Allianz

Richtlinien

AZT Automotive GmbH * Allianz Zentrum für Technik

Anforderungen an "Virtuelle Fahrzeugschlüssel"

Technische Richtlinien für die Umsetzung von vernetzten und sicherheitskritischen Funktionen aus der Sicht der Versicherer

Stand Februar 18

INHALTSVERZEICHNIS

1. Einleitung

Diebstahl ist in der Kraftfahrzeugversicherung ein dominantes Thema und zeichnet sich durch hohe Schadendurchschnitte aus. Dies führt bei einer Vielzahl von Fahrzeugmodellen zu deutlich erhöhten Schadenkosten. Diebstahl umfasst nicht nur die Totalentwendung, die signifikant typklassen-relevant ist, sondern auch den Teilediebstahl und die Entwendung aus dem Fahrzeug, die mit hohen Begleitschäden verbunden ist.

Heutzutage erlebt die Entwicklung und Integration elektronischer Bauteile in der Automobilindustrie eine neue Dimension, wobei immer mehr innovative vernetzte Komfort- und Kundenfunktionen auf den Markt kommen. Unter anderem bieten OEMs ihren Kunden neben den klassischen physischen Fahrzeugschlüsseln, auch einen virtuellen Schlüssel, als eine Applikation auf einem mobilen Endgerät, und andere digitale After-Sales Dienste an, die auf globalen vernetzten Systemen basieren. Mit Blick auf aktuelle und zukünftige Entwicklungen in der Konsum- und Automobilindustrie ergeben sich neue Angriffsvektoren auf Schnittstellen zwischen den Entitäten dieser vernetzten Systeme.

In diesem Dokument formuliert das Allianz Zentrum für Technik die Anforderungen an „Virtuelle Fahrzeugschlüssel“ aus der Sicht der Versicherer, die insbesondere die Zugangs- und die Fahrberechtigung sicher machen sollen. Diese Anforderungen können die Automobilhersteller bei der Auslegung des Systems bzw. deren Schutz gegen Missbrauch unterstützen und berücksichtigen gleichzeitig die Erfordernisse bzgl. Unterwriting und Forensik im Schadenfall.

Die folgenden Anforderungen sind aus einer generischen Risikoanalyse entstanden und lassen deshalb einen freien Raum bei der Umsetzung digitaler Geschäftsprozesse, Technologien wie Cloud Computing oder den Einsatz mobiler Geräte. Die Risikoanalyse wurde vom Fraunhofer Institut für Sichere Informationstechnologie (SIT) im Auftrag des AZT erstellt und ist grundsätzlich auf ein beliebiges vernetztes System anwendbar, wobei das Fahrzeug selbst als ein in sich geschlossener Teilnehmer zu betrachten ist und durch ein Mobilitätskonzept ersetzt oder erweitert werden kann.

Die in diesem Dokument definierten Anforderungen basieren auf den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), die den IT-Grundschutz in Deutschland durch notwendige IT-Maßnahmen und Methoden [1] vorgeben. Die Vorgaben des BSI gelten als Mindestanforderungen und sind im Entwicklungsprozess sicherheitskritischer Funktionen wie „Virtueller Fahrzeugschlüssel“ zu berücksichtigen und umzusetzen. Als Pendant zum BSI ist z.B. in den USA für Standardisierungsprozesse in der IT-Sicherheit das National Institute of Standards and Technology (NIST) zuständig.

Folgend wird zuerst eine relevante Referenzarchitektur mit beteiligten Entitäten beschrieben. Daraus resultieren die Anforderungen an „Virtuelle Fahrzeugschlüssel“ als ein über mehrere Entitäten vernetztes System. Abschließend werden die Anforderungen an den forensischen Prozess gestellt.

© AZT Automotive GmbH - Allianz Zentrum für Technik

2. Referenzarchitektur und Prozessablauf

In der Abbildung 1 ist die verwendete Referenzarchitektur für das Ökosystem „Virtueller Fahrzeugschlüssel“ (VFS) und die im Kontext VFS beteiligten Entitäten dargestellt.

Grundsätzlich besteht das Ökosystem aus drei Entitäten:

1. einem Fahrzeug
2. einem Backend
3. einem Nutzer mit seinem Mobilen Endgerät (ME).

Um die Übersichtlichkeit der Abbildung und der nachfolgenden Beschreibungen zu behalten, werden Fahrzeug und Nutzer mit entsprechenden MEs als jeweils eine Entität betrachtet, wobei die hier dargestellte Architektur auch skalierbar auf eine Vielzahl von Fahrzeugen, Nutzern und MEs (z.B. auch Kombinationen von Smartphone und Smartwatch) gültig bleibt. Daraus lassen sich Car-Sharing-Konzepte ableiten, wie bspw. Multi-User-Case, wobei mehrere Nutzer Zugriff auf ein Fahrzeug bekommen oder, wie bei Multi-Key mit unterschiedlichen Schlüsseln auf einem ME Zugriff auf mehrere Fahrzeuge ermöglicht wird.

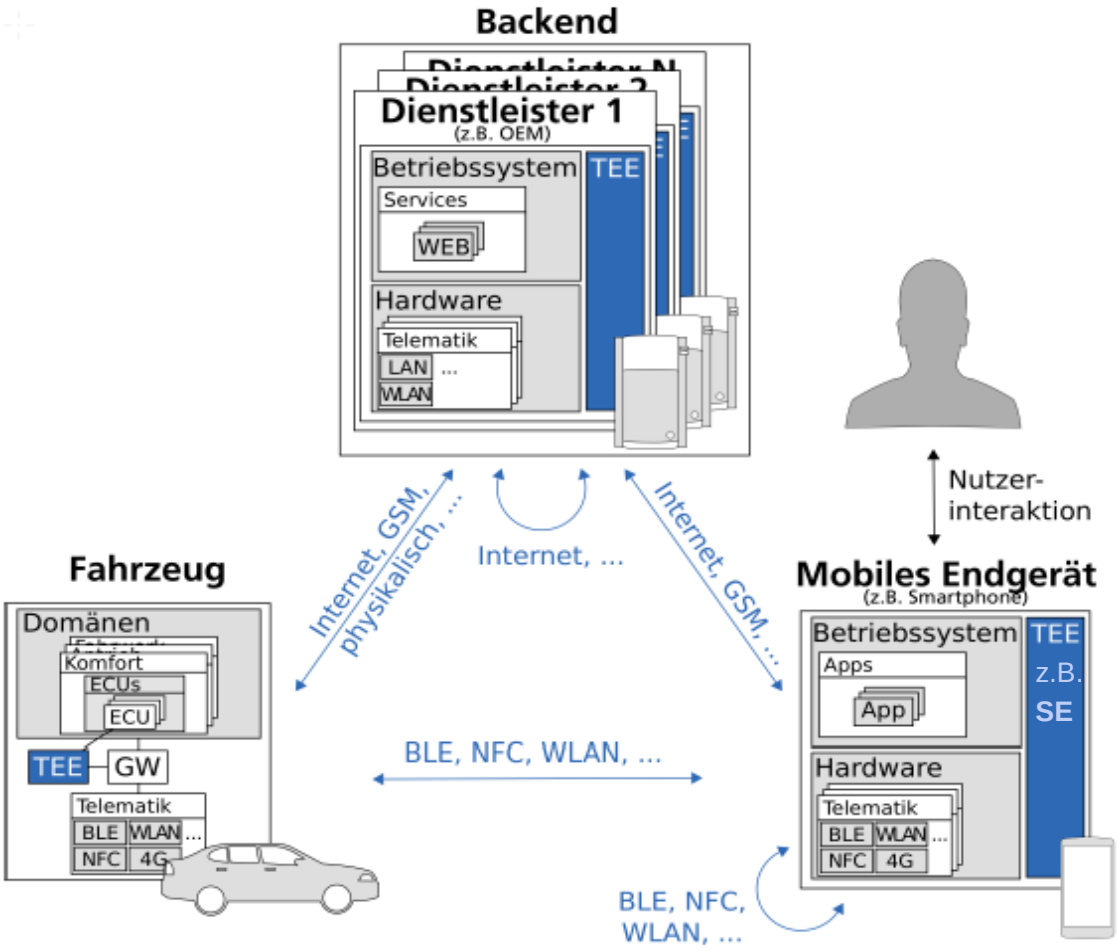

Abbildung 1: Ökosystem und beteiligte Entitäten

Die Referenzarchitektur ist bewusst einfach gehalten, um die Funktionsauslegung nicht einzuschränken und lässt neue Technologien zu, deren Entwicklung zum jetzigen Zeitpunkt nicht absehbar ist.

Das Backend kann von Dienstleistern (DL) verschiedener Parteien (z.B. Original Equipment Manufacturers (OEMs), Mobilfunkbetreiber (Mobile Network Operators (MNOs)), Händler, Car Sharing Anbieter) betrieben werden. Weiterhin werden unter dem ME z.B. Smartphones, Smartwatches und Tablets zusammengefasst, also alle Geräte, die als allgegenwärtige Begleiter vom Nutzer mitgeführt werden.

Wie in Abbildung 1 zu sehen, kommunizieren die einzelnen Entitäten über diverse Schnittstellen und Kommunikationsverbindungen miteinander. Die Kommunikation zwischen Fahrzeug und Backend als auch zwischen ME und Backend kann beispielsweise über eine Internetverbindung oder eine Global System for Mobile Communications (GSM) Verbindung erfolgen. Diese Kommunikation soll ausschließlich über beidseitig authentifizierte Kanäle stattfinden, um eine eindeutige Authentifikation zwischen den Kommunikationsteilnehmern zu gewährleisten. Diese Maßnahme schützt gegen Bedrohungen durch (Entitäten-)Spoofing, gegen unautorisiertes Versenden oder das Verändern von unverschlüsselten Nachrichten auf dem Bussystem im Fahrzeug.

Für die Kommunikation zwischen Fahrzeug und ME können Kurzstrecken-Funktechniken wie z.B. Bluetooth Low Energy (BLE), Near Field Communication (NFC) oder Wireless Local Area Network (WLAN) im ad-hoc Modus eingesetzt werden, die eine direkte Verbindung zwischen den beiden Entitäten ohne zwischengeschaltete Infrastruktur ermöglichen. Um bereits bekannte Replay- und MitM-Angriffe zu vermeiden, sollen nur die Kurzstrecken-Funktechniken verwendet werden, deren Standards vom BSI als sicher anerkannt wurden. Eine indirekte Verbindung vom ME zum Fahrzeug über das Backend ist auch möglich. Verschiedene DL im Backend können z.B. über Internetverbindungen miteinander kommunizieren.

Im Wesentlichen besteht der generelle Prozessablauf aus vier grundsätzlich zur Authentisierung zwischen Nutzer und Fahrzeug notwendigen Schritten:

1. System Initialisierung
2. Nutzer Registrierung
3. Schlüssel Download
4. Authentisierung am Fahrzeug.

Bei der System Initialisierung wird jedes Fahrzeug zu einem Backend eindeutig zugeordnet. Das Backend sollte mit Zertifikaten versehen werden, um eine gegenseitig authentifizierte und verschlüsselte Kommunikation jederzeit durchführen zu können. Da dem Schutz des kryptografischen Schlüsselmaterials eine besondere Bedeutung zukommt, sollen diese in allen beteiligten Entitäten in sicheren Speicher- und Ausführung-Umgebung, wie z.B. in Trusted Execution Environments (TEE) gespeichert werden. Speziell im Fahrzeug und auch später im mobilen Endgerät, in dem der VFS ausgeführt wird, sollen nur TEEs mit einem hohen Schutz, z.B. Hardware-TEEs eingesetzt werden.

Nachdem das System “VFS” initialisiert ist, kann sich der Nutzer registrieren lassen, um sich einen VFS herunter zu laden und später gegenüber dem entsprechenden Fahrzeug zu authentifizieren. Während der Registrierung muss eine eindeutige Identität des Fahrers bzw. Nutzers hinterlegt werden, damit bei späteren Authentifizierungen (Nutzungsberechtigung) die Berechtigung geprüft werden kann. Diese Schritte nach der Initialisierung sind für jedes ME bzw. jeden Nutzer zu durchlaufen.

Während Entitäten wie Fahrzeug und Backend ihre Credentials, die als sicherheitskritische Daten betrachtet werden müssen, in Form von schlüsselabhängigen kryptographischen Hashfunktionen oder digitalen Signaturen nachweisen, kann sich der Nutzer gegenüber dem Ökosystem mit verschiedenen Authentisierungstechniken wie Wissen (z.B. Passwort, „Personal Identification Number“ (PIN), Codetabellen, aber auch kryptographische Schlüssel), Besitz (z.B. Token wie Smartcard) oder biometrischen Merkmalen (z.B. Fingerabdrücke oder Gesichtserkennung) authentisieren. Werden zwei Authentifizierungsverfahren kombiniert (z.B. Mehr-Faktor-Authentifizierung), spricht das BSI in diesem Zusammenhang von starker Authentifizierung [2]. Das BSI beschreibt mit seinen Technischen Richtlinien [3] eine Bewertung und langfristige Orientierung für aktuelle kryptographische Verfahren, einzusetzende Protokolle und Schlüssellängen, sowie den jeweiligen Gültigkeitsbereichen, in denen diese voraussichtlich als sicher gelten und eingesetzt werden können.

Um bei einem Fahrzeugdiebstahl Schäden zu begrenzen, müssen Revokationsmechanismen im System implementiert werden, die es erlauben, ausgestellte Nutzungsberechtigungen wieder entziehen zu können. Dabei wird zwischen aktiven und passiven Maßnahmen unterschieden. Aktive Maßnahmen beinhalten Revokationslisten, die direkt im Fahrzeug gespeichert und aktualisiert werden. Passive Maßnahmen können durch eine Zeitbeschränkung in den ausgestellten Schlüsseln realisiert werden. Um auch den Offline-Fall abzudecken, bei dem es nicht möglich ist eine Verbindung mit dem Fahrzeug herzustellen und Revokationslisten zu aktualisieren, sollte der aktive Revokationsmechanismus mit dem passiven kombiniert werden, um eine regelmäßige Kommunikation mit dem Backend zwecks Schlüsselausstellung zu erzwingen, so dass weitere Schlüsselnutzungen unterbunden werden können. Ein Revokationsprozess muss zusätzlich auf dem ME umgesetzt werden. Der tatsächliche Entzug der Nutzungsberechtigung ist zu dokumentieren.

Sofern in einem Anerkennungsprozess eine Zertifizierung notwendig werden sollte, ist diese nach dem international anerkannten Standard Common Criteria (CC), sowie im Raum USA durch Federal Information Processing Standard (FIPS) zu realisieren.

3. Anforderungen an die Auslegung der Gesamtfunktion „Virtueller Fahrzeugschlüssel“ (VFS)

Folgende Anforderungen sollen grundsätzlich bei der Auslegung des Gesamtsystems umgesetzt werden:

1. Ein VFS muss nach dem aktuellen IT-Grundschutz des BSI [1] gestaltet werden:

   1.1. Alle Schnittstellen zwischen beteiligten Entitäten und entlang der Initialisierungs- und Registrierungsprozesskette müssen nach BSI ausgelegt und geprüft werden, um unautorisierte Zugriffe auf das System abzuwehren und nur berechtigten Nutzern Schließ- und/oder Fahrberechtigungen auszustellen.

   1.2. Bei der Umsetzung dürfen nur standardisierte kryptographische Verfahren [1] eingesetzt werden, um die Systemsicherheit innerhalb der Lebensdauer eines Fahrzeugs zu gewährleisten und nachträglich entsprechend neuer Erkenntnisse im Bereich IT-Sicherheit anzupassen.

   1.3. Zur Authentisierung zwischen den beteiligten Entitäten müssen nur starke Authentifizierungsverfahren benutzt werden (z.B. 2- bzw. Mehr-Faktor-Authentifizierung), diese müssen zeitgemäß auch während des Fahrzeuglebenszyklus angepasst werden können.

2. Ein VFS darf nicht kopierbar sein, d.h. analog zu einem physischen Fahrzeugschlüssel darf keine 1:1 Kopie des Schlüssels oder ein Duplikat möglich sein.

3. Für jedes Fahrzeug muss ein individueller VFS implementiert werden.
   Hintergrund: ein so genannter „Generalschlüssel“ darf nicht vorkommen, um Bedrohungen, die ganze Fahrzeugserien betreffen, auszuschließen. Es muss sowohl jedes Fahrzeug, jede Wegfahrsperre (WFS) als auch jeder Nutzer individuelle kryptographische Schlüssel besitzen, die den BSI Anforderungen an starke Kryptographie entsprechen.

4. Das Rollen- und Rechtemanagement [6] ist so auszulegen, dass unberechtigte Nutzer oder Schadsoftware keinen Zugriff auf sicherheitskritische Daten, wie z.B. Credentials, und Prozesse, wie z.B. Algorithmen, innerhalb des Systems bekommen dürfen.

5. Ein sicherer Zeitstempel muss für die Gesamtfunktion über alle Entitäten implementiert werden.

6. Für die Kommunikation zwischen Fahrzeug und ME sollen standardisierte und sichere Protokolle und ein Zeitstempel verwendet werden, um die bekannten Angriffe wie z. B. Replay-, MitM- und DoS-Angriffe zu verhindern.

7. Der VFS darf in keinem Steuergerät im Klartext oder unverschlüsselt vorliegen.

8. Alle Kommunikationskanäle in ein Fahrzeug, wie z.B. BLE, NFC, Internet, GSM, etc., und auch physische Kanäle, wie z.B. die OBD-Schnittstelle, müssen gegen bekannte Replay, MitM oder ähnliche Angriffe geschützt werden.

9. Unautorisiertes Senden von Nachrichten in das interne Fahrzeugbordnetz, die dazu dienen, eine Zutritts- und Fahrfreigabe zu erhalten, muss unterbunden werden.

10. Eine WFS darf analog zum konventionellen Schlüssel nicht deaktiviert werden, wenn das ME nicht innerhalb des Fahrzeuginnenraums registriert ist.

11. Die Zutrittsberechtigung, d.h. Öffnen und Schließen von Türen und/oder Kofferraum, muss getrennt von der Fahrberechtigung, d.h. dem Deaktivieren der WFS und Freigabe zum Motorstart, umgesetzt werden:

    11.1. die Freigabe zur Fahrberechtigung muss gesondert und erst nach der Freigabe der Zutrittsberechtigung erfolgen,

    11.2. die Freigabe zur Fahrberechtigung darf nicht nach der alleinigen Freigabe zur Öffnung des Kofferraumes erfolgen (z.B. zum Schutz von Paketdiensten),

    11.3. die Deaktivierung der WFS darf nur nach der Erteilung der Fahrberechtigung stattfinden,

    11.4. die Zutrittsberechtigung und die Deaktivierung der WFS müssen durch voneinander getrennte Authentifizierungsprozesse umgesetzt werden.

12. Revokationslisten und Policies müssen nach BSI anerkannten manipulationssicheren Methoden und Standards abgelegt werden.

4. Anforderungen an den VFS auf einem mobilen Endgerät

Folgende Anforderungen sollen bei der Auslegung des Nutzungskonzeptes auf einem mobilen Endgerät umgesetzt werden:

1. Ein VFS auf einem ME darf zu keinem Zeitpunkt vom Benutzer oder von Dritten manipulierbar sein.
2. Sicherheitskritische Funktionen (z.B. Freigabe der Fahrberechtigung oder die Erstellung von Signaturen) müssen im ME in einer sicheren Speicher- und Ausführung-Umgebung (z.B.: TEE, Secure Element, etc.) durchgeführt werden.
3. Die Speicherung sicherheitskritischer Daten, wie z.B. Credentials, muss in einer sicheren Speicher- und Ausführung-Umgebung (z.B.: TEE, Secure Element, etc.) stattfinden.
4. Der Zugriff auf den VFS soll zusätzlich mit einem Passwort, Fingerabdruck, etc. geschützt werden (Schutz des ME durch Diebstahl)
5. Zwischen der regulären Ausführungsumgebung des ME (z.B. dem Betriebssystem) und der sicheren Speicher- und Ausführung-Umgebung (z.B.: TEE, Secure Element, etc.) muss eine Trennung gewährleistet werden, um Angriffe auf sicherheitskritische Daten zu verhindern. Undefinierte Zugriffe auf Speicherinhalte der TEE müssen unterbunden werden.
6. Der Schutz der Kommunikation zwischen VFS auf einem ME und dem Fahrzeug gegen Replay-Angriffe ist zwingend erforderlich.
7. Der Nutzer bzw. sein ME muss sich gegenüber dem System mit Authentifizierungsverfahren nach BSI autorisieren.

© AZT Automotive GmbH - Allianz Zentrum für Technik

5. Anforderungen an das Backend

Das Backend im Ökosystem „Virtueller Fahrzeugschlüssel“ ist besonders kritisch zu betrachten, da ein Angreifer nicht nur in Besitz von sicherheitskritischen Daten, wie z.B. Credentials, von allen im System registrierten Benutzern kommen kann, sondern auch durch die Internet Verfügbarkeit aus sicherer Entfernung beliebige Angriffe gegenüber dem Backend, wie z.B. das Verändern oder Löschen von Logfiles, ausführen kann.

Das BSI stellt in einer eigenen Studie zur Absicherung von Backends eine Reihe von grundsätzlichen Maßnahmen [5] vor, um generische Server gegen diverse Angriffe abzusichern. Diese Maßnahmen sind als Mindestanforderungen umzusetzen.

Folgende Anforderungen sollen bei der Integration eines Backends ins Gesamtsystem umgesetzt werden:

1. Für die Datenübertragung dürfen ausschließlich standardisierte, von BSI empfohlene Protokolle verwendet werden, um bekannte Angriffe, wie z.B. DoS, MitM, etc. zu verhindern.
2. Kryptographisches Material zur Authentifizierung und zur Verschlüsselung von Kommunikationskanälen muss gegen unbefugten Zugriff oder Manipulation geschützt sein.
3. Alle sicherheitskritischen Daten und Prozesse müssen vor Manipulation oder Auslesen geschützt auf der sicheren Speicher- und Ausführung-Umgebung des Backends gespeichert werden.
4. Das Rollen- und Rechtemanagement [6] ist so auszulegen, dass die Anzahl an berechtigten Personen zur Verwaltung von sicherheitskritischen Daten minimal gehalten wird und damit das Risiko von Angriffen durch Social Engineering minimiert wird.
5. Die Logfiles zu Nutzungsberechtigungen und VFS-Vergaben müssen gegen Manipulationen und Angriffe jeder Art geschützt sein.
6. Identifizierte Angriffsversuche auf diese Logfiles sollen transparent dokumentiert werden.
7. Zur Erkennung von Angriffsversuchen auf das Backend und zeitlichen Schaden-minimierung muss ein Überwachungsprozess nach BSI [11] etabliert werden, so dass keine neuen unberechtigten VFS erstellt und betroffene VFS so schnell wie nur technisch möglich revoziert werden.

6. Plausibilisierung von Daten und Forensik

Totaldiebstahl muss von den Versicherern plausibilisiert werden können. Dabei wird die Unterstützung der Hersteller und des DL, z.B. mit Datenbereitstellung und Datenanalyse, benötigt. Bei Virtuellen Schlüsseln gilt dies noch mehr als bei physischen Schlüsseln.

Insbesondere bei späteren Rechtsstreitigkeiten werden diese Daten über eine Zeit, länger als 200 Arbeitstagen, forensisch verwendbar gespeichert bleiben müssen. Aus diesen Überlegungen resultieren besondere Anforderungen an die Protokollierung, die - wie bei den herkömmlichen Untersuchungen auch - datenschutzrechtliche Aspekte betreffen. Während bislang die Einverständniserklärung des Versicherungsnehmers genügte, können bei virtuellen Schlüsseln potentiell auch Rechte weiterer Nutzer betroffen sein. Die OEMs und DL sind in der Pflicht, solche Konflikte zu berücksichtigen bzw. zu vermeiden und ihre Systeme dementsprechend auszulegen.

Folgende Anforderungen werden an den *forensischen* Prozess erhoben:

1. Um im Fall eines Diebstahls Auskunft über die gültige VFS geben zu können, müssen auf dem Backend entsprechende Logfiles abgelegt sein, die Schlüsselausstellungen und -revokationen eindeutig und transparent protokollieren.
2. Um betrügerische oder missbräuchliche Verwendung der Nutzungsberechtigung zu vermeiden, muss die Deaktivierung eines (oder aller registrierten) VFS möglich sein, und folgende Optionen anbieten:

   2.1. Deaktivierung durch den Kunden mit Hilfe seines Kunden-Accounts

   2.2. Deaktivierung durch den OEM oder DL im Auftrag des Kunden.
3. Im Fall eines gemeldeten Diebstahls muss eine sofortige Deaktivierung aller VFS möglich sein.
4. Eine Deaktivierung des VFS muss eine sofortige Synchronisation aller Entitäten auslösen.
5. Im Fall, dass eine der Entitäten nicht erreichbar im Offline-Modus ist, muss sichergestellt werden, dass

   5.1. der Entzug des VFS transparent dokumentiert ist

   5.2. die Bestätigungen aller Entitäten inkl. ausstehender Bestätigungen transparent dokumentiert sind.
6. Das Logfile muss in unveränderlicher Form gespeichert werden, um eine nachträgliche Manipulation durch Dritte zu unterbinden.
7. Die Logfiles müssen transparent einen forensischen Datensatz wiedergeben, um den Kunden vor falschen Verdächtigungen zu schützen.

8. Aus der Sicht der Forensik muss ein Meldeprozess analog zum US-CERT Prozess [12] etabliert werden, um die Transparenz von Angriffsversuchen und die IT-Sicherheit vernetzter und sicherheitskritischer Funktionen zu gewährleisten.

9. Der forensische Datensatz spielt bei der Plausibilierung und Aufklärung eines Totaldiebstahls eine entscheidende Rolle und soll folgende Informationen beinhalten:

   9.1. Der jeweilige Zeitstempel aller Nutzer-Registrierungen

   9.2. Der jeweilige Zeitstempel aller VFS Downloads

   9.3. Der jeweilige Zeitstempel der Authentifizierung am Fahrzeug

   9.4. Die Anzahl aller aktiven VFS inkl. Multi-Keys, Card-Keys und temporäre VFS

   9.5. Der Zeitstempel einer VFS Löschung, d.h. eine vollständige Liste aller revozierten VFS

   9.6. Der Zeitstempel und die Geokoordinaten der letzten VFS Anwendung

7. Literaturverzeichnis

1 *BSI. IT-Grundschutz-Kataloge. 2017. URL:* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

2 Bundesamt für Sicherheit in der Informationstechnik. M 4.133 Geeignete Auswahl von Authentikationsmechanismen. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html

3 Bundesamt für Sicherheit in der Informationstechnik (BSI). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile%5C&v=2

4 BSI. M 4.456 Authentisierung bei Web Services. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04456.html.

5 BSI. *Absicherung eines Servers (ISi-Server) – BSI-Studie zur Internet-Sicherheit (ISiS)*. Sep. 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.pdf?__blob=publicationFile

6 BSI. G 2.191 Unzureichendes Rollen- und Berechtigungskonzept. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02191.html

7 ISO. *ISO/IEC 154082:2008*. 2014. URL: https://www.iso.org/standard/46414.html

8 Bundesamt für Sicherheit in der Informationstechnik. *Zertifizierung von Produkten*. 2016. URL: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Produktzertifizierung_node.html

9 The Common Criteria. *Members of the CCRA*. 2016. URL: http://www.commoncriteriaportal.org/ccra/members/#DE

10 National Institute of Standards und Technology. *FIPS Publications*. 2015. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

11 BSI. Leitfaden zum Informationssicherheitsmanagementsystems (ISMS). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3

12 US-SERT Gouvernement.URL: https://www.us-cert.gov/

8. Abkürzungen

Tabelle 1: Abkürzungsverzeichnis

Abkürzung	Vollständige Begriffsbeschreibung
Ad-hoc Modus	erlaubt einem Gerät mit jedem anderen direkt zu kommunizieren
Authentifikator	Authentifikator wird als Eingabe für Authentifizierungsverfahren benutzt
BLE	Bluetooth Low Energy
BSI	Bundesamt für Sicherheit in der Informationstechnik
Entität	Als Entität (auch Informationsobjekt genannt) wird in der Datenmodellierung ein eindeutig zu bestimmendes Objekt bezeichnet, über das Informationen gespeichert oder verarbeitet werden sollen. Das Objekt kann materiell oder immateriell, konkret oder abstrakt sein. Beispiel: ein Fahrzeug, eine Person, etc.
CC	Common Criteria (for Information Technology Security Evaluation)
Credentials	Credentials ist ein Instrumentarium, das einem System die Identität eines anderen Systems oder eines Benutzers bestätigen soll
DL	Dienstleister
ECU	Electronic Control Unit
Fahrzeug-lebenszyklus	Zeitraum zwischen SOP und substantiellem Update der Funktion VFS bzw. EOP jeweils plus zwei Jahre
FIPS	Federal Information Processing Standard
GW	Gateway
ME	Mobiles Endgerät
MitM	Man-in-the-Middle
MNO	Mobile Network Operator
NFC	Near Field Communication
OBC	Out of Band Channel
OEM	Original Equipment Manufacturer
PIN	Personal Identification Number
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
VFS	Virtueller Fahrzeugschlüssel
WLAN	Wireless Local Area Network
WFS	Wegfahrsperre
Zeitstempel	Tag und Uhrzeit der jeweiligen Aktion