DIGITAL KEY

WHITEPAPER

CCC Digital Key - The Future of Vehicle Access

CARCONNECTIVITY consortium®

Legal Notice

CONTENTS

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.

An increasing customer demand is seen for accessing and starting vehicles with smartphones. Existing apps for smartphones to control and manage access to our vehicle have used different, non-interoperable approaches with varying degrees of convenience, security, and privacy protection.

Passive electronic key fobs are widely used, but you still need one for each car you own. With increasing focus on our phones, a key fob is just one more thing to forget when we leave the house – your phone has replaced your travel pass and your credit card, so why not your car key?

What's missing is a worldwide standard that enables our mobile devices to be used as keys for our vehicles. The CCC Digital Key closes this gap.

01 INTRODUCTION

The CCC Digital Key is a standardized technology that enables mobile devices to store, authenticate, and share digital keys for vehicles in a secure, privacy-preserving way that works everywhere.

It allows consumers to use their mobile devices to gain access to their vehicles even when the smartphone's battery is low. Along with

convenient usage, it offers enhanced security and privacy protections. CCC Digital Key aims to complement traditional key fob implementations, while being robust enough to fully replace them.

The CCC Digital Key uses Near Field Communication® (NFC) technology for contactless communication between smartphones and vehicles. The most recent CCC Digital Key Release 3.0 adds hands-free, location-aware keyless access and location-aware features for an improved user-friendly experience. This has been achieved using Ultra-Wideband (UWB) in combination with Bluetooth Low Energy® connectivity. It maintains support for NFC technology to ensure backward compatibility.

Seamless key provisioning is an important part of the overall user experience of CCC Digital Key, as it is likely the first interaction a vehicle owner will have with the CCC Digital Key System. Any mobile device that meets the technology and security requirements of CCC Digital Key may be paired with a similarly equipped vehicle. Each vehicle can have only one ‘owner’ device, but can also have multiple CCC Digital Keys associated with it on ‘friend devices’ – great for sharing, car hire and other business uses.

02 USE CASES

CCC Digital Key allows consumers to use their mobile devices to easily access, and share access to, their vehicle. It has the potential to support many use cases beyond just unlocking doors and starting engines, such as sharing additional keys, restricting the functionality of shared keys, and disabling keys.

Let's look at how CCC Digital Key addresses these use cases.

HANDS-FREE AND NFC VEHICLE ACCESS

CCC Digital Key enables hands-free passive keyless entry at the same level of comfort and safety as classic hands-free passive entry and passive start, provided by a large number of vehicle models today. CCC Digital Key may be used to access a vehicle, start the engine, immobilize the vehicle, or authorize any other operation. No interaction with the mobile device is needed, for example activating an app. The smartphone can stay in the user's pocket.

To provide hands-free access, the mobile device and vehicle mutually authenticate, and the vehicle verifies that the mobile device's CCC Digital Key authorizes the requested operation. UWB time-of-flight measurement prevents attackers from using relay attacks (based on signal amplification) to trick the vehicle into thinking that the mobile device is nearby when it is not – this protection is called 'secure ranging'.

Alternatively, CCC Digital Key may be used by simply placing a mobile device near the vehicle's NFC reader. The limited operational range of NFC prevents attackers from fooling the car into thinking the device is closer than it is. Both the UWB – BLE combination and NFC utilize the authentication protocol's privacy to ensure that anyone monitoring wireless communications cannot track the user or their mobile device.

ADDITIONAL FUNCTIONS IMPROVE CONVENIENCE

With CCC Digital Key, users will be able to launch different actions from their phone. CCC Digital Key provides the same functions as a traditional key fob, and beyond.

For example, the traditional key fob is restricted by its nature to a limited number of buttons allowing users to lock and unlock their car, open windows or start the engine. With CCC Digital Key, the user can interact with their mobile device to launch additional features like opening the trunk, closing the window or activating the heating. At the same time the starting of the engine can be prevented, so that children could enter the vehicle without the owner having to worry about unintentional driving off.

SHARING

Today, people can share their 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 – or better.

CCC Digital Key improves the sharing experience by enabling users to share multiple CCC Digital Keys, 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.

As well as the main owner device, the user sets up the smartphones for other people as 'friend devices', just by sending a sharing link. Several friend devices can be added for a given vehicle, but may not share this access onward.

The CCC 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 the vehicle OEM server. To ensure that the shared CCC Digital Key is usable only by the intended recipient, the owner may optionally provide them with sharing passwords and/or PINs communicated on a different channel than the sharing link.

This sharing capability also provides the necessary underpinnings to support fleet, ridesharing, rental, and other commercial services.

TERMINATION AND SUSPENSION

Unlike physical keys and key fobs, CCC Digital Keys may be easily terminated or suspended at any time, from friend devices, owner devices, vehicles, and/or OEM servers. There are many reasons that CCC Digital Keys may need to be terminated or suspended. For example, a user may decide that they or a friend no longer need access to a vehicle, or they may want to terminate all CCC Digital Keys associated with a stolen or compromised mobile device – or suspend them if the device is lost. The user may have sold their vehicle or may want to factory reset it, and so on.

Because the life cycle of a mobile phone is typically shorter than a car, a user may need to change the owner phone. CCC Digital Key can be reactivated on a new owner phone, while CCC Digital Keys on friend devices still remain; something quite impossible with traditional keys.

Termination is permanent and requires the sharing of a new CCC Digital Key to restore access, while suspension is temporary and simply disables a CCC Digital Key until it is resumed.

KEY PROPERTIES

Each CCC 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 CCC Digital Key to be customized, enabling new use cases, features, and personalization.

In addition to standard properties, custom entitlements (if provided by the vehicle OEM) may also be used to enable additional use cases or to include service-specific information. For example, an owner may restrict how the shared CCC 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.

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

03 ARCHITECTURE

The CCC 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 hardware- and software-based attacks, including tampering, storage intrusion, cloning, and unauthorized access.

Secure, privacy-preserving connections are established between vehicles and the secure elements of mobile devices using BLE – UWB or NFC, providing relay attack protection and, in the case of NFC, remaining functional even when the mobile device's battery is low.

Digital Key applications on the mobile device may be native to the Operating System, provided by vehicle OEM's or third parties that potentially offer enhanced services and vehicle-specific features. Mobile devices and vehicles interact with their respective OEM servers to share and manage digital keys. The system ensures access to the vehicle even when neither mobile device nor vehicle have internet connectivity, while still allowing OEMs, if they wish, to add features that require internet access for certain operations.

As shown in Figure 1, the CCC Digital Key ecosystem consists of vehicles, vehicle OEM servers, mobile devices, and mobile device OEM servers – all communicating with each other using a combination of standardized and proprietary interfaces.

Standardized interfaces enable interoperability between different implementations of mobile device manufacturers (mobile device OEMs)

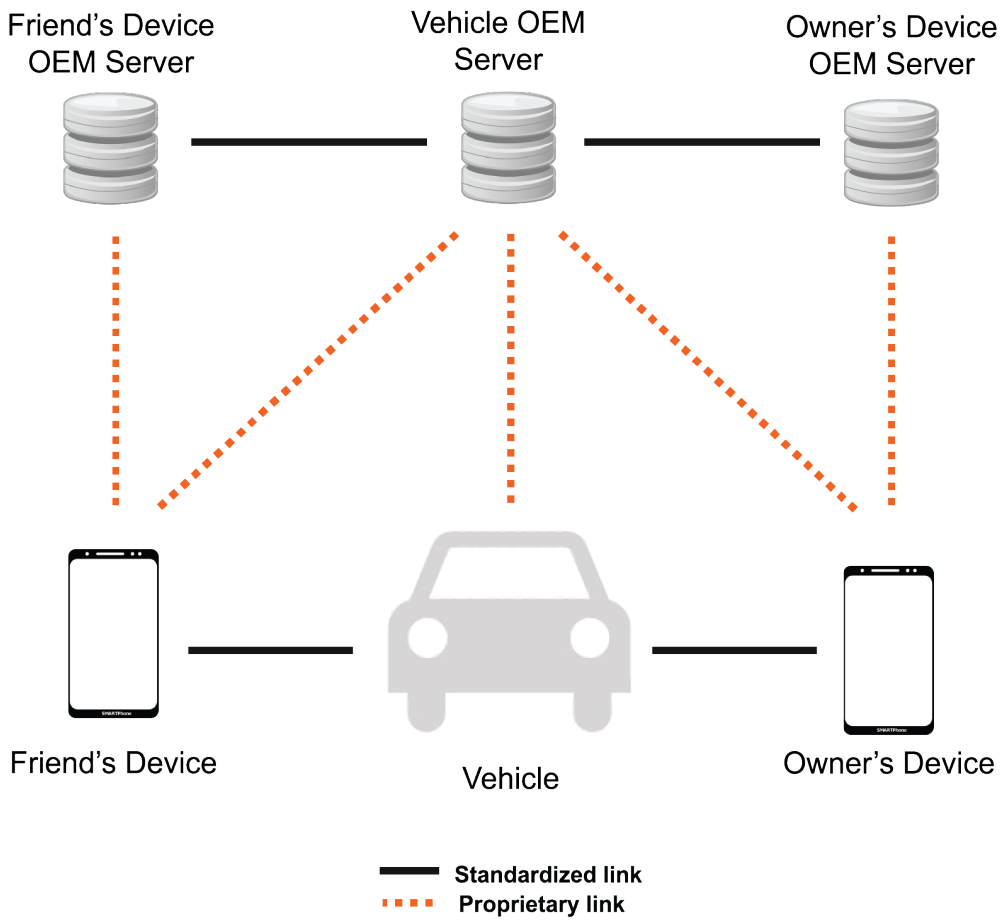

Figure 1: CCC Digital Key ecosystem

and vehicle manufacturers (vehicle OEMs), and thus are fully specified in the CCC Digital Key specification. Proprietary interfaces are shown for reference only; they do not affect interoperability, and thus are not specified. 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, BLE and UWB), protocols, and digital key structures. The vehicle-to-device interface provides a mutually-authenticated, secure communication channel that protects the user's privacy by exposing their mobile device's identity only to trusted 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 wireless interface 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 ensure that the mobile device is within close proximity of the vehicle.
- **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 for servers to notify each other of status changes.

As described above and shown in Figure 2, mobile devices secure and manage CCC Digital Keys using secure elements, native and custom apps, the CCC Digital Key framework, and communication to device OEM servers. Apps might be vehicle OEM apps, rental service apps, and so on

The CCC Digital Key applet, which resides within the secure element, performs all security-critical processing – authentication, encryption protocols, and key generation used for owner pairing, key derivation for 'secure ranging' (verifying the key is actually close by or in the car), sharing, and vehicle access and engine start transactions – while also providing secure, tamper-proof storage for CCC Digital Keys and their metadata. The NFC interface is routed directly to the CCC Digital Key applet, providing a communications path that is protected from, and that operates independently of, the rest of the mobile device.

The UWB module maintains the same system security level as the NFC interface through secure ranging, protecting against relay attacks.

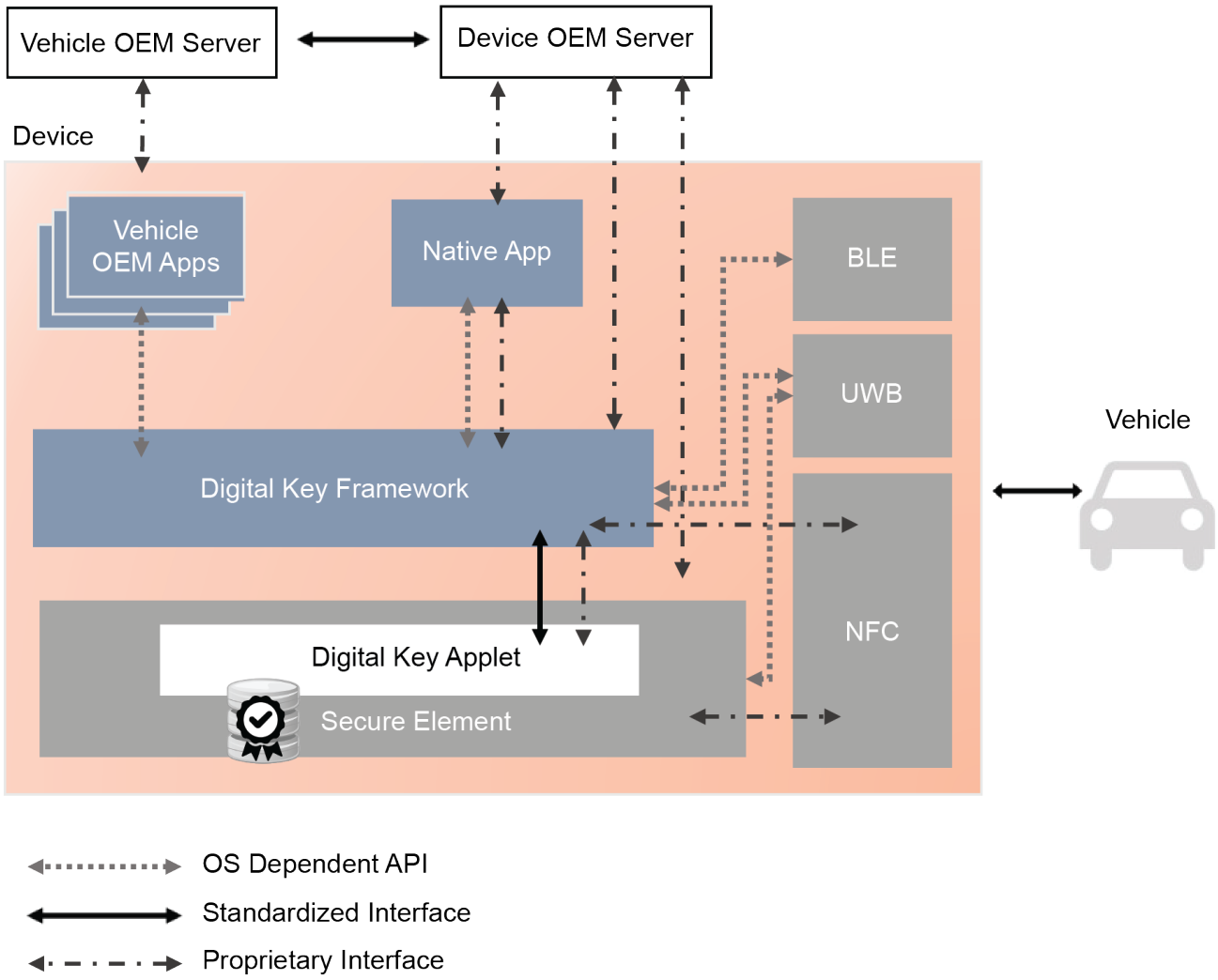

Figure 2: Mobile Device Architecture

'Ranging keys' are derived from CCC Digital Key authentication handshake and securely stored in the secure element. When in use, ranging keys have a limited 12-hour lifetime to shorten the time window for an attacker.

The CCC has adopted UWB secure ranging technology in combination with BLE connectivity technology to enable new location-aware features for CCC Digital Key and to allow secure positioning with accuracy equal to or better than existing passive key fobs. CCC member companies have been 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.

04 CCC CERTIFICATION PROGRAM

The CCC Digital Key Certification Program will ensure interoperability and security of the digital key solution, to deliver the best and most secure user experience between the mobile device and the vehicle.

The benefits of CCC Certification include:

- CCC Certified products offer benefits to both manufacturers and end-users via a standardized approach, ensuring robust and seamless user experiences across different vendors' products.

- Certification results in smooth interoperation of involved parties, thus increasing end-user satisfaction and potentially boosting sales volumes, lowering product return rates and reducing support costs.

- The CCC Certification program enforces the correct usage of the CCC Certification Logo in marketing, building trust with end-users and consumers.

The CCC Digital Key certification program is under development and targeted for release by 2022.

05 CONCLUSION

CCC Digital Key will provide the standardization and industry acceptance needed to drive widespread adoption of smartphones as vehicle keys.

ABOUT
Car Connectivity Consortium ® (CCC)

CARCONNECTIVITY consortium®

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

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 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, Google, Honda, Hyundai, LG, Mercedes-Benz AG, NXP Semiconductors, Panasonic, Samsung and Volkswagen.

In addition to CCC Digital Key, the CCC portfolio includes MirrorLink® technologies.

DIGITAL KEY

Address

3855 SW 153rd Drive Beaverton, OR 97003, USA

Phone

+1 503-619-1163

Online

Email: admin@carconnectivity.org
Website: https://carconnectivity.org
LinkedIn: https://www.linkedin.com/company/car-connectivity-consortium-ccc