Allianz

Richtlinien

AZT Automotive GmbH | Allianz Zentrum für Technik

Aktualisierte Anforderungen an die Elektronische Wegfahrsperre

Technische Richtlinien für die Implementierung einer Funktion zum Schutz gegen Diebstahl aus der Sicht der Versicherer

Stand 4. April 2023

INHALTSVERZEICHNIS

1. Einleitung

Diebstahl ist in der Kraftfahrzeugversicherung ein relevantes und durch hohe Schadendurchschnitte gekennzeichnetes Schadengeschehen. Bei besonders betroffenen Modellen kann der Anteil der Schadenaufwendungen bei über 50% des Gesamtaufwandes in Vollkasko liegen und die Typklasse maßgeblich beeinflussen.

Die wirksamste Maßnahme gegen Diebstahl ist eine manipulationssichere elektronische Wegfahrsperre (eWFS), die einen unberechtigten Motorstart und die Wiederverwendung eines gestohlenen Fahrzeuges verhindert. Daher ist eine qualifizierte Wegfahrsperre eine Anforderung der gesamten Versicherungswirtschaft.

Die Implementierung einer eWFS wird regelmäßig durch den GDV im Rahmen des Ersteinstufungsprozesses bei jedem neuen Fahrzeugtyp abgefragt. Die Erfüllung der geltenden technischen Richtlinien wird vom GDV für die Versicherungswirtschaft zur Verfügung gestellt, um neben einer risikogerechten Prämienkalkulation auch eine angemessene Forensik und kundenfreundliche Schadenprozesse zu ermöglichen.

Die Anforderungen an die eWFS setzen die Erfüllung gesetzlicher Vorschriften und Richtlinien (wie z.B. UN Regulation No.116, GRSG-106-38) und technischer Normen (wie z.B. ECE, DIN, ISO) voraus. Mit dem hier vorgelegten Dokument aktualisiert deshalb die AZT Automotive GmbH – Allianz Zentrum für Technik die im Jahr 1994 erstmalig formulierten Anforderungen an elektronische Wegfahrsperren. Diese neue Formulierung erweitert einerseits die Anforderungen entsprechend des technologischen Fortschritts, andererseits werden die Anforderungen generischer formuliert. So soll dem Hersteller eine individuelle Umsetzung ermöglicht werden, zugleich ist damit aber auch die Verpflichtung des Herstellers verbunden, im Interesse des eigenen Kunden den Stand der Technik bestmöglich anzuwenden.

Nachfolgend werden zuerst die Anforderungen an die elektronische Wegfahrsperre als System formuliert. Abschließend werden die Anforderungen an den Schlüsselsatz und an die Forensik beschrieben. Die besonderen Anforderungen an Virtuelle Fahrzeugschlüssel (VFS[1]) als ein Teil des kompletten Schlüsselsatzes wurden als RCAR Standard[2] publiziert.

[1] Smartphone oder vergleichbares persönliches Gerät als Schlüssel
[2] https://rcar.org/working-groups/cyber-security

2. Anforderungen an die elektronische Wegfahrsperre

Folgende Anforderungen müssen aus der Sicht der Versicherer grundsätzlich erfüllt werden:

1. Eine eWFS muss die bei der Ersteinstufung erreichte Diebstahlsicherheit für den ganzen Lebenszyklus des Fahrzeugmodells gewährleisten.
2. Eine eWFS muss über den Lebenszyklus des Fahrzeugmodells aktualisierbar sein, um gemeldete Sicherheitslücken schließen zu können.
3. Das Deaktivieren (Entschärfen) der eWFS muss folgende Anforderungen erfüllen:
   - 3.1. Die Zutrittsberechtigung und die Fahrberechtigung müssen durch voneinander getrennte Authentifizierungsprozesse umgesetzt werden.
   - 3.2. Die eWFS darf nur nach einer erfolgreichen Überprüfung bestehender Zutrittsberechtigung und Fahrberechtigung deaktiviert werden.
   - 3.3. Eine Freigabe zur Fahrberechtigung darf nicht nach der alleinigen Freigabe zur Öffnung des Kofferraumes erfolgen (z.B. Lieferservice).
4. Das Aktivieren (Scharfschalten) der eWFS muss folgende Anforderungen erfüllen:
   - 4.1. Sobald der Fahrer den Fahrzeuginnenraum verlässt[3], muss der (Elektro)Motor ausgeschaltet und die Fahrbereitschaft beendet werden.
   - 4.2. Sobald der berechtigte Schlüssel den Fahrzeuginnenraum verlässt[4], muss der (Elektro)Motor ausgeschaltet und die Fahrbereitschaft beendet werden. Bleibt der Fahrer im Innenraum und wird kein Schlüssel erkannt, soll der Fahrer über den anstehenden Entfall der Fahrberechtigung informiert werden.
   - 4.3. Die eWFS muss ohne Verzögerung aktiviert werden, sobald der (Elektro)Motor ausgeschaltet ist und keine Fahrbereitschaft mehr vorliegt.

[3] Beispielsweise: Kombination „Sitzbelegungserkennung = nicht belegt“ und „Fahrertür = geöffnet“
[4] Beispielsweise: Kombination „Schlüssel = nicht erkannt“ und „Fahrertür = geöffnet“

5. Unbefugte Deaktivierung bzw. Abschaltung der eWFS durch Dritte darf nicht möglich sein.
6. Unbefugte Erlangung der Zutrittsberechtigung durch Dritte, z.B. durch Manipulation des Bordnetzes, darf von außen nicht möglich sein.
7. Unbefugter Tausch von Steuergeräten – wie z.B. dem eWFS Steuergerät oder anderer an der Funktionalität der eWFS beteiligten Steuergeräte – und anschließende Wiederherstellung der eWFS Funktion darf nicht möglich sein ohne dokumentierte Autorisierung durch den Hersteller[5].
8. Kryptographisches Material zur Prüfung und Freigabe der Fahrberechtigung muss
   8.1. manipulationssicher in Steuergeräten gespeichert werden
   8.2. fahrzeugspezifisch und nicht übertragbar sein
   8.3. darf nicht im Klartext oder unverschlüsselt vorliegen.
9. Die Funktionalität der eWFS muss robust und sicher gegen Man-in-the-middle-Angriffe („Wegstreckenverlängerung“) konzipiert und konform zu ISO 21434 getestet werden. Dabei sind alle umgesetzten Übertragungstechnologien zu betrachten, wie z.B. RFID, NFC, BLE, UWB.

[5] (Fahrzeug-)Hersteller oder System-Operator: Der Fahrzeug-OEM oder ein von ihm dazu autorisierter Dritter, der Rechtspflichten und Systemverantwortungen anstelle des OEM übernimmt

3. Anforderungen an die physischen Schlüssel

Trotz der Verbreitung Virtueller Fahrzeugschlüssel werden physische Schlüssel ihre klassische Funktion beibehalten und von Versicherungsnehmern im Alltag weiterhin benutzt. Im Fall einer Totalentwendung werden physische Schlüssel in die Schadenanalyse einbezogen, um den gemeldeten Diebstahl zu plausibilisieren und einen Betrug auszuschließen.

Folgende Anforderungen werden an die physischen Schlüssel gestellt:

1. Ein sicherer Kopierschutz für den kompletten Schlüsselsatz, d.h. insbesondere die elektronischen Schlüsselbestandteile, muss gegeben sein.
2. Manuelle Eingaben einer PIN oder eines Codes zur Deaktivierung der Wegfahrsperre oder Erlangung der Zutrittsberechtigung sind nicht zulässig[6].
3. Eine Programmierung zusätzlicher Schlüssel darf nur im Online Modus und nur über einen sicheren Datenkanal zum Hersteller Backend stattfinden.
4. Jede Programmierung neuer oder zusätzlicher Schlüssel muss durch eine sofortige Protokollierung der Veränderung im Schlüsselsatz auf dem Hersteller Backend transparent dokumentiert werden.
5. Eine unautorisierte Schlüsselprogrammierung, Überschreibung oder Erweiterung des Originalschlüsselsatzes darf weltweit ohne bestehende verifizierte online Datenverbindung zum Hersteller Backend nicht möglich sein.
6. Weder eine PIN noch ein Code darf im Klartext an den Fahrzeugbesitzer oder eine Werkstatt für die Anlernprozedur neuer Schlüssel ausgehändigt werden.

[6] Hinweis: die in „AZT-Dokumente für elektronische Wegfahrsperren. Stand: Juni 1997. Letzte Ergänzung: 01.10.2007“ zugelassenen Option der PIN-Vergabe an den Fahrzeughalter, siehe „4.2 Anlernverfahren für neue Schlüssel und andere Komponenten“ wird nicht mehr akzeptiert. Daraus folgt, dass auch Eingabemöglichkeiten wie in „5.3 Manuelle Code-Eingaben“ nicht mehr zulässig sind.

4. Forensik und Datenplausibilisierung

Totaldiebstahl muss von den Versicherern plausibilisiert werden können. Für die Schadenplausibilisierung werden ereignis- und fahrzeugbezogene Daten vom Backend des Herstellers benötigt. Insbesondere bei polizeilichen Ermittlungen oder Rechtsstreitigkeiten müssen Daten zur letzten Nutzung über einen längeren Zeitraum forensisch verwendbar gespeichert bleiben, bis alle berechtigten Parteien Zugang hatten. Es muss sichergestellt werden, dass in diesen Fällen automatisierte Löschroutinen nicht angewendet werden.

Die Einverständniserklärung des Versicherungsnehmers im Rahmen seiner Mitwirkungspflicht zur Aufklärung des Sachverhalts berechtigt den Versicherer, notwendige Informationen beim Hersteller anzufragen und für die Aufklärung des Totaldiebstahls zu verwenden. Unter Berücksichtigung der Umstände des Einzelfalls ist daher insbesondere im Interesse des Versicherungsnehmers sicherzustellen, dass dieser seinen vertraglichen Mitwirkungspflichten nachkommen kann.

Für die Schadenbearbeitung und forensische Plausibilisierung einer Totalentwendung werden folgende Informationen bzgl. physischer und Virtueller Fahrzeugschlüssel benötigt:

1. Zugehörigkeit der vorgelegten Schlüssel zu dem gestohlenen Fahrzeug, d.h. passen der mechanische Schließcode und die elektronische Codierung zueinander und zu der FIN.

2. Vollständigkeit des vorgelegten Schlüsselsatzes, d.h. handelt es sich um den vollständigen Originalschlüsselsatz inkl. VFS, der mit dem gestohlenen Fahrzeug ausgeliefert wurde.

3. Gültigkeit des vorgelegten Schlüsselsatzes, d.h. wie viele Schlüssel lt. Herstellerdatenbank zum Diebstahlzeitpunkt am Fahrzeug funktionsfähig waren.

4. Nachlieferungen von Ersatzteilen und Schlüsseln, d.h. ob und wann zu dem gestohlenen Fahrzeug weitere Schlüssel und/oder Schlösser ausgeliefert wurden.

5. Veränderungen im vollständigen Originalschlüsselsatz, d.h. ob, wann und durch welchen Betrieb eine Authentifizierungsabfrage bzw. eine Onlineprogrammierung stattgefunden hat.

6. Auffälligkeiten im vorgelegten Schlüsselsatz, d.h. ob es Hinweise auf mechanische Manipulationen oder Auffälligkeiten in der Datenbank bzw. in der Fahrzeughistorie gibt.

7. Nutzungsdaten, z.B. Kilometerstände, Datum oder Betriebsdaten der letzten Benutzung im Kontext des Diebstahls.

8. Hinweise zu Schutzmaßnahmen gegen Totaldiebstahl, die für die Bewertung der schadenrelevanten Angaben hilfreich sind. Beispielsweise die Information, ob und welche Technologien gegen das bekannte Entwendungsszenario der Wegstreckenverlängerung umgesetzt wurden. Ist z.B. ein Schließsystem mit passiven[7] Schlüsseln in Kombination mit Bewegungssensoren und/oder mit UWB Technologie verbaut?

9. Spezifische Informationen zu Virtuellen Fahrzeugschlüsseln. Nutzt der Versicherungsnehmer einen VFS, wird er mit besonderen Schwierigkeiten bei seiner Mitwirkungspflicht zur Plausibilisierung konfrontiert. Die Forensik ist daher seitens des System-Operators mit folgenden Informationen gemäß dem internationalen RCAR Standard zu unterstützen:

    - Der jeweilige Zeitstempel aller VFS Nutzer-Registrierungen
    - Der jeweilige Zeitstempel aller VFS Downloads
    - Der Zeitstempel der jeweiligen Authentifizierung am Fahrzeug
    - Die Anzahl aller aktiven VFS inkl. Multi-Keys, Card-Keys und temporärer VFS
    - Der Zeitstempel einer VFS Löschung, d.h. eine vollständige Liste aller revozierten VFS
    - Der Zeitstempel und die Geokoordinaten der letzten registrierten VFS Anwendung.

[7] Schlüssel, die nicht aktiv betätigt werden müssen, um das Auto zu öffnen oder zu starten

5. Glossar

Tabelle 1: Begriffe

Begriffe	Vollständige Begriffsbeschreibung
BLE	Bluetooth Low Energy Technologie
eWFS	Elektronische Wegfahrsperre
FIN	Fahrzeug Indentifikationsnummmer
Fahrbereitschaft	Fahrbereitschaft ist nach UN ECE-R116 gegeben, wenn „sich der Zündschlüssel in der Stellung befindet, in der der Motor läuft“. Bei modernen passiven Schlüsseln entspricht dies dem Zustand nach Motorstart.
Hersteller	Der Fahrzeug-OEM bzw. Inverkehrbringer
Lebenszyklus des Fahrzeugmodells	Zeitraum zwischen SOP und EOP plus zwei Jahre
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
PIN	Personal Identification Number
Prüfung der Identität und Zugriffserlaubnis	Die *Authentisierung* stellt einen ersten Schritt zur Prüfung der Identität dar, indem eine Person aktiv eine bestimmte Identität behauptet. *Authentifizierung*: Prüfung der behaupteten Authentisierung. Die *Autorisierung* ist die Einräumung von speziellen Rechten.
System-Operator	Ein vom Fahrzeug-OEM autorisierter Dritter, der Rechtspflichten und Systemverantwortungen, z.B. Backend, anstelle des OEM übernimmt
UWB	Ultra Wide Band (Technologie)
VFS	Virtueller Fahrzeugschlüssel