LEGIC

White paper

Enabling secure mobility solutions

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

Four Design Principles for scalable Mobility Services

Summary

The trend of no longer owning vehicles but using them as required and sharing them with others has become increasingly popular with car, e-bike and e-scooter sharing services. In the sharing economy, scalability and security plays an important role for providers, while drivers expect data integrity and personalized user-journeys. Thus, vehicle access and service authorization via smartcard or smartphone must ensure that user, system and data security are guaranteed.

Enabling secure and convenient mobility applications

The latest generation of vehicles has become digitally enabled, wirelessly networked computing nodes; this is facilitating social change and altering traditional business models.

Where once the norm was to own an expensive vehicle which sat parked 95% of the time (source: Fortune), the Car Sharing Market has exceeded USD 2 billion in 2020 and is poised to grow at a CAGR of over 25% to USD 6.5 billion by 2027 (source. Global Market Insights).

There are over 43 million users of car sharing services today, and that does not even include the car rental or taxi sectors (source: Statistica).

The benefits of carsharing are compelling; individuals have access to vehicles without the costs and inconveniences of owning one. With the imminent rise of driverless vehicles which do not need to be picked-up or dropped-off, this trend will only accelerate.

Although intelligent vehicles that can wirelessly communicate with service providers to authenticate and grant access to users is the technological driver of this trend, the increased exposure of information and communications over-the-air between users and vehicles has opened up a large attack surface for potential hackers and thieves. Increased risk of service outage or compromised business models are also important issues for service providers to address.

Based on many years of experience in the field of secure, contactless authentication, LEGIC has worked out four best practices for providers when deploying new mobility services:

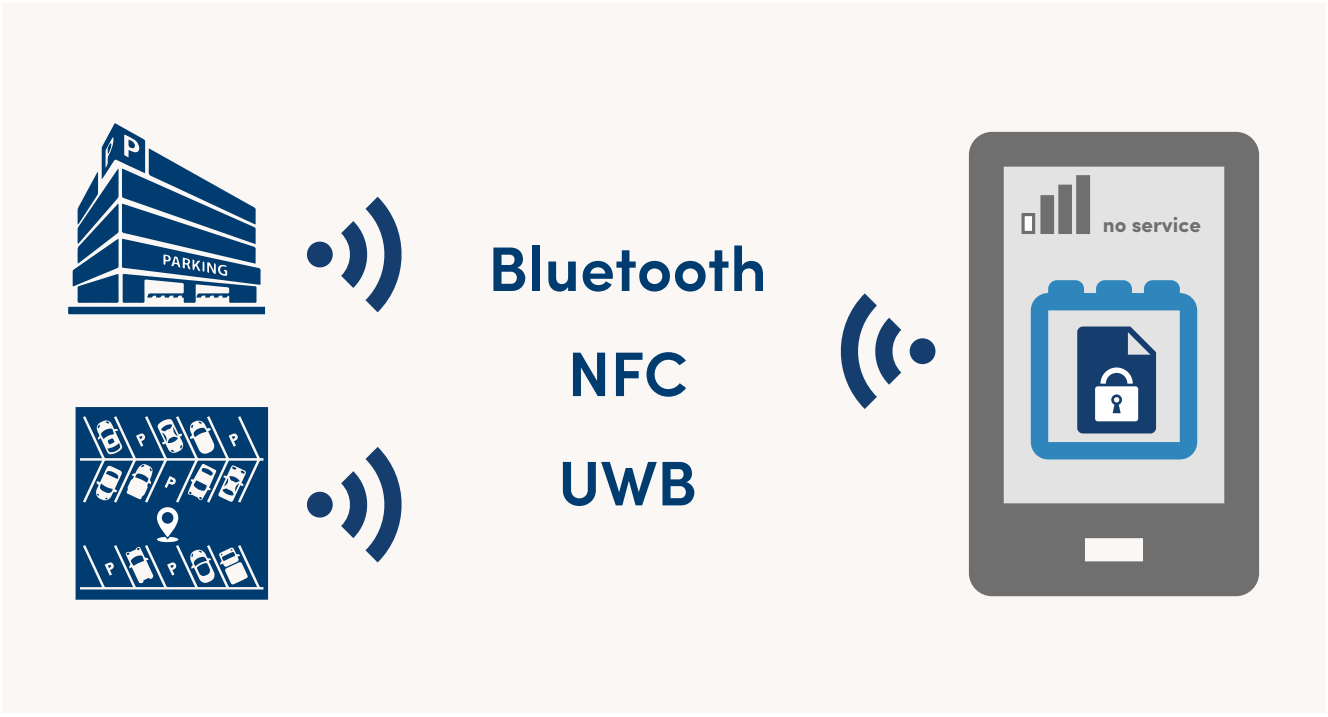
1) Local wireless communication is key

Smartphone-based access is the enabler for mobility services. Experience with requiring online connectivity show, however, that cellular services are often unreliable for use with mobility services. Nobody wants to stand in front of a locked vehicle with children and groceries, unable to open the door because there is no cellular reception in the underground park house.

A mobility service that enables vehicle access via local communications is a better and more reliable option, eliminating dependency on cellular connectivity. Local communication via RFID, NFC, Bluetooth or Ultra Wide-Band (UWB) communications between smartphone/smartcard and vehicle is fast, reliable and energy efficient.

Combining individual user-journeys with local communication is the most effective way to achieve user-satisfaction as every booking can be individualized independent of a network connection. This ensures efficient, uninterrupted service-operation as vehicles stay connected with their users' smartphones which act as gateways to the service management system, even if the vehicle itself might be offline.

Design Principle 1: Local wireless communications is key



2) Support multi-application readiness

New mobility services will require multiple application ecosystems to be hosted within a single vehicle infrastructure. The same vehicle could be used as part of a car sharing fleet, for parcel delivery services ("In-Car Delivery"), as an energy storage system ("Vehicle-to-Grid" or V2G), as well as personal mobility guarantee, all at the same time.

The goal must be to deploy a mobility infrastructure that supports multiple, different, existing as well as future services, optimizes vehicle usage, and keeps environmental impact to a minimum. These services typically need discrete security mechanisms which must still come together on the same vehicle.

3) Ensure end-to-end security and control for the service provider

In addition to maintaining safety and confidentiality for users with regards to driver's license, credit card details, personal profiles, virtual keys and location-data, the mobility service provider's business processes, the source of their revenues, must be safeguarded. Protection of valuable infrastructure from misuse must be guaranteed.

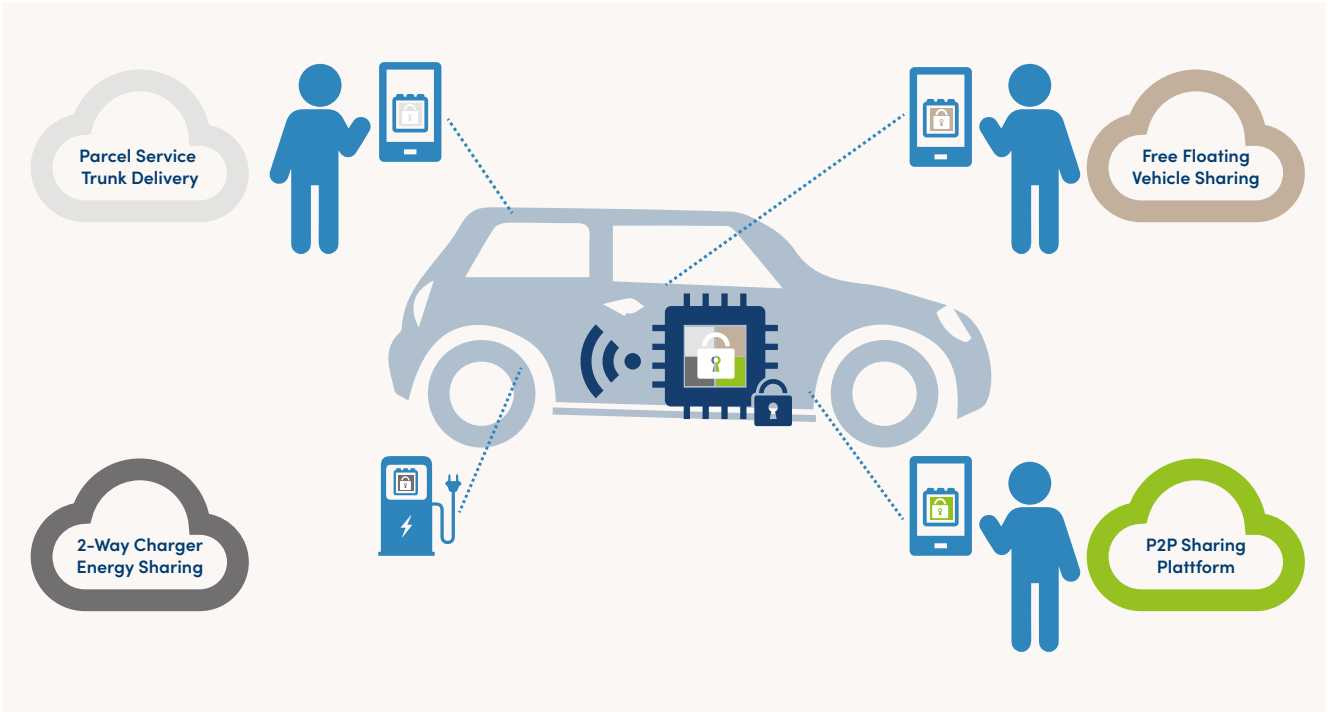
Secure interaction between service providers, users and vehicle is critical, not only over the service provider's network, but also at the network edge between users and infrastructure via short-range communications such as Bluetooth, NFC or UWB. All components must be able to communicate which each other, and the system must continue to operate should a network link fail.

When mobility services expand, it is also important to have implemented a security layer which is able to scale with the same speed and robustness as the service grows.

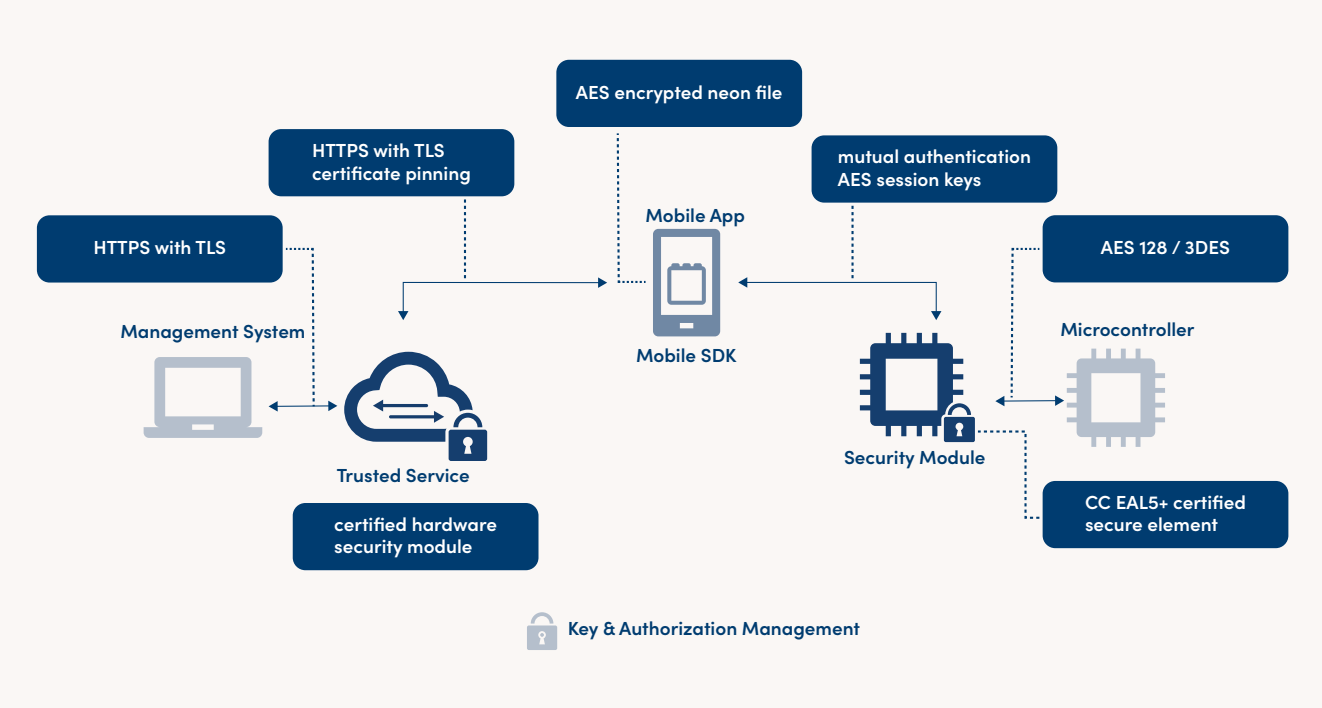
4) The user experience must be individualized

Users of mobility services will be most attracted to an individualized experience. When a driver enters a shared vehicle, he or she will expect the seat position, suspension, climate control, radio, navigation, light settings, etc. to automatically adjust to their personal preferences.

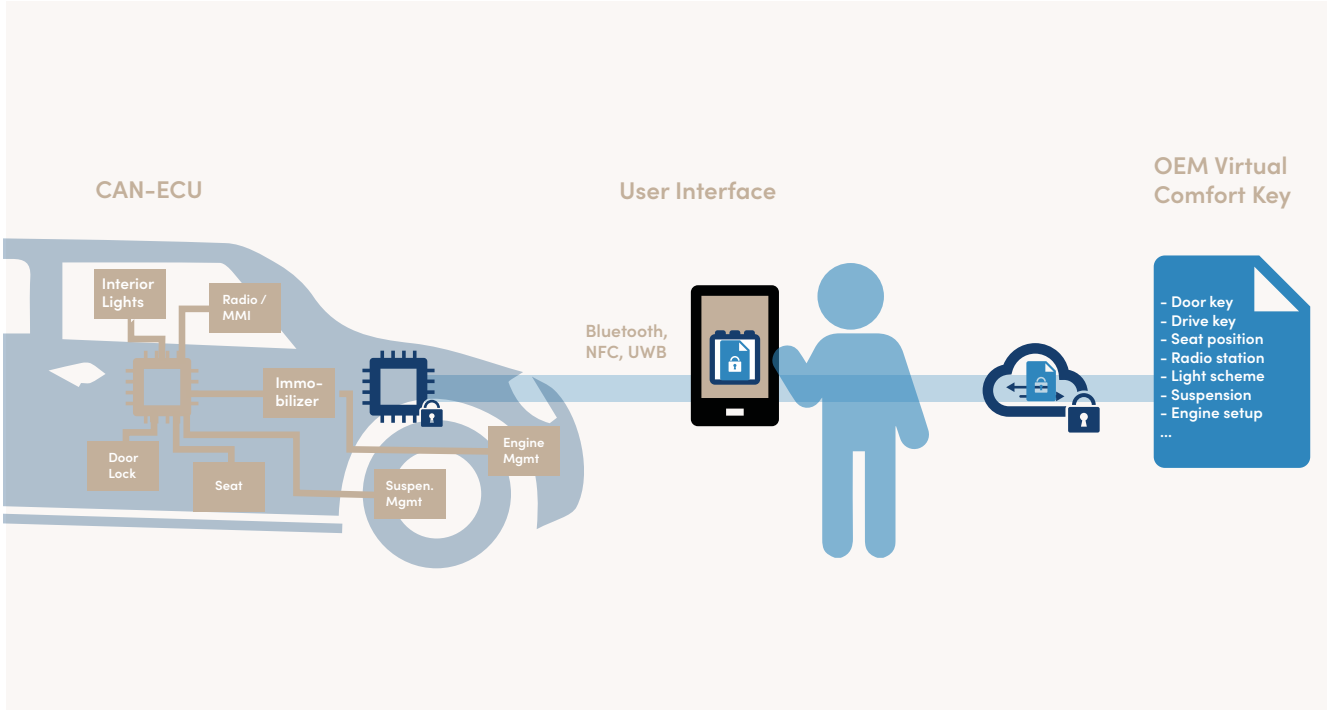
Design Principle 2: Support multi-application readiness

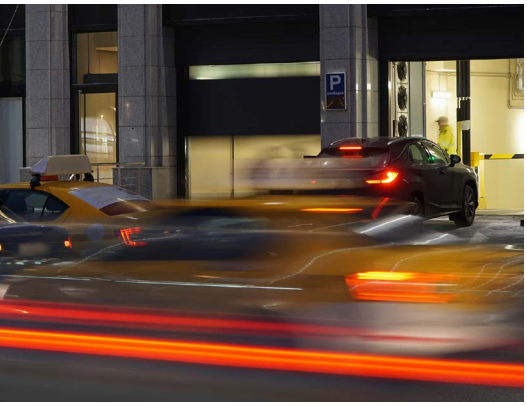


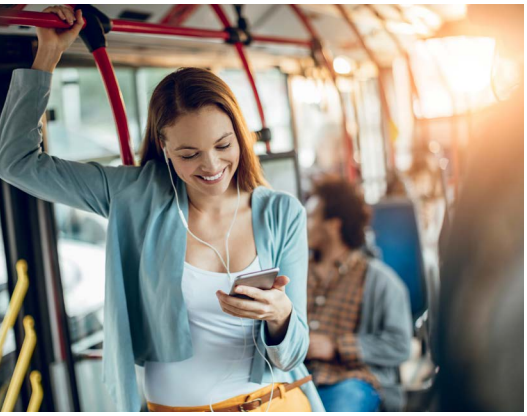
Design Principle 3: Ensure end-to-end security and control for the service provider



Design Principle 4: The user experience must be individualized







These individual settings are part of a user's mobile credential and must also work in the absence of network connectivity in order to offer a consistent user experience in both online and offline use cases.
This allows service providers to differentiate their offerings, as well as provide an added-value service that can be bundled together as an option with specific automakers and vehicle models.

LEGIC: enabling new mobility solutions

LEGIC is well equipped to help meet the demands of the new world of mobility. We enable mobility service providers to quickly deploy a secure, contactless communication solution between people and infrastructure, allowing them to concentrate their development efforts on applications and the user experience.

For details, visit:
www.legic.com/mobility

About LEGIC

For over 30 years, Swiss-based LEGIC Identsystems has enabled companies from around the world to deploy solutions with demanding security requirements. Based on key management, trusted services and secure, contactless semiconductors, the LEGIC Security Platform provides end-to-end security for smartphone- and smartcard-based access, mobility, shared resource and industrial IoT applications.

Author: Felix Pütz, , Carl Fenger

October 2022