DIGITAL KEY

白書

CCC Digital Key - 自動車アクセスの未来

CARCONNECTIVITY
consortium®

法的な通知

本文書（以下「本文書」という）の著作権は、Car Connectivity Consortium LLC（以下「CCC」という）に帰属します。この文書の使用には、この法的通知およびライセンス条項が適用されます。

CCC はCCC の会員でない受領者を含め、本書の各受領者に対し、CCC 仕様書またはその他のCCCの著作物の解釈または理解に関連する情報提供および教育目的のためにのみ本書を使用し、逐語的に複製する権利（以下「目的」といいます）を与えます。
受領者は、関連会社または下請業者以外の第三者に対して、本文書またはそのコピーを利用、または配布することはできません。ただし、その関連会社や下請け会社が目的を遂行するために知る必要がある場合は可能とします。その他による明示または黙示を問わずいかなる知的財産権に対するその他のライセンスも本書に付与されていません。

本書はいかなる保証、表明もなく「現状のまま」提供されます。CCCは明示的か黙示的か法令によるものか否かを問わず、本書および/または本書に記載された資料に関する一切の表明、保証を明示的に否認します。上記の文章を制限することなく、CCCは本契約により、特定の目的への適合性、商品性、権原、第三者の権利の非侵害または不存在、権利の有効性、および/またはその他に関する一切の保証を明示的に否認します。

CCCは、本文書の正確性または完全性に関していかなる表明も行いません。CCC、およびそのメンバーならびにライセンサーは本書および/または本書に記載されている資料に起因する一切の責任を明示的に否認し、利用者または第三者に対していかなる責任も負わないものとします。これには本書が利用者または第三者の特許権、著作権、その他の知的財産権を侵害しているとの主張に起因する一切の責任を含みますがこれらに限定されません。

CCCおよびそのメンバーならびにライセンサーは、いかなる種類の損失、費用、経費、または損害(直接的、間接的、特別、偶発的、結果的、懲罰的、および/または懲罰的損害を含むがこれらに限定されない)に対しても責任を負わず、また負わないものとします。本書または本書に記載されている資料の使用または信頼から生じたいかなる種類の損失、費用、経費、損害（直接的、間接的、特別、付随的、結果的、懲罰的、および/または懲罰的損害を含む）に対しても、ライセンサーは一切の責任を負いません。

本文書のいかなる規定も、CCCもしくはそのメンバーまたはライセンサーに対して本文書に対するまたは本文書に関連するサポートを提供する義務を課すものではありません。
CCCはCCCが必要と判断した場合には、いつでも、予告なく、この文書の変更または修正を採用する権利を留保し、かかる変更または修正を行う義務を負うものではありません。

目次

『私たちの暮らしの中で重要な役割を果たすモバイル・デバイス。日常生活のほぼすべてをサポートする情報やツールをたった1台のデバイスに集約することが可能に。』

スマートフォンで自動車にアクセスし、始動したいという顧客ニーズが高まっています。車両へのアクセスを制御・管理するための既存のスマートフォン用アプリは、利便性、セキュリティ、プライバシー保護の程度が異なる、相互運用不可能なアプローチを採用してきました。

パッシブ電子キーフォブは広く普及していますが、それでも車1台につき1つ必要です。携帯電話への依存度が高まるにつれ、キーフォブは外出時に忘れがちなものの１つになっています。携帯電話が旅行パスやクレジットカードの代わりになっているのにもかかわらず、なぜ車のキーはそうならないのでしょうか？

欠けているのは、モバイル・デバイスを車のキーとして使えるようにする世界標準です。CCCデジタル・キーはこのギャップを埋めます。

01 INTRODUCTION

CCCデジタル・キーは標準化された技術であり、モバイル・デバイスが安全かつプライバシーを保護する方法で、自動車のデジタル・キーを保存、認証、共有することを可能にします。

スマートフォンのバッテリー残量が少なくなっても、消費者はモバイル機器を使って自動車にアクセスすることができます。

これにより、スマートフォンのバッテリー残量が少なくなっても、お客様はモバイル・デバイスを使って自動車にアクセスできるようになります。
便利な使用方法とともに、セキュリティとプライバシー保護も強化されています。
このCCCデジタル・キーは、従来のキーフォブの実装を補完することを目的としながらも、完全に置き換えるのに十分な堅牢性を備えているのです。

CCCデジタル・キーはNFC（Near Field Communication®）技術を採用し、スマートフォンと車両間の非接触通信を実現しています。
最新のCCCデジタル・キー・リリース3.0では、ハンズフリー、位置認識キーレスアクセス、位置認識機能が追加され、使い勝手が向上しています。これは、Bluetooth Low Energy®接続と組み合わせたウルトラワイドバンド（UWB）を使用して実現されています。
後方互換性を確保するため、NFC技術のサポートも維持しています。

シームレスなキープロビジョニングは、CCCデジタル・キーのユーザーエクスペリエンス全体にとって重要な要素です。
CCCデジタル・キーの技術およびセキュリティ要件を満たすモバイル機器であれば同様の装備を持つ車/自動車とペアリングすることができます。
各車/自動車は1つの「オーナー」デバイスしか持つことができませんが、「フレンド・デバイス」に複数のCCCデジタル・キーを関連付けることもできます。

02 USE CASES

『CCCデジタル・キーを使えば、モバイル・デバイスを使って簡単に車にアクセス、共有が可能に。また、ドアの解錠やエンジンの始動だけでなく、追加キーの共有、共有キーの機能制限、キーの無効化など、多くのユースケースをサポートする可能性にも期待。』

CCCデジタル・キーがこれらのユースケースにどのように対応しているかを見てみましょう。

HANDS-FREE AND NFC VEHICLE ACCESS

CCCデジタル・キーは、現在多くの車種で提供されている従来のハンズフリー・パッシブ・エントリーやパッシブ・スタートと同レベルの快適性と安全性で、ハンズフリー・パッシブ・キーレス・エントリーを可能にします。CCCデジタル・キーは、車/自動車へのアクセス、エンジンの始動、車/自動車の停止、その他の操作の許可に使用することができます。アプリを起動させるなど、モバイル機器とのインタラクションは必要ありません。スマートフォンはユーザーのポケットに入れたままで結構です。

ハンズフリー・アクセスを提供するために、モバイル・デバイスと自動車は相互に認証を行い、自動車はモバイル・デバイスのCCCデジタル・キーが要求された操作を許可していることを検証します。UWB time-of-flight測定は、通信攻撃者が （信号増幅に基づく）リレー攻撃を使用して、モバイル・デバイスが近くにないにもかかわらず、車/自動車を騙して近くにあると思わせることを 防ぎます。

同様にCCCデジタル・キーは単にモバイル・デバイスを車/自動車のNFCリーダーの近くに置くことでも使用することができます。ただし、NFCの動作範囲は限定されているため、攻撃者が自動車を欺いてデバイスが実際よりも近くにあると思わせることはできません。このように、UWB-BLEの組み合わせとNFCの両方が認証プロトコルのプライバシーを利用し、無線通信を監視する者がユーザやそのモバイルデバイスを追跡できないようにします。

ADDITIONAL FUNCTIONS IMPROVE CONVENIENCE

CCCデジタルキーを使えば、ユーザーは携帯電話からさまざまなアクションを起動できるようになります。

CCCデジタルキーは従来のキーフォブと同じ機能、そしてそれ以上の機能を提供します。

例えば、従来のキーフォブはその性質上、限られた数のボタンで車の施錠・開錠、車の開閉、エンジンの始動が可能でした。CCCデジタル・キーでは、ユーザーはモバイル・デバイスと連動して、トランクを開けたり、窓を閉めたり、暖房を作動させたりすることができます。同時に、エンジンの始動を防ぐことができるため、オーナーが意図しない発進を心配することなく、子どもが車内に入ることができます。

SHARING

今日、人々は実際のキーやキーフォブを渡すだけで、友人や家族と車のキーを共有することができます。デジタル・キーの共有は、同じように簡単、シームレス、制限なし、あるいはそれ以上に望ましいことです。

CCCデジタル・キーは、複数のCCCデジタル・キーを共有できるようにすることで、物理的にキーやキーフォブを誰かに渡すことなく、共有体験を向上させます。
例えば私が休暇で遠方にいる間、友人に私の車へのアクセス権を与えることができ、彼らは私の車を使用することができます。

メインのオーナー・デバイスだけでなく、ユーザーは共有リンクを送信するだけで、他の人のスマートフォンを「フレンド・デバイス」として設定できます。1台の車/自動車に複数のフレンド・デバイスを追加することも可能ですが、このアクセス権を共有することはできません。
CCC デジタル・キーフレームワークは、2つのデバイス間の安全な通信チャネルを確立し、このチャネルを通じて所有者デバイスが友人デバイスのデジタル・キー（公開鍵）に署名承認）し、必要な署名（承認)が自動車OEMサーバから取得されます。
共有されたCCCデジタル・キーが意図された受信者のみによって使用可能であることを保証するために、所有者はオプションとして共有リンクとは異なるチャネルで通信される共有パスワードおよび/またはPINを受信者に提供することができます。

このシェアリング機能は、フリート、ライドシェア、レンタル、その他の商業サービスをサポートするために必要な基盤も提供します。

TERMINATION AND SUSPENSION

実際のキーやキーフォブとは異なり、CCCデジタル・キーはフレンド・デバイス、オーナー・デバイス、車/自動車および/またはOEMサーバーから、いつでも簡単に解除または一時停止することができます。CCCデジタル・キーは様々な理由で停 止または終了することが可能です。

例えば、ユーザが自分または友人が自動車へのアクセスが不要になったと判断した場合や、盗難または危険にさらされたモバイル・デバイスに関連付けられているす

べてのCCCデジタル・キーを停止したい場合、またはデバイスが紛失した際に一時停止したい場合などが考えられます。

また、車両を売却したり、工場出荷時の状態に戻したい場合などもあります。

携帯電話のライフサイクルは一般的に自動車よりも短いため、ユーザーは所有者の携帯電話を変更する必要があるかもしれません。CCCデジタル・キーは、新しい所有者の携帯電話で再度有効かすることができ友人デバイスのCCCデジタル・キーはそのまま残ります。

一方、終了は永続的ですので、アクセスを回復するには新しいCCCデジタル・キーの共有が必要です。これに対し、一時停止は車に一時的なものであり、再開されるまでCCCデジタル・キーを無効にするだけのものです。

KEY PROPERTIES

各CCCデジタル・キーは、標準的なアクセス権限プロファイルにカプセル化された多数の属性と権限を含んでおり、いつ、どのように使用できるかを記述しています。これらの特性により、各CCCデジタル・キーはカスタマイズが可能となり、新たなユースケースや機能、パーソナライゼーションが実現します。

標準プロパティに加え、カスタムエンタイトルメント（自動車OEMにより提供される場合）を使用して、追加ユースケースを有効にしたり、サービス固有の情報を含めることもできます。例えば所有者は、共有CCCデジタル・キーの使用方法を制限したり、特定のドライバーの最高速度を調整したり、トランクまたは特定のコンパートメントへのアクセスのみを許可したり（配送またはピックアップサービスの場合など、車室または他のコンパートメントへのアクセスは許可しない）、車室へのアクセスは許可するが、エンジン始動や出動は許可しない、などといったことが可能です。

CCCデジタル・キーはまた、カスタマイズされた体験を提供するために、自動車関連のパーソナライゼーション設定、嗜好その他のメタデータを保存する安全なストレージ・コンテナも提供します。

03 ARCHITECTURE

CCCデジタル・キー・アーキテクチャでは、標準ベースの公開鍵インフラストラクチャを使用して、エンドツーエンドの信頼を確立。

モバイル・デバイスは、改ざん、ストレージへの侵入、クローン作成、不正アクセスなど、ハードウェアおよびソフトウェア・ベースの攻撃から最高レベルの保護を提供するために、セキュア・エレメント（改ざん耐性のあるセキュアな実装を提供する組み込み技術)にデジタル鍵をさくせいし、保存します。

BLE、UWB、またはNFCを使用して、車/自動車とモバイル・デバイスのセキュア・エレメントとの間でセキュアでプライバシーを保護した接続が確立され、リレー攻撃防止を提供し、NFCの場合はモバイル・デバイスのバッテリー残量が少なくなっても機能し続けます。

モバイル・デバイス上のデジタル・キー・アプリケーションは、オペレーティング・システムにネイティブである場合もあれば、自動車OEMやサードパーティが提供し、拡張サービスや自動車固有の機能を提供する場合もあります。モバイル・デバイスと自動車は、それぞれのOEMサーバーと相互作用し、デジタル・キーを共有・管理します。

このシステムは、モバイル·デバイスも自動車もインターネットに接続できない場合でも、自動車へのアクセスを保証します。一方、OEMが希望すれば、特定の操作にインターネット·アクセスを必要とする機能を追加することもできます。

図1に示すように、CCCデジタル·キーのエコシステムは、自動車、自動車OEMサーバー、モバイル・デバイス、モバイル・デバイスOEMサーバーで構成され、これらすべてが標準化されたインターフェイスと独自のインターフェイスを組み合わせて相互に通信します。

標準化されたインタフェースは、モバイル・デバイス・メーカー（モバイル・デバイスOEM）と自動車メーカー（自動車OEM）の異なる実装間の相互運用性を可能にするため、CCCデジタル・キー仕様で完全に規定されています。

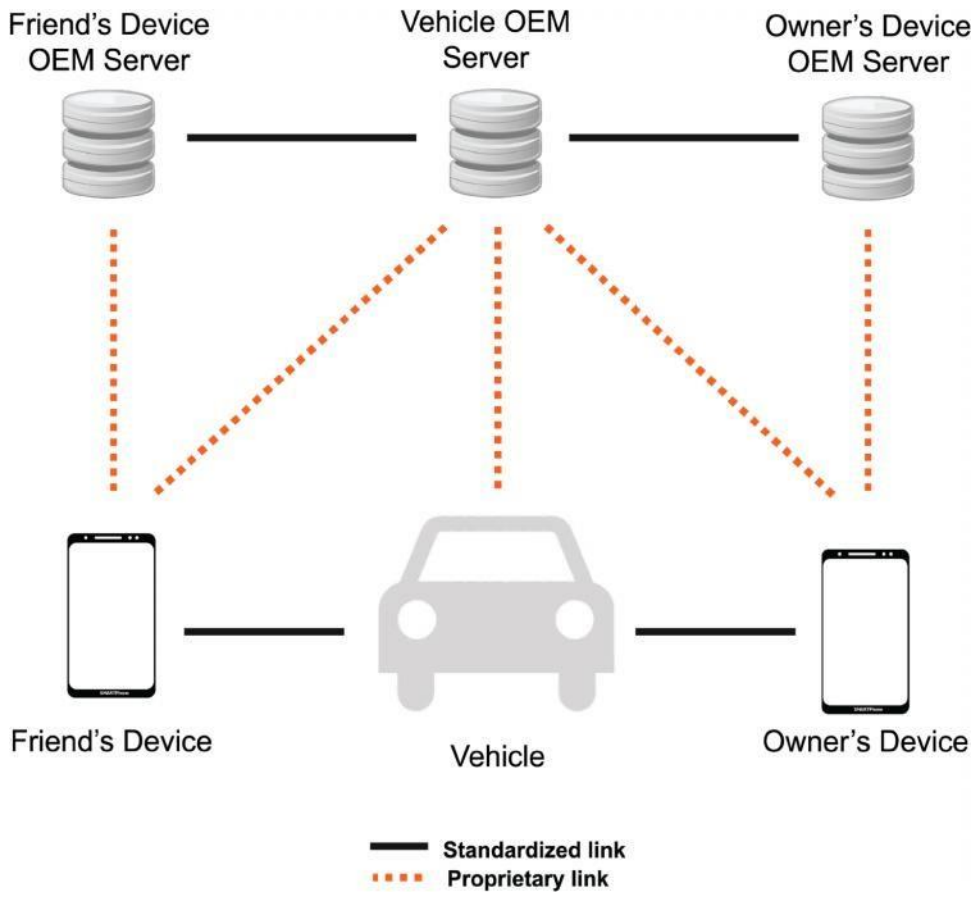

Figure 1: CCC Digital Key ecosystem

モバイル・デバイスは、オーナー・デバイスとしてもフレンド・デバイスとしても機能しますが、自動車-デバイス間インタフェースは、どちらの役割においても同じです。モバイル・デバイスと自動車間の相互運用性は、通信チャネル（NFC、BLE、UWB）、プロトコル、およびデジタル・キー構造といった自動車対デバイス・インターフェースを標準化することでサポートされます。

自動車対デバイス・インターフェースは相互に認証された安全な通信チャネルを提供し、認証後に信頼できる自動車にのみモバイル・デバイスのアイデンティティを公開することで、ユーザのプライバシーを保護します。

デバイスと自動車のOEMサーバーは、モバイル・デバイスと自動車の管理の詳細を互いに抽象化することで相互運用性をサポートし、両者間のインターフェースは、デジタル・キーの管理と顧客サービスの提供に標準化された方法を提供します。

モバイル・デバイスOEMサーバーとモバイル・デバイス間、および自動車OEMはカスタム鍵管理機能を提供できます。

標準化されたインターフェースは以下のように定義されています。

Vehicle-Device: 自動車とモバイル・デバイス間の直接通信用ワイヤレス・インタフェース。認証プロトコルを交換し、情報を安全に交換し、モバイル・デバイスと自動車をペアリングし、モバイル・デバイスが自動車の近くにあることを確認するために使用されます。

Vehicle OEM Server-Device OEM Server: デバイスOEMサーバーと自動車OEMサーバー間の安全で信頼できるインターフェース。鍵の作成、追跡、管理、共有に使用され、サーバー間でステータスの変更を通知します。

図２に示すように、モバイル・デバイスは、セキュアエレメント、ネイティブ・アプリおよびカスタムアプリ、CCCデジタル・キー・フレームワークおよびデバイスOEMサーバーへの通信を使用して、CCCデジタル・キーを保護および管理します。アプリには、自動車OEMアプリ、レンタル・サービス・アプリなどがあります。

セキュア・エレメント内に存在するCCCデジタル・キー・アプレットは、認証、暗号化プロトコル、および所有者のペアリングに使用される鍵生成、「セキュア・レンジング」（鍵が実際に近くにあるか車内にあるかの検証）用の鍵導出、共有、および自動車へのアクセスとエンジン始動トランザクションといったセキュリティ上重要な処理をすべて実行し、同時にCCCデジタル・キーとそのメタデータのための安全で改ざん防止されたストレージを提供し、NFCインターフェースはCCCデジタル・キー・アプレットに直接ルーティングされ、モバイル・デバイスの他の部分から保護され、独立して動作する通信経路を提供します。

UWBモジュールは、安全な測距によりNFCインターフェースと同じシステム・セキュリティ・レベルを維持し、リレー攻撃から保護します。

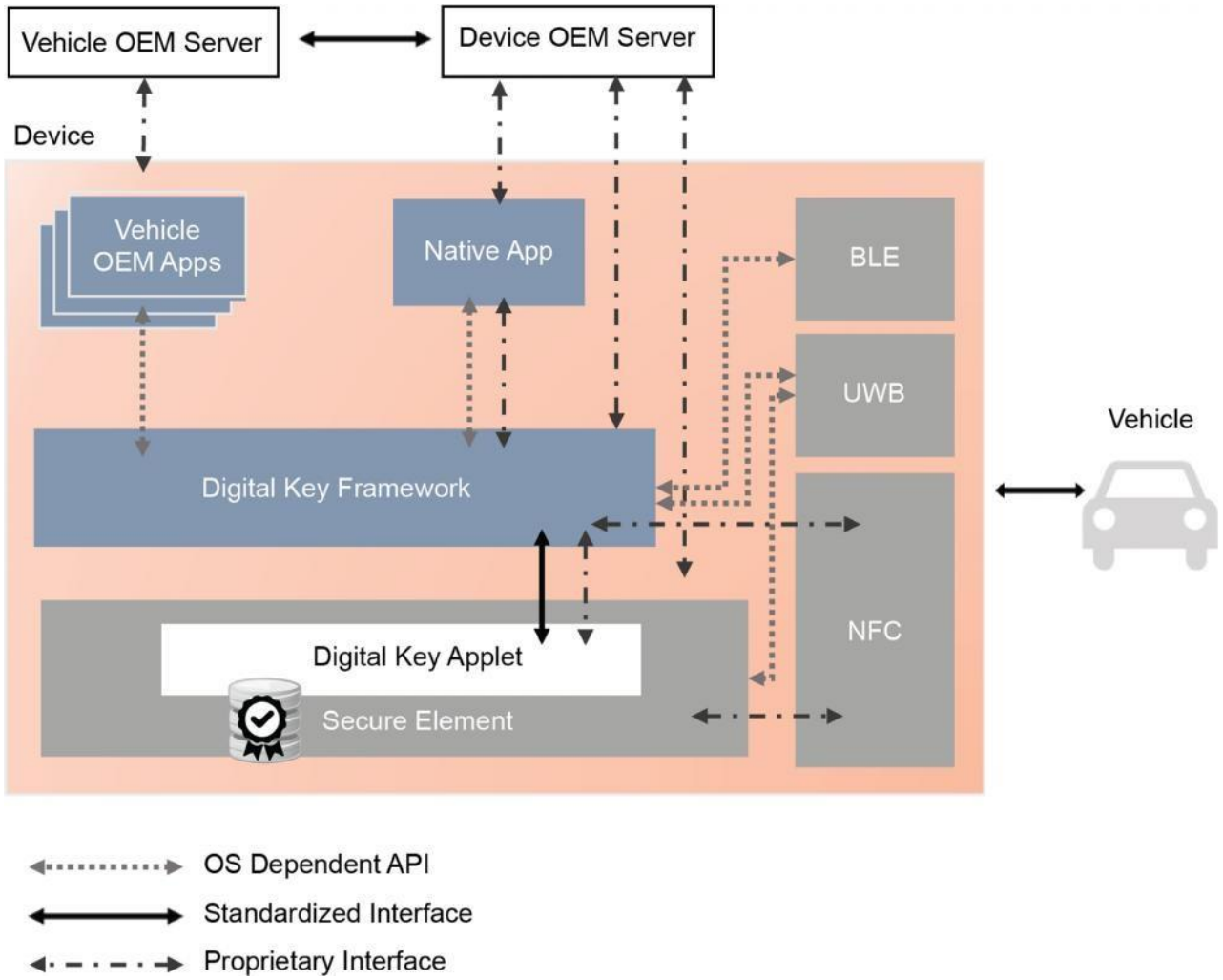

Figure 2: Mobile Device Architecture

「レンジング・キー」はCCCデジタル・キー認証ハンドシェイクから派生し、セキュア・エレメントに安全に保存されます。使用時、レンジング・キーの有効期限は12時間に制限され、攻撃者のタイム・ウィンドウを短くします。

しました。CCCメンバー企業は、IEEE 802.15.4zのHigh Rate Pulse Repetition Frequency (HRP) UWB規格を最適化し、安全性とセキュリティを確保しながら、この特定のユースケースでこのレベルの精度を実現しています。

CCCは、UWBセキュアレンジング技術をBLE コネクティビティ技術と組み合わせて採用しCCCデジタル・キーの新しい位置認識機能を実現し、既存のパッシブ・キー・フォブと同等以上の精度で安全な測位を可能に

04 CCC CERTIFICATION PROGRAM

CCCデジタル・キー認証プログラムは、デジタル・キー・ソリューションの相互運用性とセキュリティを保証し、モバイル・デバイスと自動車間で最高かつ最も安全なユーザー体験を提供します。

CCC認定のメリットは以下の通りです：

- CCC認証製品は、標準化されたアプローチによってメーカーとエンドユーザーの双方にメリットをもたらし、異なるベンダーの製品間で安定したシームレスなユーザー体験を保証します。

- 認証は関係者の円滑な相互運用につながります。その結果、エンドユーザーの満足度が向上し、販売台数が増加する可能性があります。販売台数の増加、返品率の低下、サポートコストの削減が期待できます。

- CCC認証プログラムは、マーケティングにおいてCCC認証ロゴを正しく使用することを奨励し、エンドユーザーや消費者との信頼関係を構築します。

- CCCデジタル・キー認証プログラムは現在開発中で、2022年のリリースを目指しています。

05 CONCLUSION

『CCCデジタル・キーは、自動車のキーとしてスマートフォンの普及を促進するため、必要な標準化と業界の受容性を実現。』

ABOUT
Car Connectivity Consortium ® (CCC)

CARCONNECTIVITY
consortium®

CCCは世界の自動車産業
とスマートフォン産業の
大部分を代表し、100社以
上が加盟しています。

CCCは業界横断的な標準化団体で、あらゆる自動車やモバイル機器に一貫して優れた
ユーザー体験を提供するためのインターフェース技術を標準化し、持続可能で柔軟な
エコシステムを構築することを使命としています。

CCCのメンバー企業は、スマートフォンおよび自動車メーカー、自動車用Tier1サプライヤー、
シリコン／チップベンダー、セキュリティ製品サプライヤーなどで構成されています。
CCCの理事会には、チャーターメンバー企業であるアップル、BMW、ゼネラルモーターズ、
Google、ホンダ、Hyundai、LG、Mercedes-Benz AG、NXPセミコンダクターズ、
パナソニック、サムスン、フォルクスワーゲンの関係者が名を連ねています。

CCCデジタル･キーに加え、CCCのポートフォリオにはMirrorLink®テクノロジーが含まれています。

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