DIGITAL KEY

白皮书

CCC 数字钥匙 – 进入汽车的未来

CARCONNECTIVITY consortium®

目录

01 引言 4

02 应用场景 6

无感和 NFC 汽车进入 7

功能更多，使用更便利 8

分享 9

终止和暂停使用 10

钥匙属性 11

03 架构 12

04 CCC 认证流程 16

05 总结 18

关于车连接联盟 (Car Connectivity Consortium ®, CCC) 19

移动设备在我们的生活中扮演着重要角色。它能够帮助我们在一个设备上整合信息和工具，以支持几乎所有的日常生活。

用户使用智能手机进入和启动汽车的需求与日俱增。智能手机上的现行应用，使用了不同且不兼容的途径来控制和管理汽车钥匙。这些途径的便利程度、安全性和隐私性也大相径庭。

被动电子钥匙被广泛使用，但人们仍然需要为每一辆车准备一把实体钥匙。随着我们越来越专注于手机，我们出门时可能会将车钥匙忘在家里。既然手机已经取代了我们的通行证和信用卡，那为什么它不能取代车钥匙呢？

现在缺少的是一个让移动设备能够用作车钥匙的全球标准，而 CCC 数字钥匙弥补了这一差距。

01 引言

CCC 数字钥匙是标准化技术，它可以通过安全和保护隐私的方法，让移动设备不受地点限制地存储、验证和分享车辆的数字钥匙。

即使在手机电量低的情况下，这项技术也可以让用户利用移动设备进入汽车。在方便使用的同时，它还提供了增强的安全和隐私保护。

CCC 数字钥匙旨在弥补传统车钥匙方案的不足，并提供足以完全替代后者的稳定性。

CCC 数字钥匙利用近场通信 (Near Field Communication®, NFC) 技术在智能手机和汽车之间实现非接触式通信。在最新的 CCC 数字钥匙 3.0 版本中，新增了基于位置感知与无感的无钥匙进入和其他位置感知功能，将用户体验升级到全新高度。这一升级的实现得益于超宽带 (Ultra-Wideband, UWB) 技术与低功耗蓝牙 (Bluetooth Low Energy®, BLE) 连接技术的结合使用。新版本延续了对 NFC 技术的支持，可确保后向兼容性。

就 CCC 数字钥匙的整体用户体验而言，无缝式钥匙配置是其中的重要组成部分，因为这很可能会是车主与 CCC 数字钥匙系统的第一次互动。只要是符合 CCC 数字钥匙技术和安全要求的移动设备，都可以和类似配置的车辆进行配对。每辆车除了唯一的“车主”设备外，还可以有多个在“好友设备”上与汽车绑定的 CCC 数字钥匙，这一点非常适合于分享、汽车租赁和其他商业用途。

02 应用场景

有了 CCC 数字钥匙，用户便可以使用移动设备轻松进入或允许他人进入自己的爱车。除解锁车门和启动发动机之外，它还可用来支持众多其他的应用场景，例如分享更多钥匙、限制分享钥匙的功能和禁用钥匙。

下面介绍 CCC 数字钥匙的各种应用场景。

无感和 NFC 汽车进入

CCC 数字钥匙可提供无感的被动无钥匙进入功能，并提供与传统无感被动进入和被动启动功能在同一水平的舒适性和安全性。这些传统功能被广泛应用于大量车型。CCC 数字钥匙可用于进入汽车、启动发动机、锁定汽车或授权其他操作。操作过程中无需与移动设备进行任何交互操作（如激活应用）。手机可以一直放在口袋里，而不必拿出来。

为实现无感进入，移动设备会与汽车进行相互鉴权，汽车也会确认移动设备的 CCC 数字钥匙是否允许所请求的操作。UWB 飞行时间测量可防止攻击者利用中继攻击（基于信号放大）来欺骗汽车，使其误以为移动设备就在附近，这种保护机制称为“安全测距”。

或者，用户也可以通过将移动设备放在汽车的 NFC 读卡器附近来使用 CCC 数字钥匙。有限的 NFC 工作范围可防止攻击者诱导汽车误认为设备比实际距离更近。UWB - BLE 组合和 NFC 都会利用鉴权协议的隐私保护来确保任何无线通信监控者均无法跟踪用户或其移动设备。

功能更多，使用更便利

用户可以利用 CCC 数字钥匙在手机上进行不同的操作。除传统钥匙的功能外，CCC 数字钥匙还可以提供更多其他功能。

例如，受限于其物理特性，传统车钥匙只能提供有限的按键，用户只能用它来锁定/解锁汽车、打开车窗或启动发动机。而 CCC 数字钥匙则允许用户与移动设备进行交互，从而实现更多功能，例如打开行李箱、关闭车窗或开启暖风。同时，通过阻止发动机启动，车主可以放心地让儿童上车，而不必担汽车被意外开走。

分享

今天，如果您的朋友和家人需要用车，您只要把实体钥匙交给他们即可。数字钥匙分享也同样可以轻松、无缝和没有阻碍地做到这一点，甚至可以做得更好。

CCC 数字钥匙进一步提升了分享体验，用户可以分享多个 CCC 数字钥匙，而无需亲自将实体钥匙交给他人。例如，我可以授权我的朋友进入我的爱车，这样他们可以在我外出度假时使用它，我也可以让我的孩子上车但不允许孩子启动发动机。

除了车主设备外，用户还可以通过发送分享链接将其他人的智能手机设置为“好友设备”。一辆汽车可添加多个好友设备，但好友设备则无法继续分享这种权限。

CCC 数字钥匙框架在两个设备之间建立起一条安全的通信通道。车主设备通过该通道签发（核准）好友设备的数字钥匙（公共钥匙），而汽车 OEM 服务器将提供必要的签名（许可）。为确保分享的 CCC 数字钥匙只能由预期的接收者使用，车主可以选择通过分享链接之外的其他通道向他们提供分享密码和/或 PIN。

这种分享功能还可为车队、拼车、租车和其他商业服务的顺畅运转提供必要的支持。

终止和暂停使用

与实体钥匙不同的是，我们可以随时轻松地通过好友设备、车主设备、汽车和/或 OEM 服务器终止或暂停 CCC 数字钥匙的使用。用户可能会出于多种原因终止或暂停 CCC 数字钥匙的使用。例如，用户确定自己或好友不再需要用车；由于移动设备失窃或受到攻击，用户需要终止所有与之绑定的 CCC 数字钥匙；由于移动设备丢失，用户需要暂停其使用 CCC 数字钥匙；用户卖掉爱车；用户需要恢复汽车出厂设置等等。

因为手机的生命周期通常比汽车要短，所以用户可能需要更换车主手机。CCC 数字钥匙可以在新的车主手机上重新激活，而与此同时，好友设备上的 CCC 数字钥匙依旧保持不变；这对传统钥匙来说是无法办到的。

终止使用为永久性操作，需要分享新的 CCC 数字钥匙才能恢复相关权限，而暂停使用为暂时性操作，只会暂时停用 CCC 数字钥匙，可在之后恢复使用。

钥匙属性

每个 CCC 数字钥匙均包含众多属性和授权。标准的访问权限配置文件封装了这些属性和授权，用以描述如何使用以及何时使用这把数字钥匙。利用这些属性，用户可定制每一把 CCC 数字钥匙，从而实现新的应用场景、功能和特性。

除标准属性外，自定义权限（如果汽车 OEM 提供）也可用于其他更多应用场景或引入针对特定服务的信息。例如，车主可以限制分享 CCC 数字钥匙的使用方式；针对特定驾驶员调整最高车速；只允许打开行李箱或特定空间（不允许进入车内或其他空间，例如送货或取货服务）；允许进入驾驶舱，但不允许启动发动机或移车等等。

同时，CCC 数字钥匙还可以提供安全存储空间，用以存储与汽车相关的个性化设置、偏好和其他元数据，由此提供定制化的体验。

03 架构

CCC 数字钥匙架构采用基于标准的公钥基础架构 PKI，实现端到端信任。

移动设备在安全组件 SE（实现防篡改安全功能的嵌入式技术）中创建和存储数字钥匙，能够防止基于硬件和软件的攻击，包括篡改、存储入侵、克隆和未经授权的访问，从而提供最高级别的保护。

汽车和移动设备的安全组件之间的隐私保护安全连接，使用了 BLE－UWB 或 NFC 技术，并提供中继攻击保护。即使移动设备的电池电量不足，NFC 也能保持正常工作。

移动设备上的数字钥匙应用可能是操作系统的原生应用，也可能由汽车 OEM 或第三方提供。后者可能提供增强服务和特定的汽车功能。移动设备和汽车与其各自的 OEM 服务器进行交互，实现数字钥匙的分享和管理。即使移动设备和汽车均未联网，系统也能确保用户可以进入汽车，同时允许 OEM 根据需要，为某些操作增加联网状态下的功能。

如图 1 所示，CCC 数字钥匙生态系统由汽车、汽车 OEM 服务器、移动设备和移动设备 OEM 服务器组成，它们之间通过标准化接口及专有接口来实现通信。

标准化接口实现了不同实施方案间的互操作，这些实施方案来自移动设备制造商（移动设备 OEM）和汽车制造商（汽车 OEM），因此，CCC 数字钥匙规范对标准化接口进行了全面规定。

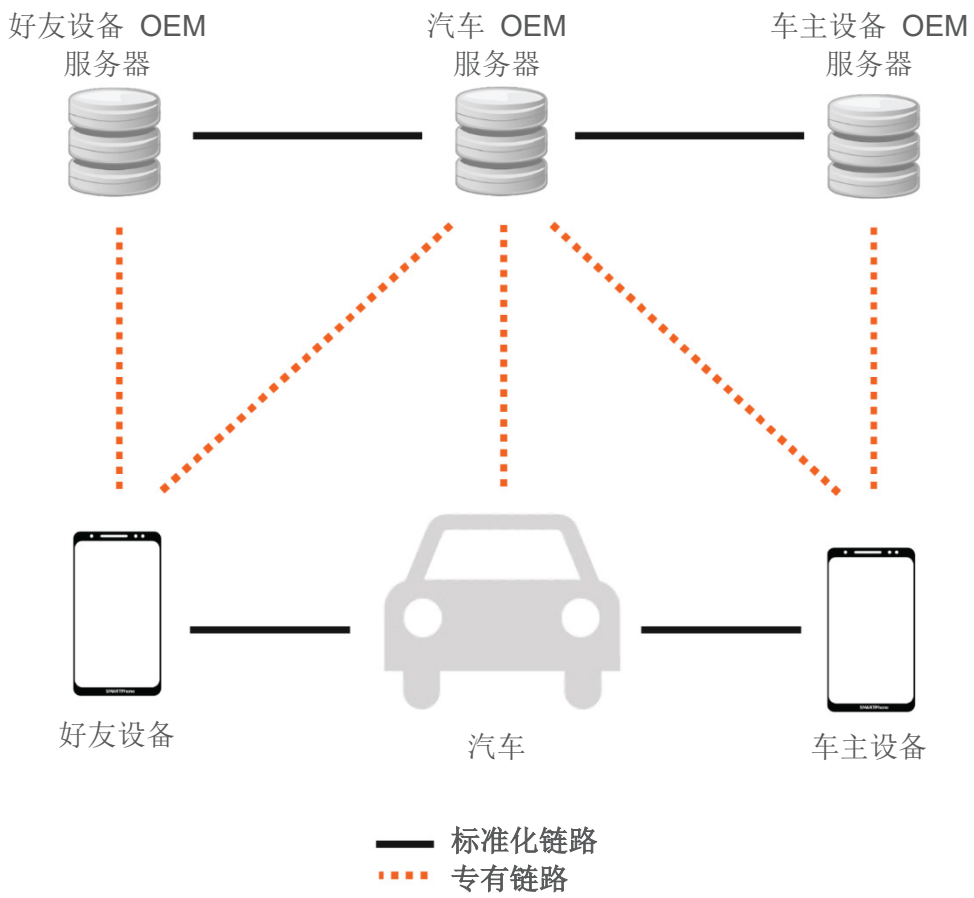

图 1：CCC 数字钥匙生态系统

图中显示的专有接口仅供参考；由于其不影响互操作性，因此没有对其进行规范。移动设备既可充当车主设备，也可充当好友设备，但无论是充当什么设备，汽车-设备接口都是一样的。对汽车-设备接口的标准化支撑了移动设备与汽车之间的互操作性。这些标准化包括通信通道（NFC、BLE 和 UWB）、协议和数字钥匙结构。汽车-设备接口提供了一个双向鉴权的安全通信通道，通过仅向经过身份验证的受信车辆展示移动设备的身份来保护用户的隐私。设备和汽车的 OEM 服务器从对方提取关于移动设备管理和汽车管理的详细信息，从而保证它们之间的互操作性；二者之间的接口提供了一种用来管理数字钥匙和提供客户服务的标准化方式。

移动设备 与其 OEM 服务器之间以及汽车与其 OEM 服务器之间都有专有接口。利用这些专用接口，OEM 能够提供定制钥匙管理功能。

标准化接口定义如下：

- **汽车 – 设备：**用于汽车和移动设备之间直接通信的无线接口。该接口可用于完成身份验证协议、安全交换信息、将移动设备与汽车配对，以及确保移动设备在汽车附近。
- **汽车 OEM 服务器 – 设备 OEM 服务器：**设备 OEM 服务器和汽车 OEM 服务器之间安全的、可信的接口。该接口用于创建、跟踪、管理和分享钥匙，以及服务器之间相互通报状态更改情况。

如上文和图 2 所示，移动设备利用安全组件、原生及定制应用、CCC 数字钥匙框架以及与设备 OEM 服务器的通信来保护和管理 CCC 数字钥匙。应用可能包括汽车 OEM 应用、租车服务应用等。

位于安全组件内的 CCC 数字钥匙小程序 applet 负责执行所有的安全关键型处理 - 身份验证、加密协议以及用于车主配对的密钥生成、用于“安全测距”（确认钥匙是否就在汽车附近或车内）、分享、汽车进入和发动机启动事务的密钥派生，同时还为 CCC 数字钥匙及其元数据提供防篡改的安全存储空间。NFC 接口可直接路由到 CCC 数字钥匙小程序，从而开辟一条独立于移动设备其余部分，并免受其干扰的通信路径。

UWB 模块的安全测距功能具有与 NFC 接口同等的系统安全水平，能够防止中继攻击。

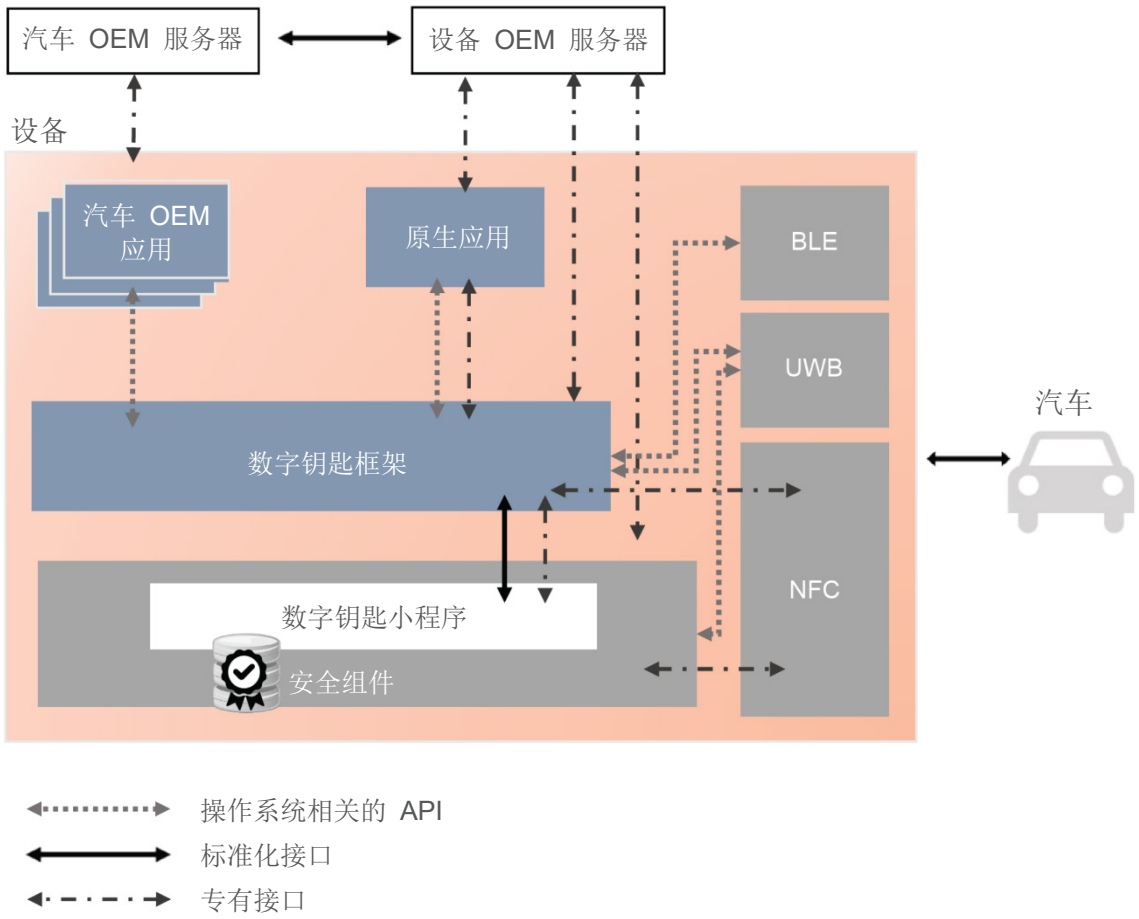

图 2：移动设备架构

“测距密钥”派生自 CCC 数字钥匙身份验证握手，并安全地存储在安全组件中。使用时，测距密钥只有短短 12 小时的有效期，可以缩短攻击者的时间窗口。

CCC 采用 UWB 安全测距技术，并结合 BLE 连接技术，实现 CCC 数字钥匙的全新位置感知功能，能够以等同或优于现有被动钥匙的精度进行安全定位。CCC 成员公司优化了 IEEE 802.15.4z 中的高速脉冲重复频率 (HRP) UWB 标准，从而达到了该特定应用场景下目前的精度水平，同时确保了安全和保全性。

04 CCC 认证流程

CCC 数字钥匙认证流程将确保数字钥匙解决方案的互操作性和安全性，从而在移动设备和汽车之间提供最为安全的绝佳用户体验。

CCC 认证带来的收益包括：

- CCC 认证产品通过标准化的方式让制造商和最终用户受益匪浅，确保用户从不同供应商的产品中均能获得一致的、无缝的使用体验。

- 认证促使相关各方顺畅地实现互操作，从而提高最终用户的满意度，并助力提高销量、降低产品退货率并减少支持成本。

- CCC 认证流程要求在营销过程中正确使用 CCC 认证标志，由此获得最终用户和消费者的信任。

CCC 数字钥匙认证流程正在制定过程中，计划于 2023 年发布。

05 总结

CCC 数字钥匙将提供必要的标准化和行业共识，以助力智能手机作为汽车钥匙的普及。

关于

车连接联盟（Car Connectivity Consortium ®, CCC）

CARCONNECTIVITY consortium®

CCC 联盟作为全球大部分汽车和智能手机行业的代表，拥有一百多家公司成员。

CCC 联盟是一家跨行业的标准化组织。其使命是打造一个可持续的、灵活的生态系统，通过标准化接口技术，为所有车辆和移动设备提供一致的卓越用户体验。

CCC 联盟的成员公司包括智能手机和汽车制造商、一级汽车供应商、硅/芯片供应商、安全产品供应商等。CCC 联盟的董事会成员包括来自苹果、小米、宝马、通用汽车、谷歌、本田、现代、LG、梅赛德斯-奔驰、恩智浦、松下、三星、大众和 Thales 等创始成员公司的相关人士。

除 CCC 数字钥匙外，CCC 联盟还提供 MirrorLink® 技术。

DIGITAL KEY

地址

3855 SW 153rd Drive Beaverton, OR 97003, USA

电话

+1 503-619-1163

网络联系方式

电子邮件：admin@carconnectivity.org
网站：https://carconnectivity.org
LinkedIn：https://www.linkedin.com/company/car-connectivity-consortium-ccc