

Virtueller Autoschlüssel muss sicher sein



· Allianz stellt Anforderungskatalog für Virtuellen Schlüssel vor · Totaldiebstahl muss für Kunden weiterhin nachweisbar sein · Nur der nicht kopierbare Virtuelle Schlüssel ist sicher

Die Heizung von unterwegs regeln, schnell eine Überweisung per App tätigen – das Smartphone ist längst mehr als ein Gerät zum Telefonieren und Nachrichtenschreiben. Musik hören, SMS vorlesen lassen – auch im Auto sind alle Geräte vernetzt. Im nächsten Schritt wird das Smartphone jetzt zum Autoschlüssel. Der Fahrer öffnet und startet das Fahrzeug künftig über die App, der Schlüssel wird virtuell.

Das ist komfortabel, birgt aber auch Risiken. Wie steht es beispielsweise um die Datensicherheit, was passiert, wenn das System gehackt wird? Auch für die Versicherung wirft diese Technik viele Fragen auf, insbesondere im Falle eines Totaldiebstahls. Bisher reicht der Kunde für die Regulierung den vollständigen Schlüsselsatz bei der Versicherung ein. Dies gilt grundsätzlich auch für den Virtuellen Fahrzeugschlüssel. Kein Kunde wird dem Versicherer im Falle eines Fahrzeugdiebstahls sein Smartphone zuschicken wollen. Er muss deshalb jeden Berechtigten nennen, der zum Zeitpunkt der Totalentwendung im Besitz eines Virtuellen Schlüssels war, und einen Nachweis über die Löschung der Berechtigung vorlegen. „Wir müssen sicherstellen, dass wir unsere Kunden bei einem Totaldiebstahl auch bei der Verwendung Virtueller Schlüssel komplikationslos entschädigen können. Deshalb fordern wir verbindliche Standards für den Virtuellen Schlüssel“, sagt Jochen Haug, Schadenvorstand der Allianz.

Virtueller Fahrzeugschlüssel darf nicht kopierbar sein

Die Experten des Allianz Zentrum für Technik (AZT) haben deshalb Anforderungen an die Gestaltung des Virtuellen Schlüssels formuliert, die ein Leitfaden für die Systemauslegung und zugleich offen für unterschiedliche technische Lösungen sind. „Der Kunde muss dem Virtuellen

Schlüssel vertrauen können. Das geht nur, wenn Datensicherheit garantiert ist. Das heißt, der Schlüssel darf zum Beispiel nicht kopierbar sein“, sagt Christoph Lauterwasser, Leiter des AZT. „Außerdem brauchen wir im Falle eines Totaldiebstahls einen transparenten Überblick, wer wann für welchen Schlüssel berechtigt wurde.“

Die vier wichtigsten Anforderungen an den Virtuellen Fahrzeugschlüssel

- Der Virtuelle Fahrzeugschlüssel darf nicht kopierbar sein, analog zum physischen Schlüssel muss erkennbar sein, wie viele Schlüssel im Umlauf sind.
- Alle berechtigten Fahrzeugnutzer müssen übersichtlich, transparent und unveränderlich für den Kunden – sowie im Schadenfall für die Versicherung aufgeführt sein. Der Kunde muss zudem bei einem Totaldiebstahl sofort alle Virtuellen Schlüssel nachweisbar zurückziehen können.
- Die Zugangsberechtigung des Autos muss von der Fahrberechtigung getrennt sein, um das bestehende Schutzniveau der elektronischen Wegfahrsperre nicht zu unterlaufen und die Sicherheit bei zukünftigen Dienstleistungsmodellen wie „Lieferung in den Kofferraum“ zu gewährleisten.
- Die Datenumgebung von Ausführung und Speicherung des Virtuellen Schlüssels muss strikt von sonstigen Applikationen getrennt sein. Alle sicherheitskritischen Daten wie z.B. Berechtigungen und Schlüsselberechnung müssen in einer sicheren Speicher- und Ausführungsumgebung gespeichert bzw. ausgeführt werden.

Eine vollständige Übersicht der Forderungen des AZT an Fahrzeughersteller finden Sie hier:
http://azt-automotive.com/index.php/download_file/47/

Kontaktdaten:

Allianz Deutschland AG
Unternehmenskommunikation
Christian Weishuber
Telefon: +49 (0)89 3800 18169
E-Mail: christian.weishuber@allianz.de