile

[42] *Access Point Name*: Übergabepunkt um Datenpakete aus dem Mobilfunk-Netz in ein externes paket-basiertes Netz, i. Allg. das Internet, zu leiten.

[43] Die folgenden Abschnitte unterliegen daher dem Copyright von T-Mobile.

IP VPN basic insbesondere für den mobilen Einsatz geschäftskritischer Anwendungen deutliche Vorteile gegenüber herkömmlichen Verbindung Mobilfunk-Verbindungen.

Die Highlights im Überblick:

- Preisgünstiges Komplettprodukt für die Einwahl über Mobilfunk inkl. netzbasierten Sicherheitsverfahren.
- Keine zusätzliche VPN-Lösung erforderlich, d.h. keine Zusatzkosten und geringer Aufwand für Management und Administration.
- Verbindungen über Mobile IP VPN basic sind transparent, Kunden können eigene IP-Adressen für die mobilen Clients verwenden um darüber z.B. ein Berechtigungskonzept zu realisieren.
- Spezifischer technischer Service für die technischen Ansprechpartner auf Kundenseite.
- Ideale Ergänzung mit Business LAN-Produkten der T-Systems für ein durchgängiges Produkt- und Serviceangebot.

Weitere optionale Komponenten zu Mobile IP VPN basic erhöhen zusätzlich die Sicherheit und eröffnen weitere Einsatzszenarien:

- Die Teilnehmerverwaltung ermöglicht zusätzliche Sicherheit durch eine Authentifizierung der Clients / Anwender über die Mobilfunknummer oder per Benutzername und Passwort.
- Statische IP-Adressen in Verbindung mit der Teilnehmerverwaltung ermöglichen den Kunden, Berechtigungskonzepte auf Basis von IP-Adressen zu erstellen und auch das aktive Polling mobiler Geräte.
- Mobile to Mobile Kommunikation ermöglicht die direkte Verbindung zwischen mobilen Geräten, ohne dass eine Festnetzanbindung erforderlich ist.
- Redundanzbausteine erhöhen die Verfügbarkeit der Gesamtlösung durch die Einbeziehung weiterer, d.h. redundanter für die Kommunikation relevanter Netzelemente und Verbindungen.

Literaturverzeichnis

[1] sim^{TD}. Öffentliches Deliverable D21.2 „Konsolidierter Systemarchitekturentwurf“, 2009

[2] Eckert, C., „IT-Sicherheit – Konzepte, Verfahren, Protokolle“. Oldenbourg Verlag 2008, ISBN 978-3-486-58270-3

[3] Bundesdatenschutzgesetz (BDSG), 2007

[4] Teledienstedatenschutzgesetz (TDDSG), 2007

[5] sim^{TD} Internes Deliverable D21.1 „Bewertende Übersicht existierender Systemarchitekturen“, 2009

[6] Stone-Gross, Brett and Cova, Marco and Cavallaro, Lorenzo and Gilbert, Bot and Szydlowski, Martin and Kemmerer, Richard and Kruegel, Christopher and Vigna, Giovanni, "Your Botnet is My Botnet: Analysis of a Botnet Takeover," UCSB, Santa Barbara, CA, Technical Report, April 2009

[7] Qin, Y. and Hao, H. and Jim, L. and Jidong, G. and Jian, L., „An approach to ensure service behavior consistency in OSGi,“ 12th Asia-Pacific Software Engineering Conference (APSEC'05), 2005

[8] J. Krumm, „Inference attacks on location tracks“, in Fifth International Conference on Pervasive Computing, Toronto, Canada, May 2007, pp. 127–143

[9] sim^{TD}. Eingeschränktes Deliverable D21.4 „Spezifikation der Kommunikationsprotokolle“, 2009

[10] sim^{TD}. Eingeschränktes Deliverable D11.4 „Anforderungen der Funktionen an das Gesamtsystem“, 2009

[11] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. IEEE Std 1609.2-2006

[12] DiDio, Laura, „Unix, Linux Uptime and Reliability Increase; Patch Management Woes Plague Windows, “ Yankee Group, Januar 2008

[13] Bundesamt für Sicherheit in der Informationstechnologie, http://www.bsi.de

[14] National Institute of Standards and Technology, http://www.nist.gov