CARCONNECTIVITY consortium®

Whitepaper

Digital Key – The Future of Vehicle Access

Address

3855 SW 153rd Drive
Beaverton, OR 97003, USA

Phone

+1 503-619-1163

Online

Email: admin@carconnectivity.org
Website: https://carconnectivity.org

Legal Notice

The copyright in this information document (the "Document") is owned by the Car Connectivity Consortium LLC ("CCC"). Use of this Document is governed by this legal notice and these license terms.

CCC hereby grants each recipient of this Document, including recipients that are not Members of CCC, a right to use and to make verbatim copies of the Document only for informational and educational purposes in connection with interpreting or understanding the CCC Specifications or other CCC work (the "Purpose"). Recipients are not permitted to make available or distribute this Document or any copies thereof to third parties, other than to their affiliates or subcontractors, but only to the extent that such affiliates and subcontractors have a need to know for carrying out the Purpose. No other license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

THIS DOCUMENT IS PROVIDED "AS IS," WITHOUT ANY WARRANTY, REPRESENTATION, OR GUARANTEE WHATSOEVER. CCC HEREBY EXPRESSLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND GUARANTEES, WHETHER EXPRESS OR IMPLIED, STATUTORY, OR OTHERWISE, REGARDING THIS DOCUMENT AND/OR THE MATERIALS TAUGHT THEREIN. WITHOUT LIMITING THE FOREGOING SENTENCE, CCC HEREBY EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, TITLE, NON-INFRINGEMENT OF OR ABSENCE OF THIRD-PARTY RIGHTS, VALIDITY OF RIGHTS IN, AND/OR OTHERWISE.

CCC MAKES NO REPRESENTATIONS AS TO THE ACCURACY OR COMPLETENESS OF THIS DOCUMENT. CCC, AND ITS MEMBERS AND LICENSORS, EXPRESSLY DISCLAIM ANY AND ALL LIABILITY, AND WILL HAVE NO LIABILITY WHATSOEVER TO YOU OR ANY THIRD PARTY, ARISING IN ANY WAY OUT OF THIS DOCUMENT AND/OR THE MATERIALS TAUGHT THEREIN, INCLUDING WITHOUT LIMITATION ANY LIABILITY ARISING FROM CLAIMS THAT THIS DOCUMENT, INFRINGES YOUR OR ANY THIRD PARTY'S PATENT RIGHTS, COPYRIGHTS, OR OTHER INTELLECTUAL PROPERTY RIGHTS.

CCC AND ITS MEMBERS AND LICENSORS ARE NOT, AND SHALL NOT BE, LIABLE FOR ANY LOSSES, COSTS, EXPENSES, OR DAMAGES OF ANY KIND WHATSOEVER (INCLUDING WITHOUT LIMITATION DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, AND/OR EXEMPLARY DAMAGES) ARISING IN ANY WAY OUT OF USE OR RELIANCE UPON THIS DOCUMENT, OR THE MATERIALS TAUGHT THEREIN.

NOTHING IN THIS DOCUMENT OBLIGATES CCC OR ITS MEMBERS OR LICENSORS TO PROVIDE YOU WITH SUPPORT FOR, OR RELATED TO, THIS DOCUMENT.

CCC reserves the right to adopt any changes or alterations to this Document at any time, without notice, as it deems necessary, but is not obligated to make such changes or alterations.

COPYRIGHT © 2023. Car Connectivity Consortium LLC. Unauthorized Use Strictly Prohibited. All Rights Reserved. The CAR CONNECTIVITY CONSORTIUM logo™ and CAR CONNECTIVITY CONSORTIUM® word mark are registered and unregistered trademarks of Car Connectivity Consortium LLC in the United States and other countries.

Table of Content
Whitepaper

Digital Key – The Future of Vehicle Access

Our mobile devices play an important role in our lives, enabling us to consolidate information and tools supporting nearly all of our daily activities into a single device.

We expect the performance and capability of our smartphones to continuously improve in response to our growing demands, and we expect them to secure our information and protect our privacy with growing rigor. We have been able to use our smartphones to access our vehicles for some time now, using mobile apps provided by vehicle manufacturers and rental companies; however, these apps use different, non-interoperable approaches with varying degrees of convenience, security, and privacy protection. What's missing is a worldwide standard that enables our mobile devices to be used as keys for our vehicles. Digital Key closes this gap.

Introduction
Digital Key

01

The Car Connectivity Consortium® (CCC) Digital Key is a standardized ecosystem that enables mobile devices to store, authenticate, and share Digital Keys for vehicles in a secure, privacy-preserving way that works everywhere, even when the smartphone's battery is low.

Digital Key allows consumers to easily and confidently use their mobile devices to access vehicles. Along with robust capability and convenience, it offers enhanced security and privacy protections. Digital Key aims to complement traditional methods, while being robust enough to fully replace them.

Introduction
Digital Key, Release 2.0

The Digital Key, Release 2.0 specification was designed to meet vehicle manufacturer requirements for use and to form the basis of deveoping the future releases that will continue to expand the capability, ease of use, and convenience of mobile vehicle access.

Vehicle access systems are sophisticated and tightly controlled. Even though the user experience is relatively consistent from vehicle to vehicle, and the underlying technologies are mostly common, the capabilities and protocols vary widely. Consequently, it is challenging for mobile devices to interact with existing vehicle access systems.

Traditional vehicle access systems use multiple low frequency radio technologies that are not present in smartphones. Unfortunately, due to size, construction, cost, and performance constraints, it is not practical to integrate all of these technologies, and their various protocols, into mobile devices.

Conversely, mobile devices do not provide the same security and user experience guarantees to which users of vehicle access systems are accustomed. For example, today's smartphones cannot guarantee that each vehicle's mobile app implements access protocols securely and in a way that protects the user's privacy; that credentials are isolated, tamper-proofed, and protected from cloning and other host vulnerabilities when stored; or that radio technologies are available that provide secure positioning with enough accuracy to satisfy automotive requirements, while providing a consistent user experience in all use cases.

The CCC Digital Key standardization consortium has brought together all of the relevant industries to create a solution that serves everyone. In this whitepaper, we discuss the Digital Key, Release 2.0 specification. This release, the second in a series of releases, allows individual owners to use their mobile devices as keys to their vehicles. The specification enables:

* Security and privacy equivalent to physical keys.
* Interoperability and user experience consistency across mobile devices and vehicles.
* Vehicle access, start, mobilization, and other use cases.
* Owner pairing and key sharing with friends, with standard or custom entitlement profiles.
* Support for mobile devices with low batteries.

02. Architecture

Architecture

02

The Digital Key architecture uses standards-based public key infrastructure to establish end-to-end trust. Mobile devices create and store Digital Keys in Secure Elements – embedded technology that provides a tamper-resistant secure implementation – to provide the highest-level of protection from the plethora of known hardware- and software-based attacks, including tampering, storage intrusion, cloning, and unauthorized access as well as side-channel, interface, and many other forms of attack.

The mobile device‘s native app allows consumers to use and manage Digital Keys without any extra apps, and its Digital Key framework enables developers to build custom apps that provide enhanced services and vehicle-specific features. Mobile devices and vehicles interact with their respective OEM servers to share and manage Digital Keys across mobile device and vehicle platforms. The system ensures that you’re able to access your vehicle even when neither your mobile device nor vehicle have Internet connectivity, while still allowing OEMs to add features that require Internet connectivity for certain operations.

Architecture
Architecture

As shown below in Figure 1, the Digital Key ecosystem consists of vehicles, Vehicle OEM Servers, mobile devices, and Mobile Device OEM Servers communicating with one another using a combination of standardized and proprietary interfaces.

Standardized interfaces ensure interoperability between the implementations of mobile device manufacturers (Mobile Device OEMs) and vehicle manufacturers (Vehicle OEMs), and thus, are fully specified in the Digital Key, Release 2.0 specification. Proprietary interfaces are shown for reference only; they do not affect interoperability, and thus are not specified.

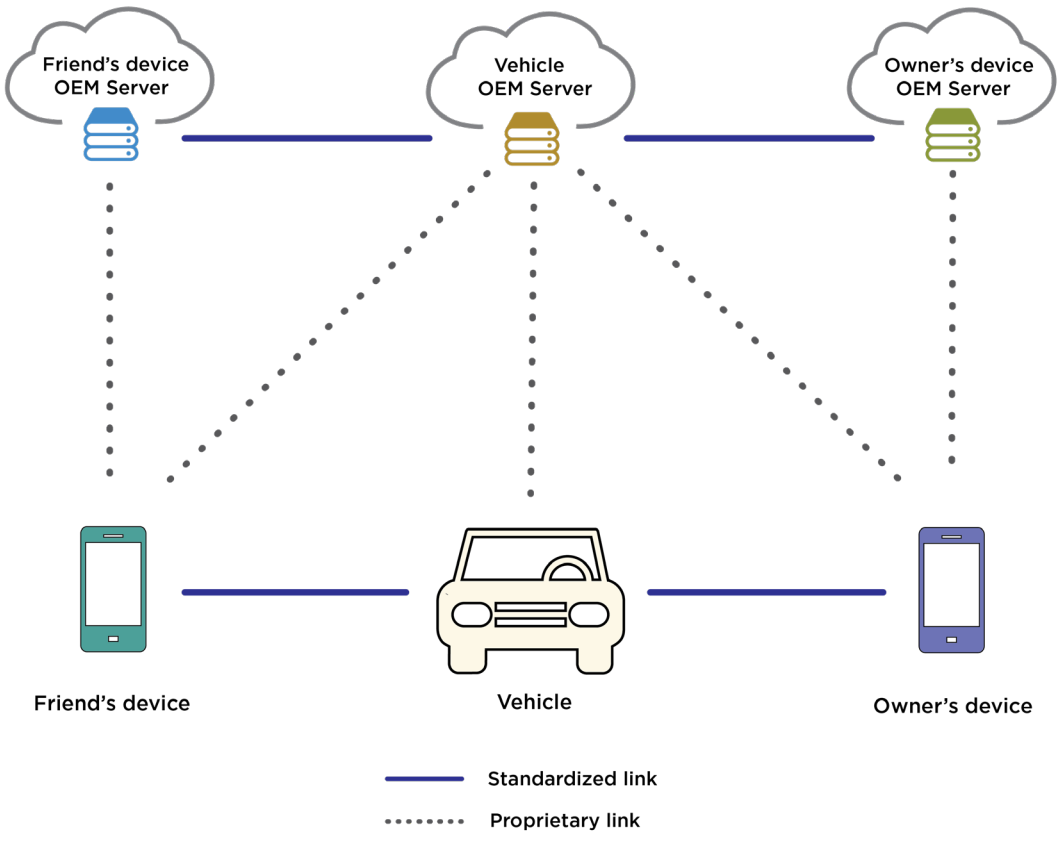
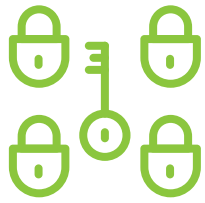


Figure 1: Digital Key System Architecture

Architecture

Architecture

Mobile devices may act as either owner or friend devices, but the vehicle-to-device interface is the same in either role. Interoperability between mobile devices and vehicles is supported by standardizing the vehicle-to-device interface – the communication channel (NFC), protocols, and Digital Key structures.



The vehicle-to-device interface provides a mutually authenticated, secure communications channel that protects your privacy by exposing your mobile device's identity only to known vehicles after they have been authenticated.

Device and Vehicle OEM Servers support interoperability by abstracting the details of managing mobile devices and vehicles from each other; the interface between them provides a standardized way to manage Digital Keys and to provide customer services. The proprietary interfaces between Mobile Device OEM Servers and mobile devices, as well as between Vehicle OEM Servers and vehicles, enable OEMs to provide custom key management functionality. The standardized interfaces are defined as follows:

Vehicle – Device:
The NFC-based wireless interface designed for direct communication between the vehicle and mobile device. It is used to complete the authentication protocol, securely exchange information, pair a mobile device with the vehicle, and so on.

Vehicle OEM Server – Device OEM Server:
The secure, trusted interface between Device OEM Servers and Vehicle OEM Servers. It is used to create, track, manage, and share keys as well as to notify each other of status changes.

Architecture
Architecture

As described above and shown below in Figure 2, mobile devices secure and manage Digital Keys using Secure Elements, native and custom apps (e.g., Vehicle OEM apps, rental service apps, etc.), the Digital Key framework, and communication to Device OEM Servers.

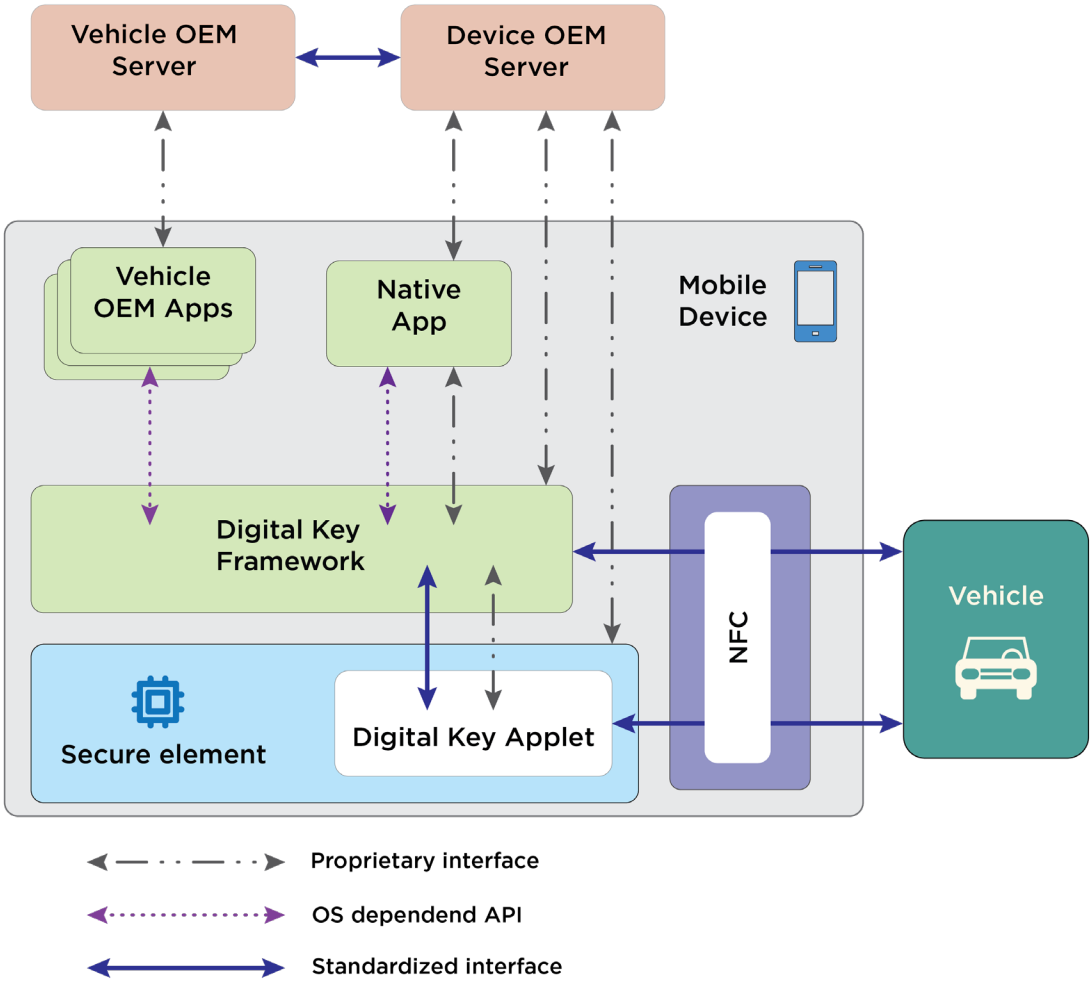


Figure 2: Mobile Device Architecture

Secure and privacy-preserving connections are established between vehicles and the Secure Elements of mobile devices using NFC, providing relay attack protection and remaining functional even when the mobile device's battery is low.

The Digital Key applet, which resides within the Secure Element, performs all security-critical processing – authentication, encryption protocols, and key generation used for owner pairing, sharing, and vehicle access and engine start transactions – while also providing secure, tamper-proof storage for Digital Keys and their metadata. The NFC interface is routed directly to the Digital Key applet, providing a communications path that is protected from, and that operates independently of, the rest of the mobile device.

03. Use Cases

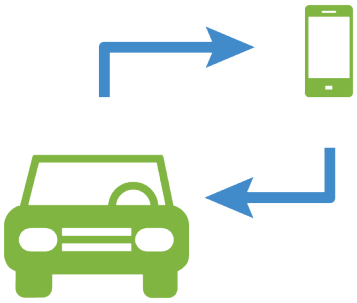
Use Cases

03

Digital Key allows us to use our mobile devices to easily access, and share access to, our vehicles.

Existing vehicle access systems support many use cases beyond just the ability to unlock doors and start engines, such as sharing additional keys, restricting the functionality of shared keys (e.g., vehicle access only), and disabling keys. Digital Key has the potential to support all of these use cases.

Use Cases
Owner Pairing



Seamless key provisioning is an important part of the overall user experience of Digital Key, as it is likely the first interaction a vehicle owner will have with the system. Any mobile device that meets the technology and security requirements of Digital Key may be paired as an owner device with a vehicle. Each vehicle may have only one owner device; an owner device has full authority over the paired vehicle and all associated Digital Keys.

Use Cases
Vehicle Access / Engine Start

Digital Key may be used to access a vehicle, start the engine, mobilize the vehicle, or authorize any other operation by placing a mobile device near an NFC reader, without requiring you to interact with a user interface of the mobile device (e.g., an app).

When such an operation occurs, the mobile device and vehicle mutually authenticate and the vehicle verifies that the mobile device's Digital Key authorizes the requested operation. The limited operational range of NFC prevents attackers from tricking the vehicle into thinking that your mobile device is nearby when it's not, and the authentication protocol's privacy protections ensure that anyone observing wireless communications cannot track you or your mobile device.

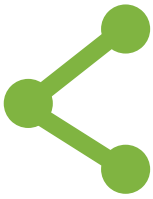
In addition to the above, users may choose to configure their mobile devices to require recent user authentication in order to complete certain operations for a particular vehicle – that is, you may require your mobile device to ensure that you are using your device and not someone else. Mobile devices may perform user authentication by requiring you to enter a passcode or via biometric authentication mechanisms (e.g., facial recognition, fingerprints, iris scans, etc.), as determined by the Device OEM policy and user preference.

Example operations include:

Unlocking the door: You may unlock the door of the vehicle by placing your mobile device near the exterior door handle.

Starting the engine: You may start the engine of the vehicle by pressing the START/STOP button, after placing your mobile device near a specific location inside the vehicle (typically, in the center console).

Use Cases
Sharing



Today you can share your car keys with friends and family by simply giving them the physical key or key fob. Sharing Digital Keys should be just as effortless, seamless, and unrestricted. Digital Key improves the sharing experience by enabling you to share as many Digital Keys, with as many authorization profiles (entitlements), as needed – without having to physically give someone a key or key fob. For example, I can give my friends access to my vehicle, so they can use it while I'm far away on vacation, or I can give my child access, but without authorization to start the engine.

A friend device is a mobile device that is not an owner device for a given vehicle. There is no limit to the number of friend devices with Digital Keys for a given vehicle, but friend devices may not share access with other friend devices.

An owner device shares a Digital Key with a friend device by sending a sharing link to the friend device (e.g., via SMS). When the Digital Key is accepted (e.g., by tapping the sharing link), the friend device creates a Digital Key with the appropriate parameters (vehicle, entitlements, etc.), the Digital Key framework establishes a secure communications channel between the two devices, through which the owner device signs (approves) the friend device's digital key (public key), and necessary signatures (approvals) are obtained from cloud services (e.g., Vehicle OEM Servers). To ensure that the shared Digital Key is usable only by the intended recipient, the owner may optionally provide them with one or more sharing passwords and/or PINs communicated on a different channel than the sharing link.

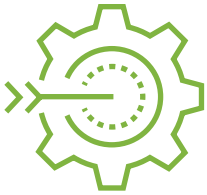
This release focuses on enabling and securing services for individuals – vehicle owners using mobile devices to access vehicles and share Digital Keys with friends and family. But it also provides the necessary underpinnings to support fleet, ridesharing, rental, and other commercial services.

Use Cases
Termination and Suspension

Unlike physical keys and key fobs, Digital Keys may be easily terminated or suspended by friend devices, owner devices, vehicles, and/or OEM Servers. There are many reasons that Digital Keys may need to be terminated or suspended. For example, you may decide that you no longer need access to a vehicle or that your friend should no longer have access to your vehicle; you may want to terminate all Digital Keys associated with a stolen mobile device – or suspend them if your device is lost; a particular mobile device may have experienced a security breach; you may have sold your vehicle or you may want to factory reset it; you may want to ensure a particular mobile device cannot access a vehicle directly within the vehicle (e.g., via the infotainment system); and so on.

Digital Keys may be terminated or suspended at any time. Termination is permanent and requires the sharing of a new Digital Key to restore access, while suspension is temporary and simply disables a Digital Key until it is resumed.

Use Cases
Key Properties



Each Digital Key contains a number of attributes and authorizations, encapsulated in standard access entitlement profiles, that describe how and when it may be used. These properties allow each Digital Key to be customized, enabling a variety of new use cases, features, and personalization.

In addition to standard properties, custom entitlements may also be used to enable additional use cases or to include service-specific information. For example, you may restrict when the Digital Key may be used; adjust the maximum speed for a particular driver; only allow access to the trunk or a particular compartment (and not access the vehicle cabin or other compartments, such as for delivery or pick-up services); allow cabin access, but not engine start or mobilization; and so on.

Digital Keys also provide a secure storage container to store vehicle-related personalization settings, preferences, and other metadata, to provide a customized experience.

04. Outlook
Digital Key, Release 3.0

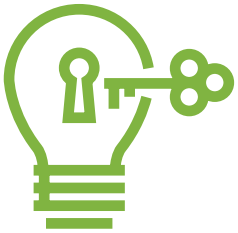
04

The Digital Key Release 3.0 specification will extend the Digital Key Release 2.0 by adding passive, location-aware keyless access.

Rather than having to pull their mobile devices out to access a car, consumers will be able to leave their mobile devices in their bag or pocket when accessing and/or starting their vehicle. Passive access is not only vastly more convenient and a better overall user experience; it allows vehicles and mobile devices to offer new location-aware features.

Outlook
Digital Key, Release 3.0

CCC continues to bring together member companies from all relevant industries to develop future Digital Key releases that advance the mobile vehicle access experience and its capabilities.



The CCC has adopted Bluetooth Low Energy (BLE) in combination with Ultra-Wideband (UWB) wireless connectivity technologies to enable these new location-aware features for Digital Key and to allow secure positioning with accuracy equal to or better than existing passive key fobs.

Member companies have been working on optimizing the High Rate Pulse repetition frequency (HRP) UWB standard in IEEE 802.15.4z to achieve this level of accuracy within this specific use case, while ensuring safety and security.

05. Conclusion

Conclusion

05

Digital Key enables mobile devices to store, authenticate, and share Digital Keys for vehicles in a secure, privacy-preserving way that works everywhere, even when the smartphone's battery is low. It is an important addition to the automotive industry, enabling a significantly improved vehicle access experience that builds consumer confidence through its ease of use, convenience, security and privacy protections, and extensive capability. The CCC, representing the majority of the global automotive and smartphone industries, enables the Digital Key's broad cross-industry support and facilitates the coordination of mobile Device OEMs and Vehicle OEMs to provide a consistent user experience by increasing interoperability and reducing market fragmentation.

About
Car Connectivity Consortium ® (CCC)

The CCC is a cross-industry standards organization with a mission to create sustainable and flexible ecosystems that standardize interface technologies to provide consistently great user experiences across all vehicles and mobile devices.

> **The CCC represents a large portion of the global automotive and smartphone industries, with more than one hundred member companies.**

The CCC member companies consisting of smartphone and vehicle manufacturers, automotive tier-1 suppliers, silicon/chip vendors, security product suppliers, and more. The Board of Directors of CCC includes individuals from charter member companies Apple, BMW, General Motors, Honda, Hyundai, LG, Panasonic, Samsung and Volkswagen.

In addition to Digital Key, the CCC portfolio includes MirrorLink® technologies. For further information about CCC projects and to get involved, please visit www.carconnectivity.org.