infopulse

Case for **Manufacturer of Electric Cars**

Digital Key Concept: Modernized Access to a Shared Vehicle

Simplified Vehicle Access and Improved Fleet Management
with a Digital Key Solution

Industry: Automotive   **Location: Germany**

Client Background

The company we collaborate with produces commercial EVs used solely for logistics needs. They wanted to streamline their fleet management by simplifying a complicated procedure of granting access to the same vehicle from one driver to another and eliminating the number of lost keys to commercial vehicles.

Business Challenge

As an avid follower of sustainable manufacturing, the company we collaborate with produces commercial EVs used solely for logistics needs. They wanted to streamline their fleet management by:
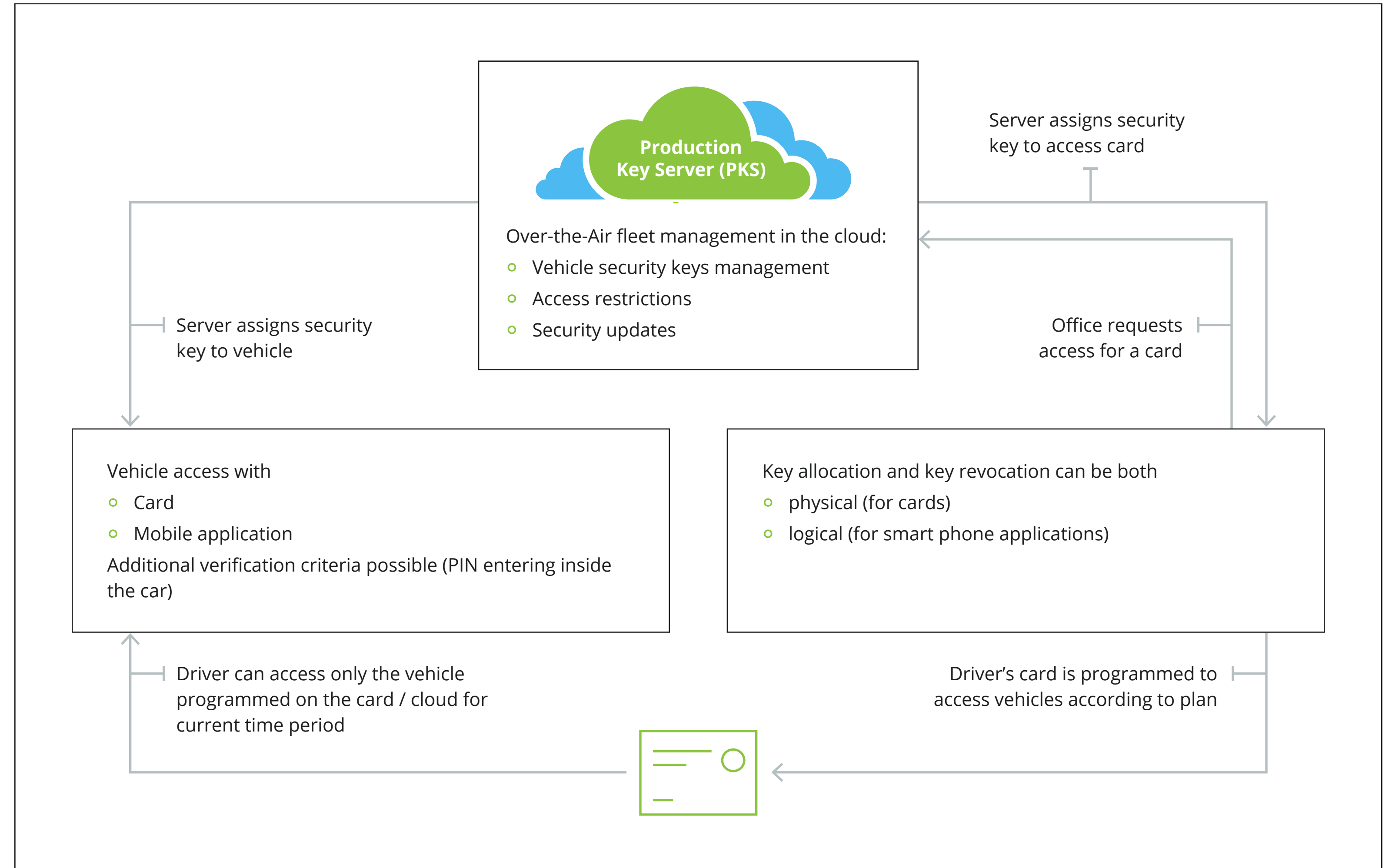
○ Simplifying a complicated procedure of granting access to the same vehicle from one driver to another.

○ Eliminating the number of lost keys to commercial vehicles.

Therefore, the company decided to replace physical keys with digital ones and that is when Infopulse team was addressed to come up with a viable concept of a Digital Key Solution.

Solution

The developed concept of the Digital Key Solution had to enable access via a smartphone or an employee's ID card integrated into the complex ecosystem of a logistics center.

General Workflow

Production Key Server (PKS)

Over-the-Air fleet management in the cloud:
- Vehicle security keys management
- Access restrictions
- Security updates

Server assigns security key to access card

Server assigns security key to vehicle

Office requests access for a card

Vehicle access with
- Card
- Mobile application

Additional verification criteria possible (PIN entering inside the car)

Key allocation and key revocation can be both
- physical (for cards)
- logical (for smart phone applications)

Driver can access only the vehicle programmed on the card / cloud for current time period

Driver's card is programmed to access vehicles according to plan

Powered by NFC technology, the solution **envisions a number of use cases**, such as:

○ Locking or unlocking a vehicle, starting an engine in close proximity;

○ Key provisioning and management including key revoking at any time;

○ Sharing access with a mechanic, other drivers, etc.;

○ Restrict the maximum speed with the key;

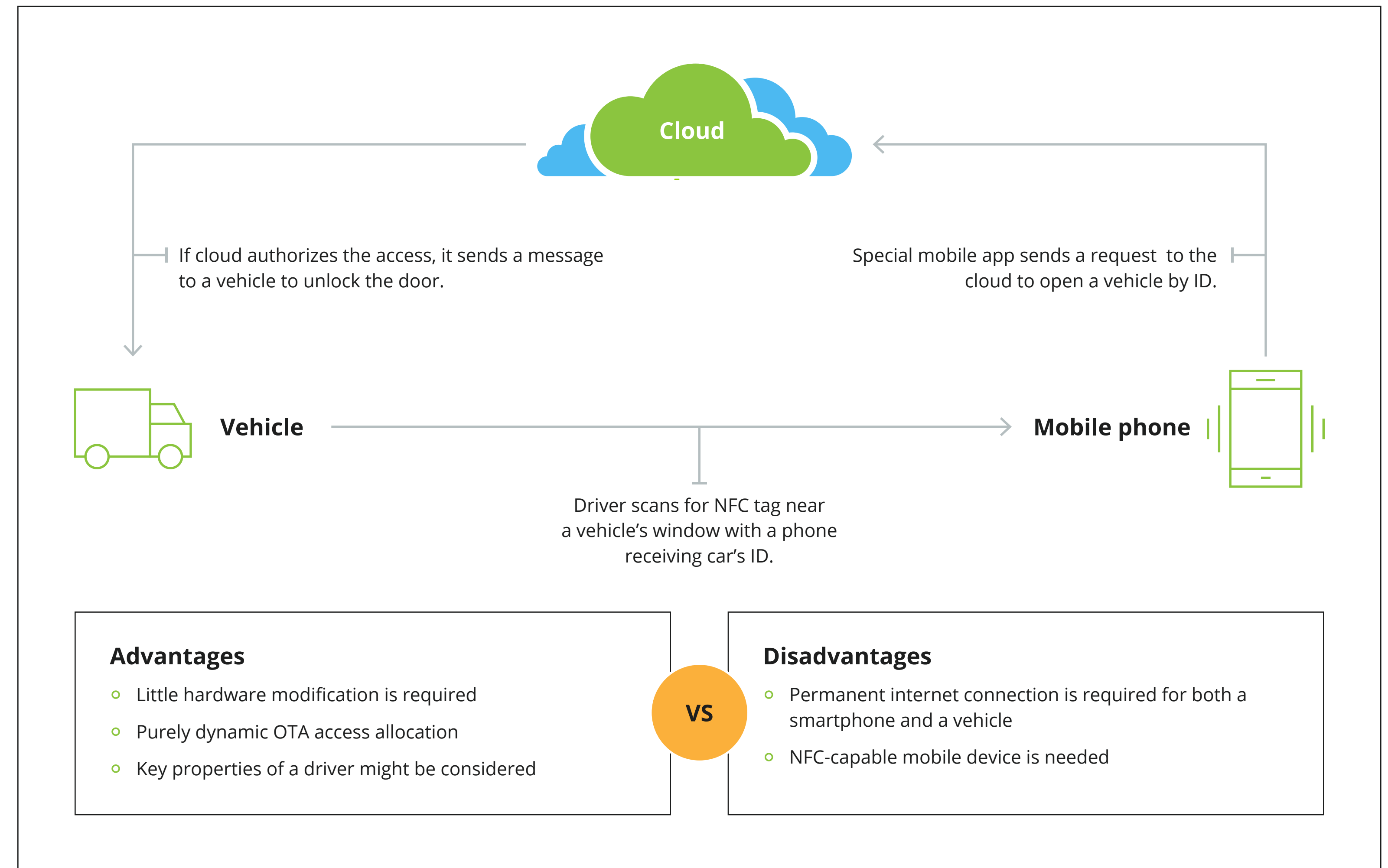○ Lending access to the trunk of the car and not the car itself.

infopulse

4

There are three possible ways to implement communication flows using NFC technology:

1. **Using an NFC-enabled smartphone, which scans the vehicle's NFC tag.**

In this case, there's no need to modify the vehicle's hardware because a programmable NFC tag, containing a little unpowered NFC chip and functioning as the vehicle's identifier, can be simply stuck to the side window. The car access is additionally secured by authorization via cloud. Below, you can see how all these units communicate to enable an access to the car and what are advantages and disadvantages of this communication flow.
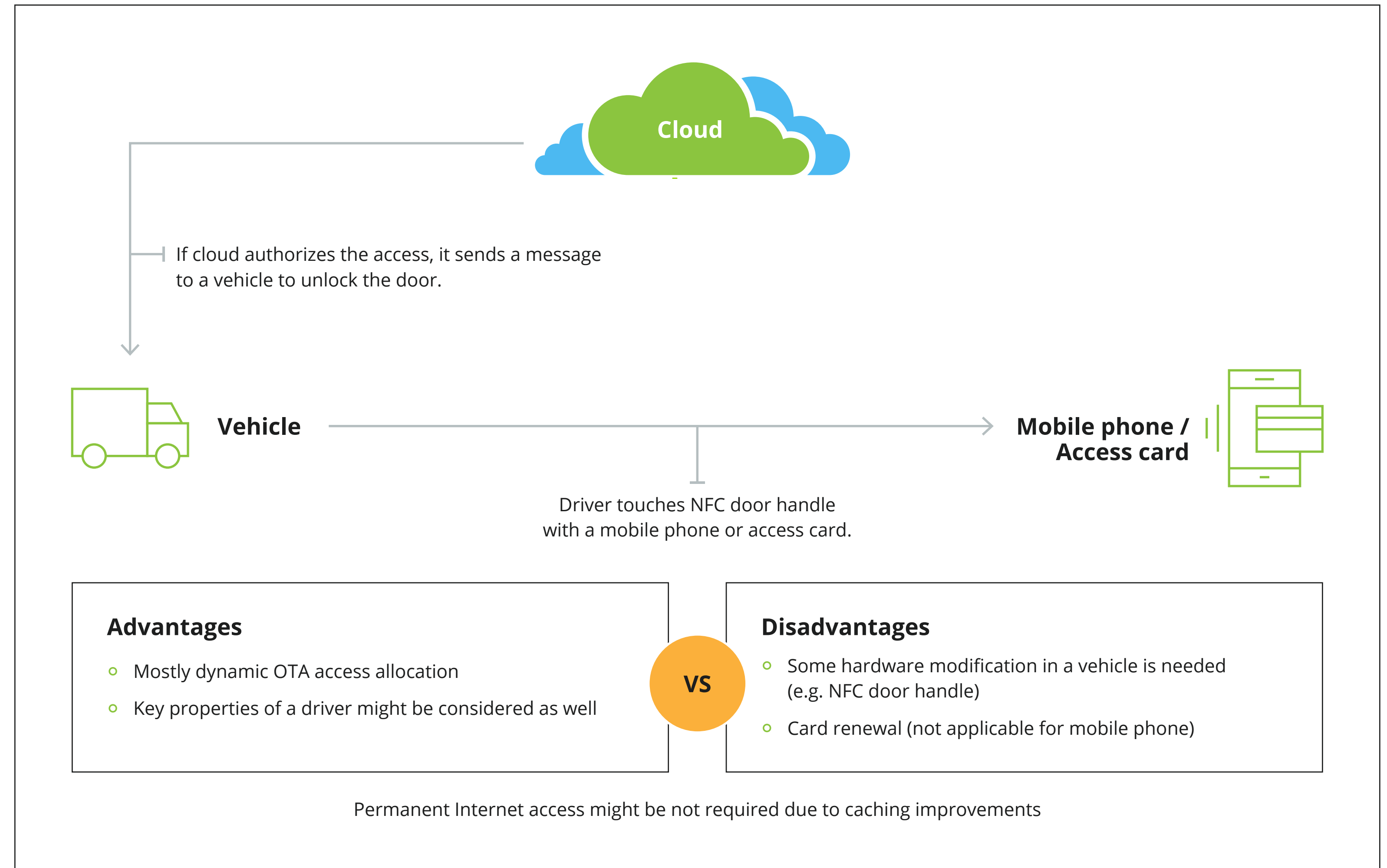
Flow 1: NFC-enabled smartphone to scan vehicle's NFC tag

Cloud

If cloud authorizes the access, it sends a message to a vehicle to unlock the door.

Special mobile app sends a request to the cloud to open a vehicle by ID.

Vehicle

Mobile phone

Driver scans for NFC tag near a vehicle's window with a phone receiving car's ID.

Advantages
- Little hardware modification is required
- Purely dynamic OTA access allocation
- Key properties of a driver might be considered

VS

Disadvantages
- Permanent internet connection is required for both a smartphone and a vehicle
- NFC-capable mobile device is needed

infopulse

2. Applying an embedded NFC reader and managing authorization via cloud.

Another option is to use an NFC reader (e.g., NXP's NCx3320) embedded in the vehicle's door handle instead of the NFC tag. Unlike tags, this NFC frontend integrated circuit (IC) provides low-power card detection quickly and reliably identifying the driver's ID card or smartphone. Thus, to enable the following communication flow, hardware modifications as well as card renewal are required. However, compared to the previous flow, this one may go without the permanent Internet connection.
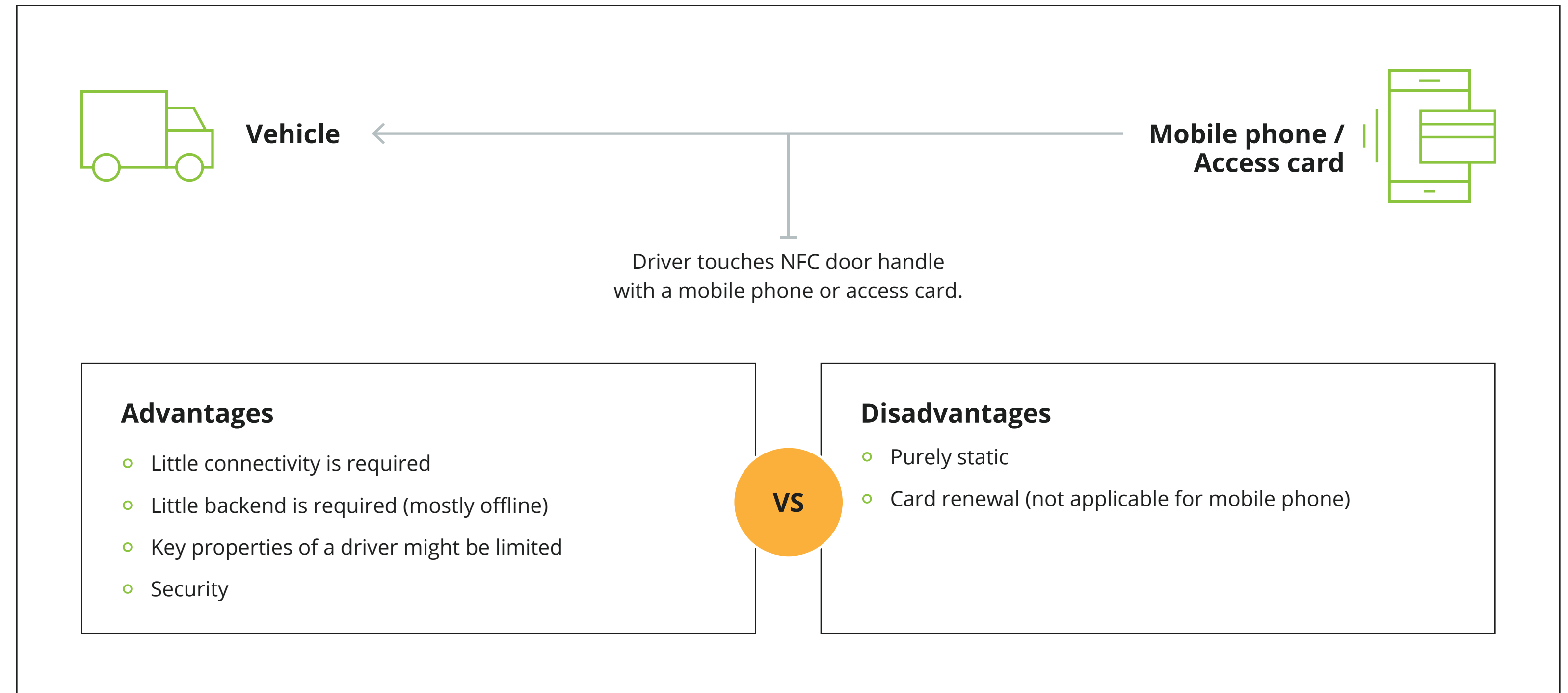
Flow 2: Embedded NFC reader with authorization via cloud

Cloud

If cloud authorizes the access, it sends a message to a vehicle to unlock the door.

Vehicle

Mobile phone / Access card

Driver touches NFC door handle with a mobile phone or access card.

Advantages	VS	Disadvantages
○ Mostly dynamic OTA access allocation ○ Key properties of a driver might be considered as well		○ Some hardware modification in a vehicle is needed (e.g. NFC door handle) ○ Card renewal (not applicable for mobile phone)

Permanent Internet access might be not required due to caching improvements

3. Applying embedded NFC reader without cloud.

Another communication flow incorporates the same units (NFC frontend IC + access card/mobile phone), yet it excludes authorization via cloud and thus, no Internet connection is needed.

Flow 3: Embedded NFC reader without cloud

Vehicle ← **Mobile phone / Access card**

Driver touches NFC door handle
with a mobile phone or access card.

Advantages

- Little connectivity is required
- Little backend is required (mostly offline)
- Key properties of a driver might be limited
- Security

VS

Disadvantages

- Purely static
- Card renewal (not applicable for mobile phone)

Addressing security concerns of NFC-powered car access

To safeguard access distribution to the vehicle, the team had to combine two approaches:

1. The access card is provisioned with a certificate for different cars based on their security keys.

2. The vehicle requests access confirmation from the server to allow access for each card.

Embracing advantages of both approaches, it's possible to introduce the flow when the vehicle sends a request to the cloud and caches the result.
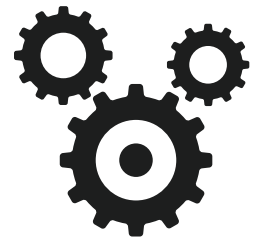
To address multiple NFC-related security issues, that are likely to appear alongside the described communication flows, the team built a security approach based on a number of protocols, cryptographic algorithm and tools that ensure a hack-proof authentication and reliable access control.

Security Approach
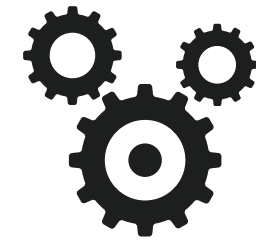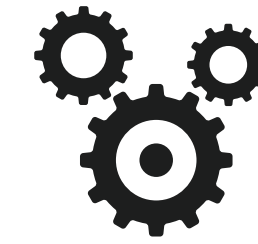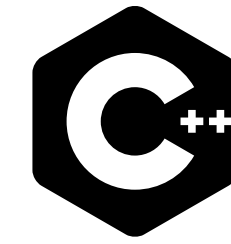
AWS CloudHSM (PKCS #11) for the programming interface to create and manipulate cryptographic tokens

Production Key Server

TLS for end-to-end communications security over a computer network

TLS for end-to-end communications security over a computer network

Vehicle

AUTHLIM – Limiting negative verification attempts is applicable to both an access card and a vehicle

Production Site Manager
No security-related information is exposed at this point

ECDSA – cryptographically supported digital signature originality check

PWD_AUTH – Password read/write verification protection

Access card

Technologies

NXP NFC API

NXP NCx3320 board

MIFARE Plus NFC cards

C++17

Business Value

The company can opt for one or more options to select an economically efficient NFC-based digital key:

○ Employee's ID card can be used not only to determine a driver's identity but also to allow them to access company's vehicles. Its apparent advantage is **lower cost for provisioning**. Moreover, if an ID card is lost or forgotten, it can be easily replaced in just several minutes and without compromising delivery timelines, which is important for **business continuity**.

○ An alternative way is to use a mobile app on an NFC-enabled smartphone, which allows **remotely changing a driver's access rights by** over-the-air updates at any time.

○ Flexibility of using a smartphone for unlocking a vehicle can also **simplify a car rental procedure**.

○ At the same time, both ID cards and smartphones can be used concurrently to **match individual preferences of drivers**.

○ Each access card/app can be **programmed in advance to access different vehicles and to reach long-term delivery plans**.

○ **Several cards/apps can be set up to access the same vehicle** within different timelines of a delivery calendar.

According to Car Connectivity Consortium release report, the Digital Key Solution brings in the following business benefits:

○ **For OEMs** – higher security, simplified use and ability to collect end users' data.

○ **For device vendors** – ability to create integrated smart home solutions and transportation apps.

○ **For rental companies** – higher flexibility and privacy, rentals management.

○ **For car sharing companies** – secure transfer of keys, optimized vehicle management.

○ **For transport enterprises** – streamlined fleet management.

infopulse

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL   +48 (221) 032-442

DE   +49 (69) 505-060-4719

US   +1 (888) 339-75-56

UK   +44 (8455) 280-080

UA   +38 (044) 585-25-00

BG   +359 (876) 92-30-90

BR   +55 (21) 99298-3389

✉   info@infopulse.com