Building Digital Key Solution for Automotive

Content

Overview

The objective of this document is to describe the scope of the ongoing standardization activities in Car Connectivity Consortium (CCC) for using smart devices as keys. The abundance of smart devices in the market and the similarity of the usages of these devices as keys that many companies are investigating is the driving force for the technical standardization of the underlying technology in CCC. The initial focus of CCC is the usage of Digital Key in the automotive industry but the technology is not limited to any specific industry and can be used for other applications such as hotels, real state, fleet management, car sharing etc.

The guiding principle for using smart devices as car keys is the convenience and ease of use for the consumer. Digital Key is not intended to completely replace the traditional car key at least in the initial phase, but rather would be an enhancement and convenience function for the consumer.

The Digital Key standardization effort in CCC is intended to be based on existing standard technologies, such as GlobalPlatform, GSMA, and NFC. The CCC standards shall be able to support future standards as well as they become available. The CCC intends to coordinate and collaborate with other standardization organizations as necessary to create a lean solution based on existing established standards.

CCC has identified a number of core use cases, focusing on vehicle access (lock/unlock), starting of the engine and provisioning the key to smart devices.

1 Unlocking/Locking/Engine Start Use Cases

To facilitate seamless usage of Digital Keys with their physical counterparts all functions currently supported by smart keys are expected to be digitally realized.

Unlocking/locking the vehicle when the smart device with a Digital Key is in/out close proximity: This use case is also known as Passive Entry. The system will unlock/lock the vehicle door when the driver is in/out close proximity to the car without any user interaction with the smart device. From the user perspective the driver is "recognized" by the vehicle. The definition and accuracy of "close proximity" plus a number of localization and security aspects need to be defined for this use case.

Unlocking/locking by placing the smart device close to a sensor: In this use case, the user places the smart device close to a sensor of the vehicle to unlock/lock the vehicle door, without interacting with the UI of the smart device itself.

Unlocking/locking by user interaction with the smart device: The user opens an app or a function of the smart device and unlocks/locks the car.

Starting the vehicle engine: Determining the position of the smart device within the vehicle allows the user to start the engine simply by pressing the START/STOP button, without any user interaction with the smart device. If localization inside the vehicle is not available, the user can tap the smart device at a specific location inside the vehicle to start the engine.

Additional authentication: Before using Digital Key on the smart device some additional user authentication mechanism may be required. This may be in the form of entering simple passcodes up to biometric authentication mechanisms such as fingerprint or iris scans.

2 Key Provisioning Use Cases

Seamless key provisioning use cases are important for the overall user experience of Digital Key. The following provisioning and key management use cases are in focus:

Provisioning the key to a smart device: The Digital Key can be provisioned to any capable device that fulfills the technology and security requirements, using a backend or peer-to-peer mechanism.

Revoking the key: The car owner can revoke the Digital Key at any time.

Key management for car sharing agencies and fleets: Car sharing and rental car agencies provision Digital Keys to the smart devices of the customer for the duration of the rental. This mechanism works agnostic of the brand of the car or the smart device, so that the rental agency is the single contact point for the customer.

Selling the vehicle: When the car is sold, the new owner is able to revoke all keys that have been provisioned during the previous ownership.

3 Key Sharing Use Cases

Users are accustomed to sharing or lending their keys to family or friends as well as to repair shops or valets. The Digital Key user experience should enable and support similar usages seamlessly.

Proximity Sharing: A user in proximity to the Digital Key owner can be granted temporary access via proximity connectivity connections.

Remote Sharing: A user far in range from the Digital Key owner can be granted temporary access via long range communication connections.

Since key sharing usage usually is a short term transaction, it is expected that the key can be bound by properties limiting its usage as explained in the section below.

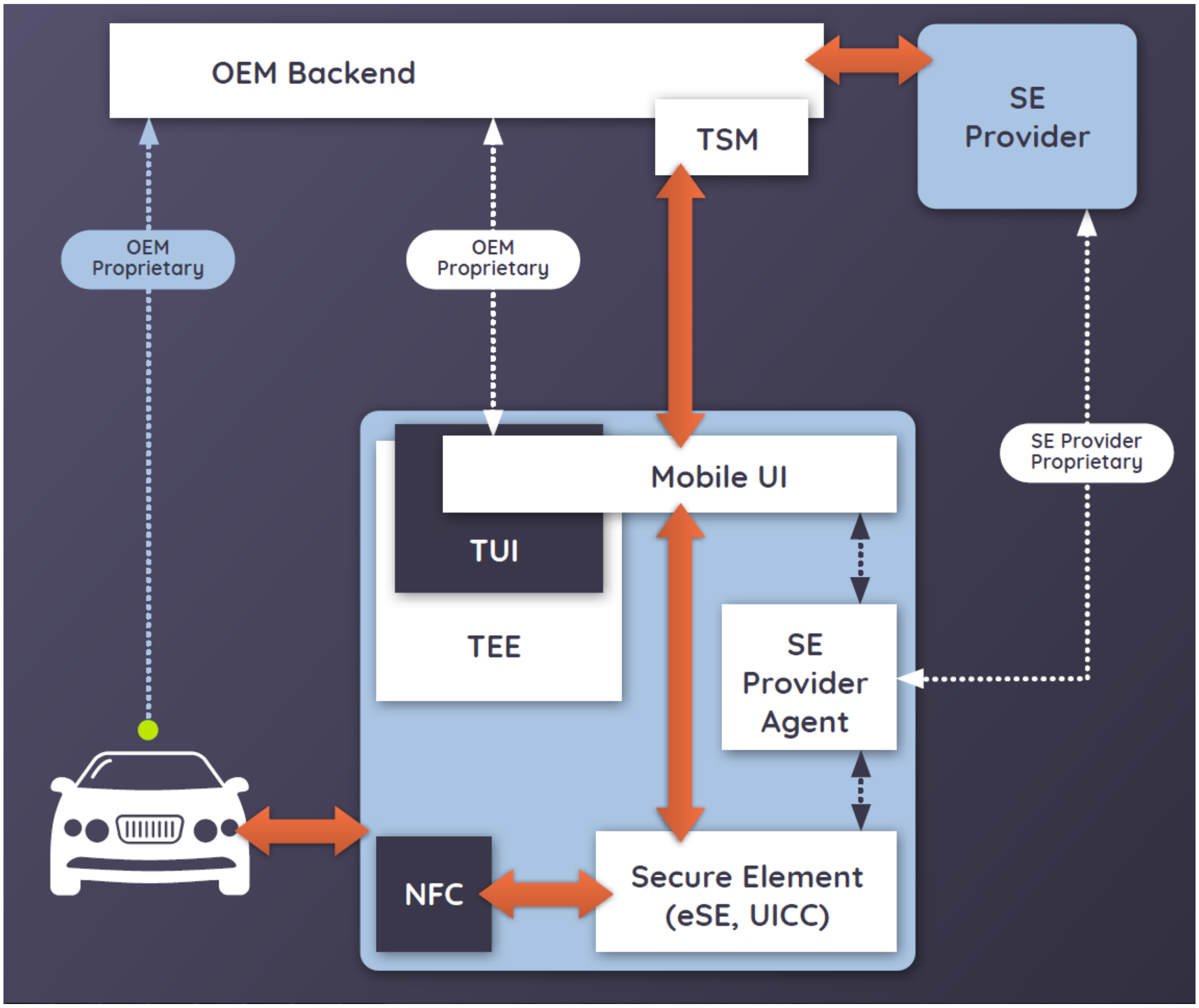
4 Key Properties

A Digital Key can have properties or rights and restrictions associated with the key. These properties enable a variety of new usages and functions. For example, the user may be able to restrict the validity time or maximum speed when the car is accessed with Digital Key. A usage scenario for these restrictions is the usage of the key for valet parking. Other properties may only allow opening the trunk of the car and not the car itself, for example for delivery-to-trunk use cases. Vendors can always extend the standard properties with their own custom properties and enable additional use cases. Additionally, the key may also store vehicle related personal settings or preferences of the user for a more customized user experience.

These may include mirror settings or seat positioning but can also be more complex such as head unit settings, climate control settings or even driving mode settings.

High Level Architecture and Related Standards

The diagram below provides a high level architecture highlighting the focus of CCC efforts including the interfaces to be standardized.



Description of entities in High Level Architecture

TSM (Trusted Service Manager): Enables service providers (OEMs) to distribute and manage their contactless applications remotely by allowing access to the (embedded) secure element in smart devices.

Mobile UI: Interface between OEM/TSM and smart device. This is also known as OEM application.

Secure Element: Secure storage on smart device. It can be in the form of embedded Secure Element or UICC Secure Element..

SE Provider: The owner of the SE which provides SE access to a TSM.

SE Provider Agent: SE access interface for SE Provider. It may be accessed by the SE provider via proprietary interface/functions.

TUI: Trusted User Interface. It is usually part of the TEE.

TEE: Trusted Execution Environment. Secure application environment on the host application processor.

It is expected that the CCC standardization activities will rely on reusing and referencing existing industry adopted standards as much as possible to ensure high interoperability and adoption. Candidate standards in realizing a Digital Key standard are only technologies delivering the highest level of security as introduced below:

GlobalPlatform: Enables secure and interoperable deployment and management of multiple embedded applications on secure chip technology.

NFC: Enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content and connect electronic devices with a single touch

Security Requirements

Consumer devices holding a Digital Key must implement mechanisms to protect the Digital Key as well as to prevent unauthorized use of the same. Key *protection* is required to prevent unauthorized copying, modification and deletion of existing keys; the unauthorized creation and provisioning of new ones; and Denial of Service such as interfering with the connection between the OEM App or vehicle and smart device. The *unauthorized* usage of the Digital Key includes use from unauthorized users, or use from authorized users outside the allowed usage boundaries. Security mechanisms will need to handle the following threats:

- A *Software attacker* gains root access rights and installs malicious applications on the device and reset the device.
- A *Physical attacker* reads and modifies any data persistently stored on the device.
- A *Communication attacker* controls all communication between the device and the vehicle or relays communication to pretend proximity.

Digital Key related messages are exchanged between the device holding the Digital Key with the vehicle (key use), another device (peer-to-peer key sharing) and a remote backend (key provisioning). A security architecture must enable the receiver of these messages to verify the trustworthiness of the messages. Any message exchange with the device holding the digital key must fulfill the following objectives:

- *Trustworthiness*: The devices should only accept messages of trusted devices, i.e. an attacker should not be able to create false messages.
- *Completeness*: The device should detect that an attacker has removed entire messages or parts of them.
- *Freshness*: The attacker must not be able to replay old messages.
- *Binding*: The Digital Key should be securely bound the current user, i.e. the attacker must not be able to masquerade as a previous user.
- *Independence*: Message exchanges should not disclose information about not required properties of the same or of another Digital Key.

For devices holding and managing Digital Key, we assume a hardware based trusted execution environment, which may either support the secure execution of arbitrary manufacturer signed code or it may be limited to pre-defined functionality. Additionally, we assume that the device has an operating system (OS) security framework in which access to security services can be limited. The OS security framework provides runtime isolation and isolated storage. We assume that the integrity of the OS security framework itself is protected.

Conclusion

Digital Key for automotive is one of the new entrants in the connected car world and development of the solution has been on the horizon from many automakers and handset vendors. There are already a few proprietary solutions in the market. However, without coordination between automakers and handset vendors the market will be fragmented and consumer experience will suffer. CCC plays an important role in this by bringing together automakers and smart device manufacturers to develop an interoperable Digital Key solution for the automotive industry.

The board of directors of CCC has acknowledged the importance of Digital Key technology and approved this project in June 2016. The project is leveraging the expertise of the automakers and handset vendors contributing to development of an entire Digital Key ecosystem while addressing the concerns of reliability and security. The board of directors of CCC comprised of representative from the following companies: General Motors, Volkswagen, Daimler, RealVNC, HTC, PSA, Honda, LG Electronics, Hyundai, Alpine, Toyota, and Samsung. The need for Digital Key technology is driven by the changing needs and attitudes of drivers' desire of using a smart device as a Key to allow them to lock, unlock, start the engine and share access to the car. For further information about the Digital key project please contact CCC.

About the Car Connectivity Consortium (CCC)

The CCC is dedicated to cross-industry collaboration in developing global standards and solutions for smart device and in-vehicle connectivity. The organization's more than 80 plus members represent more than 70 percent of the world's auto market, more than 60 percent of the global smart device market and a who's who of aftermarket consumer electronics vendors. For further information, please visit www.carconnectivity.org.