LEGIC

White Paper

Enabling secure mobility solutions

Dr. Felix Pütz, Head of Business Unit Mobility and Smart City,
LEGIC Identsystems AG

Vier Gestaltungsprinzipien für skalierbare Mobilitätsdienste

Zusammenfassung

Der Trend, Fahrzeuge nicht mehr zu besitzen, sondern nach Bedarf zu nutzen und mit anderen zu teilen, ist bei Auto-, E-Bike- und E-Scooter-Sharing-Diensten immer beliebter geworden. In der Sharing Economy spielen Skalierbarkeit und Sicherheit für Anbieter eine wichtige Rolle, während Benutzer Datenintegrität und personalisierte Nutzererlebnisse erwarten. Daher müssen Fahrzeugzugriff und Serviceberechtigungen per Smartcard oder Smartphone sicherstellen, dass die Integrität der Benutzer, Systeme und Daten garantiert ist.

Enabling secure and convenient mobility applications

Die neueste Generation von Fahrzeugen hat sich zu komplett digitalisierten, drahtlos vernetzten Rechnerknoten entwickelt. Dies erleichtert den sozialen Wandel und verändert herkömmliche Geschäftsmodelle.

Früher besass man in der Regel ein teures Fahrzeug, das zu 95% der Zeit irgendwo auf einem Parkplatz stand (Quelle: Fortune).

Heute dagegen erzielt der durch die drahtlose Kommunikation ermöglichte Carsharing-Markt eine durchschnittliche jährliche Wachstumsrate (CAGR) von 16,2% und dürfte bis 2027 einen globalen Markt von fast 6.5 Billiarden USD erreichen.

Heute nutzen mehr als 43 Millionen Personen Carsharing-Dienste, wobei die Sektoren Autovermietung und Taxi noch nicht berücksichtigt sind (Quelle: Statista).

Die Vorteile von Carsharing sind überzeugend. Einzelpersonen haben Zugang zu privaten Autos, ohne die Kosten und Verantwortung, die mit dem Eigentum an einem Fahrzeug verbunden sind. Mit der bevorstehenden Zunahme fahrerloser Fahrzeuge, die weder abgeholt noch zurückgebracht werden müssen, wird sich dieser Trend weiter beschleunigen.

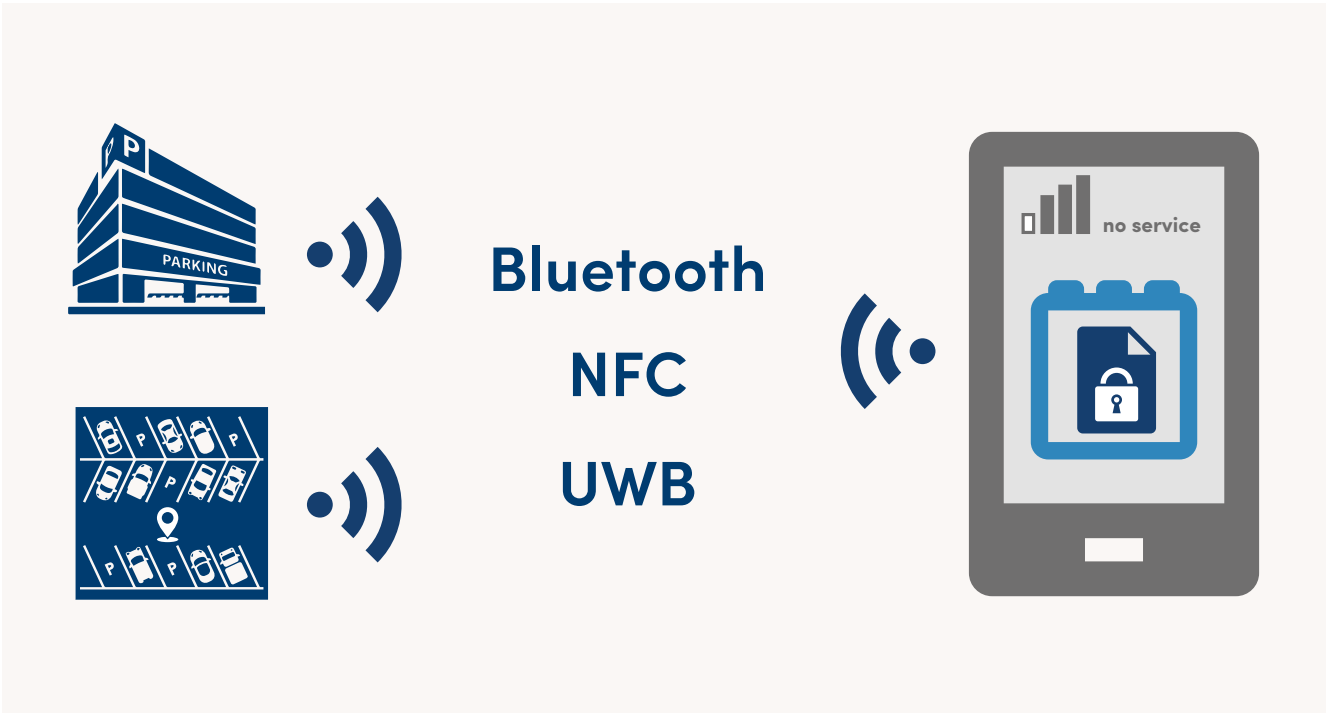
Intelligente Fahrzeuge, die drahtlos kommunizieren können, um Benutzer zu authentifizieren und ihnen Zugang zu gewähren, bilden eine technologische Triebfeder dieses Trends. Allerdings sind Informationen, die Over-the-Air zwischen Benutzern und Fahrzeugen übertragen werden, gefährdet, denn sie stellen eine Angriffsfläche für potenzielle Hacker und Diebe dar. Damit ist auch ein Risiko durch Dienstausfälle ein Thema, dem Beachtung geschenkt werden sollte.

Aufgrund der langjährigen Erfahrung auf dem Gebiet der sicheren, kontaktlosen Authentifizierung hat LEGIC vier Best Practices für Anbieter bei der Einführung neuer Mobilitätsdienste erarbeitet:

1) Lokale drahtlose Kommunikation ist ein Muss

Der Smartphone-basierte Fahrzeugzugang ist die Voraussetzung für das Sharing von Fahrzeugen. Erfahrungen mit Diensten, die eine Online-Konnektivität erfordern, zeigen jedoch, dass Mobilfunkdienste für die Nutzung von Mobilitätsdiensten oft nicht ausreichend zuverlässig sind. Niemand will beispielsweise mit Kindern und Lebensmitteln vor einem verschlossenen Fahrzeug stehen und es nicht aufschliessen können, weil es in der Tiefgarage keinen Mobilfunkempfang gibt. Ein Mobilitätsdienst, der den Zugang zum Fahrzeug über lokale Kommunikation ermöglicht, ist eine bessere und zuverlässigere Option, die die Abhängigkeit von der Mobilfunkkonnektivität beseitigt. Die lokale Kommunikation über RFID, Bluetooth oder Ultra Wide Band (UWB) zwischen Smartphone/

Gestaltungsprinzip 1: Lokale drahtlose Kommunikation ist ein Muss



Smartcard und Fahrzeug ist schnell, zuverlässig und energieeffizient.

Die Kombination einzelner User Journeys mit lokaler Kommunikation beschreibt den bequemsten Weg zur Benutzerzufriedenheit, da jede Buchung individuell sein kann. Darüber hinaus wirdein effizienter und unterbrechungsfreier Service-betrieb sichergestellt, da Fahrzeuge als Gateways zum Sevice-Manage-ment-System mit den Smartphones ihrer Benutzer verbunden bleiben, auch wenn das Fahrzeug selbst, möglicherweise offline ist.

2) Unterstützung für Interopera-bilität

Neue Mobility Services erfordern häufig, dass mehrere Anwendungen in einer einzigen Fahrzeuginfras-truktur untergebracht sind. Dasselbe Fahrzeug kann gleichzeitig als Teil einer Carsharing-Flotte, für Paket-zustelldienste („In-Car Delivery"), als Energiespeichersystem („Vehicle-to-Grid" oder V2G) sowie als persönliche Mobilitätsgarantie genutzt werden. Ziel muss es sein, eine Mobilitätsin-frastruktur zu schaffen, die eine Vielzahl bereits vorhandener und zukünftiger Dienste unterstützt, die Fahrzeugnutzung optimiert und gleichzeitig die Umweltbelastung so gering wie möglich hält.

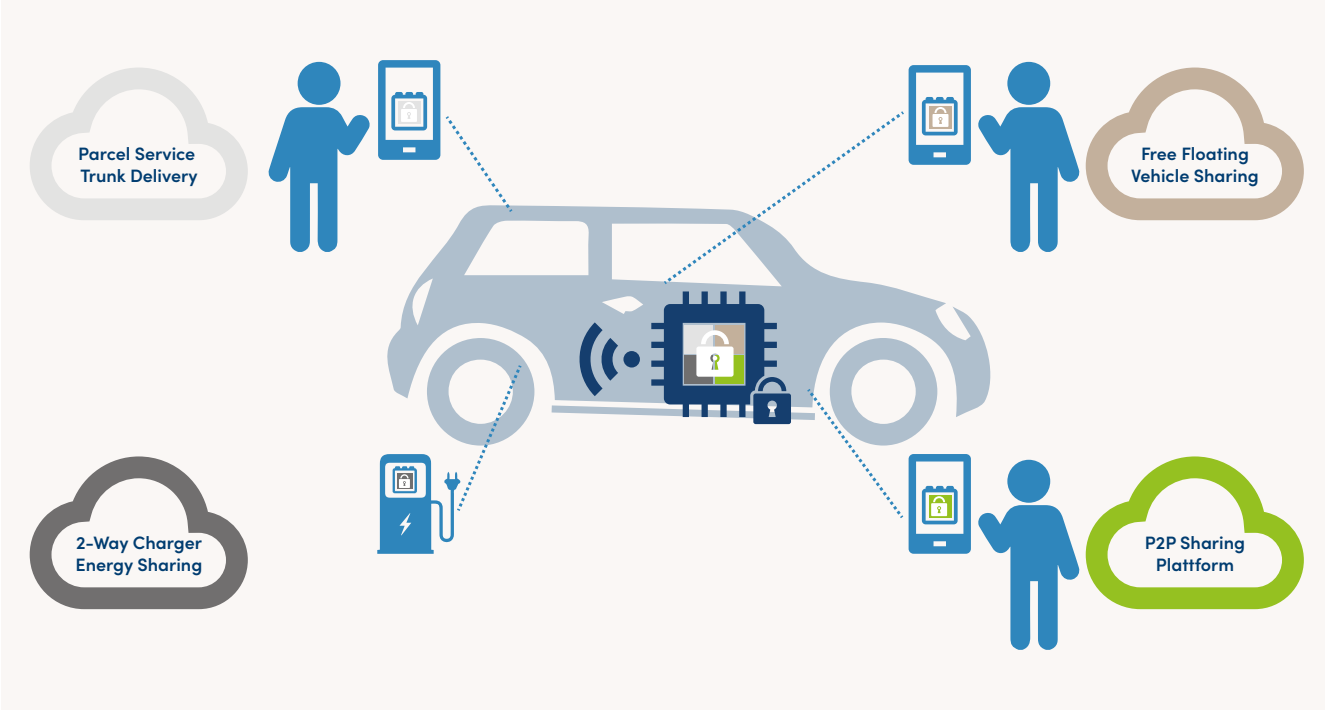
3) Sicherheit und Kontrolle für den Service-Anbieter sicherstellen

Neben der Wahrung der Sicherheit und Vertraulichkeit für die Nutzer in Bezug auf Führerschein, Kredit-kartendaten, persönliche Profile, virtuelle Schlüssel und Standortdat-en, muss auch das Geschäftsmodell des Anbieters von Mobilitätsdiensten geschützt werden. Der Schutz wert-voller Infrastruktur vor Missbrauch muss sichergestellt sein.

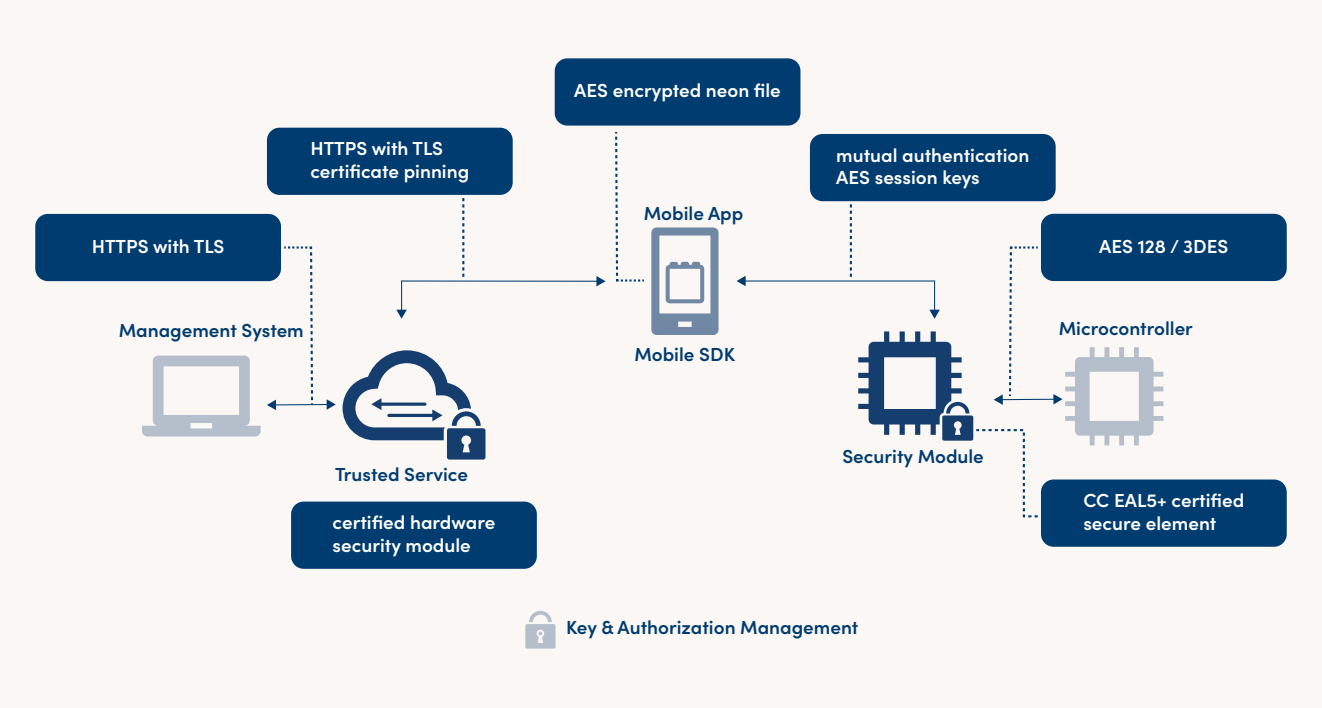
Die sichere Interaktion zwischen Service-Anbietern, Nutzern und Fahrzeugen muss sichergestellt werden, nicht nur mit dem Netzwerk des Service Providers, sondern auch am Netzwerkrand zwischen Nutzern und Infrastruktur über Kurzstrecken-kommunikation wie Bluetooth und NFC. Alle Komponenten müssen mit-einander kommunizieren können, und das System muss bei Ausfall einer Netz- werkverbindung weiter-hin sicher funktionieren.

Insbesondere wenn der Service grösser skaliert werden soll, ist es

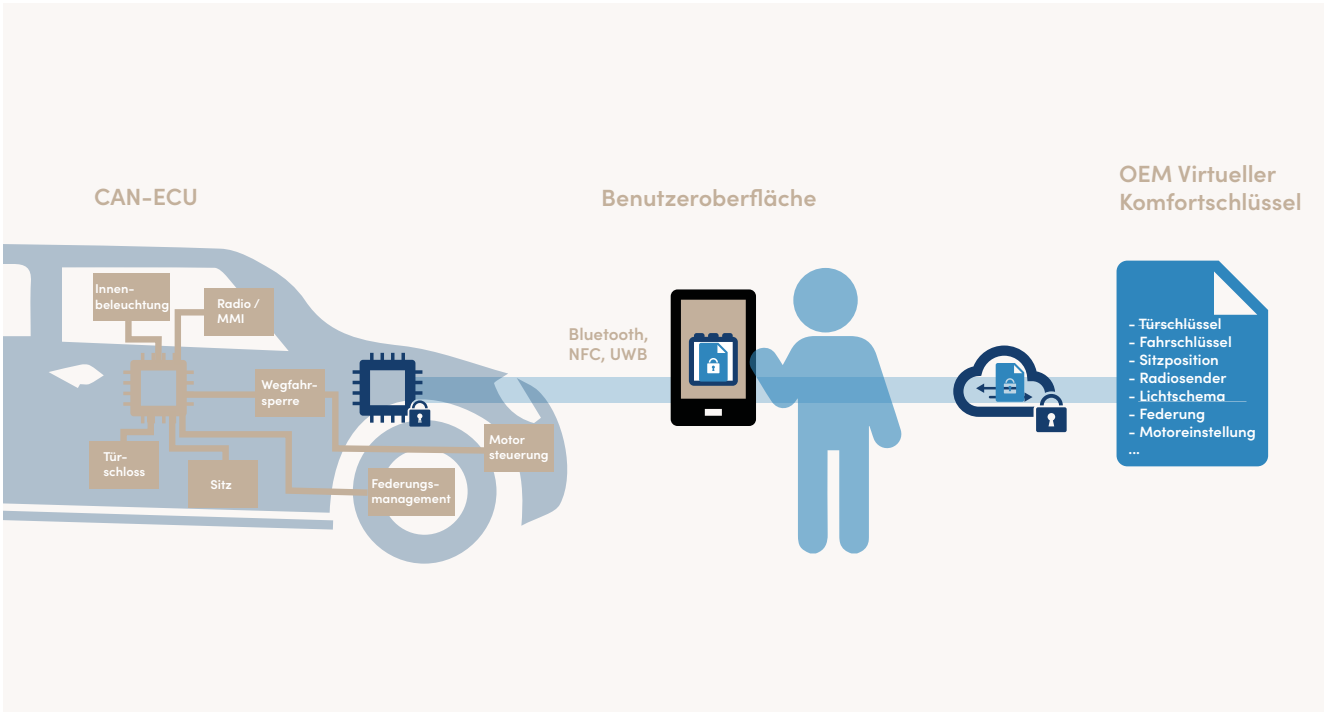
Gestaltungsprinzip 2: Unterstützung für vielfältige Anwendungen möglich machen

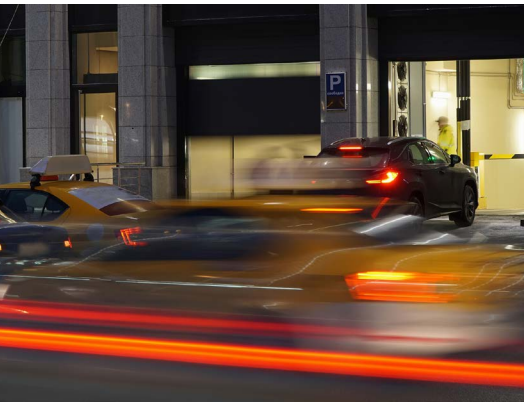


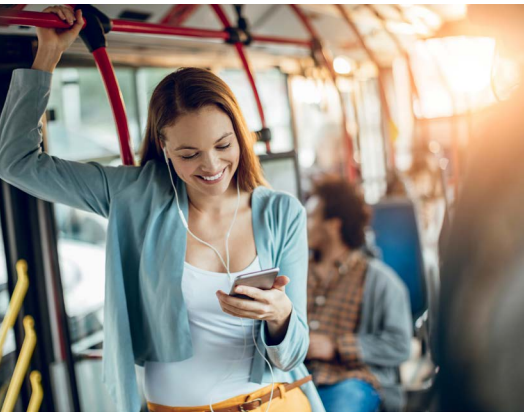
Gestaltungsprinzip 3: Sicherheit und Kontrolle für den Service-Anbieter sicherstellen



Gestaltungsprinzip 4: Flächendeckende und sichere Konnektivität bereitstellen







wichtig, eine Sicherheitsschicht zu implementieren, die mit der gleichen Geschwindigkeit und Robustheit wie der Service selber, skaliert werden kann.

4) Das Nutzererlebnis muss individualisiert werden

Die Nutzer von Mobilitätsdiensten werden sich am meisten von einem individuellen Erlebnis angesprochen fühlen. Wenn ein Fahrer in ein gemeinsam genutztes Fahrzeug einsteigt, erwartet er oder sie, dass sich Sitzposition, Federung, Klimaregelung, Radio, Navigation, Lichteinstellungen usw. automatisch an seine persönlichen Vorlieben anpassen.

Diese individuellen Einstellungen sind Teil des Mobile Credentials eines Benutzers und müssen auch ohne Netzverbindung funktionieren, um ein einheitliches Benutzererlebnis sowohl in Online- als auch in Offline-Nutzungsfällen zu bieten.

Dies ermöglicht es Dienstanbietern, ihre Angebote zu differenzieren und einen Mehrwertdienst anzubieten, der als Option mit bestimmten Autoherstellern und Fahrzeugmodellen gebündelt werden kann

LEGIC ermöglicht neue Mobilitätslösungen

LEGIC ist gut gerüstet, um den Anforderungen dieser schönen, neuen Mobilitätswelt gerecht zu werden. Wir ermöglichen Anbietern von Mobility Services die schnelle Implementierung einer sicheren, kontaktlosen Kommunikationslösung zwischen Menschen und Infrastruktur, so dass die Anbieter ihre Entwicklungsanstrengungen auf Anwendungen und die Benutzererfahrung konzentrieren können. Wir helfen Ihnen bei der Implementierung sicherer, überzeugender Mobility Services, die über die bereits vorhandene Telekommunikationsinfrastruktur verwaltet werden.

Einzelheiten finden Sie unter www.legic.com/mobility

Über LEGIC

Seit über 30 Jahren ermöglicht LEGIC Unternehmen aus aller Welt die Implementierung von Lösungen mit anspruchsvollen Sicherheitsanforderungen. Auf der Grundlage von Schlüsselverwaltung, Trusted Services und sicheren, kontaktlosen Halbleitern bietet die LEGIC-Sicherheitsplattform End-to-End-Sicherheit für Smartphone- und Smartcard-basierten Zugriff, Mobilität, gemeinsam genutzte Ressourcen und industrielle IoT-Anwendungen.

Author: Felix Pütz, Carl Fenger

Oktoberr 2022