UWB Spectrum Regulatory Position

Car Connectivity Consortium 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

© 2022 Car Connectivity Consortium

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.

Introducing the Car Connectivity Consortium

The Car Connectivity Consortium® (CCC) is a cross-industry organization advancing global technologies for smartphone-to-car connectivity solutions. CCC has developed the Digital Key Specification and Certification Program, an open standard to allow smart consumer electronic devices such as smartphones, to act as a vehicle key and more. Digital Key securely and conveniently enables the normal lock, unlock and start engine functions, but goes further to allow key sharing, offering access to friends or valets, and many more features by using their phones and other devices.

Now over 170 strong, the CCC member companies consist of consumer electronics manufacturers and vehicle manufacturers, automotive tier-1 suppliers, semiconductor manufacturers, security product suppliers, and more. The Board of Directors of CCC includes individuals from charter member companies Apple, BMW, Ford, General Motors, Google, Honda, Hyundai, Mercedes-Benz AG, NXP, Panasonic, Samsung, Thales, Volkswagen, and Xiaomi.

CCC Digital Key

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 use their mobile devices easily and confidently, regardless of manufacturer or operating system type, 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.

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.

CCC Digital Key operates with radio interfaces that ensure safety and convenience, with the highest available level of security and privacy protections to unify the world of mobile devices and vehicles.

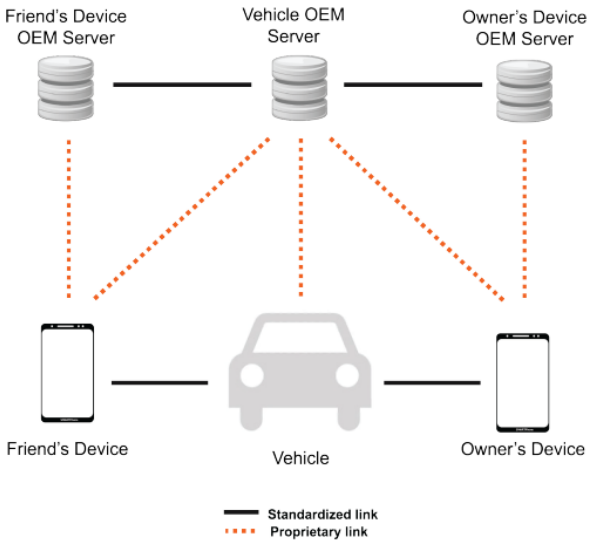
Supported Use Cases include:

- Unlock the Vehicle – Smart device in vehicle's proximity
- Lock the Vehicle
- Start the Engine – Smart device within a vehicle
- User Authentication
- Digital Key Provisioning (typically upon purchase)
- Digital Key Revocation
- Selling the Vehicle
- Digital Key Sharing – Remote & Peer-to-Peer
- Digital Key Properties – Restricting (shared) key usage

© 2022 Car Connectivity Consortium

The ability to instantly share a key, from anywhere in the world, across and between mobile phone platforms (incl. operating systems) and between any vehicle manufacturer is utterly unique to the CCC Digital Key. With the vast majority of the world's smartphone and vehicle manufacturers by volume as members, we are now making this vision real.

Digital Key Operation



Secure, privacy-preserving connections are at the core of Digital Key operation. These are established between vehicles and the secure elements (a hardware-based component) of mobile devices using Bluetooth Low-energy (BLE) and Ultra-wideband (UWB) or Near-field Communications (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.

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. The UWB module maintains the same system security level as the NFC interface through secure ranging, protecting against relay attacks. Ranging keys are derived from the CCC Digital Key authentication handshake and securely stored in the secure element. When in use, ranging keys have a limited lifetime to shorten the time window for an attacker. The CCC has adopted UWB secure ranging technology in combination with BLE 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, while ensuring safety, privacy and security.

Rapidly Growing Market Adoption of Digital Key

Historically, UWB technology has been used for proprietary secure ranging applications in automotive markets since 2017. HELLA GmbH and LEAR Corp. implemented a secure ranging solution to accompany the passive keyless entry system used at the time. This UWB solution is available now from numerous car manufacturers and has been proven to be a reliable and highly secure while fulfilling the stringent requirements of quality and durability that the car industry requires. The inclusion in the key fob has also shown that the technology can be very low power and suited to battery operated applications.

Since the completion of the CCC Digital Key Release 2 in April, 2020, vehicle and phone OEMs have started the implementation in end-user products. With the completion of Digital Key Release 3 in May

© 2022 Car Connectivity Consortium

of 2021, UWB radios utilized in both vehicles and smartphones are being deployed and utilized for CCC Digital Key functions. As of this writing in late 2022, a number of our members have publicly announced the volume shipment of products with CCC Digital Key.

These include:

- BMW (BMW announces BMW Digital Key Plus with Ultra-Wideband technology)
- Hyundai (Hyundai Digital Key Features in the Genesis G90)
- HELLA Smart Access (HomePage | HELLA)
- Samsung Unlocks a New Experience (link to PR)
- Apple – releases powerful new features to stay focused (link).
- Google (Google has added an Ultra-wideband (UWB) API in Android (xda-developers.com)
- Continental (Continental Wins BMW Group Supplier Innovation Award for CoSmA UWB Digital Vehicle Access Solution - Continental AG)
- Qorvo estimates 300 million UWB devices end of 2021 Qorvo Press release

UWB Technology in Digital Key and Beyond

UWB secure ranging is a core technology that enables Digital Key 3.0. Based on the IEEE 802.15.4z standard, it defines secure ranging, preventing car theft while preserving full user convenience.

UWB secure ranging works by sending pulses of radio energy, measuring the time to cover the distance between transmitter and receiver. By using strong encryption technology this distance measurement cannot be hacked by car thieves and the distance can be established quickly, precisely and securely.

UWB secure ranging consumes very little power and is ultra-precise – better than 5 cm in a typical Digital Key application. Unlike many other distance measurement technologies UWB works in adverse environmental conditions: fog, smoke, rain and in multi-path reflective conditions.

Outside of the use for Digital Key, UWB secure ranging is being used in many different applications to benefit both consumer electronics users (smartphones, watches, etc.) and vehicles of many types. Within smartphones, UWB is used with smart-tags to allow owners to find lost items, not only providing angular direction and distance, but also azimuth or elevation. Many more applications that build upon these features are envisioned in the near future. Likewise, with vehicle applications, benefits based on the unique features of UWB can identify children left behind in a potentially hot car, as well as many more safety and convenience benefits. Taken together, UWB applications that utilize their unique qualities are serving to strongly accelerate market adoption in the primary markets of smart consumer electronic devices and vehicles, but also open opportunities for smaller companies to innovate with niche products, potentially benefitting those with disabilities, among other groups.

The Car Connectivity Consortium is cooperating with several alliances and consortia that represent parts of the UWB ecosystem, as well as complementary uses of UWB that use the same spectrum. The CCC request for UWB spectrum should be regarded in the context of the full ecosystem of UWB applications currently developing, each application supporting broader adoption of UWB technology thus spawning new innovative applications, all based on world-wide aligned spectrum availability.

Digital Key use of spectrum

UWB technology as applied in Digital Key does not require dedicated spectrum. It coexists on a non-interference/non-protection basis in spectrum used by incumbent spectrum users like satellite systems, scientific applications, fixed links and radar systems. Digital Key also selectively uses the UWB

© 2022 Car Connectivity Consortium

secure ranging protocol in time, further reducing use of the spectrum and potential interference with other systems.

Technical Spectrum Facts:

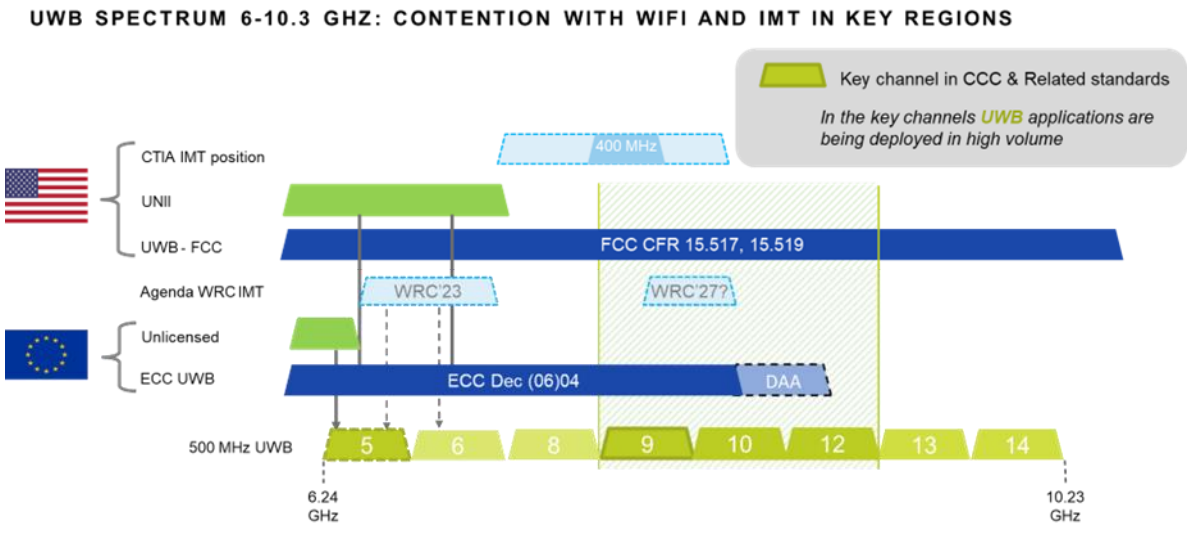
- Digital Key UWB uses IEEE UWB channel 9 (7.737 – 8.236 GHz), and uses IEEE UWB channel 5 (6.240 – 6.739 GHz) as an alternate channel.
- It uses very low power during transmission: more than 1000x lower than a Wi-Fi (-14.3 dBm)
- It spreads its energy over a wide part of the spectrum, thus causing even less interference in narrow-band receivers (-41.3 dBm/MHz).
- UWB ranging transmissions only use the spectrum briefly: between 1-5% during the ranging action. This is called the Duty Cycle.
- Ranging is triggered very selectively and only after establishing a trusted key – car match over Bluetooth. Therefore, ranging will be triggered modestly, while the user is in close proximity of the car. A typical Activity Factor is 0.1% on a daily basis.
- It handles interference from longer distance narrow-band transmitters very well since the time-domain correlation discrimination in UWB receivers intrinsically filters out such signals.
- However, Digital Key UWB receivers are susceptible to interference from higher power wideband communication transmitters located closely to the UWB receiver. International Mobile Telephony (IMT) and Wi-Fi are key examples.
- High power applications in the 7.7 – 8.3GHz. and 6.2 – 6.8GHz. spectrum would overwhelm the sensitive UWB receivers and destroy the growing consumer market.

Summary:

The CCC strongly recommends that investigations into spectrum for 5G and 6G cellular telephony (IMT) do not consider UWB channel 9 (7.7 - 8.3 GHz). Furthermore, CCC recommends to avoid allocation of IMT coinciding with UWB Channel 5 (6.2-6.8 GHz), or if such allocation is unavoidable, continue unabated access for Digital Key application to UWB channel 5 on a coexistence basis with no unnecessary regulatory barriers for the deployment of Digital Key.

Secure car key is part of an ecosystem of new UWB applications that amplify each other's adoption in the market. CCC supports the request of other UWB organizations to focus the ecosystem development to the higher mid-band in UWB channels 9, 10 and 12 (7.7 - 9.3 GHz), and that no IMT indication should be provided in UWB channels 9, 10 and 12 (7.7 - 9.3 GHz).

The figure below shows the main UWB channels and the issues UWB users face with other radio frequency users: UNI, IMT @WRC, CTIA IMT position.



© 2022 Car Connectivity Consortium