
Bild: doubleslash

# Wie digitale Schlüssel Nutzfahrzeuge sicherer und effizienter machen

## Physische Schlüssel als Sicherheitsproblem

Viele Unternehmen der Nutzfahrzeugbranche setzen immer noch auf ein analoges Schlüsselmanagement: Physische Schlüssel werden ausgegeben, verteilt und wieder eingezogen. Dieser Prozess ist nicht nur zeitaufwändig, sondern birgt auch erhebliche Sicherheitsrisiken. Gehen Schlüssel verloren oder werden sie gestohlen, hat das Unternehmen ein Sicherheitsproblem und organisatorischen Aufwand. Niemand kann mehr kontrollieren, wer tatsächlich Zugang zu den Fahrzeugen hat. Hinzu kommen alltägliche organisatorische Herausforderungen wie kurzfristige Ausfälle von Fahrern oder Schichtwechsel. Je größer der Fuhrpark, desto komplexer die Verwaltung. Fuhrparkmanagement mit physischen Schlüsseln ist unflexibel und birgt Risiken, doch es gibt bessere Lösungen: digitale Schlüssel.

## Der Digitale Schlüssel des Car Connectivity Consortiums

Eine Alternative zur klassischen Schlüsselverwaltung bieten moderne digitale Zugangssysteme. Ein Beispiel hierfür ist der digitale Schlüssel des Car Connectivity Consortium (CCC). Das Car Connectivity Consortium ist eine Organisation, die sich auf die Entwicklung und Förderung von Standards für die Verbindung zwischen Fahrzeugen und mobilen Geräten konzentriert. Im CCC arbeiten Unternehmen aus der Automobil- und Technologiebranche gemeinsam an neuen Standards. Der digitale Schlüssel des CCC kann über das Smartphone genutzt werden. Damit haben Flottenbetreiber die Möglichkeit, ihren Mitarbeitenden gezielt digitale Schlüssel zuweisen und diese bei Bedarf flexibel anzupassen oder zu entziehen. Das reduziert den administrativen Aufwand, erleichtert das Nutzfahrzeugmanagement und minimiert Sicherheitsrisiken. Durch die individuelle Vergabe von Berechtigungen können Flottenbetreiber sicherstellen, dass nur berechtigte Personen Zugang zu bestimmten Fahrzeugbereichen wie Fahrerkabine oder Laderaum erhalten.

## Server-based Owner Device als zusätzliche Komponente

Ein wesentlicher technologischer Fortschritt ist das Server-based Owner Device (SBOD) als zusätzliche Systemkomponente. Die digitalen Schlüssel werden

zentral auf einem Server verwaltet und nicht mehr auf den einzelnen Endgeräten. Dies ermöglicht eine effiziente und sichere Verteilung von Zugangsberechtigungen innerhalb einer Nutzfahrzeugflotte. So kann beispielsweise ein Fahrer Zugang zur Fahrerkabine und zum Laderaum erhalten, während ein Mechaniker nur Zugang zu den Wartungsbereichen des Fahrzeugs hat. Zusätzlich erhöht die Speicherung der digitalen Schlüssel im Secure Element eines Smartphones die Sicherheit, da dieses wie ein verschlüsselter Tresor funktioniert. Auch unter erschwerten Bedingungen, z. B. in Gebieten mit eingeschränkter Netzabdeckung, bleibt der Zugriff durch Offline-Funktionalitäten gewährleistet.

## Integration von Digital Keys in die Hardware des Fahrzeugs

Damit digitale Schlüssel in der Praxis eingesetzt werden können, müssen zunächst die entsprechenden Fahrzeuge Digital-Key-fähig sein. Dies setzt eine Backend-Lösung voraus, die sich nahtlos in die Fahrzeughardware des OEM integrieren lässt. Wie beim Digital Key von doubleSlash geschieht dies über standardisierte Schnittstellen, die eine direkte Kommunikation mit der Electronic Control Unit (ECU) ermöglichen. So entsteht ein harmonisiertes Zusammenspiel zwischen Fahrzeug und Backend. Die Lösung basiert auf einem modularen und flexiblen Design und ist CCC-konform. Die hardware- und cloud-agnostische Architektur ermöglicht eine einfache Integration in unterschiedlichste Systemlandschaften. Das Server-Based Owner Device (SBOD) ermöglicht die Anbindung von Flottenmanagementsystemen über standardisierte Schnittstellen, so dass Fahrzeugflotten effizient und sicher verwaltet werden können.

Ein wesentlicher wirtschaftlicher Vorteil dieser Technologie ist die Reduzierung des administrativen Aufwands und der Verlust von Schlüsseln. Erste Fallstudien zeigen, dass Unternehmen durch den Einsatz digitaler Schlüssel die Übergabedauer deutlich verkürzen und die Kosten für verlorene Schlüssel eliminieren können. Eine detaillierte Kosten-Nutzen-Analyse kann Unternehmen helfen, die möglichen Einsparungen und Effizienzsteigerungen realistisch einzuschätzen.

## Fazit: Digitales Schlüsselmanagement als Standard der Zukunft

Die Nutzfahrzeugindustrie steht vor der Herausforderung, betriebliche Abläufe effizienter zu gestalten und gleichzeitig Sicherheitsrisiken zu minimieren. Digitale Schlüsseltechnologien bieten hierfür eine zukunftsorientierte Lösung, indem sie eine flexible Berechtigungsvergabe ermöglichen, den administrativen Aufwand reduzieren und die Betriebssicherheit erhöhen. Unternehmen, die frühzeitig auf digitale Zugangslösungen setzen, können nicht nur ihre internen Prozesse kosteneffizient optimieren, sondern sich auch langfristig Wettbewerbsvorteile sichern.

MANUEL TEUFEL

*Autorenprofil Manuel Teufel, Produktmanager doubleSlash Digital Key*

*Manuel Teufel ist studierter Software-Produktmanager. Er verfügt über 10 Jahre Erfahrung in Software-Projekten und -Produkten in der Mobility Branche. Manuel ist verantwortlicher Produktmanager für den doubleSlash Digital Key und treibt den Wandel vom physischen zum digitalen Schlüssel voran.*