

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7550124号
(P7550124)

(45)発行日 令和6年9月12日(2024.9.12)

(24)登録日 令和6年9月4日(2024.9.4)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62

請求項の数 11 (全54頁)

(21)出願番号	特願2021-159413(P2021-159413)	(73)特許権者	000004260 株式会社デンソー
(22)出願日	令和3年9月29日(2021.9.29)		愛知県刈谷市昭和町1丁目1番地
(65)公開番号	特開2023-49593(P2023-49593A)	(73)特許権者	519260337
(43)公開日	令和5年4月10日(2023.4.10)		アイデミア フランス
審査請求日	令和6年2月5日(2024.2.5)		フランス国, 9 2 4 0 0 クルブボア, プラス サミュエル ドゥ シャンプラン 2
		(74)代理人	矢作 和行
		(74)代理人	100121991
			弁理士 野々部 泰平
		(74)代理人	100145595
			弁理士 久保 貴則
		(72)発明者	松下 傑
			愛知県刈谷市昭和町1丁目1番地 株式 最終頁に続く

(54)【発明の名称】 車両用デジタルキーシステム、車両用デジタルキー管理方法、車両用装置、携帯端末

(57)【特許請求の範囲】

【請求項1】

車両に搭載されて使用される車両用装置（4）と、
携帯可能な情報処理端末である少なくとも1つの携帯端末（1）と、
前記車両を使用するための鍵情報として、前記携帯端末ごとに固有のサービス鍵を生成し、前記携帯端末に配信するサーバ（3）と、を含む車両用デジタルキーシステムであって、
前記サーバは、
オーナーと紐付けられた前記携帯端末であるオーナー端末から送信されるゲスト鍵発行要求信号に基づき、前記オーナー端末以外の前記携帯端末であるゲスト端末のための前記サービス鍵であるゲスト鍵を発行することと、
発行した前記ゲスト鍵を前記ゲスト端末に配信することと、を実施するように構成されており、
前記車両用装置は、
動作モードとして、前記車両のオーナーとしての権限を有する前記サービス鍵であるオーナー鍵を登録可能なオーナー登録可能モードと、前記オーナー鍵の登録を拒否するオーナー登録禁止モードと、を備え、
前記携帯端末又は前記サーバと通信することにより、前記サービス鍵を取得し、所定の車両側記憶装置（45）に保存し、
所定の専用デバイス又は前記サーバから、特定のオーナー登録開始信号が入力されたこと

に基づいて前記オーナー登録禁止モードから前記オーナー登録可能モードに移行し、

前記オーナー登録可能モードで動作している場合には、前記オーナー端末又は前記サーバから、前記車両のオーナーとしての権限を有する前記サービス鍵であるオーナー鍵を取得するための通信を実行する一方、

前記オーナー登録禁止モードで動作している場合には、前記オーナー端末又は前記サーバから前記オーナー鍵を取得するための通信そのもの、又は、受信した前記オーナー鍵を前記車両側記憶装置に保存する処理を実行せず、

前記ゲスト鍵に関しては、前記オーナー登録禁止モードにおいても、前記ゲスト端末又は前記サーバから前記ゲスト鍵を受信するためのシーケンスを実施可能に構成されており、

前記ゲスト端末又は前記サーバから前記ゲスト鍵を受信した場合には当該ゲスト鍵を前記車両側記憶装置に保存するように構成されている車両用デジタルキーシステム。

10

【請求項 2】

請求項 1 に記載の車両用デジタルキーシステムであって、

前記携帯端末と前記車両用装置は、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能に構成されており、

前記サーバは、任意の 1 つの前記携帯端末のために発行した前記サービス鍵は、前記車両用装置には配信せずに、当該携帯端末に配信するように構成されており、

前記車両用装置は、前記携帯端末と近距離無線通信することによって、前記サーバが発行した前記サービス鍵を取得し、前記車両側記憶装置に保存するように構成されている車両用デジタルキーシステム。

20

【請求項 3】

請求項 2 に記載の車両用デジタルキーシステムであって、

前記サーバは、

前記オーナー端末から送信されるオーナー鍵発行要求信号を受信したことに基づき、前記オーナー鍵を発行することと、

発行した前記オーナー鍵を、前記車両用装置には配信せずに、前記オーナー端末に配信することと、を実施し、

前記車両用装置は、

前記携帯端末と近距離無線通信することによって、前記サーバが発行した前記サービス鍵を取得し、前記車両側記憶装置に保存するように構成されており、

30

前記オーナー登録可能モード時には、前記近距離無線通信にて前記オーナー端末から前記オーナー鍵を取得するための通信シーケンスを実行する一方、

前記オーナー登録禁止モード時には、前記オーナー端末から前記オーナー鍵を取得するための通信を実行しないように設定されている車両用デジタルキーシステム。

【請求項 4】

請求項 1 から 3 の何れか 1 項に記載の車両用デジタルキーシステムであって、

前記携帯端末と前記車両用装置は、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能に構成されており、

前記サーバは、

前記オーナーと紐付けられた前記携帯端末であるオーナー端末から発せられるゲスト鍵発行要求信号を受信したことに基づき、前記オーナー端末以外の前記携帯端末であるゲスト端末のための前記サービス鍵であるゲスト鍵を発行することと、

40

前記ゲスト鍵を前記ゲスト端末に送信することと、を実施し、

前記ゲスト鍵は、前記車両用装置と前記ゲスト端末とが前記近距離無線通信を実行する事により有効化される車両用デジタルキーシステム。

【請求項 5】

請求項 1 から 4 の何れか 1 項に記載の車両用デジタルキーシステムであって、

前記車両用装置は、前記オーナー鍵は 1 つしか保存できないように構成されている車両用デジタルキーシステム。

【請求項 6】

50

請求項 1 から 5 の何れか 1 項に記載の車両用デジタルキーシステムであって、

前記サーバは、前記サービス鍵の発行に伴い、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を生成し、前記携帯端末に配信するように構成されており、

前記携帯端末は、前記ワンタイム認証鍵を用いて前記車両用装置に対して通信相手としての正当性を証明するように構成されており、

前記携帯端末は、前記ワンタイム認証鍵の残数が所定値以下となっていることに基づいて前記サーバに対して前記ワンタイム認証鍵の補充を要求する補充要求信号を送信し、

前記サーバは、前記補充要求信号の受信に基づいて新たに複数の前記ワンタイム認証鍵を生成し前記携帯端末に送信するように構成されている車両用デジタルキーシステム。

【請求項 7】

車両に搭載されて使用される車両用装置（4）と、

携帯可能な情報処理端末である少なくとも 1 つの携帯端末（1）と、

前記車両を使用するための鍵情報として、前記携帯端末ごとに固有のサービス鍵を生成し、前記携帯端末に配信するサーバ（3）と、を含む車両用デジタルキーシステムであって、

前記車両用装置は、前記携帯端末又は前記サーバと通信することにより、前記サービス鍵を取得し、所定の車両側記憶装置（45）に保存するように構成されており、

前記車両用装置は、所定の専用デバイス又は前記サーバから、特定のオーナー登録開始信号が入力されたことを条件として、前記車両のオーナーとしての権限を有する前記サービス鍵であるオーナー鍵を、前記車両側記憶装置へ保存するように構成されており、

前記サーバは、前記サービス鍵の発行に伴い、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を生成し、前記携帯端末に配信するように構成されており、

前記携帯端末は、前記ワンタイム認証鍵を用いて前記車両用装置に対して通信相手としての正当性を証明するように構成されており、

前記携帯端末は、前記ワンタイム認証鍵の残数が所定値以下となっていることに基づいて前記サーバに対して前記ワンタイム認証鍵の補充を要求する補充要求信号を送信し、

前記サーバは、前記補充要求信号の受信に基づいて新たに複数の前記ワンタイム認証鍵を生成し前記携帯端末に送信するように構成されている車両用デジタルキーシステム。

【請求項 8】

所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能であって、かつ、携帯可能に構成された情報処理端末である少なくとも 1 つの携帯端末（1）と、

車両に搭載されて使用される、前記近距離無線通信を実施可能に構成されている車両用装置（4）と、

前記携帯端末からの要求に基づき前記車両を使用するための鍵情報であるサービス鍵を生成するサーバ（3）と、とによって実施される車両用デジタルキー管理方法であって、

前記サーバが、前記車両のオーナーが所持する前記携帯端末としてユーザデータベースに登録されているオーナー端末からの要求に基づき、前記オーナーとしての権限を有する前記サービス鍵であるオーナー鍵を発行することと、

前記サーバが、発行された前記オーナー鍵を前記車両用装置には送信せずに、前記オーナー端末には配信することと、

前記サーバが、前記オーナー端末から送信されるゲスト鍵発行要求信号に基づき、前記オーナー端末以外の前記携帯端末であるゲスト端末のための前記サービス鍵であるゲスト鍵を発行することと、

前記サーバが、発行した前記ゲスト鍵を前記ゲスト端末に配信することと、

前記車両用装置が、所定の専用デバイス又は前記サーバから、所定の登録開始信号が入力されたことに基づいて、前記オーナー鍵の登録を拒否するオーナー登録禁止モードから前記オーナー鍵を登録可能なオーナー登録可能モードへと切り替わることと、

前記オーナー端末が、前記車両用装置が前記オーナー登録可能モードであることを条件として、前記近距離無線通信にて前記車両用装置に前記オーナー鍵を送信することと、

前記車両用装置が、前記オーナー登録可能モードであることを条件として、前記オーナー端

10

20

30

40

50

末から前記オーナー鍵を受信し、所定の不揮発性の車両側記憶装置（４５）に保存することと、

前記車両用装置は、前記オーナー登録禁止モードで動作している場合、前記車両用装置は、前記オーナー端末又は前記サーバから前記オーナー鍵を取得するための通信そのもの、又は、受信した前記オーナー鍵を前記車両側記憶装置に保存する処理を実行しない一方、前記オーナー登録禁止モードにおいても、前記ゲスト端末又は前記サーバから前記ゲスト鍵を受信するためのシーケンスは実施することと、

前記車両用装置が、前記ゲスト端末又は前記サーバから前記ゲスト鍵を受信した場合に、は当該ゲスト鍵を前記車両側記憶装置に保存することと、を含む車両用デジタルキー管理方法。

【請求項９】

所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能であって、かつ、携帯可能に構成された情報処理端末である少なくとも１つの携帯端末（１）と、車両に搭載されて使用される、前記近距離無線通信を実施可能に構成されている車両用装置（４）と、

前記携帯端末からの要求に基づき前記車両を使用するための鍵情報であるサービス鍵を生成するサーバ（３）と、とによって実施される車両用デジタルキー管理方法であって、

前記サーバが、前記車両のオーナーが所持する前記携帯端末としてユーザデータベースに登録されているオーナー端末からの要求に基づき、前記オーナーとしての権限を有する前記サービス鍵であるオーナー鍵を発行することと、

前記サーバが、発行された前記オーナー鍵を前記車両用装置には送信せずに、前記オーナー端末には配信することと、

前記車両用装置が、所定の専用デバイス又は前記サーバから、所定の登録開始信号が入力されたことに基づいて、前記オーナー鍵の登録を拒否するオーナー登録禁止モードから前記オーナー鍵を登録可能なオーナー登録可能モードへと切り替わることと、

前記オーナー端末が、前記車両用装置が前記オーナー登録可能モードであることを条件として、前記近距離無線通信にて前記車両用装置に前記オーナー鍵を送信することと、

前記車両用装置が、前記オーナー登録可能モードであることを条件として、前記オーナー端末から前記オーナー鍵を受信し、所定の不揮発性の車両側記憶装置（４５）に保存することと、

前記サーバが、前記サービス鍵の発行に伴い、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を生成し、前記携帯端末に配信することと、

前記携帯端末が、前記ワンタイム認証鍵を用いて前記車両用装置に対して通信相手としての正当性を証明することと、

前記携帯端末が、前記ワンタイム認証鍵の残数が所定値以下となっていることに基づいて前記サーバに対して前記ワンタイム認証鍵の補充を要求する補充要求信号を送信することと、

前記サーバが、前記補充要求信号の受信に基づいて新たに複数の前記ワンタイム認証鍵を生成し前記携帯端末に送信することと、を含む車両用デジタルキー管理方法。

【請求項１０】

ユーザによって携帯される情報処理端末である携帯端末（１）と、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信にてデータ通信可能に構成されている車両用装置であって、

少なくとも１つのプロセッサ（４１）を用いてなる車両制御部（４０）を備え、

前記車両制御部は、

動作モードとして、オーナーとしての権限を有する鍵情報であるオーナー鍵の登録を拒否するオーナー登録禁止モードと、前記オーナー鍵を登録可能なオーナー登録可能モードと、を備え、

所定の専用デバイス又はサーバから特定の登録開始信号が入力されたことに基づいて前記オーナー登録禁止モードから前記オーナー登録可能モードへ切り替わるように構成されており、

10

20

30

40

50

前記オーナ登録可能モードである場合には、前記オーナが所持する前記携帯端末であるオーナ端末から、前記近距離無線通信によって前記オーナ鍵を取得するための通信シーケンスを開始し、

前記オーナ登録禁止モードで動作している場合には、前記オーナ端末又は前記サーバから前記オーナ鍵を取得するための通信そのもの、又は、受信した前記オーナ鍵を所定の車両側記憶装置に保存する処理を実行しない一方、ゲスト端末又は前記サーバからゲスト鍵を受信するための通信は実施可能に構成されており、

前記ゲスト鍵を受信した場合に、当該ゲスト鍵を前記車両側記憶装置に保存するように構成されている車両用装置。

【請求項 1 1】

ユーザの操作を受け付ける入力装置（1 2）と、

所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施するための近距離通信部（1 6）と、

インターネットにアクセスするためのネット接続部（1 7、1 8）と、

少なくとも1つのプロセッサを用いてなる端末制御部（1 0）と、を備える携帯端末であって、

前記端末制御部は、

前記ユーザの操作に基づいて、車両を使用するためのサービス鍵を生成するサーバ（3）に向けて、当該ユーザが所有する前記車両についての前記サービス鍵であって、オーナとしての権限を有するオーナ鍵を発行するように要求する、オーナ鍵発行要求信号を送信することと、

前記オーナ鍵発行要求信号に対する前記サーバの応答として、前記サーバから前記オーナ鍵を受信することと、

受信した前記オーナ鍵を所定の端末側記憶装置（1 0 5）に保存することと、

前記車両に搭載されている車両用装置（4）と前記近距離無線通信の通信リンクが確立していることを条件として、前記オーナ鍵を前記車両用装置に登録するための通信を開始することと、

前記サーバから、前記サービス鍵とともに、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を受信することと、

前記ワンタイム認証鍵を用いて前記車両用装置に対して通信相手としての正当性を証明することと、

前記ワンタイム認証鍵の残数が所定値以下となっていることに基づいて前記サーバに対して前記ワンタイム認証鍵の補充を要求する補充要求信号を送信することにより、前記サーバから、新しい複数の前記ワンタイム認証鍵を受信することと、を実行するように構成されている携帯端末。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本開示は、車両を施錠／開錠するための鍵情報であるデジタルキーを生成及び配信する技術に関する。

【背景技術】

【0 0 0 2】

特許文献 1－2 には、車両の管理者から発行される鍵情報を、ユーザによって携帯されるデバイスである携帯端末及び車載器のそれぞれに配信することにより、当該携帯端末を車両の電子キーとして使用可能とするシステムが開示されている。携帯端末としては例えばスマートフォンなどのインターネット接続可能な通信端末が想定される。このようにスマートフォンなどの携帯端末を車両キーとして使用することができれば、ユーザは車両使用の際に専用の電子キーを所持する必要がなくなり、利便性がよくなる。なお、特許文献 1－2 には、車両のオーナーと、その他の人物（ゲスト）とで、車両の使用権限を異ならせる構成についても言及されている。

10

20

30

40

50

【0003】

なお、車両に接続するデバイスの正当性を検証する方法としては多様な方法が存在する。例えば特許文献3には、動的に変更されるパラメータである変動符号と固定的な鍵情報とを組み合わせることで生成される認証コードを用いて、車両に接続するデバイスを認証する方法が開示されている。これら先行技術文献の記載内容は、この明細書における技術的要素の説明として、参照により援用することができる。

【先行技術文献】

【特許文献】

【0004】

【文献】特許第6635102号公報

10

【文献】特表2019-536329号公報

【文献】特許第6078686号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

一般的にオーナは車両の使用に関する全ての権限を有しうる。よって、オーナ用の鍵情報の車両への登録に際しては、セキュリティ向上の観点から、その他のユーザであるゲスト用の鍵情報の登録方法とは異なる方法／規則にて実施されることが好ましい。

【0006】

特許文献1-3にはオーナ用の鍵情報を車載器に登録する際の具体的な手順等については何ら検討されていない。

20

【0007】

本開示は、上記の検討又は着眼点に基づいて成されたものであり、その目的の1つは、よりセキュリティを向上可能な車両用デジタルキーシステム、車両用デジタルキー管理方法、携帯端末、車両用装置を提供することにある。

【課題を解決するための手段】

【0008】

ここに開示される第1の車両用デジタルキーシステムは、車両に搭載されて使用される車両用装置(4)と、携帯可能な情報処理端末である少なくとも1つの携帯端末(1)と、車両を使用するための鍵情報として、携帯端末ごとに固有のサービス鍵を生成し、携帯端末に配信するサーバ(3)と、を含む車両用デジタルキーシステムであって、サーバは、オーナと紐付けられた携帯端末であるオーナ端末から送信されるゲスト鍵発行要求信号に基づき、オーナ端末以外の携帯端末であるゲスト端末のためのサービス鍵であるゲスト鍵を発行することと、発行したゲスト鍵をゲスト端末に配信することと、を実施するように構成されており、車両用装置は、動作モードとして、車両のオーナとしての権限を有するサービス鍵であるオーナ鍵を登録可能なオーナ登録可能モードと、オーナ鍵の登録を拒否するオーナ登録禁止モードと、を備え、携帯端末又はサーバと通信することにより、サービス鍵を取得し、所定の車両側記憶装置(45)に保存し、所定の専用デバイス又はサーバから、特定のオーナ登録開始信号が入力されたことに基づいてオーナ登録禁止モードからオーナ登録可能モードに移行し、オーナ登録可能モードで動作している場合には、オーナ端末又はサーバから、車両のオーナとしての権限を有するサービス鍵であるオーナ鍵を取得するための通信を実行する一方、オーナ登録禁止モードで動作している場合には、オーナ端末又はサーバからオーナ鍵を取得するための通信そのもの、又は、受信したオーナ鍵を車両側記憶装置に保存する処理を実行せず、ゲスト鍵に関しては、オーナ登録禁止モードにおいても、ゲスト端末又はサーバからゲスト鍵を受信するためのシーケンスを実施可能に構成されており、ゲスト端末又はサーバからゲスト鍵を受信した場合には当該ゲスト鍵を車両側記憶装置に保存するように構成されている。

30

40

本開示に含まれる第2の車両用デジタルキーシステムは、車両に搭載されて使用される車両用装置(4)と、携帯可能な情報処理端末である少なくとも1つの携帯端末(1)と、車両を使用するための鍵情報として、携帯端末ごとに固有のサービス鍵を生成し、携帯

50

端末に配信するサーバ（３）と、を含む車両用デジタルキーシステムであって、車両用装置は、携帯端末又はサーバと通信することにより、サービス鍵を取得し、所定の車両側記憶装置（４５）に保存するように構成にされており、車両用装置は、所定の専用デバイス又はサーバから、特定のオーナー登録開始信号が入力されたことを条件として、車両のオーナーとしての権限を有するサービス鍵であるオーナー鍵を、車両側記憶装置へ保存するように構成されており、サーバは、サービス鍵の発行に伴い、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を生成し、携帯端末に配信するように構成されており、携帯端末は、ワンタイム認証鍵を用いて車両用装置に対して通信相手としての正当性を証明するように構成されており、携帯端末は、ワンタイム認証鍵の残数が所定値以下となっていることに基づいてサーバに対してワンタイム認証鍵の補充を要求する補充要求信号を送信し、サーバは、補充要求信号の受信に基づいて新たに複数のワンタイム認証鍵を生成し携帯端末に送信するように構成されている。

10

【０００９】

上記の車両用デジタルキーシステムによれば、特定のオーナー登録開始信号が入力された場合にしか、オーナー鍵のデータが車両に登録されない。よって、比較構成として想定される、オーナー鍵を常時登録可能な構成よりもセキュリティを高めることができる。

【００１０】

また、本開示に含まれる第１の車両用デジタルキー管理方法は、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能であって、かつ、携帯可能に構成された情報処理端末である少なくとも１つの携帯端末（１）と、車両に搭載されて使用される、近距離無線通信を実施可能に構成されている車両用装置（４）と、携帯端末からの要求に基づき車両を使用するための鍵情報であるサービス鍵を生成するサーバ（３）と、とによって実施される車両用デジタルキー管理方法であって、サーバが、車両のオーナーが所持する携帯端末としてユーザデータベースに登録されているオーナー端末からの要求に基づき、オーナーとしての権限を有するサービス鍵であるオーナー鍵を発行することと、サーバが、発行されたオーナー鍵を車両用装置には送信せずに、オーナー端末には配信することと、サーバが、オーナー端末から送信されるゲスト鍵発行要求信号に基づき、オーナー端末以外の携帯端末であるゲスト端末のためのサービス鍵であるゲスト鍵を発行することと、サーバが、発行したゲスト鍵をゲスト端末に配信することと、車両用装置が、所定の専用デバイス又はサーバから、所定の登録開始信号が入力されたことに基づいて、オーナー鍵の登録を拒否するオーナー登録禁止モードからオーナー鍵を登録可能なオーナー登録可能モードへと切り替わることと、オーナー端末が、車両用装置がオーナー登録可能モードであることを条件として、近距離無線通信にて車両用装置にオーナー鍵を送信することと、車両用装置が、オーナー登録可能モードであることを条件として、オーナー端末からオーナー鍵を受信し、所定の不揮発性の車両側記憶装置（４５）に保存することと、車両用装置は、オーナー登録禁止モードで動作している場合、車両用装置は、オーナー端末又はサーバからオーナー鍵を取得するための通信そのもの、又は、受信したオーナー鍵を車両側記憶装置に保存する処理を実行しない一方、オーナー登録禁止モードにおいても、ゲスト端末又はサーバからゲスト鍵を受信するためのシーケンスは実施することと、車両用装置が、ゲスト端末又はサーバからゲスト鍵を受信した場合には当該ゲスト鍵を車両側記憶装置に保存することと、を含む。

20

30

40

本開示に含まれる第２の車両用デジタルキー管理方法は、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施可能であって、かつ、携帯可能に構成された情報処理端末である少なくとも１つの携帯端末（１）と、車両に搭載されて使用される、近距離無線通信を実施可能に構成されている車両用装置（４）と、携帯端末からの要求に基づき車両を使用するための鍵情報であるサービス鍵を生成するサーバ（３）と、とによって実施される車両用デジタルキー管理方法であって、サーバが、車両のオーナーが所持する携帯端末としてユーザデータベースに登録されているオーナー端末からの要求に基づき、オーナーとしての権限を有するサービス鍵であるオーナー鍵を発行することと、サーバが、発行されたオーナー鍵を車両用装置には送信せずに、オーナー端末には配信することと、車両用装置が、所定の専用デバイス又はサーバから、所定の登録開始信号が入力されたことに基

50

づいて、オーナ鍵の登録を拒否するオーナ登録禁止モードからオーナ鍵を登録可能なオーナ登録可能モードへと切り替わることと、オーナ端末が、車両用装置がオーナ登録可能モードであることを条件として、近距離無線通信にて車両用装置にオーナ鍵を送信することと、車両用装置が、オーナ登録可能モードであることを条件として、オーナ端末からオーナ鍵を受信し、所定の不揮発性の車両側記憶装置（４５）に保存することと、サーバが、サービス鍵の発行に伴い、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を生成し、携帯端末に配信することと、携帯端末が、ワンタイム認証鍵を用いて車両用装置に対して通信相手としての正当性を証明することと、携帯端末が、ワンタイム認証鍵の残数が所定値以下となっていることに基づいてサーバに対してワンタイム認証鍵の補充を要求する補充要求信号を送信することと、サーバが、補充要求信号の受信に基づいて新たに複数のワンタイム認証鍵を生成し携帯端末に送信することと、を含む。

10

【００１１】

上記の方法によれば、車両用デジタルキーシステムと同様の作用により、セキュリティを高めることができる。

【００１２】

本開示の車両用装置は、ユーザによって携帯される情報処理端末である携帯端末（１）と、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信にてデータ通信可能に構成されている車両用装置であって、少なくとも１つのプロセッサ（４１）を用いてなる車両制御部（４０）を備え、車両制御部は、動作モードとして、オーナとしての権限を有する鍵情報であるオーナ鍵の登録を拒否するオーナ登録禁止モードと、オーナ鍵を登録可能なオーナ登録可能モードと、を備え、所定の専用デバイス又はサーバから特定の登録開始信号が入力されたことに基づいてオーナ登録禁止モードからオーナ登録可能モードへ切り替わるように構成されており、オーナ登録可能モードである場合には、オーナが所持する携帯端末であるオーナ端末から、近距離無線通信によってオーナ鍵を取得するための通信シーケンスを開始し、オーナ登録禁止モードで動作している場合には、オーナ端末又はサーバからオーナ鍵を取得するための通信そのもの、又は、受信したオーナ鍵を所定の車両側記憶装置に保存する処理を実行しない一方、ゲスト端末又はサーバからゲスト鍵を受信するための通信は実施可能に構成されており、ゲスト鍵を受信した場合に、当該ゲスト鍵を車両側記憶装置に保存するように構成されている。

20

【００１３】

上記の車両用装置によれば、車両用デジタルキーシステムと同様の作用により、セキュリティを高めることができる。

30

【００１４】

本開示の携帯端末は、ユーザの操作を受け付ける入力装置（１２）と、所定の近距離無線通信規格に準拠した無線通信である近距離無線通信を実施するための近距離通信部（１６）と、インターネットにアクセスするためのネット接続部（１７、１８）と、少なくとも１つのプロセッサを用いてなる端末制御部（１０）と、を備える携帯端末であって、端末制御部は、ユーザの操作に基づいて、車両を使用するためのサービス鍵を生成するサーバ（３）に向けて、当該ユーザが所有する車両についてのサービス鍵であって、オーナとしての権限を有するオーナ鍵を発行するように要求する、オーナ鍵発行要求信号を送信することと、オーナ鍵発行要求信号に対するサーバの応答として、サーバからオーナ鍵を受信することと、受信したオーナ鍵を所定の端末側記憶装置（１０５）に保存することと、車両に搭載されている車両用装置（４）と近距離無線通信の通信リンクが確立していることを条件として、オーナ鍵を車両用装置に登録するための通信を開始することと、サーバから、サービス鍵とともに、当該サービス鍵に基づいて複数の使い捨てのワンタイム認証鍵を受信することと、ワンタイム認証鍵を用いて車両用装置に対して通信相手としての正当性を証明することと、ワンタイム認証鍵の残数が所定値以下となっていることに基づいてサーバに対してワンタイム認証鍵の補充を要求する補充要求信号を送信することにより、サーバから、新しい複数のワンタイム認証鍵を受信することと、を実行するように構成されている。

40

50

【0015】

上記の携帯端末によれば、オーナーが所持する携帯端末が車両用装置と近距離無線通信リンクが確立していない場合には、オーナー鍵が車両には登録されない。必然的に車両周辺にオーナーが存在する場合にしかオーナー鍵が車両に登録されないため、セキュリティを高めることができる。

【0016】

なお、特許請求の範囲に記載した括弧内の符号は、一つの態様として後述する実施形態に記載の具体的手段との対応関係を示すものであって、本開示の技術的範囲を限定するものではない。

【図面の簡単な説明】

【0017】

【図1】車両用デジタルキーシステムの全体像を示す図である。

【図2】携帯端末の構成を示すブロック図である。

【図3】端末制御部の機能ブロック図である。

【図4】専用キーの構成を示すブロック図である。

【図5】デジタルキーサーバの構成を示すブロック図である。

【図6】車両データベースに格納されるデータの種類の一例を示す図である。

【図7】ユーザデータベースに格納されるデータの種類の一例を示す図である。

【図8】データ処理部の機能ブロック図である。

【図9】車両とオーナー鍵とゲスト鍵の関係を説明するための図である。

【図10】車載システムの構成を示すブロック図である。

【図11】認証ECUの機能ブロック図である。

【図12】サービス鍵の発行及び登録にかかる処理の全体像を説明するための図である。

【図13】オーナー鍵の発行処理を説明するためのシーケンス図である。

【図14】オーナー鍵を車両に登録する処理を説明するためのシーケンス図である。

【図15】オーナー鍵を車両へ登録するための携帯端末の表示画面の一例を示す図である。

【図16】車両との通信接続にかかる携帯端末の表示画面の一例である。

【図17】ゲスト鍵の発行処理を説明するためのシーケンス図である。

【図18】ゲスト鍵発行要求信号に含まれるべき情報の一例を示す図である。

【図19】ゲスト端末に向けて送信される端末登録用パッケージに含まれるべき情報の一例を示す図である。

【図20】ゲスト鍵を車両に登録する処理を説明するためのシーケンス図である。

【図21】ゲスト鍵を車両に登録するための携帯端末の表示画面の一例を示す図である。

【図22】駐車中における認証ECUの作動例を説明するためのフローチャートである。

【図23】認証ECUが携帯端末を認証する処理の一例を示すシーケンス図である。

【図24】認証ECUが携帯端末を認証する処理の他の例を示すシーケンス図である。

【図25】携帯端末がワンタイム認証鍵を補充する処理のシーケンス図である。

【図26】携帯端末が鍵情報記憶部に保管されているワンタイム認証鍵を入れ替える処理のシーケンス図である。

【図27】認証ECUが実施する、ECU時刻の修正及び有効期限に基づくゲスト鍵の削除を説明するためのシーケンス図である。

【図28】サービス鍵の削除にかかるシーケンスの全体像を説明するための図である。

【図29】オーナー鍵を削除する際の携帯端末とDKSとのインタラクションを示すシーケンス図である。

【図30】オーナー鍵を削除する際のオーナー端末と認証ECUとのインタラクションを示すシーケンス図である。

【図31】ゲスト鍵を削除する際の携帯端末とDKSとのインタラクションを示すシーケンス図である。

【図32】ゲスト鍵を削除する際の携帯端末と認証ECUとのインタラクションを示すシーケンス図である。

10

20

30

40

50

【図 3 3】車載 H M I を介してサービス鍵を削除する場合の一連の処理の流れを示すシーケンス図である。

【図 3 4】発行件つきゲスト鍵が削除された場合の D K S の作動例を説明するための図である。

【図 3 5】オーナーが所持する携帯端末が機種変更された場合の D K S の作動を説明するためのフローチャートである。

【発明を実施するための形態】

【0018】

以下、本開示の車両用デジタルキーシステム S y s について図を用いて説明する。車両用デジタルキーシステム S y s は、車両 H v を利用するための電子的な鍵であるサービス鍵を携帯端末 1 に配布することにより、ユーザが専用キー 2 を持たずとも車両 H v へのアクセスを可能とするためのシステムである。車両用デジタルキーシステム S y s は、図 1 に示すように、携帯端末 1、専用キー 2、デジタルキーサーバ (D K S : Digital Key Server) 3、及び、車両 H v に搭載された車載システム 7 を含む。車載システム 7 は、認証 E C U 4 を含む。E C U は Electronic Control Unit の略であって、電子制御装置を指す。

【0019】

<前置き>

以下の説明における車両 H v は、一例として個人によって所有される車両である。もちろん、車両 H v は会社組織が保有する社用車や、公的機関が保有する公用車であってもよい。さらに、車両 H v は、貸出サービスに供される車両（いわゆるレンタカー）であってもよいし、カーシェアリングサービスに供される車両（いわゆるシェアカー）であってもよい。車両 H v は、ロボットタクシーなど、旅客輸送サービスに供される車両でもよい。

【0020】

車両 H v は例えばエンジン車である。もちろん、車両 H v は、ハイブリッド車や、電気自動車であってもよい。ここでのエンジン車は動力源としてエンジンのみを備える車両を指し、ハイブリッド車は動力源としてエンジンとモータを備える車両を指す。電気自動車は、モータのみを駆動源として備える車両を指す。本開示における走行用電源とは、車両 H v が走行するための電源であって、車両がエンジン車である場合にはイグニッション電源を指す。車両 H v が電気自動車やハイブリッド車である場合、システムメインリレーが走行用電源に相当する。本開示は四輪自動車に限らず、トレーラや、二輪自動車、三輪自動車等、道路上を走行可能な多様な車両に搭載可能である。原動機付き自転車も二輪自動車に含めることができる。

【0021】

以下では、主として 1 つの車両 H v を対象に車両用デジタルキーシステム S y s の説明を行うが、D K S 3 が管理する車両は複数存在しうる。また、1 人のオーナーが保持する車両 H v は複数存在してもよい。

【0022】

本開示のユーザとは、車両用デジタルキーシステム S y s が提供するサービスの利用者を指す。車両用デジタルキーシステム S y s が提供するサービスを利用するためのアカウントを作成済みの人物、換言すれば、後述するデジタルキーアプリ 104 をインストール済みの携帯端末 1 の所有者がユーザに相当する。

【0023】

本開示の種々のシーケンス図及びフローチャートは何れも一例である。各シーケンス図／フローチャートが備えるステップ数や処理順序、実行条件等は適宜変更可能である。

【0024】

<全体像の概略>

携帯端末 1 は、複数のユーザのそれぞれによって所持／携帯されうる汎用的な情報処理端末である。図 1 に示す携帯端末 1 a は車両 H v のオーナーが所持する携帯端末 1 を示している。携帯端末 1 b は例えばオーナーの家族が所有する携帯端末 1 であり、携帯端末 1 c はオーナーの友人が所持する携帯端末 1 である。携帯端末 1 には、端末毎に固有の識別情報で

10

20

30

40

50

あるデバイスIDが割り当てられている。

【0025】

デバイスIDとしては例えばデバイスアドレスや、UUID (Universally Unique Identifier) などを採用可能である。なお、Bluetooth (登録商標) におけるデバイスアドレスは、48ビットで表現されうる。また、UUIDは128ビットで表現されうる。デバイスアドレスは、固定的なパブリックアドレスであってもよいしランダムアドレスであってもよい。パブリックアドレスはEthernet (登録商標) におけるMAC (Media Access Control) アドレスに相当する。その他、デバイスIDは、後述するデジタルキーアプリ104のインストール時に決定される乱数であってもよい。

【0026】

携帯端末1は、無線基地局8及び広域通信ネットワーク9を介してDKS3とデータ通信可能に構成されている。図1に示す無線基地局8は、例えばセルラー通信の基地局であっても良いし、Wi-Fi (登録商標) 用のアクセスポイントであってもよい。アクセスポイントは、無線LAN (Local Area Network) を形成する通信設備である。アクセスポイントの概念にはルーターの他、路側機も含めることができる。広域通信ネットワーク9は、例えばインターネットである。広域通信ネットワーク9を形成する設備にとって、携帯端末1はユーザ装置 (UE: User Equipment) に相当する。

【0027】

セルラー通信とは、例えば4Gや5Gといった規格に準拠した無線通信を指す。Wi-Fiの規格としては、IEEE 802.11nやIEEE 802.11ac、IEEE 802.11ax (いわゆるWi-Fi 6) など、多様な規格を採用可能である。本開示ではWi-Fi (登録商標) 規格に準拠した無線通信をWi-Fi通信とも記載する。携帯端末1とDKS3との通信は、暗号化されたセルラー通信又はWi-Fi通信で実施される。

【0028】

DKS3は、車両Hvの外部に配置されたサーバである。DKS3は、広域通信ネットワーク9に接続可能に構成されている。DKS3は、広域通信ネットワーク9を介して携帯端末1と相互通信を行いうる。DKS3は、携帯端末1からの要求に基づき、所定のユーザに対して車両Hvを使用するためのサービス鍵を発行する。

【0029】

また、車載システム7と携帯端末1は、近距離無線通信を実施可能に構成されている。ここでの近距離無線通信とは、実質的な通信可能距離が例えば5mから30m、最大でも100m程度となる所定の近距離無線通信規格に準拠した通信を指す。近距離無線通信の規格としては、例えばBLE (Bluetooth Low Energy) や、Bluetooth Classic、Wi-Fi (登録商標)、ZigBee (登録商標) 等を採用することができる。近距離無線通信の方式としては、UWB-IR (Ultra Wide Band - Impulse Radio) も採用可能である。本実施形態では一例として車載システム7と携帯端末1は、BLE規格に準拠した無線通信であるBLE通信を実施可能に構成されている場合を例にとって各部の作動を説明する。以下におけるBLE通信との記載は、近距離無線通信と置き換えて実施することができる。通信接続及び暗号通信などにかかる通信方法の細部はBLE規格で規定されるシーケンスによって実施される。

【0030】

なお、以下では車載システム7が携帯端末1との通信におけるマスターとして振る舞うように設定されている場合について説明する。携帯端末1は、スレーブとして振る舞う。BLE通信におけるスレーブは、間欠的にアドバタイズ信号を送信するとともに、マスターからの要求に基づいてデータの送受信を実行するデバイスである。スレーブは、ペリフェラルとも称される。マスターは、スレーブとの通信接続状態や通信タイミングを制御する。マスターは、セントラルとも称される。他の態様として、携帯端末1が車載システム7との通信におけるマスターとして動作するように設定されていても良い。

【0031】

10

20

30

40

50

車載システム 7 は、B L E 通信を行うための B L E 通信部 5 7 と認証 E C U 4 とを含む。認証 E C U 4 は、車載システム 7 を構成する E C U の 1 つである。認証 E C U 4 が車両用装置に相当する。認証 E C U 4 は、サービス鍵を有する携帯端末 1 と無線通信による自動的な認証処理を行う。そして、認証が成功していることを条件として、車両 H v に対するユーザの位置に応じた車両制御を実施するパッシブエントリパッシブスタート機能を提供する。ここでの車両制御とは、ドアの施錠／開錠、電源オン／オフ、エンジン始動などである。なお、携帯端末 1 はユーザに対応するものであるため、携帯端末 1 を認証することは、ユーザを認証することに相当する。

【 0 0 3 2 】

＜サービス鍵の説明＞

サービス鍵は、携帯端末 1 毎に相違する。例えばサービス鍵は、デバイス I D に応じて定まる、携帯端末 1 ごとに異なるコードである。サービス鍵は、所定の文字数を備える英数字の羅列とする事ができる。例えば D K S 3 は、デバイス I D に所定の長さを有する乱数を加えた値を、所定のハッシュ関数に入力して得られる出力値をサービス鍵として採用する。ハッシュ関数としては、F N V 1 3 2 や、F N V 1 6 4、M D - 5、S H A - 1、S H A - 2 5 6、S H A - 5 1 2 など多様な関数を採用可能である。サービス鍵の生成に使用する関数は、サービス鍵として必要とされるビット数（出力長）に合わせて適宜選択されうる。

【 0 0 3 3 】

サービス鍵は 8 ビット以上の長さを有するビット列で表現されうる。サービス鍵は長いほどそのセキュリティ性が強固となり好適である。サービス鍵は例えば 1 6 バイト、2 4 バイト、2 7 バイトなどで表現されうる。ここでは一例として、サービス鍵は、2 4 バイトで構成されるものとする。サービス鍵を 2 7 バイト以下とする構成によればサービス鍵を 1 つの B L E 暗号通信パケットに収容可能となる。

【 0 0 3 4 】

なお、サービス鍵は、車両 H v と携帯端末 1 の組み合わせ毎に異なる値とすることが好ましい。例えば車両 I D とデバイス I D を結合した値を入力値とする所定のハッシュ関数の出力値をサービス鍵としてもよい。車両 I D は車両ごとに割り当てられる固有の識別番号である。車両 I D としては例えば車両識別コード（V I N : Vehicle Identification Number）などを採用可能である。

【 0 0 3 5 】

さらにサービス鍵は、車両 I D とデバイス I D にさらに、発行要求を受け付けたエポック秒に対応する値を連結したデータを所定のハッシュ関数に入力して得られる出力値であってもよい。また、必ずしもサービス鍵の生成にハッシュ関数を使用する必要はない。サービス鍵は、デバイス I D に車両 I D を乗算、加算、又は連結して得られる値であってもよい。サービス鍵の材料としては、その他、ユーザが設定したパスワードなども採用可能である。例えばサービス鍵は、ユーザが登録した所定文字数のパスワードを所定のハッシュ関数に入れた値であっても良い。

【 0 0 3 6 】

サービス鍵には、複数の種類が存在する。サービス鍵の種類としては大きくはオーナー鍵とゲスト鍵がある。オーナー鍵は、車両 H v のオーナーに対して発行されるサービス鍵であって、概ね車両 H v の使用に関する全ての権限を有する。オーナー鍵は、走行用電源のオンオフやドアの施開錠、遠隔操作など、車両 H v の使用にかかる全ての権限を有するとともに、他のユーザのためのサービス鍵を発行する権限を有する。また、オーナー鍵は基本的に有効期限が設定されていない、無期限のサービス鍵である。

【 0 0 3 7 】

ゲスト鍵はゲストのためのサービス鍵であって、基本的にはオーナーによって発行される。ここでのゲストとはオーナー以外のユーザを指す。ゲスト鍵は、オーナー鍵よりも権限が制限されたサービス鍵であって、有効期限も設定される。

【 0 0 3 8 】

10

20

30

40

50

ゲスト鍵は、より細かくは、他のゲスト鍵を発行する権限を有する発行権付きゲスト鍵と、他のゲスト鍵の発行権限を有さない発行権なしゲスト鍵に区分される。ユースケースの一例として、オーナーの家族に対しては、オーナーからの要求に基づき発行権付きゲスト鍵が発行されうる。また、オーナーの友人／知人などに対しては発行権なしゲスト鍵が発行されうる。

【0039】

以降ではオーナーが所持する携帯端末1、換言すればオーナー鍵が保存されている携帯端末1をオーナー端末と称する。ゲストが所持する携帯端末1、換言すればゲスト鍵が保存されている携帯端末1をゲスト端末と称する。また、ゲスト端末のうち、発行権付きゲスト鍵が付与されている携帯端末1のことを発行権付きゲスト端末と称し、発行権なしゲスト鍵が付与されている携帯端末1のことを発行権なしゲスト端末と称する。図1に示す例においては携帯端末1aがオーナー端末に相当し、携帯端末1bが発行権付きゲスト端末に相当する。また、携帯端末1cが発行権なしゲスト端末に相当する。

【0040】

オーナー端末を親とすると、オーナー端末が発行したゲスト鍵を有する携帯端末1は、オーナー端末にとっての子に相当する。また発行権付き端末が発行したゲスト鍵を有する携帯端末1はオーナー端末にとっての孫に相当する。各ゲスト鍵の権限は、発行元によって決定される。ゲスト鍵の権限は、発行元よりも小さく（狭く）設定される。ただし、車両用デジタルキーシステムS y sは他の態様として、発行元と同等の権限を有するゲスト鍵を発行可能に構成されていても良い。DKS3は、オーナー端末又は発行権付きゲスト端末からの要求に基づき、ゲスト鍵を新規発行する。新規発行されたサービス鍵のタイプや権限設定は、発行元によって指定される。例えばDKS3は、オーナー端末からの要求に基づきゲスト鍵を新規発行する際、当該ゲスト鍵を発行権付きゲスト鍵とするか発行権なしゲスト鍵とするかは、オーナー端末から受信した信号に基づいて決定する。なお、発行権付きゲスト鍵は、発行権なしゲスト鍵しか発行できないように制限される。

【0041】

<携帯端末の構成及び機能について>

ここではまず携帯端末1が備える構成／機能について図2を用いて説明する。携帯端末1としては、例えば、スマートフォンや、タブレット端末、ウェアラブルデバイスなどを採用することができる。ウェアラブルデバイスは、ユーザの身体に装着されて使用されるデバイスであって、リストバンド型、腕時計型、指輪型、メガネ型、イヤホン型など、多様な形状のものを採用可能である。

【0042】

携帯端末1は、端末制御部10、ディスプレイ11、タッチパネル12、慣性センサ13、生体認証装置14、近接場通信部15、BLE通信部16、セルラー通信部17、及びWi-Fi通信部18を備える。

【0043】

端末制御部10は、携帯端末1全体の動作を制御するモジュールである。端末制御部10は、例えば端末プロセッサ101、RAM(Random Access Memory)102、ストレージ103等を備えた、コンピュータとして構成されている。端末プロセッサ101はRAM102と結合された演算処理のためのハードウェア（換言すれば演算コア）である。端末プロセッサ101は、例えばCPU(Central Processing Unit)である。端末プロセッサ101は、ユーザが使用するデバイスで使用されるプロセッサであるため、ユーザプロセッサあるいはUEプロセッサと呼ぶことができる。端末プロセッサ101は、RAM102へのアクセスにより、後述する各機能部の機能を実現するための種々の処理を実行する。RAM102は揮発性の記憶媒体である。ストレージ103は、フラッシュメモリ等の不揮発性の記憶媒体を含む構成である。

【0044】

デジタルキーアプリ104は、ユーザの認証や、サービス鍵の取得／保存、車載システム7との通信等をセキュアに行うためのアプリケーションソフトウェアである。デジタル

10

20

30

40

50

キーアプリ 104 は、例えばストレージ 103 などにインストールされている。

【0045】

端末制御部 10 は、ディスプレイ 11、タッチパネル 12、慣性センサ 13、生体認証装置 14、近接場通信部 15、BLE 通信部 16、セルラー通信部 17、及び Wi-Fi 通信部 18 のそれぞれと相互通信可能に構成されている。端末制御部 10 が備える機能については後述する。

【0046】

ディスプレイ 11 は、例えば液晶ディスプレイや有機 EL ディスプレイである。ディスプレイ 11 は端末制御部 10 からの入力信号に応じた画像を表示する。タッチパネル 12 は、静電容量式のタッチパネルであって、ディスプレイ 11 に積層されている。タッチパネル 12 及びディスプレイ 11 は、ユーザが携帯端末 1 に鍵情報を登録したり、携帯端末 1 と車載システム 7 とをペアリングしたりするためのインターフェースに相当する。タッチパネル 12 は入力装置である。タッチパネル 12 が出力する信号は、携帯端末 1 に対するユーザの操作に対応する。以降では、タッチパネル 12 の出力信号を操作信号とも記載する。

【0047】

慣性センサ 13 は、携帯端末 1 に作用する慣性力を検出するセンサである。加速度センサやジャイロセンサが慣性センサ 13 に相当する。慣性センサ 13 の出力（検出データ）は端末制御部 10 に入力される。

【0048】

生体認証装置 14 は、例えばユーザの指紋や、顔画像などを用いて、ユーザを認証する装置である。生体認証装置 14 は、手や指の静脈パターンや、虹彩パターンを用いてユーザを認証する装置であってもよい。また生体認証装置 14 は、例えば声紋など、発話音声の特徴を用いて認証を行う装置であってもよい。ユーザの認証結果は、端末制御部 10 に提供される。

【0049】

近接場通信部 15 は、NFC（Near Field Communication）の規格に従った無線通信である近接場通信を実施するための通信モジュールである。ここでの近接場通信とは、通信可能な距離が数 cm から数十 cm 程度となる通信を指す。近接場通信は、BLE 通信よりも通信可能な距離が十分に小さい通信方式に相当する。通信可能な距離が十分に小さい通信方式とは、通信距離が 10 分の 1 以下となる通信方式を指す。近接場通信を実現するための具体的な通信規格としては、例えば ISO/IEC 14443 や ISO/IEC 18092 等の多様な規格を採用することができる。近接場通信は、Type-F 規格に適合するものであっても良いし、Type-A 又は Type-B 規格に適合するものであってもよい。Type-F 規格は、いわゆる FeliCa（登録商標）に相当する。携帯端末 1 において近接場通信部 15 は任意の要素であって省略されても良い。

【0050】

BLE 通信部 16 は、BLE 通信を実施するための通信モジュールである。BLE 通信部 16、57 が近距離通信部に相当する。セルラー通信部 17 は、セルラー通信を実施するための通信モジュールである。セルラー通信部 17 は、例えば LTE 等の無線通信プロトコルにおけるデータリンクレイヤ及び物理レイヤを担当する通信モジュールである。セルラー通信部 17 は、無線基地局 8 との接続状況、例えば通信圏外か否かなどを示す情報を端末制御部 10 に提供する。

【0051】

Wi-Fi 通信部 18 は、Wi-Fi 通信を実施可能に構成されている。Wi-Fi 通信部 18 は、アクセスポイントを介して広域通信ネットワーク 9 に接続可能に構成されている。Wi-Fi は所定の無線 LAN 規格の一種である。故に、Wi-Fi 通信部 18 は、無線 LAN 規格に準拠した通信を実施するための通信モジュールである、無線 LAN モジュールに相当する。

【0052】

種々の通信モジュールは、送受信の対象とする周波数帯の電波を送受信可能なアンテナや、通信を制御するマイクロコンピュータである通信マイコン、変復調回路などを備える。なお、携帯端末1は、D K S 3との通信手段として、セルラー通信と、W i - F i 通信の少なくとも何れか一方を実施可能に構成されていればよい。携帯端末1は、セルラー通信部17とW i - F i 通信部18の両方を備えている必要はない。セルラー通信又はW i - F i 通信にて携帯端末1が広域通信ネットワーク9に接続された、いわゆるオンラインの状態にある場合、端末制御部10はD K S 3と種々のデータ通信を行う。データ通信は、例えば、T L S (Transport Layer Security) を用いた暗号通信によって実施される。セルラー通信部17及びW i - F i 通信部18がネット接続部に相当する。

【0053】

端末制御部10は、端末プロセッサ101がデジタルキーアプリ104を実行することで発現される機能部として図3に示すようにサービス鍵管理部F1、ワンタイム認証鍵管理部F2、及び車両応答部F3を備える。各種機能部は、デジタルキーアプリ104がユーザを認証している状態において有効となりうる。

【0054】

ユーザの認証（ログイン）は、デジタルキーアプリ104に対して所定のユーザIDとパスワードを入力することによって行われうる。ユーザの認証は、生体認証装置14を用いて実施されても良い。デジタルキーアプリ104は車両用デジタルキーシステムS y sの一部であるため、デジタルキーアプリ104にユーザがログインしている状態は、車両用デジタルキーシステムS y sにユーザがログインしている状態に対応する。なお、ログイン状態はログインから所定の有効期限が過ぎた場合に解除され、デジタルキーアプリ104はユーザの再認証が必要なログオフ状態に移移するものとする。

【0055】

また、端末制御部10は端末側記憶部105を備える。端末側記憶部105は、サービス鍵など、デジタルキーアプリ104が使用する種々のデータが格納される記憶領域である。端末側記憶部105は、ストレージ103又はR A M 102が備える記憶領域を用いて実現される。端末側記憶部105は、鍵情報記憶部M1と、車両用データ一時記憶部M2とを備える。鍵情報記憶部M1は、サービス鍵や後述するワンタイム認証鍵、ユーザIDなどを格納するための記憶領域である。車両用データ一時記憶部M2は、D K S 3から受信した車両H vへ転送するためのデータを一時的に保存するための記憶領域である。端末側記憶部105が端末側記憶装置に相当する。

【0056】

サービス鍵管理部F1は、D K S 3が発行した自端末のユーザ用のサービス鍵を管理する。本開示における自端末とは、端末制御部10から見て自身が設けられている携帯端末1を指す。サービス鍵管理部F1は、タッチパネル12から入力される操作信号に基づいて、自端末向けのサービス鍵の発行を要求したり、自端末用のサービス鍵を削除したりする。自端末向けのサービス鍵とは自端末のユーザのためのサービス鍵に相当する。

【0057】

サービス鍵管理部F1は、D K S 3から自端末向けのサービス鍵を取得し、鍵情報記憶部M1に保存する。サービス鍵管理部F1は、サービス鍵の取得時、サービス鍵そのものとともに、付加的な情報である鍵関連情報を取得する。鍵関連情報とは、例えば、サービス鍵IDや、有効期限、権限設定、タイプなどを指す。これらの情報は1つのデータセットとしてパッケージ化されて配信される。

【0058】

サービス鍵IDとは、サービス鍵を識別するための番号である。サービス鍵IDは、たとえばユーザ毎にユニークな値が設定される。サービス鍵IDは、アカウント作成時に生成された乱数であってもよい。仮にオーナーが携帯端末1の機種変更を行ってサービス鍵の値が変更されたとしても、オーナーに紐づくサービス鍵IDは変更されない。なお、サービス鍵IDは、車両IDとユーザIDの組み合わせに応じたユニークな値に設定されても良い。

10

20

30

40

50

【0059】

有効期限データは、無期限を示す所定値、又は、発行元が指定した期間／日付を示す。権限設定データは、自端末のユーザに許可されている機能（つまり権限）を示す。権限設定データは、例えばドアごとの施開錠の可否、走行用電源のオン／オフの可否などを示す。サービス鍵タイプはオーナー鍵かゲスト鍵かを示す。タイプ情報は権限設定データと統合されていても良い。

【0060】

サービス鍵管理部F1は、自端末向けのサービス鍵の取得の他、自端末用のサービス鍵に関するステータス確認画面を表示する処理や、自端末向けのサービス鍵を削除するための処理を実行する。ステータス確認画面は、自端末用のサービス鍵のステータスを示す画面である。サービス鍵のステータスには、有効期限や、権限設定、有効／無効状態などが含まれる。ステータス確認画面に、発行元に相当するユーザの名称等に関する情報を含みうる。

【0061】

なお、サービス鍵管理部F1が提供する機能は、自端末に割り当てられているサービス鍵のタイプ、換言すればサービス鍵の権限設定によって相違しうる。例えばオーナー端末のサービス鍵管理部F1は、ユーザが指定したゲスト用のゲスト鍵を発行するための処理や、ゲスト鍵を削除／一時的に無効化する処理を実行可能に構成されている。なお、オーナー端末に限っては、ゲスト鍵の発行時に、権限設定の一種として、ゲスト鍵を発行する権限の有無を指定可能に構成されている。また、オーナー端末のサービス鍵管理部F1は、車両Hvにかかるサービス鍵を保有するゲストのリストや、各ゲスト鍵のステータスを示す画面を表示する。オーナー端末は、例えばDKS3よりゲスト鍵の情報を取得して表示しうる。さらに、オーナー端末のサービス鍵管理部F1は、DKS3から取得する所定のデータセットを用いて、オーナー鍵に関する情報を車両Hvに登録する処理も実施可能に構成されている。

【0062】

また、発行権付き端末が備えるサービス鍵管理部F1は、ユーザが指定したゲストに対して発行権なしゲスト鍵を新規発行する処理を実行可能に構成されている。また、発行権付き端末が備えるサービス鍵管理部F1は、自分自身が発行したゲスト鍵のステータス確認や、当該ゲスト鍵の削除／無効化などを実行可能に構成されている。発行権なし端末のサービス鍵管理部F1は、ステータス確認や、自端末用のサービス鍵の削除／無効化が実施可能に構成されている。その他、ゲスト端末のサービス鍵管理部F1は、有効期限データに基づき、自端末用のサービス鍵の有効期限の確認を実施しうる。なお、ゲスト鍵の有効期限チェックはDKS3が実施してもよい

【0063】

ワンタイム認証鍵管理部F2は、DKS3から、車両Hvとの認証処理に使用するワンタイム認証鍵を取得し、鍵情報記憶部M1に保存する。ワンタイム認証鍵管理部F2そのものは、ワンタイム認証鍵を生成する機能を備えない。当該構成によればワンタイム認証鍵の生成方法の詳細を秘匿化することができる。ひいては車両用デジタルキーシステムSysのセキュリティ性能を高めることができる。

【0064】

ワンタイム認証鍵は、サービス鍵に、変動コード（変動因子）を組み合わせることによって得られるコードである。変動コードは、発行ごとに異なる値である。変動コードは、例えばエポック秒や、発行回数のカウント値、又は乱数とすることができる。さらに、変動コードは、所定の初期値から認証鍵の発行回数を減算した値であってもよい。仮にワンタイム認証鍵をKa、サービス鍵をSK、変動コードをCd、ワンタイム認証鍵の生成関数をGとすると、ワンタイム認証鍵は、 $Ka = G(SK, Cd)$ で表現されうる。この場合、生成関数Gは、サービス鍵と変動コードの2つの入力を取る関数である。生成関数Gは、1つの入力値をとる関数であっても良く、その場合には、例えば $Ka = G(SK + Cd)$ 等によってワンタイム認証鍵は生成されうる。SK + Cdは、サービス鍵と変動コー

ドを単純につなぎ合わせた（つまり連結させた）コードであってもよいし、それらに対応する数列を2進数又は16進数の概念で加算したものであってもよい。

【0065】

なお、ワンタイム認証鍵を生成するための第1因子をサービス鍵とすると、変動コードはワンタイム認証鍵を生成するための第2因子と呼ぶことができる。変動コードは、認証鍵生成因子の1つである。さらに、ワンタイム認証鍵は、サービス鍵と変動コードの他に、所定の第3の因子を用いて生成されても良い。例えばワンタイム認証鍵は、発行回数を示すカウント値と、ECU番号と、サービス鍵とを所定の順に結合してなるビット列を、所定の関数に入力することで生成されても良い。ワンタイム認証鍵は、1回使用されると破棄される、いわゆる使い捨ての認証鍵である。第3の因子は、認証ECU4に事前に登録される情報であることが好ましい。

10

【0066】

ワンタイム認証鍵管理部F2は、鍵情報記憶部M1に、所定数以上のワンタイム認証鍵が保存されている状態が維持されるよう、DKS3に対してワンタイム認証鍵の配信を要求する信号を随時送信する。例えばワンタイム認証鍵管理部F2は、鍵情報記憶部M1に保存されているワンタイム認証鍵の残数(Notk)が所定の補充閾値(ThRp)未満となったことに基づいて、補充要否フラグをオンに設定する。ワンタイム認証鍵管理部F2は、補充要否フラグがオンに設定されており、且つ、オンライン状態であることに基づいて、DKS3との通信により、複数のワンタイム認証鍵を取得する。補充閾値は例えば150や300とすることができる。補充要否フラグは任意の要素であって、省略されても良い。補充閾値ThRpは、200や、400、500であってもよい。

20

【0067】

なお、ワンタイム認証鍵には、発行日を起算とする有効期限が設定される。有効期限は例えば1ヶ月や3ヶ月、6ヶ月に設定されうる。ワンタイム認証鍵の有効期限もまたDKS3によって設定される。DKS3は、オーナーの指示操作に基づき、ワンタイム認証鍵に対する有効期限の長さを変更可能に構成されていても良い。仮に車両Hvがレンタカーである場合には、ワンタイム認証鍵の有効期限はレンタル期間に対応するように設定されうる。なお当該技術思想はゲスト鍵の有効期限設定にも同様に適用可能である。

【0068】

ワンタイム認証鍵管理部F2は、所定のタイミングで鍵情報記憶部M1に保存されているワンタイム認証鍵の有効期限をチェックし、有効期限切れとなっているワンタイム認証鍵については削除する。ワンタイム認証鍵の有効期限チェックはDKS3が実施してもよい。なお、期限切れのワンタイム認証鍵を削除した結果として、ワンタイム認証鍵の残数が補充閾値未満となった場合には、補充要否フラグをオンに設定するなど、DKS3からワンタイム認証鍵を取得するための処理を実施する。

30

【0069】

車両応答部F3は、認証ECU4とBLE通信のリンク(コネクション)が確立したことに基づいて、認証ECU4とBLEによるデータ通信を実行する構成である。例えば車両応答部F3は、認証ECU4とBLE通信リンクが確立したことに基づいて、ユーザ認証のための無線通信を実施する。車載システムユーザ間との認証処理は例えばチャレンジレスポンス方式によって実施されうる。その場合、車両応答部F3は、認証ECU4から送信されてきたチャレンジコードに対して、ワンタイム認証鍵を用いてレスポンスコードを生成し、認証ECU4に返送する。

40

【0070】

また、車両応答部F3は、認証ECU4からの要求に基づき、認証ECU4とDKS3との通信を中継する処理を行う。例えば車両応答部F3は、認証ECU4からBLE通信で受信した時刻要求信号を、セルラー通信のフォーマットに変換してDKS3に送信する。また、DKS3から受信した認証ECU4向けのデータ、例えばサーバ時刻情報などを、BLE通信のフォーマットに変換して認証ECU4に転送する。

【0071】

50

その他、携帯端末 1 は、近接場通信によって、車載システム 7 との認証処理を実行可能に構成されていても良い。携帯端末 1 は、近接場通信によって車載システム 7 と B L E 通信にかかるペアリングを実施するように構成されていても良い。また、端末制御部 1 0 は、デジタルキーアプリ 1 0 4 の機能として、車両 H v のステータスを確認する画面である車両状態確認画面を表示可能に構成されていてもよい。車両状態確認画面は、ガソリン／バッテリーの残量や、各窓及び各ドアの開閉状態、施錠状態、車内温度などを示す画面である。また、端末制御部 1 0 は、車両 H v が備える電装設備の一部を遠隔操作可能に構成されていても良い。例えば空調装置のオン／オフや、窓の開閉、ハザードランプの点灯／消灯などを遠隔操作可能に構成されていても良い。なお、車両状態確認や遠隔操作可能な内容は、サービス鍵の権限に応じて変更されても良い。

10

【 0 0 7 2 】

< 専用キーの構成及び機能について >

ここでは専用キー 2 の構成及び機能について図 4 を用いて説明する。専用キー 2 は、車両 H v を操作するための専用の電子キーである。専用キー 2 は、車両 H v の購入時に、車両 H v のオーナーであることの証、又は、実体を有するマスターキーとして、車両 H v とともにオーナーに提供される。専用キー 2 は、基本的にオーナーによって所持される。専用キー 2 は車両 H v の付属物の 1 つと解することができる。専用キー 2 は、扁平な直方体型や、扁平な楕円体型（いわゆるフォブタイプ）、カード型など、多様な形状を採用可能である。専用キー 2 は、車両用携帯機、キーフォブ、キーカード、カードキー、アクセスキーなどと呼ばれうる。

20

【 0 0 7 3 】

専用キー 2 には、車両 H v の鍵であることを証明する所定のコードである専用キーコードが登録されている。専用キーコードは、認証 E C U 4 にも登録されている。専用キー 2 は、認証 E C U 4 と所定の手順で通信することにより、車両 H v にアクセスしようとしている人物がオーナーであることを証明可能に構成されている。なお、専用キー 2 は任意の要素であって、省略されても良い。

【 0 0 7 4 】

専用キー 2 は、図 4 に示すように制御回路 2 0、及び近接場通信部 2 1 を備える。制御回路 2 0 は、専用キー 2 の動作を制御する回路である。制御回路 2 0 は、M C U (Micro Controller Unit) 2 0 1、R A M 2 0 2、フラッシュメモリ 2 0 3 などを用いて実現されている。制御回路 2 0 は M C U の代わりに、M P U (Micro-Processing Unit) や F P G A (Field-Programmable Gate Array) を用いて実現されていてもよい。フラッシュメモリ 2 0 3 には前述の専用キーコードが保存されている。

30

【 0 0 7 5 】

近接場通信部 2 1 は、近接場通信を実施するための通信モジュールである。専用キー 2 は、例えば車両 H v が備える近接場通信部 5 6 からの電波を電力に変換して機能するパッシブ型の無線タグとして構成されている。制御回路 2 0 は、車両 H v が備える近接場通信部 5 6 と近接場通信部 2 1 が通信接続している場合、認証 E C U 4 からの要求に基づき、専用キーコードそれ自体又は専用キーコードをもとに生成されるレスポンスコードを返送する。認証 E C U 4 は、専用キーコードを用いた認証処理が成功したことに基づいて、オーナー登録可能な状態に遷移しうる。このように専用キー 2 は、認証 E C U 4 をオーナー情報の登録が可能な状態に切り替えるためのデバイスとして機能しうる。

40

【 0 0 7 6 】

< D K S の構成及び機能について >

ここでは D K S 3 の構成及び機能について説明する。D K S 3 は図 5 に示すように、データ処理部 3 0、ネットワーク接続装置 3 1、車両 D B 3 2、及びユーザ D B 3 3 を備える。部材名称中の D B は、データベース (Database) の略である。

【 0 0 7 7 】

データ処理部 3 0 は、ネットワーク接続装置 3 1 から入力される信号／データに基づき多様な処理を実行する構成である。データ処理部 3 0 はネットワーク接続装置 3 1、車両

50

DB32、及びユーザDB33のそれぞれと相互通信可能に接続されている。データ処理部30は、サーバプロセッサ301、RAM302、ストレージ303を用いて構成されている。サーバプロセッサ301は、各種演算処理を実行する演算コアであって、例えばCPUやGPUなどを用いて実現されている。ストレージ303には、所定のデジタルキー管理プログラムが格納されている。サーバプロセッサ301が当該デジタルキー管理プログラムを実行することにより、後述する種々の機能部が実現される。なお、サーバプロセッサ301が当該デジタルキー管理プログラムを実行することは、当該プログラムに対応する方法である車両用デジタルキー管理方法が実行されることに対応する。

【0078】

ネットワーク接続装置31は、広域通信ネットワーク9に接続するための通信モジュールである。ネットワーク接続装置31は、例えば光ファイバなどを用いて広域通信ネットワーク9を構成する通信設備と相互通信可能に構成されている。これにより、携帯端末1がオンライン状態である場合、DKS3は携帯端末1とデータ通信可能となる。

【0079】

車両DB32は、車両用デジタルキーシステムSysが管理する車両についての情報が登録されるデータベースである。車両DB32には図6に示すように、車両ごとの車両IDが、車両モデル情報や、オーナー情報、ゲスト情報と対応付けられて保存されている。車両モデル情報は、対象車両の車種や、年式、グレード、OS (Operating System) などにかかる情報を含む。

【0080】

車両モデル情報は、認証ECU4で使用されるソフトウェアのバージョンや、ECU番号などを含んでも良い。ここでのECU番号は、複数の車両のそれぞれで使用される認証ECU4を区別するための番号であって、認証ECU4毎に相違する番号である。ECU番号としては認証ECU4の製造番号などを採用可能である。DKS3は、ECU番号を用いることで、仮に複数の車両Hvに同一モデルの認証ECU4が搭載されている場合であっても、特定の認証ECU4を対象としたデータ配信などを実行可能となる。

【0081】

オーナー情報は、車両Hvのオーナーについての情報であって、例えばユーザIDや、連絡先としての電話番号、メールアドレス、デバイスIDなどを含む。ゲスト情報は、車両Hvに関するサービス鍵が配布されているユーザ（つまりゲスト）についての情報である。例えば車両DB32には車両Hvについてのゲスト情報として、ゲスト毎のユーザIDなどが登録されている。なお、車両DB32は、ゲスト情報を備えていなくともよい。

【0082】

ユーザDB33は、ユーザについての情報が登録されるデータベースである。ユーザDB33には、ユーザ毎のユーザデータとして、図7に示すように、ユーザID、パスワード、デバイスID、鍵関連情報、備考情報などが保存される。ユーザIDとパスワードは、ユーザを認証するためのデータセットである。ユーザIDとパスワードは、例えばアカウント作成時にユーザによって登録される。サービス利用のためのアカウントは、専用のウェブページ又はデジタルキーアプリ104を介して作成可能である。ユーザが所持する携帯端末1のデバイスIDは、例えばDKS3がデジタルキーアプリ104と通信することで登録されうる。

【0083】

鍵関連情報は、例えば対象車両情報や、サービス鍵ID、サービス鍵、鍵属性、権限設定、オーナー鍵IDを含む。対象車両情報は、ユーザが使用可能な車両のIDを示す。車両毎のサービス鍵情報が車両DB32で管理される場合、ユーザDB33は鍵関連情報として対象車両情報を備えていなくとも良い。鍵タイプは、例えばオーナー鍵であるか、ゲスト鍵であるかなどを示す。鍵タイプは、対象車両に対するユーザの属性（オーナー／ゲスト）を示す情報と解することもできる。権限設定は前述の通り、施開錠可能なドアや、走行用電源のオン／オフが許可されているか否かなどを示す。オーナー鍵IDは、対象車両のオーナーのサービス鍵IDを示す。オーナー鍵IDがオーナー鍵番号に相当する。オーナーのユーザデ

10

20

30

40

50

ータにおけるオーナー鍵IDの欄は空白であってもよいし、当該オーナー自身のサービス鍵IDが登録されてもよい。

【0084】

備考欄は、年齢や、運転技能の習熟度などが登録されうる。運転技能の習熟度は初心者か否か、例えば運転免許を取得してから1年以内か否かなどが登録されうる。その他、備考欄には事故の履歴などが登録されていても良い。これらの備考情報は、仮にカーシェアリングサービスなどに適用した場合の利用料金や、保険料金などの算出材料として使用されうる。

【0085】

車両DB32及びユーザDB33は何れも書き換え可能な不揮発性の記憶媒体を用いて実現されている。また、車両DB32及びユーザDB33は何れもサーバプロセッサ301によるデータの書き込み、読出、削除等が実施可能に構成されている。なお、車両DB32とユーザDB33は統合されていても良い。上述したデータベースの構成は一例である。車両DB32及びユーザDB33は、上述した項目を全て保持している必要はない。また、車両DB32は、別のサーバが備えていても良い。そもそも、本開示のDKS3は、複数のサーバに分けて実施されても良い。サーバ毎の役割分担／機能配置は適宜変更可能である。

【0086】

データ処理部30は、機能部として図8に示すように、ユーザ管理部G1、ユーザ認証部G2、サービス鍵発行部G3、ワンタイム認証鍵発行部G4、サービス鍵削除部G5、及び機種変更受付部G6を備える。

【0087】

ユーザ管理部G1は、ユーザ情報を管理する構成である。例えばユーザ管理部G1は、ユーザの新規登録、削除、登録内容の変更をネットワーク接続装置31から入力されるデータに基づいて実施する。ユーザの新規登録／削除とはアカウントの発行／削除に対応する。新規登録、削除、登録内容の変更にかかるユーザ操作／指示は例えば携帯端末1及びネットワーク接続装置31を介して取得する。

【0088】

以降ではアカウントの作成や削除、登録内容の変更、サービス鍵の発行／削除／無効化等といった、車両用デジタルキーシステムSysに対するユーザの操作／指示に対応する信号のことを、簡略的に操作信号とも記載する。もちろん、ユーザの操作を直接的に受け付けるインターフェースは携帯端末1に限定されない。DKS3は、オフィスや家庭に設置されたコンピュータを介して上記操作信号を取得しうる。つまりDKS3は、デジタルキーアプリ104や専用のウェブページを介してユーザの操作信号を取得可能に構成されている。

【0089】

ユーザ認証部G2は、ユーザIDとパスワードとの組み合わせからユーザを認証する処理を実施する。ユーザ認証部G2が、認証成功と判定していることに基づいて、サービス鍵発行部G3やワンタイム認証鍵発行部G4、サービス鍵削除部G5、機種変更受付部G6などは、ユーザの操作信号又はデジタルキーアプリ104からの要求に応じた処理を実行する。

【0090】

サービス鍵発行部G3は、携帯端末1等に対するユーザ操作に基づき、サービス鍵を発行する。具体的には、オーナー端末や発行権付きゲスト端末から送信されてくるサービス鍵の発行要求信号に基づき、要求内容に応じたサービス鍵を発行する。ワンタイム認証鍵発行部G4は、携帯端末1から送信されてくるワンタイム認証鍵発行要求信号に基づき、要求元用のワンタイム認証鍵を発行する。サービス鍵削除部G5は、携帯端末1からの要求に基づき、指定されたサービス鍵を削除する。機種変更受付部G6は、機種変更の申請を受け付け、新たなデバイスIDに応じたサービス鍵を発行する構成である。

【0091】

ワンタイム認証鍵発行部 G 4、サービス鍵削除部 G 5、及び機種変更受付部 G 6 の詳細は別途後述する。

【0092】

データ処理部 30 は以上の機能部を備えることにより、システムが管理する車両毎のオーナーとゲストとの対応関係を保持する。1つの車両に対して、オーナーとなるユーザはただ1人である一方、ゲストは複数存在しうる。データ処理部 30 は、1つの車両及びオーナーに紐づくゲストの情報を統合的に管理する。

【0093】

図 9 は 1つの車両に対するオーナー鍵とゲスト鍵との対応関係を概念的に示したものである。データ処理部 30 は、オーナー鍵のサービス鍵 ID、つまりオーナー鍵 ID を元に、1つの車両及び 1つのオーナー鍵に紐づく複数のゲスト鍵を管理する。なお、図 9 では 1つの車両に対して 3つのゲスト鍵が発行されている場合を示している。各ゲスト鍵は前述の通り、権限設定や有効期限が相違しうる。

【0094】

<車載システム 7 の構成及び機能について>

ここでは車載システム 7 の構成及び機能について説明する。図 10 に示すように車載システム 7 は、認証 ECU 4、ディスプレイ 51、入力装置 52、ボディ ECU 53、ロックモータ 54、電源 ECU 55、近接場通信部 56、BLE 通信部 57、及びセルラー通信部 58 を備える。

【0095】

認証 ECU 4 は、ディスプレイ 51、入力装置 52、ボディ ECU 53、電源 ECU 55、近接場通信部 56、BLE 通信部 57、及びセルラー通信部 58 のそれぞれと車両内ネットワーク Nw を介して又は専用の信号線によって相互通信可能に接続されている。ボディ ECU 53 はロックモータ 54 と通信可能に接続されている。車両内ネットワーク Nw は、車両 Hv 内に構築されている通信ネットワークである。車両内ネットワーク Nw の規格としては、Controller Area Network（以降、CAN：登録商標）や、Ethernet（登録商標）、FlexRay（登録商標）など、多様な規格を採用可能である。なお、ボディ ECU 53 などの一部は、車両内ネットワーク Nw を介さずに認証 ECU 4 と専用線で接続されていてもよい。装置同士の接続形態は適宜変更可能である。

【0096】

認証 ECU 4 は、BLE 通信部 57 等との協働により、携帯端末 1 の認証処理を実行する ECU である。また、認証 ECU 4 は、携帯端末 1 の認証が成功していることを条件として、ドアの開錠や走行用電源オンなどといった、所定の車両制御を他の ECU との協働により実施する。認証 ECU 4 は上記処理を実行するコアモジュールとして車両制御部 40 を備える。

【0097】

当該認証 ECU 4 は、コンピュータを用いて実現されている。すなわち、認証 ECU 4 は、認証プロセッサ 41、RAM 42、ストレージ 43、I/O 44、及びこれらの構成を接続するバスラインなどを備えている。認証プロセッサ 41 は、例えば CPU である。認証プロセッサ 41 は、RAM 42 へのアクセスにより、後述する各機能部の機能を実現するための種々の処理を実行する。認証プロセッサ 41 と RAM 42 を含む構成が車両制御部 40 に相当する。認証プロセッサ 41 は、サーバプロセッサ 301 と対比して、車両プロセッサと呼ぶこともできる。ストレージ 43 には、車両 Hv にアクセスするユーザ（実態的には携帯端末）の認証処理にかかるプログラムである車両用認証プログラムが格納されている。また、ストレージ 43 には、認証 ECU 4 の ECU 番号が保存されていてもよい。I/O 44 は、他装置と通信するための回路モジュールである。認証 ECU 4 の機能の詳細は後述する。

【0098】

ディスプレイ 51 は、画像を表示するデバイスである。例えばディスプレイ 51 は認証 ECU 4 からの入力に基づき、オーナー登録開始画面やサービス鍵削除画面などを表示しう

10

20

30

40

50

る。オーナー登録開始画面は、オーナー鍵の登録を開始するための操作画面であって、例えばオーナーのパスワードを入力するフォームなどを含みうる。サービス鍵削除画面は、ユーザにて指定されたサービス鍵のデータを車両側記憶部45から削除するための画面である。認証ECU4が保持するオーナー鍵のデータもまた、当該サービス鍵削除画面を介して削除可能に構成されている。ディスプレイ51は、例えばインストゥルメントパネルの車幅方向の中央領域に設けられた、センターディスプレイである。ディスプレイ51は、運転席の正面領域に配置された、いわゆるメータディスプレイであってもよい。

【0099】

入力装置52は、車載システム7、より具体的には認証ECU4に対するユーザの指示操作を受け付けるための装置である。入力装置52としては、例えばディスプレイ51に積層されたタッチパネルを採用可能である。入力装置52はステアリングホイールやインストゥルメントパネル等に設けられた機械的スイッチであっても良い。入力装置52は、当該装置に対してユーザが行った操作に対応する電気信号を操作信号として認証ECU4に出力する。入力装置52が出力する操作信号は、ユーザの操作内容を示す。ディスプレイ51及び入力装置52は、認証ECU4に対するサービス鍵の登録／削除／動作設定の変更などをユーザが行うためのインターフェースに相当する。ディスプレイ51及び入力装置52をまとめて、車載HMI50とも称する。HMIはヒューマンマシンインターフェース (Human Machine Interface) の略である。

【0100】

ボディECU53は、認証ECU4からの要求及びユーザの操作信号に基づいてボディ系アクチュエータを制御するECUである。ボディECU53は、種々のボディ系アクチュエータと通信可能に接続されている。ここでのボディ系アクチュエータには、各ドアのロック機構を構成するロックモータ54が含まれる。

【0101】

電源ECU55は、車両Hvに搭載された走行用電源のオンオフ状態を制御するECUである。例えば電源ECU55は、例えば認証ECU4からの指示信号に基づき、走行用電源をオンに設定する。なお、車両Hvがエンジン車である場合には、電源ECU55は上記指示信号に基づきエンジンを始動させる。

【0102】

近接場通信部56は、近接場通信を実施するための通信モジュールである。近接場通信部56は、専用キー2からデータを受信するためのリーダとしての機能を有している。近接場通信部56は、通信距離内の専用キー2に近接場通信によってアクセスし、オーナー検証にかかる情報、例えば専用キーコード又は専用キーコードに基づくレスポンスコードを受信する。近接場通信部56は、専用キー2に限らず、携帯端末1等、通信圏内に位置する多様なデバイスとも近接場通信を実施しうる。

【0103】

近接場通信部56としては、例えば車外用の通信モジュールと、車内用のモジュールとが設けられうる。車外用の近接場通信部56は、施開錠制御に向けた認証を行うための構成に相当する。車内用の近接場通信部56は、走行用電源のオンオフ制御に向けた認証を行うための構成に相当する。車外用の近接場通信部56は、例えば運転席用の外側ドアハンドル付近に設けられている。外側ドアハンドル付近とは例えば外側ドアハンドルから0.2m以内を指す。外側ドアハンドル付近には、外側ドアハンドルの内部も含まれる。また、車内用の近接場通信部56は、車室内の運転席周りに配置されている。例えば車室内用の近接場通信部56は、インストゥルメントパネルに配されたスタートボタン付近に配置されている。車内用の近接場通信部56は、スタートボタンに内蔵されていてもよい。さらに、近接場通信部56は、センターコンソールや、インストゥルメントパネルの車幅方向中央部に設けられていても良い。

【0104】

BLE通信部57は、BLE通信を実施するための通信モジュールである。BLE通信部57は、例えばセンターコンソールや、車内の天井部、フロント／リアガラスの上端部

10

20

30

40

50

、Ｃピラーなどに配置されている。セルラー通信部５８はセルラー通信を実施するための通信モジュールである。車載システム７は、セルラー通信部５８の代わりに、又は、セルラー通信部５８と合わせて、Ｗｉ－Ｆｉ通信用のモジュールを備えていても良い。

【０１０５】

認証ＥＣＵ４は、ＤＫＳ３及び携帯端末１と通信することにより、ユーザの認証にかかる処理を実行する。なお、認証ＥＣＵ４と携帯端末１との通信は、より具体的には、携帯端末１が備えるＢＬＥ通信部１６と、車載システム７が備えるＢＬＥ通信部５７の協働によって実現されうる。

【０１０６】

認証ＥＣＵ４は、図１１に示すように機能部として、ユーザ管理部Ｈ１、及び、認証処理部Ｈ２を備える。これらの機能部は例えば認証プロセッサ４１が車両用認証プログラムを実行することによって実現される。また、認証ＥＣＵ４は、オーナ鍵等を記憶するための車両側記憶部４５を備える。車両側記憶部４５は、ストレージ４３又はＲＡＭ４２が備える記憶領域を用いて実現される。車両側記憶部４５は、オーナ鍵記憶部４５１と、ゲスト鍵記憶部４５２とを備える。

【０１０７】

オーナ鍵記憶部４５１は、オーナ鍵に関する情報を格納するための記憶領域である。ゲスト鍵記憶部４５２は、ゲスト鍵に関する情報を格納するための記憶領域である。オーナ／ゲスト鍵に関する情報とは、サービス鍵そのものの他、サービス鍵ＩＤや、ユーザＩＤ、ユーザ名などを指す。ゲスト鍵に関する情報には、有効期限や権限設定なども含まれる。ゲスト鍵記憶部４５２は複数のゲスト鍵を保存可能に構成されている一方、オーナ鍵記憶部４５１は１つのオーナ鍵しか保存できないように構成されている。故に、新規オーナ鍵の登録は、古いオーナ鍵のデータ削除を伴う。車両側記憶部４５が車両側記憶装置に相当する。

【０１０８】

ＤＫＳ３が発行したサービス鍵は、車両側記憶部４５に登録されることによって、有効化される。すなわち、ユーザは、当該ユーザ向けのサービス鍵が車両側記憶部４５に保存されていることを条件として、サービス鍵に割り当てられている権限の範囲において車両Ｈｖを利用可能となる。

【０１０９】

ユーザ管理部Ｈ１は、車両Ｈｖを利用可能なユーザ、つまり、車両側記憶部４５に保存されているサービス鍵を管理する構成である。ユーザ管理部Ｈ１は、別途後述するように、携帯端末１とＢＬＥ通信を実施することにより、携帯端末１を介してＤＫＳ３が発行したサービス鍵に関するデータを取得し、車両側記憶部４５に保存する。また、ユーザ管理部Ｈ１は、携帯端末１を介して車両側記憶部４５に保存されているサービス鍵を削除するためのデータを取得し、対象となるサービス鍵に関するデータを削除する。

【０１１０】

認証ＥＣＵ４は、動作モードとして、オーナ鍵の登録を受付可能なオーナ登録可能モードと、オーナ登録を受け付けない／拒否するオーナ登録禁止モードとを備える。認証ＥＣＵ４は、基本的にはオーナ登録禁止モードで動作する。そのため、オーナ登録禁止モードは通常モードと呼ぶことができる。認証ＥＣＵ４は、別途後述するセキュリティ解除コードが入力されたことに基づいて、一時的にオーナ登録禁止モードからオーナ登録可能モードへと移行する。

【０１１１】

認証処理部Ｈ２は、ＢＬＥ通信部５７と連携して、通信相手が車両Ｈｖのユーザが所持する携帯端末１であることを確認（換言すれば認証）する処理を実施する。認証のための通信は、暗号化されて実施される。認証方式自体は、チャレンジャーレスポンス方式など多様な方式を用いて実施されうる。本実施形態では一例として、チャレンジコードとワンタイム認証鍵を用いたチャレンジャーレスポンス方式で認証が行われる。認証処理の詳細なシーケンスについては別途後述する。認証処理部Ｈ２は、認証処理で必要となるワンタイム

10

20

30

40

50

認証鍵を動的に生成するワнтаム認証鍵生成部 H 2 1 をサブ機能部として備える。なお、ワнтаム認証鍵生成部 H 2 1 は任意の要素であって省略されても良い。

【0112】

認証処理部 H 2 が認証処理を実施するタイミングは、例えば B L E 通信部 5 7 と携帯端末 1 との通信接続が確立したタイミングとすることができる。認証処理部 F 4 は、B L E 通信部 5 7 と携帯端末 1 とが通信接続している間、所定の周期で認証処理を実施するように構成されていても良い。また、車両 H v に対する所定のユーザ操作をトリガとして認証処理のための暗号通信を実施するように構成されていても良い。

【0113】

認証処理の実行トリガとなるユーザ操作としては、ドアボタンの押下／ドアハンドルへのタッチ、スタートボタンの押下、ドアの開閉などが採用可能である。ドアボタンとは、ドアハンドルに設けられた、ドアを開錠／施錠するためのボタンを指す。ドアハンドルのへのタッチは、ドアハンドルに設けられたタッチセンサによって検出されうる。スタートボタンは、インストゥルメントパネルなどの車室内に設けられた、走行用電源のオン／オフを切り替えるためのボタンである。

【0114】

＜オーナー鍵登録シーケンスについて＞

ここでは図 1 2、図 1 3、及び図 1 4 を用いてオーナー鍵の発行から車両へ登録するまでのシーケンスの一例について説明する。オーナー鍵の発行から車両へ登録するまでのシーケンスは、図 1 2 に示すように大きくは発行フェーズ P h 1 と、車両登録フェーズ P h 2 に分けることができる。

【0115】

発行フェーズ P h 1 は、D K S 3 が、ユーザからの要求、実態的には携帯端末 1 から送信される鍵発行要求信号に基づき、サービス鍵を発行するフェーズである。発行されたサービス鍵は、携帯端末 1 にのみ配布される。D K S 3 が発行したサービス鍵は、車両 H v に直接配布されることはなく、携帯端末 1 を経由して車両に登録される。車両登録フェーズ P h 2 は、B L E 通信によって携帯端末 1 が保持しているサービス鍵の情報を車両 H v に登録するフェーズである。D K S 3 が発行したサービス鍵は車両 H v に登録されて初めて実質的に使用可能な状態、つまり有効化される。そのため車両登録フェーズ P h 2 は、有効化フェーズと呼ぶこともできる。なお、オーナー鍵に限らず、ゲスト鍵の発行～有効化も、発行フェーズ P h 1 と、車両登録フェーズ P h 2 とを含む。

【0116】

図 1 3 は、オーナー鍵の発行フェーズに対応する各デバイスのインタラクションを示すシーケンス図である。オーナー鍵の発行シーケンスは、オーナー端末と D K S 3 によって実行される。オーナー鍵の発行シーケンスは図 1 3 に示すように、ステップ S 1 0 ～S 1 7 を含む。

【0117】

ステップ S 1 0 は、D K S 3 が、ユーザ／携帯端末 1 を認証し、通信相手がオーナー／オーナー端末であることを確認するステップである。オーナーであることの認証は、ユーザ I D 及びパスワードを用いて実施されても良いし、生体情報を用いて認証されても良い。生体情報を用いた認証は、生体認証装置 1 4 によって実行されうる。なお、ステップ S 1 0 は携帯端末 1 のデジタルキーアプリ 1 0 4 がユーザを認証するステップであってもよい。

【0118】

ステップ S 1 1 は、オーナー端末としての携帯端末 1 が、ユーザの操作に基づいて鍵発行要求信号を送信するステップである。ここで送信される鍵発行要求信号は、オーナー鍵の発行を要求する信号であるため、オーナー鍵発行要求信号と呼ぶことができる。鍵発行要求信号は、例えばデバイス I D 又はユーザ I D など、D K S 3 が要求元を特定するための情報を含む。また、鍵発行要求信号は、発行対象とするサービス鍵のタイプを含む。なお、発行対象とするサービス鍵がゲスト鍵である場合には、鍵発行要求信号は、権限の設定や有効期限の設定などを示す情報を追加的に含む。その他、鍵発行要求信号は、対象とする車両の情報などを含んでいても良い。ただし、対象車両の情報は、ユーザ I D などを検

10

20

30

40

50

索キーとして車両DB32を参照することにより特定可能であるため、鍵発行要求信号に含まれていなくとも良い。

【0119】

ステップS12では、DKS3が、オーナー端末から取得したオーナー鍵発行要求信号に基づいて、オーナー鍵としてのサービス鍵及びサービス鍵IDを生成する。ステップS12の実行主体は、より具体的にはサービス鍵発行部G3である。

【0120】

ステップS13ではDKS3が、ステップS12で生成したサービス鍵をもとに、ワンタイム認証鍵を所定数作成する。ステップS13の実行主体は、より具体的にはワンタイム認証鍵発行部G4である。サービス鍵発行時に生成するワンタイム認証鍵の数である初回発行数は、例えば300など、補充閾値よりも所定量多く設定されている。

【0121】

ステップS14ではDKS3が、ステップS12～S13で生成した各種データを含むデータセットである端末登録用パッケージをオーナー端末に向けて送信する。端末登録用パッケージは、サービス鍵、サービス鍵ID、複数のワンタイム認証鍵、及び、各ワンタイム認証鍵の生成に用いた変動コードを含む。個々のワンタイム認証鍵は、当該ワンタイムの生成に使用された変動コードと紐付けられている。複数のワンタイム認証鍵及び変動コードを含むデータセットは、認証鍵パッケージとしてサービス鍵を含むデータセットとは別に送信されても良い。

【0122】

また、端末登録用パッケージは、端末チェックコードと、対象車両に搭載されている認証ECU4のECU番号を含みうる。端末チェックコードは、データの完全性、受信データの正当性、及び改ざんの有無を、受信側である携帯端末1が検証するためのコードである。端末チェックコードは、ハミング符号であってもよいし、ペイロードを所定のハッシュ関数に入力して得られるハッシュ値であってもよい。端末チェックコードは、DKS3と携帯端末1とが暗号通信するための鍵として事前に発行された暗号鍵を用いて生成されても良い。

【0123】

ステップS15では、オーナー端末としての携帯端末1が、DKS3から配信された端末登録用パッケージを受信し、その中身を鍵情報記憶部M1に保存するステップである。サービス鍵管理部F1は、前述の端末チェックコードを用いて受信データの正当性を検証した上で、受信したサービス鍵及びその関連情報を鍵情報記憶部M1に保存する。

【0124】

ステップS16は、DKS3が、車両Hvにオーナー情報を登録するためのデータセットである車両登録用パッケージをオーナー端末に向けて送信する。車両登録用パッケージは、サービス鍵、サービス鍵IDの他、車両チェックコードを含みうる。車両チェックコードは、データの完全性、受信データの正当性、及び改ざんの有無を、最終的な受信デバイスである認証ECU4が検証するためのコードである。車両チェックコードは、端末チェックコードと同様にペイロードに応じたハミング符号やハッシュ値であってもよい。車両チェックコードは、DKS3と認証ECU4とが暗号通信するための鍵として事前に発行された暗号鍵を用いて生成されても良い。また、車両チェックコードは、ECU番号をもとに生成されてもよい。なお、車両登録用パッケージには、端末チェックコードが付加されていても良い。当該構成によれば、DKS3と認証ECU4との通信の中継役であるオーナー端末も、受信した車両登録用パッケージの完全性、正当性等を検証可能となる。

【0125】

ステップS17では、オーナー端末としての携帯端末1が、DKS3から配信された車両登録用パッケージを受信し、その中身を車両用データ一時記憶部M2に保存するステップである。受信処理には、前述の端末チェックコードを用いた検証処理が行われてもよい。なお、本実施形態では車両登録用パッケージと端末登録用パッケージを別々に送信するが、各種データの送信態様はこれに限らない。車両登録用パッケージと端末登録用パッケー

10

20

30

40

50

ジは一連のデータとして送信されても良い。その際、重複するデータは省略されても良い。

【0126】

次の図14を用いてオーナー鍵を車両Hvに登録するシーケンスについて説明する。オーナー鍵の車両Hvへの登録シーケンスは、ステップS20～S29を含む。

【0127】

まず本シーケンス開始時の初期状態（ステップS20）として、認証ECU4はオーナー登録禁止モード（つまり通常モード）で動作している。ステップS21は、所定のセキュリティ解除ツール又はDKS3が、所定のセキュリティ解除信号を認証ECU4に入力するステップである。セキュリティ解除ツール又はDKS3を用いた認証ECU4へのセキュリティ解除信号の入力は、オーナー又はディーラスタッフによって実行される。

10

【0128】

セキュリティ解除信号は、セキュリティ解除コードを含む信号である。セキュリティ解除信号は、1つの局面において、登録者がオーナー自身であることを証明する信号に相当する。セキュリティ解除信号は、認証ECUをオーナー登録禁止モード（通常モード）から、一時的にオーナー登録可能モードに切り替えるための信号に相当する。認証ECU4はセキュリティ解除信号が入力されたことに基づいて、オーナー登録可能モードに移行する（ステップS22）。セキュリティ解除信号がオーナー登録開始信号に相当する。

【0129】

セキュリティ解除ツールは、例えば専用キー2である。また、セキュリティ解除コードとしては専用キーコードを採用可能である。例えば認証ECU4は、車内用の近接場通信部56が専用キー2と近接場通信を行い、専用キーコードを受信したことに基づいて、オーナー登録可能モードに移行してもよい。なお、認証ECU4は、専用キーコードを受信したことに加えて、車載HMI50を介して所定のパスワードが入力されたことを条件に、オーナー登録可能モードに移行するよう構成されていても良い。

20

【0130】

また、セキュリティ解除ツールは、ディーラショップなどで管理される専用ツールであってもよい。専用ツールと認証ECU4との通信方式は、近接場通信であってもよいし、例えばUSBケーブルなどを用いた有線通信であってもよい。DKS3からのセキュリティ解除信号は、セルラー通信部58を介して受信する。なお、DKS3は、オーナー端末からの要求、又は、ディーラショップに設けられた所定の端末からの要求に基づいて、車両Hvを宛先とするセキュリティ解除信号を送信する。当該構成によればオーナー又はディーラショップのスタッフは、オーナー端末又はディーラショップに設けられた所定の端末を操作することにより、認証ECU4をオーナー登録可能モードに切り替えることができる。

30

【0131】

認証ECU4は、オーナー登録モードに移行すると、ステップS24aとして所定のスキャン間隔でBLE通信部57を待受状態に設定し、携帯端末1の探索（いわゆるスキャンング）を実施させる。ここでの待受状態とは、アドバタイズ信号を受信可能な状態を指す。本実施形態ではパッシブスキャン方式にて車両周辺に存在する携帯端末1を検出する。他の態様として認証ECU4は、スキャン要求の送信を伴うアクティブスキャン方式によって携帯端末1を探索しても良い。

40

【0132】

一方、オーナー端末は、タッチパネル12を介してオーナー鍵の登録開始操作を受け付ける（ステップS23）と、オーナー鍵の登録に向けたアドバタイズの発信を所定の間隔で発信する（ステップS24b）。当該アドバタイズがBLE通信部57を介して認証ECU4で受信されることにより、認証ECU4と携帯端末1は通信接続のための通信を開始する（ステップS25）。なお、オーナー鍵の登録開始操作とは、例えば図15に示すように、ディスプレイ11に表示されるオーナー鍵登録開始ボタンB1の押下である。オーナー鍵の登録開始操作は、オーナー鍵の登録開始を指示する音声コマンドの入力であってもよい。

【0133】

オーナー端末は、認証ECU4とBLE通信の接続が確立すると、例えば図16に示すペ

50

アリング確認画面を表示する。ペアリング確認画面は例えばペアリングを実行するか否かをユーザが選択するためのボタンB 2 a、B 2 bを含む。オーナ端末は、タッチパネル1 2からの信号に基づき肯定ボタンB 2 aが押下されたことを検知すると（ステップS 2 6）、認証E C U 4とのペアリング処理を実行する（ステップS 2 7）。これにより、認証E C U 4とオーナ端末との間で暗号化されたデータ通信が可能となる。ここでのペアリング処理には、暗号鍵の交換だけでなく、暗号鍵の保存（いわゆるボンディング）も含まれる。

【0 1 3 4】

ペアリング処理が完了し、認証E C U 4－オーナ端末間の暗号通信リンクが確立すると、オーナ端末は、車両用データ時記憶部M 2に保管されていた車両登録用パッケージをB L E通信で認証E C U 4に送信する（ステップS 2 8）。ステップS 2 4 a～S 2 8までの一連の通信が、認証E C U 4にとってはオーナ端末からオーナ鍵を取得するための通信に相当する。

【0 1 3 5】

認証E C U 4は、オーナ端末からB L E通信で車両登録用パッケージを受信すると、当該パッケージに含まれる鍵関連データを車両側記憶部4 5に保存する。より具体的には、受信したサービス鍵や、サービス鍵I D、をオーナ鍵記憶部4 5 1に保存する。これにより、オーナ鍵の車両登録が完了し、オーナ鍵が有効化される。

【0 1 3 6】

なお、オーナ登録禁止モードは、例えばオーナ権限を有するサービス鍵の受信又は保存を拒否することによって実現されてもよいし、通信接続そのものを拒否することで実現されても良い。また、1つの態様として認証E C U 4は、所定のオーナ登録用I Dを含むアドバタイズを起点とする通信リンクで受信したサービス鍵を、オーナ鍵としてオーナ鍵記憶部4 5 1に保存するように構成されていてもよい。その場合、認証E C U 4は、オーナ登録禁止モード時にはオーナ登録用I Dを含むアドバタイズを無視する一方、オーナ登録モードにはオーナ登録用I Dを含むアドバタイズに基づく通信接続を行う。オーナ登録用I Dは、オーナ情報を登録するための通信であることを示すI Dであって、U U I D、M a j o r、M i n o rといった3種類の識別子の組み合わせで表現されうる。

【0 1 3 7】

上記の構成によれば、特定のオーナ登録開始信号が入力された場合にしか、オーナ鍵のデータが車両H vには登録されない。よって、オーナ鍵を常時登録可能な構成よりもセキュリティを高めることができる。

【0 1 3 8】

<ゲスト鍵登録シーケンスについて>

次に、図1 7、図1 8、図1 9、図2 0を用いてゲスト鍵の発行から、当該ゲスト鍵を車両H vに登録するまでのシーケンスの一例について説明する。ゲスト鍵の発行から車両登録までのシーケンスもまた、発行フェーズP h 1と、車両登録フェーズP h 2とに分けることができる。

【0 1 3 9】

図1 7は、ゲスト鍵の発行フェーズP h 1に対応する各デバイスのインタラクションを示すシーケンス図である。ゲスト鍵の発行シーケンスは、オーナ端末と、対象ゲスト端末と、D K S 3によって実行される。対象ゲスト端末とは、サービス鍵の発行対象とするゲストに紐づく携帯端末1を指す。ゲスト鍵の発行シーケンスは図1 7に示すように、ステップS 3 0～S 3 7を含む。

【0 1 4 0】

ゲスト鍵の発行及び車両への登録シーケンスの説明におけるゲスト端末とは、対象ゲスト端末を指す。なお以下ではオーナがゲスト鍵を発行する場合について説明するが、ゲスト鍵の発行者は、発行権付きゲスト鍵が付与されているゲストであってもよい。発行権付きゲスト鍵が付与されているゲストのことを、発行権もちゲストとも記載する。ゲスト鍵の発行等の説明におけるオーナ端末／オーナとの記載は、発行権付きゲスト端末／発行権

10

20

30

40

50

もちゲストと読み替えて実施することができる。

【0141】

ステップS30は、サービス鍵の発行を希望するゲストの操作に基づいて、ゲスト端末が、オーナー端末に向けてゲスト鍵の発行依頼を送信するステップである。オーナー端末はゲスト端末からの発行依頼を受領すると、DKS3に向けて、ゲスト鍵発行要求信号を送信する（ステップS31）。なお、図示は省略しているが、ゲスト鍵の発行シーケンスもまた、DKS3が、オーナーとしてのユーザを認証するステップを含みうる。また、ステップS30は任意の要素である。ゲスト端末からの発行依頼がなくとも、オーナー端末はオーナーの操作に基づき所定のゲストを対象とするゲスト鍵発行要求信号を送信しうる。例えばオーナーは、ゲストとの電話／メール等のやり取りに基づいてオーナー端末を操作することにより、任意のゲストに対してゲスト鍵を発行可能に構成されている。

10

【0142】

ゲスト鍵発行要求信号は、例えば図18に示すように、要求元情報、対象車両情報、対象ユーザID、有効期限情報、及び権限の設定情報のそれぞれを収容するデータフィールドを含む。要求元情報は、ゲスト鍵の発行要求元を示す情報であって、例えばオーナーのユーザIDや、サービス鍵ID、デバイスIDなどを採用可能である。対象車両IDは、新規発行するゲスト鍵で利用可能な車両を特定するための情報であって、ここでは車両Hvの車両IDを指す。対象ユーザIDは、ゲスト鍵の発行対象とするゲストのユーザIDである。ユーザIDの代わりにデバイスIDなどが対象ユーザ情報として採用されてもよい。有効期限に対応するデータフィールドには、オーナーが指定した期間／日時に対応する値、又は所定値が入力される。権限設定情報は、ゲスト鍵の発行権の有無、走行用電源の切り替え権限の有無、施開錠できるドアなどを示す。

20

【0143】

DKS3は、オーナー端末からのゲスト鍵発行要求信号を受信すると、ステップS32として、受信したゲスト鍵発行要求信号に基づいて、対象ゲスト向けのサービス鍵及びサービス鍵IDを生成する。また、ステップS33ではDKS3のワンタイム認証鍵発行部G4が、ステップS32で生成したサービス鍵をもとに、ワンタイム認証鍵を所定の初回発行数だけ作成する。

【0144】

ステップS34ではDKS3が、ステップS32～S33で生成した各種データを含むデータセットである端末登録用パッケージをゲスト端末に向けて送信する。ゲスト鍵にかかる端末登録用パッケージは、例えば図19に示すように、基本情報に加えて、ゲスト用情報を含みうる。基本情報は、オーナー鍵発行時に配信されるパッケージと概ね同様の項目を有する。つまり基本情報は、サービス鍵、サービス鍵ID、複数のワンタイム認証鍵、及び、ワンタイム認証鍵毎の変動コードを含む。ゲスト用情報は、ゲスト鍵用の付加的な情報である。例えばゲスト用情報は、発行元情報、オーナー鍵ID、対象車両情報、有効期限情報、権限設定情報を含む。発行元情報は、基本的にはオーナーを示す。ただし、新規発行されたゲスト鍵が、発行権付きゲスト端末からの要求に基づいて生成されたものである場合、発行元情報のデータフィールド（欄）には、発行元としてのゲストを示す情報が格納されてもよい。端末登録用パッケージは、発行元情報とオーナー鍵IDの何れか一方だけを備えるように構成されていても良い。ゲスト端末に向けて発せられる端末登録用パッケージもまた、端末チェックコードなどを含む。

30

40

【0145】

ステップS35では、ゲスト端末としての携帯端末1が、DKS3から配信された端末登録用パッケージを受信し、その中身を鍵情報記憶部M1に保存する。ステップS36では、DKS3が、車両Hvにゲスト鍵情報を登録するためのデータセットである車両登録用パッケージをゲスト端末に向けて送信する。ゲスト鍵にかかる車両登録用パッケージに含まれる情報種別は、ステップS36で送信される車両登録用パッケージと同様とすることができる。ステップS37では、ゲスト端末としての携帯端末1が、DKS3から配信された車両登録用パッケージを受信し、その中身を車両用データ一時記憶部M2に保存す

50

るステップである。

【0146】

次の図20を用いて、ゲスト端末がDKS3から受領したゲスト鍵を車両Hvに登録するシーケンスについて説明する。ゲスト鍵の車両Hvへの登録シーケンスは、ステップS40～S47を含む。前提としてゲスト端末は車両Hvの周辺、より具体的にはBLE通信可能な位置に存在するものとする。ゲスト端末が実行するステップの、実質的な実行主体は端末プロセッサ101である。また、認証ECU4が実行するステップの、実質的な実行主体は認証プロセッサ41である。

【0147】

まず本シーケンス開始時の初期状態（ステップS40）として、認証ECU4は通常モードで動作している。認証ECU4はゲスト鍵に関しては通常モードでも登録可能である。そのため、オーナー鍵の登録シーケンスと違い、オーナー及びゲストは、セキュリティ解除ツール等を用いて認証ECU4の動作モードを変更する必要はない。認証ECU4は、通常モード時においても、所定のスキャン間隔でスキャンングを実施する（ステップS42a）。

10

【0148】

一方、ゲスト端末は、タッチパネル12を介してゲスト鍵の登録開始操作を受け付けると（ステップS41）、ゲスト鍵の登録に向けたアダプタイズの発信を所定の間隔で発信する（ステップS42b）。当該アダプタイズがBLE通信部57を介して認証ECU4で受信されることにより、認証ECU4と携帯端末1は通信接続のための通信を開始する（ステップS43）。なお、ゲスト鍵の登録開始操作とは、例えば図21に示すように、ディスプレイ11に表示されるゲスト鍵登録開始ボタンB3の押下である。ゲスト鍵の登録開始操作は、所定の音声フレーズの入力であってもよい。

20

【0149】

ゲスト端末は、認証ECU4とBLE通信の接続が確立すると、例えば図16に示すペアリング確認画面を表示する。ゲスト端末は、タッチパネル12からの信号に基づき肯定ボタンB2aが押下されたことを検知すると（ステップS44）、認証ECU4とのペアリング処理を実行する（ステップS45）。これにより、認証ECU4とゲスト端末との間で暗号化されたデータ通信が可能となる。

【0150】

ペアリング処理が完了し、認証ECU4－ゲスト端末間の暗号通信リンクが確立すると、ゲスト端末は、車両用データ一時記憶部M2に保管されていた車両登録用パッケージをBLE通信で認証ECU4に送信する（ステップS46）。

30

【0151】

認証ECU4は、ゲスト端末からBLE通信で車両登録用パッケージを受信すると、当該パッケージに含まれる鍵関連データを車両側記憶部45に保存する。より具体的には、受信したサービス鍵や、サービス鍵ID、権限設定、有効期限などをゲスト鍵記憶部452に保存する。これにより、ゲスト鍵の車両Hvへの登録が完了し、ゲスト鍵が有効化される。

【0152】

上記構成によれば、ゲスト鍵を有効化するためにオーナー端末と認証ECU4とがBLE通信で接続する必要がない。つまり、ゲスト鍵を発行するたびに、オーナーが車両Hvの近くまでオーナー端末を持っていく必要がない。よって、上記の構成によれば、ゲスト鍵の有効化にかかるオーナーの負担を低減することができる。また、本実施形態では認証ECU4は、オーナー鍵、ゲスト鍵といったサービス鍵のタイプによらずに、携帯端末1とのBLE通信によって車両登録用パッケージを取得し、保存する。当該構成によれば、車両Hvにおけるデータ通信量を抑制可能となる。さらに、車両Hvが地下駐車場など、通信圏外にある場合においても、ユーザの接近に伴ってサービス鍵を車両Hvに登録可能となる。もちろん、他の態様として、認証ECU4は、セルラー通信又はWi-Fi通信によってDKS3から、車両登録用パッケージを取得しても良い。なお、携帯端末1を経由してサー

40

50

ビス鍵を車両H vに送信する構成は、サービス鍵を間接的に認証E C U 4に配布する構成に相当する。

【0153】

＜ユーザが車両を使用する場合のシステム作動例＞

ここでは図22、図23を用いて、ユーザが車両H vを利用する際の認証E C Uの作動について説明する。前提として、ここで述べるユーザとは、車両H vのサービス鍵が保存されている携帯端末1を携帯している人物である。つまり、ここでのユーザとはオーナー又はゲストに相当し、携帯端末1とはオーナー端末又はゲスト端末に相当する。

【0154】

まず、車両H vが駐車されている間、認証E C U 4は定期的にB L E通信部57にスキヤニングを実施させ、携帯端末1が車両周辺に存在するか否かを判定する（ステップS51）。携帯端末1が車両周辺に存在するか否かの判定は、アドバタイズ等、携帯端末1から発せられるB L E信号を受信しているか否かに基づいて実施される。仮に携帯端末1からのB L E信号を受信している場合には（ステップS51 Y E S）、当該携帯端末1と通信接続する（ステップS52）。一方、スキヤニングの結果、携帯端末1を発見できなかった場合には本フローを終了する。なお、フローを終了した場合には、所定のスキャン間隔が経過したタイミングでステップS51を再実行する。図22に示すフローチャートは、車両H vが駐車されている状態において所定のスキャン間隔で繰り返し実施されうる。

【0155】

認証E C U 4は、携帯端末1と通信接続できた場合、ステップS53として認証処理を実行する。認証処理については別途後述する。認証処理の結果として携帯端末1（ひいてはユーザ）の認証が成功した場合には（ステップS54 Y E S）、スタンバイモードに移行する（ステップS55）。

【0156】

スタンバイモードは、ドアボタン等に対するユーザ操作に基づいて、開錠／施錠、走行用電源のオン／オフ切り替えなどを実施可能な状態に相当する。スタンバイモードは、1つの側面においてサービス鍵を有する携帯端末1／ユーザが車両周辺に存在すると認証プロセッサ41が認識している状態に対応する。車両周辺には、車外だけでなく車室内も含まれる。本実施形態では一例として、認証成功との判定結果には有効期限が設定される。有効期限は例えば3秒や5秒、10秒などに設定される。

【0157】

一方、認証処理の結果として携帯端末1の認証に失敗した場合には（ステップS54 N O）、本フローを終了する。なお、認証処理が失敗した場合には、認証が成功していないことをユーザが認識可能なように車載設備を動作させてもよい。例えば、認証処理が成功していない場合には、ディスプレイ51に所定の認証失敗画像を表示しても良いし、サイドミラー等に設けられた灯火装置を所定パターンで点灯させても良い。認証E C U 4は、認証処理が失敗した場合、携帯端末1に向けてB L E通信で所定の制御信号を送信する事により、ディスプレイ11に認証失敗画面を表示させてもよい。認証E C U 4は、ドア周りの路面に向けて光を発するウェルカムライトを所定パターンで点灯されることで、認証失敗したことを表現してもよい。

【0158】

ステップS56では、認証プロセッサ41がドアボタンやタッチセンサ、スタートボタンなどからの信号に基づき、車両H vを使用するためのユーザ操作が行われたか否かを判定する。車両H vを使用するためのユーザ操作とは、例えばドアハンドルに触れる／握るなどといった、ドアを開けようとする行為を指す。スタートボタンの押下も車両H vを使用するためのユーザ操作に該当する。

【0159】

認証プロセッサ41は、上記ユーザ操作に対応する信号が車載センサより入力された場合（ステップS56 Y E S）、ユーザが操作した部材及び車両H vの状態に応じた車両制御を実行する（ステップS57）。例えば認証プロセッサ41は、車両H vが施錠され

10

20

30

40

50

た状態において、ドアボタンが押下／ドアハンドルが把持されたことを検知した場合には、ドアを開錠する。また、認証プロセッサ 4 1 は、スタートボタンが押下されたことを検知した場合には、走行用電源をオフからオンに、又はオンからオフに切り替える。

【0160】

なお、実際に上記ドアの開錠／施錠、走行用電源のオン／オフといった車両制御を行う際には、認証結果だけでなく、携帯端末 1 の推定位置やサービス鍵の権限、車両 H v の状態が参照される。そして、所定の制御実行条件が充足されていない場合には、ユーザ操作に応じた車両制御の実行はキャンセルされうる。制御実行条件が充足されていない場合とは、例えばサービス鍵に設定されている権限が不足している場合や、検出されている携帯端末 1 の位置が車両から 2 m 以上離れている場合などである。携帯端末 1 の位置は、携帯端末 1 からの信号の受信状況に基づき特定されうる。携帯端末 1 の位置推定材料としては受信強度や、信号の到来方向、T o F (Time of Flight)、R T T (Round-Trip Time) など、多様な指標を採用可能である。

【0161】

一方、車両 H v を使用するためのユーザ操作が行われていない場合には（ステップ S 5 6 N O）、認証結果の有効期限が切れたか否か、すなわち、認証成功と判定してから所定時間経過したか否かを判定する。有効期限内である間は（ステップ S 5 8 N O）、スタンバイモードを維持する。一方、有効期限が切れた場合に、認証プロセッサ 4 1 は認証処理のための通信を再度実行する。

【0162】

上記の構成によれば、ユーザは専用キー 2 や携帯端末 1 を操作することなく、車両 H v にアクセス可能となる。つまり、パッシブエントリパッシブスタート機能が実現され、ユーザの利便性を高めることができる。

【0163】

<認証処理について>

ここでは認証 E C U 4 が携帯端末 1 を認証する処理のシーケンスについて説明する。認証 E C U 4 による携帯端末 1 の認証処理は、例えば図 2 3 に示すようにステップ S 6 1 ～ S 6 8 を備える。なお、認証処理は、携帯端末 1 と認証 E C U 4 との暗号化された通信リンクが確立していることを前提として実行される。

【0164】

ステップ S 6 1 は認証 E C U 4 から携帯端末 1 に向けて、チャレンジコードを送信するステップである。チャレンジコードとしては、予め用意された乱数表を用いて生成される所定長の乱数を採用することができる。チャレンジコードは、認証 E C U 4 が備える時刻情報（いわゆるシステム時刻）を S E E D として用いて生成された乱数であっても良い。チャレンジコードは多様な方法で決定されうる。

【0165】

ステップ S 6 2 は携帯端末 1 が、鍵情報記憶部 M 1 に保存されている任意のワンタイム認証鍵と、受信したチャレンジコードを、所定の方式で組み合わせることにより、レスポンスコードを生成するステップである。ステップ S 6 3 は携帯端末 1 が、ステップ S 6 2 で生成したレスポンスコード、及び、当該レスポンスコードの生成に使用したワンタイム認証鍵に対応する変動コードを、まとめて／別々に認証 E C U 4 に返送するステップである。或るワンタイム認証鍵に対応する変動コードとは、D K S 3 において当該ワンタイム認証鍵の生成に使用された変動コードを指す。

【0166】

ステップ S 6 4 は、認証 E C U 4 が携帯端末 1 から受信した変動コードと、車両側記憶部 4 5 に保存されている、通信相手に対応するサービス鍵とを用いて、D K S 3 のワンタイム認証鍵発行部 G 4 と同様の手法により、ワンタイム認証鍵を生成する。ここで認証 E C U 4 がワンタイム認証鍵の生成に使用するサービス鍵と変動コードの組み合わせは、携帯端末 1 がレスポンスコードの生成に使用したワンタイム認証鍵の生成材料と同じである。故にステップ S 6 4 で認証 E C U 4 が生成するワンタイム認証鍵は、携帯端末 1 がレス

ポンスコードの生成に使用したワンタイム認証鍵と同じとなる。このようなステップ S 6 4 は、携帯端末 1 から受信した変動コードと自信が保持する携帯端末 1 のサービス鍵をもとに、携帯端末 1 がレスポンスコードの生成に使用したワンタイム認証鍵を復元する処理に相当する。

【0167】

ステップ S 6 5 では、認証 E C U 4 がステップ S 6 4 で生成したワンタイム認証鍵と、ステップ S 6 1 で送信したチャレンジコードをもとに、検証用コードを生成するステップである。検証用コードの生成方法自体は、レスポンスコードの生成と同一である。通信相手が、車両側記憶部 4 5 に登録されているサービス鍵を保持する携帯端末 1 である場合には、検証用コードとレスポンスコードは一致することが期待できる。また、通信相手が未登録のデバイスである場合には、レスポンスコードが返送されないか、又は、レスポンスコードと検証用コードとが不一致となる。よって以上で生成／受信するコードは、通信相手の正当性を検証するための情報として機能する。

【0168】

ステップ S 6 6 では、認証 E C U 4 がステップ S 6 5 で生成した検証用コードと、携帯端末 1 から受信したレスポンスコードとを比較することで、通信相手の正当性を判断する。つまり、2つのコードが一致している場合には認証成功と判定する（ステップ S 6 7）。一方、2つのコードが相違する場合には認証失敗と判定する（ステップ S 6 8）。なお、チャレンジコードの送信から所定の応答待機時間が経過してもレスポンスコードが返って来ない場合、認証 E C U 4 は認証失敗と判定しうる。

【0169】

上記構成によれば、携帯端末 1 ごとに固有のサービス鍵をもとに生成される、ワンタイム認証鍵を用いて携帯端末 1 及びユーザの認証を行う。そのため、固定的な鍵情報を用いて携帯端末の認証を行う構成に比べてセキュリティを高める事ができる。また、上記の方法によれば、レスポンスコードの生成に際して認証 E C U 4 と携帯端末 1 の間でやり取りされる情報は変動コードとチャレンジコードである。認証に際してワンタイム認証鍵自体は認証 E C U ー携帯端末間で送受信されない。ワンタイム認証鍵の生成には、別途、サービス鍵の発行フェーズで配信されるサービス鍵が必要であり、変動コードを傍受しただけではワンタイム認証鍵の復元はできない。さらに、認証に使用されるワンタイム認証鍵は毎回変更される。よって、上記の方法によれば、無関係な人物が不正に認証処理を成功させる恐れを低減可能となる。ここでの無関係な人物とは、車両 H v のサービス鍵が付与されていない人物を指す。

【0170】

なお、上述した認証シーケンスは一例であって、これに限らない。携帯端末 1 と認証 E C U 4 とで、レスポンスコード／検証用コードの生成に使用するワンタイム認証鍵が同一のものとなるように、各デバイスの動作は設計されていれば良い。例えば認証処理は図 2 4 に示す手順で実施されても良い。つまり、認証処理は他の一例として、ステップ S 6 1 a ～ S 6 9 a を備えうる。

【0171】

なお、図 2 4 に示す認証処理パターンを採用する場合、前提構成として、認証 E C U 4 と携帯端末 1 は共通の複数のワンタイム認証鍵を保持しているものとする。例えば認証 E C U 4 は、車両登録用パッケージとして、複数のワンタイム認証鍵を含むデータセットを受信することにより、携帯端末 1 が保持するものと同じワンタイム認証鍵を取得する。また、車両側記憶部 4 5 に保存されているワンタイム認証鍵が所定の補充閾値未満となった場合には、携帯端末 1 の認証が成功していることを条件として、携帯端末 1 から認証 E C U 4 が未取得のワンタイム認証鍵を受信する。これにより、認証 E C U 4 は、車両側記憶部 4 5 に保存されているワンタイム認証鍵を補充しうる。なお、携帯端末 1 は別途後述するように随時 D K S 3 との通信によりワンタイム認証鍵を補充する。認証 E C U 4 は D K S 3 から直接ワンタイム認証鍵を取得するように構成されていても良い。その他、各ワンタイム認証鍵には、それらを識別するための番号が付与されているものとする。

【0172】

ステップS61aは、認証ECU4が、携帯端末1に向けて使用鍵確認信号を送信するステップである。使用鍵確認信号は、使用予定鍵の番号を問い合わせる信号である。使用予定鍵は、以降のレスポンスコードの生成に使用するワンタイム認証鍵を指す。使用鍵確認信号が調整メッセージに相当する。

【0173】

携帯端末1は、使用鍵確認信号を受信すると、ステップS62aとして、使用予定鍵の番号を認証ECU4に通知する。使用予定鍵の決定方法としては任意の方法を採用可能である。例えば携帯端末1が保持するワンタイム認証鍵の中で最も番号が小さいものを使用予定鍵に選定する。

10

【0174】

なお、携帯端末1は後述するワンタイム認証鍵の有効期限管理によって有効期限が切れたものを順次削除する。認証ECU4も同様の有効期限管理を行うが、認証ECU4とい携帯端末1の時刻情報は完全に一致しているとは限らない。また、有効期限に基づくワンタイム認証鍵の廃棄処理を行うタイミングも相違しうる。それらの事情から、携帯端末1が保持する使用予定鍵を認証ECU4が保持しているとは限らない。

【0175】

認証ECU4は、携帯端末1から通知された使用予定鍵を自身が保持していない場合には、別の鍵を使用するように携帯端末1に要求しても良い。ステップS61a～S62aは認証ECU4と携帯端末1の両方が保持するワンタイム認証鍵が選択されるまで繰り返し実施されてもよい。なお、使用予定鍵のすり合わせをより効率的に行うため、使用鍵確認信号は、認証ECU4が保持するワンタイム認証鍵の中からランダムに／所定規則で選択された複数の候補の番号を含んでいても良い。携帯端末1はそれら複数の候補の中からランダムに／所定の規則に則って使用予定鍵を選択して回答するように構成されていても良い。

20

【0176】

ステップS63aは、認証ECU4がステップS61と同様に、認証ECU4がチャレンジコードを送信するステップである。ステップS64aは認証ECU4が、携帯端末1から使用予定鍵として通知された番号に対応するワンタイム認証鍵と、ステップS63aで送信したチャレンジコードをもとに検証用コードを生成するステップである。ワンタイム認証鍵自体は、車両側記憶部45に保存されているワンタイム認証鍵が使用される。

30

【0177】

ステップS65aは、携帯端末1が、使用予定鍵として選定した番号に対応するワンタイム認証鍵と、認証ECU4から受信したチャレンジコードと、を用いてレスポンスコードを生成するステップである。レスポンスコードの生成に使用されるワンタイム認証鍵自体は、事前にDKS3から取得して端末側記憶部105に保存済みのものである。携帯端末1は、レスポンスコードの生成が完了するとステップS66aとして当該レスポンスコードを認証ECU4に向けて送信する。

【0178】

認証ECU4は、携帯端末1からレスポンスコードを受信すると、ステップS67aとして、当該レスポンスコードとステップS65aで生成した検証用コードとを比較することで、通信相手の正当性を判断する。つまり、2つのコードが一致している場合には認証成功と判定する（ステップS68a）。一方、2つのコードが相違する場合には認証失敗と判定する（ステップS69a）。

40

【0179】

上記の方法によれば、レスポンスコードの生成に際して認証ECU4と携帯端末1の間でやり取りされる情報は、使用予定鍵の番号とチャレンジコードであり、ワンタイム認証鍵自体は通信で送受信されない。鍵番号だけではワンタイム認証鍵を復元することはできない。よって、上記の方法によっても、前述の認証方法と同様に、無関係な人物が不正に認証処理を成功させる恐れを低減可能となる。なお、上記の例では、レスポンスコードの

50

生成前に、携帯端末 1 が使用予定鍵の番号を認証 E C U 4 に通知する態様を述べたが、処理順序はこれに限らない。携帯端末 1 はレスポンスコードを生成した後に、認証 E C U 4 に対して、レスポンスコードの生成に使用したワンタイム認証鍵の番号を通知しても良い。

【0180】

＜ワンタイム認証鍵の補充シーケンス＞

ここでは図 25 を用いて、携帯端末 1 が実行するワンタイム認証鍵補充処理について説明する。ワンタイム認証鍵補充処理は、ワンタイム認証鍵が所定の補充閾値 $ThRp$ 未満となったら補充する処理である。ワンタイム認証鍵補充処理は、図 25 に示すようにステップ S 71 ~ S 77 を備える。ワンタイム認証鍵補充処理は、例えば所定の残数確認周期で定期的に行われる。ワンタイム認証鍵補充処理は、携帯端末 1 がオンライン状態であることを条件として実行されても良い。ワンタイム認証鍵補充処理は、その他、DKS3 から送信された残数確認指示信号を受信したことや、ユーザが所定の残数確認操作を実施したことに基づいて開始されてもよい。ワンタイム認証鍵補充処理は、後述する保存認証鍵更新処理の一部として実行されても良い。残数確認指示信号の受信や、残数確認操作の受け付けなどが、確認イベントに相当する。

10

【0181】

ワンタイム認証鍵補充処理の実行主体としての携帯端末 1 との表現は、端末プロセッサ 101 / ワンタイム認証鍵管理部 F2 と解することができる。

【0182】

ステップ S 71 は、携帯端末 1 が、端末側記憶部 105 に保存されているワンタイム認証鍵の残数 ($Notk$) を確認するステップである。ステップ S 72 は携帯端末 1 が、ステップ S 71 で取得したワンタイム認証鍵の残数 ($Notk$) が所定の補充閾値 ($ThRp$) 未満であるか否かを判定するステップである。 $Notk < ThRp$ を充足する場合、携帯端末 1 はステップ S 73 として認証鍵要求信号を DKS3 に向けて送信する。認証鍵要求信号が、ワンタイム認証鍵の配布を要求する信号である。認証鍵要求信号が補充要求信号に相当する。一方、 $Notk \geq ThRp$ を充足する場合、携帯端末 1 はワンタイム認証鍵の補充にかかるシーケンスを終了する。

20

【0183】

なお、ワンタイム認証鍵の補充の要否は、前述の通り、補充要否フラグで管理される。 $Notk < ThRp$ を充足する場合、携帯端末 1 は補充要否フラグをオンに設定する。また、 $Notk \geq ThRp$ を充足する場合、携帯端末 1 は補充要否フラグをオフに設定する。仮に携帯端末 1 がオフライン状態である場合には補充要否フラグをオンに設定した状態を維持し、その後、オンラインとなったことに基づいて認証鍵要求信号を送信する。

30

【0184】

DKS3 が、携帯端末 1 からの認証鍵要求信号を受信すると、ステップ S 74 として、ユーザ DB33 から要求元のサービス鍵を読み出す。そして、DKS3 は、当該サービス鍵とランダムに / 所定の規則で生成される変動コードを用いて、複数のワンタイム認証鍵を生成する (ステップ S 75)。ステップ S 75 で生成するワンタイム認証鍵の個数は、一定数であってもよいし、補充閾値と残数の差に所定値 (例えば 100) を加えた値であっても良い。認証鍵要求信号は、DKS3 が必要な発行数を特定可能なように、携帯端末 1 におけるワンタイム認証鍵の残数を示す情報を含んでいても良い。

40

【0185】

DKS3 は、ワンタイム認証鍵の生成が完了すると、ステップ S 76 として、認証鍵パッケージを携帯端末 1 に向けて送信する。認証鍵パッケージは、個々のワンタイム認証鍵に変動コードを紐付けたデータセットである。携帯端末 1 は DKS3 から認証鍵パッケージを受信すると、それに含まれるデータを端末側記憶部 105 に保存する (ステップ S 77)。

【0186】

以上の構成によれば、携帯端末 1 が保持するワンタイム認証鍵が所定値未満となったことに基づいて随時補充される。よって、ワンタイム認証鍵が枯渇することによってユーザ

50

が車両Hvを使用不能となる恐れを低減できる。また、補充閾値は例えば100以上の十分に大きい値に設定される。当該設定によれば、ユーザが山間部などの通信圏外に一時的に滞在した場合であっても、通信圏外滞在中にワンタイム認証鍵が不足する恐れを低減できる。なお、デジタルキーアプリ104は、所定の最小値よりも大きい範囲において、ユーザが任意の値を補充閾値として登録可能に構成されていても良い。

【0187】

＜ワンタイム認証鍵の定期更新シーケンス＞

ここでは図26を用いて、携帯端末1が実行する保存認証鍵更新処理について説明する。保存認証鍵更新処理は、端末側記憶部105に保存されているワンタイム認証鍵の一部又は全部を定期的に入れ替える処理である。保存認証鍵更新処理は、図26に示すようにステップS81～S83を備える。保存認証鍵更新処理は例えば所定の入れ替え周期で定期的に行われる。保存認証鍵更新処理は、携帯端末1がオンライン状態であることを条件として実行されても良い。保存認証鍵更新処理を構成する処理ステップの実行主体としての携帯端末1との表現は、端末プロセッサ101／ワンタイム認証鍵管理部F2と解することができる。

【0188】

ステップS81は、携帯端末1が、自身が保持する時刻情報である端末時刻に基づいて、端末側記憶部105に保存されているワンタイム認証鍵毎の有効期限を確認するステップである。携帯端末1は、有効期限が切れているワンタイム認証鍵に関しては削除する（ステップS82）。なお、有効期限の確認は、有効期限として示されている日時と現在の日時とを比較することに相当する。端末時刻は、DKS3などの所定サーバとの通信により随時修正される。

【0189】

ステップS83は携帯端末1が、DKS3と連携して、ワンタイム認証鍵補充処理を実行するステップである。ワンタイム認証鍵補充処理については前述のとおりである。なお、有効期限に基づく補充処理においては、残数(Notk)が補充閾値(ThRp)未満であるか否かによらず、ステップS82で削除した数だけ補充するように構成されていても良い。例えば携帯端末1は、ステップS82で20個のワンタイム認証鍵を削除した場合には、認証鍵要求信号として、20個のワンタイム認証鍵の発行を要求する信号を送信しても良い。認証鍵要求信号は、発行希望数を示す情報を含んでいても良い。

【0190】

上記の構成によれば、定期的に携帯端末1に保存されているワンタイム認証鍵の一部又は全部が、有効期限に基づいて入れ替えられる。当該構成によれば、使用可能なワンタイム認証鍵は経時的に変更される。そのため、セキュリティをより一層強固にすることができる。

【0191】

＜認証ECUにおける時刻情報の更新について＞

認証ECU4は、自身が保持する時刻情報であるECU内部時刻に基づいてゲスト鍵の有効期限をチェックする。そのため、ECU内部時刻は、DKS3の時刻情報と同期していることが好ましい。ここでは、図27を用いてECU内部時刻をDKS3の時刻情報と同期するように補正した上で、ゲスト鍵の有効期限する処理について説明する。ECU時刻情報の更新及びゲスト鍵の有効期限チェックにかかる一連のシーケンスは、図27に示すように、ステップS91～S97を含む。なお、少なくともECU内部時刻の更新にかかるシーケンスは、認証ECU4と携帯端末1との間でBLEの通信リンクが確立していることを条件として実行される。ここでの携帯端末1は、オーナー端末又はゲスト端末のどちらであってもよい。

【0192】

ステップS91は、認証ECU4が携帯端末1に向けて時刻要求信号を送信する。時刻要求信号は、DKS3が保持している時刻情報であるサーバ時刻情報を要求する信号である。時刻要求信号は、例えばECU番号あるいは車両IDなどの、要求元を示す情報を含

10

20

30

40

50

んでいても良い。

【0193】

携帯端末1は、認証ECU4からの時刻要求信号をBLE通信で受信すると、ステップS92として、セルラー通信又はWi-Fi通信のフォーマットに準拠した時刻要求信号を生成し、DKS3に送信する。ステップS92は認証ECU4からのデータをDKS3に転送するステップに相当する。なお、携帯端末1からDKS3に送信する時刻要求信号には、DKS3がサーバ時刻情報の返送先を特定可能なように、携帯端末1の情報を含んでいることが好ましい。

【0194】

DKS3は、携帯端末1からの時刻要求信号を受信すると、サーバ時刻情報を要求元の携帯端末1に返送する（ステップS93）。また、携帯端末1は、DKS3から受信したサーバ時刻情報をBLE通信で認証ECU4に転送する（ステップS94）。

【0195】

認証ECU4は、携帯端末1からサーバ時刻情報を受信すると、当該サーバ時刻情報を用いてECU内部時刻を修正する（ステップS95）。ECU内部時刻は、認証ECU4が保持する時刻情報を指す。なお、各デバイスにおけるデータの受信処理には、チェックコードを用いた正当性の検証処理が含まれていてもよい。チェックコードを用いた検証処理の結果、正当性が認められなかった場合には、要求は棄却されうる。以上で述べたステップS91～S95がECU時刻情報の更新にかかるシーケンスSq1に相当する。

【0196】

認証ECU4は、例えばECU内部時刻の修正が行われたことに基づいて、修正された時刻情報を用いて車両側記憶部45に登録されているゲスト鍵毎の有効期限を確認する（ステップS96）。そして、認証ECU4は、有効期限が切れているゲスト鍵のデータを削除する（ステップS97）。なお、ステップS97は、鍵データは残したまま、フラグなどを用いて有効期限切れのゲスト鍵を無効化する処理であっても良い。

【0197】

ステップS96～S97が、ゲスト鍵の有効期限チェックにかかるシーケンスSq2に相当する。なお、ECU時刻情報の更新にかかるシーケンスSq1と、ゲスト鍵の有効期限チェックにかかるシーケンスSq2は、別々に実施されても良い。ゲスト鍵の有効期限のチェックにかかるシーケンスSq2は、ECU時刻情報が更新された場合に限らず、所定の周期で実行されても良い。また、ゲスト鍵の有効期限のチェックは、走行用電源がオンからオフに切り替わったタイミングや、オフからオンに切り替わったことに基づいて実行されても良い。

【0198】

認証ECU4が備える時刻情報は、認証ECU4が備えるクロック発振器の精度等により、実際の時刻あるいはサーバ時刻とずれうる。以上の構成によれば、携帯端末1と接続するたびに、ECU内部時刻が修正される。そのため、認証ECU4が誤った時刻情報に基づいてゲスト鍵を削除／無効化してしまう恐れを低減できる。

【0199】

＜オーナー鍵の削除処理について＞

車両Hvの売買／譲渡において車両Hvのオーナーは変わりうる。オーナーが変わった場合には、古いオーナーのサービス鍵などは削除されることが好ましい。そのような事情から車両用デジタルキーシステムSysは、ゲスト鍵だけでなく、オーナー鍵の情報を削除可能に構成されている必要がある。

【0200】

本実施形態のDKS3は、オーナー端末及び車載HMIのどちらのデバイスからもオーナー鍵の削除要求を受付可能に構成されている。DKS3は、オーナー端末に対する操作に基づいてオーナー鍵を削除する場合、処理全体としては図28に示すように端末内データ削除フェーズPh3と、車両内データ削除フェーズPh4とを含みうる。端末内データ削除フェーズPh3は、携帯端末1から指定されたサービス鍵（ここではオーナー鍵）のデータを削

10

20

30

40

50

除するフェーズである。車両内データ削除フェーズ P h 4 は、認証 E C U 4 から指定されたサービス鍵を削除するフェーズである。ここではオーナー端末に対する操作に基づいてオーナー鍵を削除する場合のシーケンスについて図 29、図 30 を用いて説明する。

【0201】

図 29 は、端末内データ削除フェーズ P h 3 に対応する各デバイスのインタラクションを示すシーケンス図である。オーナー鍵データを携帯端末 1 から削除するシーケンスは、図 29 に示すように、ステップ T 10 ~ T 18 を含む。

【0202】

ステップ T 10 は、ステップ S 10 と同様に、D K S 3 が、ユーザ／携帯端末 1 を認証するステップである。ステップ T 11 は、オーナー端末としての携帯端末 1 が、ユーザの操作に基づいてオーナー鍵削除要求信号を送信するステップである。オーナー鍵削除要求信号は、例えばデバイス I D、ユーザ I D、又はサービス鍵 I D など、D K S 3 が要求元を特定するための情報を含む。また、オーナー鍵削除要求信号は、削除対象とするサービス鍵を特定するための情報としてサービス鍵 I D、E C U 番号、又は車両 I D の情報などを含んでも良い。1 人のユーザが複数の車両のオーナーである場合を想定すると、オーナー鍵削除要求信号は削除対象とするサービス鍵を特定するための情報を含んでいることが好ましい。

【0203】

D K S 3（サービス鍵削除部 G 5）は、オーナー端末からオーナー鍵削除要求信号を受信すると、ステップ T 12 として、車両用オーナー削除パッケージをオーナー端末に向けて送信する。車両用オーナー削除パッケージは、車両 H v から全てのサービス鍵に関連するデータを削除するためのデータセットである。車両用オーナー削除パッケージは、端末チェックコードや車両チェックコードを含みうる。オーナー端末は、D K S 3 から配信された車両用オーナー削除パッケージを受信すると、端末チェックコードを用いてその正当性を検証した上で、車両用データ一時記憶部 M 2 に保存する（ステップ T 13）。

【0204】

また、D K S 3 は、車両 H v に対してゲスト鍵が発行されている場合、オーナー端末からのオーナー鍵削除要求信号に基づいて、ゲスト端末に向けてゲスト鍵削除コマンドを送信する（ステップ T 14）。車両 H v に対してゲスト鍵が発行されている場合とは、換言すれば削除対象とするオーナー鍵に紐づくゲスト鍵が存在する場合に相当する。ゲスト鍵削除コマンドは、ゲスト端末から車両 H v 用のサービス鍵にかかるデータを削除するように指示する信号である。ゲスト鍵削除コマンドは、削除対象とするサービス鍵 I D や、端末チェックコードなどの情報を含む。ゲスト端末は、ゲスト鍵削除コマンドを受信すると、端末チェックコードを用いてその正当性を検証した上で、鍵情報記憶部 M 1 から指定されたサービス鍵に関連するデータを全て削除する（ステップ T 15）。より好ましい態様として、ゲスト端末は、ゲスト鍵の削除処理が完了するとその旨を D K S 3 に報告する。

【0205】

D K S 3 は、オーナー端末からのオーナー鍵削除要求信号に基づいて、オーナー端末に向けてオーナー鍵削除コマンドを送信する（ステップ T 16）。オーナー鍵削除コマンドは、オーナー端末から車両 H v 用のサービス鍵にかかるデータを削除するように指示する信号である。オーナー鍵削除コマンドは、削除対象とするサービス鍵 I D や、端末チェックコードなどの情報を含む。オーナー鍵削除コマンド及びゲスト鍵削除コマンドは、サービス鍵を削除するための指示コマンド、すなわちサービス鍵削除コマンドの一種に相当する。

【0206】

オーナー端末は、オーナー鍵削除コマンドを受信すると、端末チェックコードを用いてその正当性を検証した上で、鍵情報記憶部 M 1 から指定されたサービス鍵に関連するデータを全て削除する（ステップ T 17）。なお、オーナー鍵削除コマンドは、車両用データ一時記憶部 M 2 に保存されているデータにまでは作用しない。つまり、オーナー端末は、オーナー鍵削除コマンドを受信しても、車両用データ一時記憶部 M 2 に保存されている車両用オーナー鍵削除パッケージは削除せずに所定期間残す。より好ましい態様として、オーナー端末は、オーナー鍵の削除処理が完了するとその旨を D K S 3 に報告する。

【0207】

DKS3は、例えばオーナ端末及びゲスト端末からサービス鍵の削除が完了したことを受信したことに基づいて、削除要求されたオーナ鍵に関するデータをユーザDB33及び車両DB32から削除する（ステップT18）。なお、サーバ内データの削除は、車両Hvから、車両内のデータ削除も完了したことの報告を受信してから実行されてもよい。本実施形態では車両用オーナ削除パッケージとオーナ鍵削除コマンドを別々に送信するが、各種データの送信態様はこれに限らない。車両用オーナ削除パッケージとオーナ鍵削除コマンドは一連のデータとしてまとめて送信されても良い。

【0208】

次の図30を用いて車両Hvからオーナ鍵に関連するデータを削除するシーケンスについて説明する。オーナ鍵に関連する情報には、ゲスト鍵のデータも含まれる。車両Hvからオーナ鍵に関連するデータを削除するシーケンスは、ステップT21～T24を含む。なお、オーナ鍵の登録シーケンスと違って、認証ECU4は通常モードでもオーナ鍵の削除指示は受け付ける。図30の説明における携帯端末1とは、車両用オーナ削除パッケージを保持している携帯端末1であり、旧オーナ端末と呼ぶことができる。

10

【0209】

車両用オーナ削除パッケージを保持している携帯端末1が車両HvのBLE通信圏内に入ると、サービス鍵を保持している状態と同様に、認証ECU4は当該携帯端末1とBLEによる通信接続を行う（ステップT21）。そして、暗号通信が開始される（ステップT22）。携帯端末1は、認証ECU4との暗号通信リンクが確立したことに基づき、車両用データ一時記憶部M2に保存されている、車両Hv向けの車両用オーナ削除パッケージを送信する（ステップT23）。

20

【0210】

認証ECU4は、携帯端末1から車両用オーナ削除パッケージを受信すると、当該パッケージに含まれる命令／プログラムに基づいて、車両側記憶部45に保存されている全てのサービス鍵に関連するデータを削除する。このようにオーナ端末は、認証ECU4との間にBLE通信のリンクが確立している場合に認証ECU4からオーナ鍵を削除可能に構成されている。

【0211】

なお、ステップT11～T13を含むシーケンスは、オーナ端末がDKS3と通信接続している状態において実行されても良い。その場合、オーナ端末がDKS3から取得した車両用オーナ削除パッケージは、ステップT23により速やかに認証ECU4へと転送され、車両側記憶部45からもオーナ鍵が削除される。なお、認証ECU4は、車両用オーナ削除パッケージを受信した場合、受信データに含まれる車両チェックコードに基づいて受信データの正当性を検証した上で、全てのサービス鍵データの削除を実行してもよい。

30

【0212】

<オーナ権限によるゲスト鍵の削除処理について>

ゲストからの申し出や利用規約違反等に基づき、オーナは、有効期限内であってもゲスト鍵を削除可能に構成されていることが好ましい。ここではDKS3は、オーナ端末からの要求に基づき、指定されたゲスト鍵を削除する処理の流れについて図31、図32を用いて説明する。

40

【0213】

オーナ鍵の削除と同様に、ゲスト鍵の削除処理も、携帯端末1からゲスト鍵に関連するデータを削除するフェーズPh3と、車両Hvからゲスト鍵のデータを削除するフェーズPh4に分けることができる。図31は、携帯端末1からゲスト鍵データを削除するフェーズPh3に対応する各デバイスのインタラクションを示すシーケンス図である。ゲスト鍵データを携帯端末1から削除するシーケンスは、図31に示すように、ステップT30～T39bを含む。

【0214】

なお、オーナの操作を受け付けるデバイスは携帯端末1に限らず、デスクトップ／ノー

50

ト P C (ラップトップ)であってもよい。以降におけるオーナ端末は、オーナが操作するデスクトップ／ノート P Cであってもよい。

【0215】

ステップ T 3 0 は、オーナ端末におけるデジタルキーアプリ 1 0 4 が、操作者がオーナであることを認証するステップである。デジタルキーアプリ 1 0 4 における認証方法は、パスワードを用いる方法であっても良いし、生体情報を用いる方法であっても良い。オーナであるか否かの検証には、パスワードと生体情報の両方が使用されても良い。ユーザ認証は 2 段階認証など多用な方法が採用可能である。

【0216】

ステップ T 3 1 は、オーナ端末が、タッチパネル 1 2 から入力される操作信号に基づき、ディスプレイ 1 1 に削除対象選択画面を表示するステップである。削除対象選択画面は、削除対象とするゲスト鍵、又は、それに対応するゲストを選択するための画面である。削除対象選択画面は、ゲスト又はゲスト鍵のリストを含む。なお、削除対象選択画面は、ゲストの一覧を示すゲストリスト画面あるいはゲスト削除画面と呼ぶこともできる。

【0217】

ステップ T 3 2 では、オーナ端末が、タッチパネル 1 2 の出力信号が示す、削除対象選択画面に対するユーザ操作に基づいて、削除対象とするゲスト鍵を特定する。削除対象とするゲスト鍵を選択するユーザ操作が削除指示操作に相当する。オーナ端末は、削除対象とするゲスト鍵がオーナによって選択されると、当該ゲスト鍵を対象とするゲスト鍵削除要求信号を D K S 3 に送信する (ステップ T 3 3)。ゲスト鍵削除要求信号は、削除対象とするサービス鍵を特定するための情報として、削除対象のサービス鍵 I D 又はユーザ I D を含む。なお、ゲスト鍵削除要求信号は、複数のゲスト鍵をまとめて削除するように要求する信号であっても良い。例えばゲスト鍵削除要求信号は、オーナ鍵に紐づく全てのゲスト鍵をまとめて削除するように要求する信号であっても良い。

【0218】

D K S 3 は、ゲスト鍵削除要求信号を受信すると、当該受信信号にて指定されているゲスト鍵に紐づくゲスト端末に向けて、ゲスト鍵削除コマンドを送信する (ステップ T 3 4)。ゲスト端末は、ゲスト鍵削除コマンドを受信すると、端末チェックコードを用いてその正当性を検証した上で、指定されたサービス鍵に関連するデータを鍵情報記憶部 M 1 から全て削除する (ステップ T 3 5)。ゲスト鍵削除コマンドが削除指示信号に相当する。ゲスト端末は、より好ましい態様として、ゲスト鍵の削除処理が完了するとその旨を D K S 3 に報告する。

【0219】

ステップ T 3 6 は、D K S 3 が、オーナ端末に向けてゲスト鍵の削除が完了したことを通知するステップである。D K S 3 は、ゲスト鍵削除コマンドの送信が完了したことに基づいてゲスト鍵削除完了通知を送信してもよいし、ゲスト端末から削除完了の報告を受信してからゲスト鍵削除を送信してもよい。

【0220】

オーナ端末は、D K S 3 からゲスト鍵削除完了通知を受信すると、削除完了通知画面をディスプレイ 1 1 に表示する (ステップ T 3 7)。削除完了通知画面は、削除したゲスト鍵に紐づくユーザ名などを含みうる。

【0221】

また、D K S 3 は、オーナ端末、及び、削除対象に設定されたゲスト鍵に対応するゲスト端末に向けて、車両用ゲスト鍵削除パッケージを送信する (ステップ T 3 8 a、T 3 8 b)。各デバイスは、車両用ゲスト鍵削除パッケージを受信すると、それを車両用データ一時記憶部 M 2 に保存する (ステップ T 3 9 a、T 3 9 b)。車両用ゲスト鍵削除パッケージが削除用データセットに相当する。

【0222】

次に、図 3 2 を用いて車両 H v からゲスト鍵に関連するデータを削除するシーケンスについて説明する。車両 H v からゲスト鍵に関連するデータを削除するシーケンスは、ステ

10

20

30

40

50

ップ T 4 1 ~ T 4 4 を含む。車両 H v からゲスト鍵に関連するデータを削除するシーケンスに登場するゲスト端末とは、車両用ゲスト削除パッケージを保持しているゲスト端末に相当する。

【 0 2 2 3 】

オーナー端末又はゲスト端末としての携帯端末 1 が車両 H v の B L E 通信圏内に入ると、認証 E C U 4 は当該携帯端末 1 と B L E による通信接続を行う（ステップ T 4 1）。そして、暗号通信が開始される（ステップ T 4 2）。携帯端末 1 は、認証 E C U 4 との暗号通信リンクが確立したことに基づき、車両用データ一時記憶部 M 2 に保存されている、車両 H v 向けの車両用ゲスト削除パッケージを送信する（ステップ T 4 3）。

【 0 2 2 4 】

認証 E C U 4 は、オーナー端末／ゲスト端末から車両用ゲスト削除パッケージを受信すると、当該パッケージに含まれる命令／プログラムに基づいて、削除対象に指定されているゲスト鍵に関連するデータを、車両側記憶部 4 5 から削除する。

【 0 2 2 5 】

なお、ステップ T 4 1 ~ T 4 3 を含むシーケンスは、オーナー端末／ゲスト端末が D K S 3 と通信接続している状態において実行されても良い。また、認証 E C U 4 は、車両用ゲスト削除パッケージを受信した場合、受信データに含まれる車両チェックコードに基づいて受信データの正当性を検証した上で、全てのサービス鍵データの削除を実行してもよい。

【 0 2 2 6 】

上記の構成によれば、オーナーは任意のタイミングで任意のゲスト鍵を削除可能となる。よって、ゲストによる車両 H v の利用状況や、オーナーの都合に応じて、ゲストによる車両 H v の使用を停止させることが可能となる。

【 0 2 2 7 】

なお、ゲストが車両 H v を使用している際に急にゲスト鍵が削除されると、ゲストに不都合が生じうる。特に、ゲストが車両 H v を用いて本来の車両 H v の保管場所から離れた場所に移動している場合に、急に車両 H v が使用不可となると、ゲストもオーナーも不都合が生じうる。そのような事情からゲスト鍵の削除の申請から、実際に削除処理が実行されるまでには一定時間の猶予が設けられうる。ゲスト鍵等の削除は、車両 H v が規定された保管場所に駐車されていることを条件として実行されてもよい。D K S 3 は、オーナーによるゲスト鍵の削除申請が行われたことを示す画面を該当するゲスト端末に表示させても良い。

【 0 2 2 8 】

なお、上記の通り、オーナー端末は、車両に紐づくゲスト鍵を選択的に削除するための操作は受付可能に構成されている。一方、ゲスト鍵を削除せずに有効期限又は権限にかかる設定だけを変更する操作は受け付け不能に構成されている。D K S 3 もまた、発行済みのサービス鍵に関し、当該サービス鍵を残したまま、権限設定及び有効期限を変更することは不能に構成されている。オーナーは、あるゲストに対するサービス鍵の権限設定や有効期限を変更したい場合は、該当するゲスト鍵を一旦削除したのちに、所望の権限設定を行ったゲスト鍵を発行する事となる。

【 0 2 2 9 】

以上では、オーナーがオーナー端末等を操作することでゲスト鍵を削除する場合を述べたが、ゲスト鍵はゲスト自身の操作でも削除されうる。D K S 3 は、ゲストの操作に基づき、ゲスト鍵を削除した場合には、当該ゲスト鍵に紐づくオーナー端末に対してゲスト鍵が削除されたことの通知を送信する。オーナー端末は、当該通知に基づき、例えば削除されたゲスト鍵又はそのユーザ名を含むゲスト削除画面を表示する。あるいは、D K S 3 からの通知に基づき、ゲストごとのステータス情報を更新する。

【 0 2 3 0 】

< 車載 H M I を用いてサービス鍵の削除処理について >

ここでは図 3 3 を用いて車載 H M I に対するユーザ操作に基づき、ユーザにより指定されたサービス鍵を削除する処理の流れについて説明する。車載 H M I に対するユーザ操作

10

20

30

40

50

に基づき、ユーザにより指定されたサービス鍵を認証 ECU 4 及び関連する携帯端末 1 から削除するシーケンスは、図 33 に示すように、ステップ T50～T57 を含む。なお、前提として、DKS 3 は、車載 HMI を介して、操作者の権限に応じたサービス鍵の削除要求を受付可能に構成されている。例えば車載 HMI 50 の操作者がオーナーである場合、認証 ECU 4 及び DKS 3 は、ゲスト鍵のみならず、オーナー鍵に対する削除指示も車載 HMI 50 を介して受付可能に構成されている。図 33 を構成するステップのうち、認証 ECU 4 が実行するステップについて、その具体的な実行主体は認証プロセッサ 41 と解することができる。

【0231】

ステップ T50 は認証 ECU 4 が、車載 HMI 50 を操作しているユーザを認証するステップである。認証方法としては前述の通り、パスワードの入力を伴う方法や生体情報を用いる方法など多様な方法を採用可能である。当該ステップ T50 は、車載 HMI 50 の操作者を識別するステップと解することができる。また、認証 ECU 4 によるユーザの認証は、認証 ECU 4 による携帯端末 1 の認証結果が流用されても良い。認証 ECU 4 は、通信相手としての携帯端末 1 に対応するユーザを、車載 HMI 50 の操作者とみなしても良い。

10

【0232】

ステップ T51 は、入力装置 52 から入力される操作信号に基づいて認証 ECU 4 がディスプレイ 51 にサービス鍵削除画面を表示する。サービス鍵削除画面は、削除対象とするサービス鍵 ID、又は、ユーザを選択するための画面である。操作者がオーナーであると認識されている場合、サービス鍵削除画面は、削除対象としてオーナー鍵も選択可能に構成されている。サービス鍵削除画面は、操作者としてのユーザの権限で削除可能なサービス鍵のリスト、又は、対応するユーザのリストを含みうる。

20

【0233】

ステップ T52 では認証 ECU 4 が、入力装置 52 の出力信号が示す、サービス鍵削除画面に対するユーザ操作に基づいて、削除対象とするサービス鍵を特定する。そして認証 ECU 4 は、ステップ T53 として車両側記憶部 45 から削除対象に指定されたサービス鍵に関するデータを削除する。認証 ECU 4 は車両側記憶部 45 からのデータ削除が完了すると、削除完了画面を表示する（ステップ T54）。削除完了画面は削除したサービス鍵に紐づくユーザ名などの情報を含みうる。なお、削除完了画面の表示は任意の要素であって省略されても良い。

30

【0234】

認証 ECU 4 は、指定されたサービス鍵に関連するデータの削除が完了すると、ステップ T55 として、サービス鍵の削除シーケンスが完了したことを示す削除完了通知信号を DKS 3 に向けて送信する。削除完了通知信号は、削除したサービス鍵の ID 又はそれに対応するユーザ ID などを含む。なお、削除対象としてオーナー鍵が指定された場合には、ステップ T53 にて、車両側記憶部 45 からすべてのサービス鍵が削除される。

【0235】

DKS 3 は、認証 ECU 4 からの削除完了通知信号を受信すると、当該受信信号にて指定されているサービス鍵に紐づく携帯端末 1 に向けて、サービス鍵削除コマンドを送信する（ステップ T56）。仮に車載 HMI 50 に対する操作に基づき車両側記憶部 45 からオーナー鍵が削除された場合には、DKS 3 は、オーナー端末及び当該オーナー端末に紐づくすべてのゲスト端末に向けて、サービス鍵削除コマンドを送信する。

40

【0236】

携帯端末 1 は、サービス鍵削除コマンドを受信すると、端末チェックコードを用いてその正当性を検証した上で、鍵情報記憶部 M1 から指定されたサービス鍵に関連するデータを全て削除する（ステップ T57）。各携帯端末 1 は、より好ましい態様として、サービス鍵の削除処理が完了するとその旨を DKS 3 に報告する。

【0237】

上記の通り、オーナーは、車載 HMI 50 を用いても任意のゲストのサービス鍵を削除可

50

能である。また、オーナは、車載HMI50を用いてオーナ鍵も削除可能である。なお、オーナの代わりに、ディーラショップのスタッフが車載HMI50を用いて同様の削除処理を実行可能である。

【0238】

なお、認証ECU4は、セキュリティ解除ツール又はDKS3からセキュリティ解除信号が入力されたことを条件として車載HMI50を用いたオーナ鍵の削除処理を実行するように構成されていても良い。そのような構成によれば、操作ミスや不正な操作によってオーナ鍵及びそれに紐づく全てのゲスト鍵が削除されてしまう恐れを低減できる。オーナ鍵の削除はゲスト鍵の削除よりもその影響範囲が大きい。故に、オーナ鍵の削除に向けたユーザ認証は、ゲスト鍵の削除に向けたユーザ認証よりも、より高度／複雑に構成されていてもよい。例えばオーナ鍵の削除するためのユーザ認証のステップ数は、ゲスト鍵を削除する際のユーザ認証ステップ数よりも多く設定されていても良い。

10

【0239】

また、DKS3は、以上で述べたようにオーナ鍵の削除操作が車載HMI50を介して実施されたか否かに応じて、オーナ端末に対して異なるデータを送信する。例えばオーナ鍵の削除操作がオーナ端末で行われた場合には、DKS3はオーナ端末に向けて、車両用オーナ鍵削除パッケージを送信する一方、オーナ鍵の削除操作が車載HMI50で行われた場合には、DKS3は車両用オーナ鍵削除パッケージを送信しない。当該構成によれば、オーナ端末のデータ通信量を抑制できる。また、そもそもオーナ鍵の削除操作が車載HMI50で行われた場合には、認証ECU4はDKS3から削除用データセットを受信することなく、すべてのサービス鍵を削除する。つまり、DKS3の通信量自体も削減できる。

20

【0240】

<DKSによるサービス鍵の管理方法の補足>

DKS3は、1つのオーナ鍵に紐づくゲスト鍵は、何れもオーナ鍵のサービス鍵IDによって管理する。DKS3は、発行権付きゲスト鍵を削除した場合であっても、図34に示すように、当該発行権付きゲスト鍵の権限で発行された、孫世代／第3世代のゲスト鍵は削除しない。孫世代／第3世代のゲスト鍵はオーナ鍵に紐づくゲスト鍵として存続する。なお、図34中の1xはオーナ鍵を、1yは発行権付きゲスト鍵を、1zは孫世代／第3世代のゲスト鍵を、それぞれ示している。1vは、オーナ鍵が発行したゲスト鍵であって、発行権の有無は任意である。便宜上、1つのオーナ鍵に紐づくゲスト鍵のグループをファミリーとも称する。ファミリーを構成するサービス鍵はオーナ鍵IDで管理される。

30

【0241】

さらに、DKS3は、ユーザによる携帯端末1の機種変更の申請を受付可能に構成されている。ユーザによって機種変更が行われた場合、デバイスIDは変化しうる。しかしながら、サービス鍵IDに関しては、機種変更が行われた場合であっても、変更されない。ファミリーはオーナ鍵のサービス鍵IDによって形成されるため、仮にオーナが携帯端末1の機種を変更した場合であっても、ゲスト鍵には影響はなく、ファミリー自体は存続する。例えばオーナが携帯端末1の機種を変更した場合であっても、オーナ端末のデバイスID及びサービス鍵が変更されるだけとなる。発行権限付きゲスト鍵を有するゲストの携帯端末1が変更された場合も同様である。つまり、車両用デジタルキーシステムSysは、ゲスト鍵の発行元となる携帯端末1が別のデバイスに変更された場合であっても、他のゲスト鍵に影響を及ぼさないように構成されている。

40

【0242】

DKS3は、例えば図35に示す手順で、オーナ端末変更処理を実施する。オーナ端末変更処理は、オーナ端末の機種変更にかかる処理である。図35に示すようにオーナ端末認証処理は、ステップT61～T68を含みうる。オーナ端末変更処理は、携帯端末1又はPCなどから、機種変更の申し出に相当する信号が入力されたことに基づいて開始される。オーナが操作する端末は、機種変更前の携帯端末1である旧端末であってもよいし、機種変更後の携帯端末1である新端末であってもよい。また、オーナが機種変更を申請す

50

るデバイスは、デスクトップ／ラップトップPCなど、インターネットにアクセスな端末であれば何でも良い。オーナーによる所定のデータ引き継ぎ操作により、新端末にもデジタルキーアプリ104はインストールされ、且つ、ユーザID等の情報が登録されているものとする。

【0243】

ステップT61は、操作者／申請者がオーナーであることを認証するステップである。オーナーであることの認証方法は前述の通りである。DKS3は、操作者がオーナーであることを認証すると、ユーザID等に基づいてユーザDB33を参照し、オーナーの旧デバイスID及びサービス鍵IDを取得する（ステップT62）。旧デバイスIDは、旧端末のデバイスIDを指す。また、DKS3は新端末とデータ通信を実施することで、新端末のデバイスIDである新デバイスIDを取得する（ステップT63）。ステップT64は、DKS3が新デバイスIDを用いてオーナー鍵としてのサービス鍵を新規発行するステップである。具体的なサービス鍵の生成方法は前述のとおりである。

10

【0244】

DKS3は、新オーナー鍵を生成すると、ユーザDB33の登録内容を更新する（ステップT65）。例えば、オーナーのユーザデータにおいては、旧オーナー鍵を削除して、新オーナー鍵を登録する。旧オーナー鍵とは機種変更前まで使用されていたサービス鍵であって、旧デバイスIDに基づくサービス鍵である。なお、本実施形態ではオーナーのデバイスが変更された場合であってもオーナーのサービス鍵IDは変更されずに従前のIDが維持されるため、ゲストのユーザデータに関しては特段の処置は不要である。他の態様として、サービス鍵IDも変更される場合には、DKS3は、ゲスト鍵に紐づくオーナーのサービス鍵IDを新オーナー鍵IDに置き換えうる。その他、DKS3は、新オーナー鍵を生成すると、新オーナー鍵に対応するワンタイム認証鍵を所定数作成する。

20

【0245】

そして、DKS3は、新端末に向けて端末用鍵交換パッケージを送信する（ステップT66）。端末用鍵交換パッケージは、少なくとも新オーナー鍵を含む。端末用鍵交換パッケージは、鍵情報記憶部M1に保存されているオーナー鍵を新オーナー鍵に置き換えさせるコマンド／プログラムであってもよい。端末用鍵交換パッケージは、新オーナー鍵に対応する複数のワンタイム認証鍵と、変動コードと、を含みうる。その他、端末用鍵交換パッケージは、端末チェックコードを含んでも良い。ワンタイム認証鍵にかかるデータセットは、認証鍵パッケージとして端末用鍵交換パッケージとは別に送信されても良い。

30

【0246】

新端末としての携帯端末1は、DKS3から端末用鍵交換パッケージを受信すると、端末チェックコードをもとにデータの正当性を検証したのちに、新オーナー鍵にかかる受信データを鍵情報記憶部M1に保存する。具体的には、端末プロセッサ101は、受信した新オーナー鍵としてのサービス鍵と、変動コードと紐付けられた複数のワンタイム認証鍵を保存する。

【0247】

また、DKS3は、新オーナー鍵に関するデータを認証ECU4に登録するためのデータセットである車両用鍵交換パッケージを、新端末に送信する。車両用鍵交換パッケージは、新オーナー鍵としてのサービス鍵と、車両チェックコードを含む。車両用鍵交換パッケージは、車両側記憶部45に保存されているオーナー鍵を新オーナー鍵に置き換えさせるコマンド／プログラムであってもよい。

40

【0248】

新端末としての携帯端末1は、車両用鍵交換パッケージを受信すると、車両用データ一時記憶部M2に保存する。そして、認証ECU4とBLE暗号通信リンクが確立したことに基づいて、車両用鍵交換パッケージを認証ECU4に転送する。つまり、車両用鍵交換パッケージもまた、車両用登録パッケージと同様に携帯端末1を介して認証ECU4に配信される。

【0249】

50

認証 ECU 4 は車両用鍵交換パッケージを受信すると、車両チェックコードをもとにデータの正当性を検証したのちに、新オーナー鍵にかかる受信データを車両側記憶部 45 に保存する。具体的には、認証プロセッサ 41 は、受信した新オーナー鍵としてのサービス鍵をオーナー鍵記憶部 451 に保存する。なお、これに伴い認証 ECU 4 は、オーナー鍵記憶部 451 に保存されていた旧オーナー鍵を削除する。サービス鍵 ID に関しては機種変更後も維持されるため、削除せずに流用しても良い。もちろんサービス鍵 ID も一旦削除した後に新規登録されてもよい。

【0250】

なお、認証 ECU 4 は、オーナー鍵記憶部 451 にオーナー鍵が保存されている状態で、オーナー鍵の登録操作を受け付けた場合には、所定の警告メッセージをディスプレイ 11、51 に表示させても良い。警告メッセージは、例えばオーナーがすでに登録済みであることを示すメッセージである。その他、認証 ECU 4 は、オーナー鍵記憶部 451 にオーナー鍵が保存されている状態でオーナー鍵の登録操作を受け付けた場合には、所定のパスワードの入力を促す画面をディスプレイ 11、51 に表示させても良い。ここで入力を要求するパスワードとしては、例えば、オーナーのユーザ ID に紐づくパスワード、あるいは、オーナー鍵を削除するための所定コードを採用することができる。

【0251】

その他、DKS 3 は、ステップ T68 として、旧端末に向けてサービス鍵削除コマンドを送信する。これにより、旧端末がオンライン状態を維持している場合には、旧端末からサービス鍵が削除される。なお、ステップ T68 は任意の要素であって省略されても良い。

【0252】

<システム全体にかかるその他の補足>

以上では、車両 Hv は、一例として個人によって所有される車両とし、オーナーもまた個人である場合を想定したが、上記の車両用デジタルキーシステム Sys は MaaS (Mobility as a Service) にも適用可能である。オーナーは、例えば車両貸し出しサービスやシェアリングサービスを提供する企業／組織であってもよい。その場合、当該企業／組織に属するオペレータとしてのスタッフが、オーナー端末の操作を行いうる。また、オーナーが保有する車両 Hv は 50 台や 100 台など、多数であってもよい。オーナーとしてのサービス鍵 ID は、複数の車両に対して共通であってもよいし、車両ごとに相違していても良い。DKS 3 の構成は、事業の形態に応じて、車両情報を管理するサーバと、サービス鍵を管理するサーバと分けられていても良い。

【0253】

上述した実施形態では認証 ECU 4 はサービス鍵の登録／削除にかかるデータを、携帯端末 1 から取得する構成について述べたが、これに限らない。認証 ECU 4 はセルラー通信又は Wi-Fi 通信によって、携帯端末 1 を介さずに DKS 3 から各種パッケージを受信するように構成されていても良い。

【0254】

<付言(1)>

以上で述べた携帯端末 1 は、

ユーザの操作に基づいて車両を使用するためのサービス鍵を生成するサーバ(3)に向けて、当該ユーザが所有する車両についてのサービス鍵であって、オーナーとしての権限を有するオーナー鍵を発行するように要求する、オーナー鍵発行要求信号を送信することと、

オーナー鍵発行要求信号に対するサーバの応答として、サーバからオーナー鍵を受信することと、

受信したオーナー鍵を所定の端末側記憶装置(105)に保存することと、

車両に搭載されている車両用装置(4)と近距離無線通信の通信リンクが確立していることを条件として、オーナー鍵を車両用装置に登録するための通信を開始することと、を実行するように構成されている、携帯可能な汎用的情報処理端末と解することができる。

【0255】

また、デジタルキーアプリ 104 は、汎用的なコンピュータを携帯端末 1 として実行さ

10

20

30

40

50

せるコンピュータプログラムと解することができる。加えて、デジタルキーアプリ104が保存されている記憶媒体は、コンピュータを上記の携帯端末1として動作させる命令セットが格納された記憶媒体に相当する。

【0256】

<付言(2)>

本開示に記載の装置、システム、並びにそれらの手法は、コンピュータプログラムにより具体化された一つ乃至は複数の機能を実行するようにプログラムされたプロセッサを構成する専用コンピュータにより、実現されてもよい。また、本開示に記載の装置及びその手法は、専用ハードウェア論理回路を用いて実現されてもよい。さらに、本開示に記載の装置及びその手法は、コンピュータプログラムを実行するプロセッサと一つ以上のハードウェア論理回路との組み合わせにより構成された一つ以上の専用コンピュータにより、実現されてもよい。

【0257】

例えば認証プロセッサが備える機能の一部又は全部はハードウェアとして実現されても良い。或る機能をハードウェアとして実現する態様には、1つ又は複数のICなどを用いて実現する態様が含まれる。プロセッサ(演算コア)としては、CPUや、MPU、GPU、DFP(Data Flow Processor)などを採用可能である。また、認証プロセッサが備える機能の一部又は全部は、複数種類の演算処理装置を組み合わせで実現されていてもよい。認証プロセッサが備える機能の一部又は全部は、システムオンチップ(SoC: System-on-Chip)や、FPGA、ASICなどを用いて実現されていても良い。FPGAはField-Programmable Gate Arrayの略である。ASICはApplication Specific Integrated Circuitの略である。上記補足説明は、端末プロセッサ及びサーバプロセッサについても同様に適用可能である。また、コンピュータプログラムは、コンピュータにより実行されるインストラクションとして、コンピュータ読み取り可能な非遷移有形記録媒体(non-transitory tangible storage medium)に記憶されていてもよい。プログラムの保存媒体としては、HDD(Hard-disk Drive)やSSD(Solid State Drive)、フラッシュメモリ等を採用可能である。

【符号の説明】

【0258】

1 携帯端末、2 専用キー、3 デジタルキーサーバ(DKS)、4 認証ECU、7 車載システム、10 端末制御部、11 ディスプレイ、12 タッチパネル(入力装置)、16・57 BLE通信部(近距離通信部)、17 セルラー通信部(ネット接続部)、18 Wi-Fi通信部(ネット接続部) 101 端末プロセッサ、104 デジタルキーアプリ、105 端末側記憶部(端末側記憶装置)、M1 怪情報記憶部、M2 車両用データ1次記憶部、20 制御回路、21・56 近接場通信部、30 データ処理部、32 車両データベース、33 ユーザデータベース、301 サーバプロセッサ、303 ストレージ、40 車両制御部、41 認証プロセッサ、45 車両側記憶部(車両側記憶装置)、451 オーナ鍵記憶部、452 ゲスト鍵記憶部、50 車載HMI、51 ディスプレイ、52 入力装置。

10

20

30

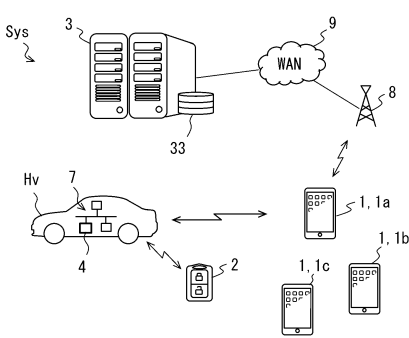
40

50

【図面】

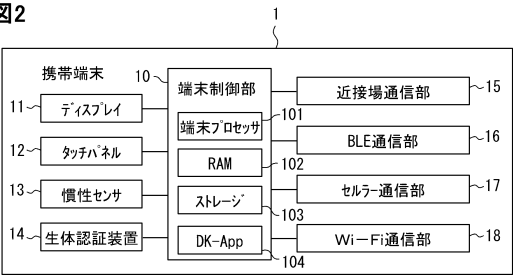
【図 1】

図 1



【図 2】

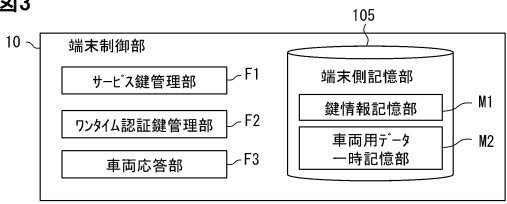
図 2



10

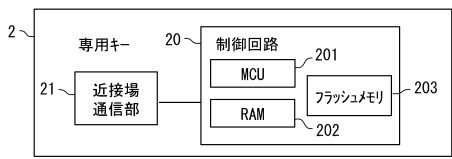
【図 3】

図 3



【図 4】

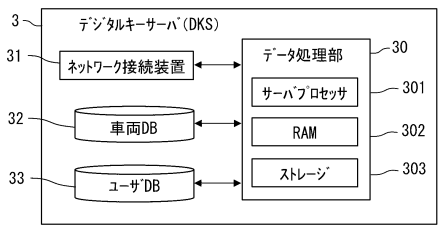
図 4



20

【図 5】

図 5



【図 6】

図 6

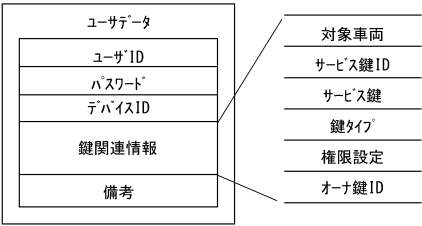


30

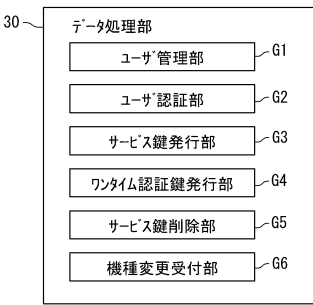
40

50

【図 7】
図7

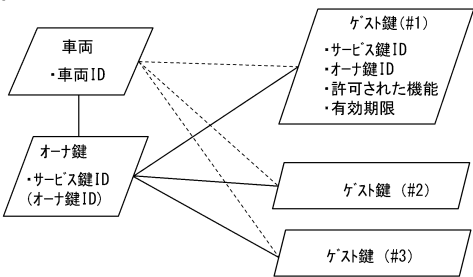


【図 8】
図8

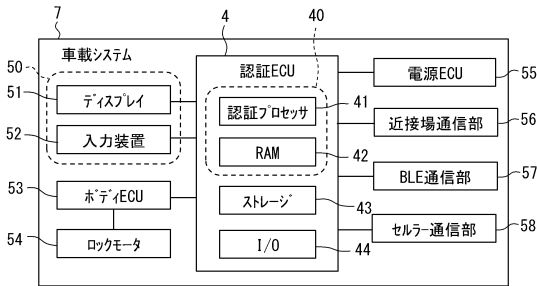


10

【図 9】
図9

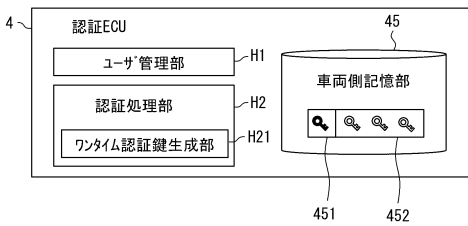


【図 10】
図10

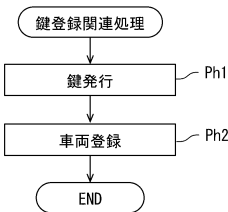


20

【図 11】
図11



【図 12】
図12

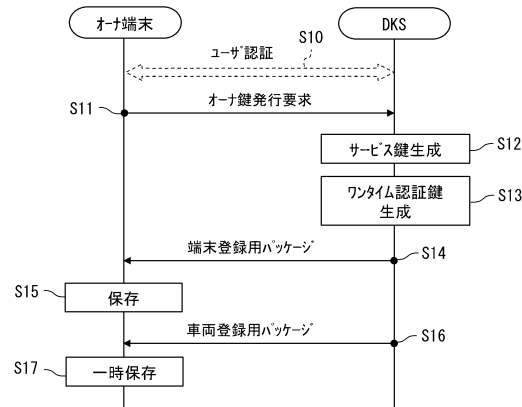


30

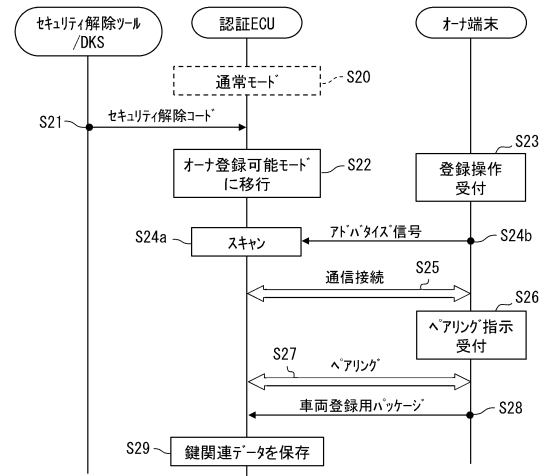
40

50

【図 1 3】
図 13

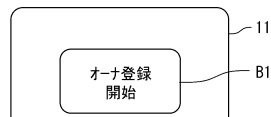


【図 1 4】
図 14

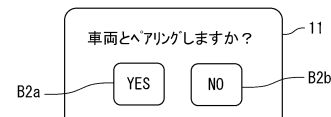


10

【図 1 5】
図 15

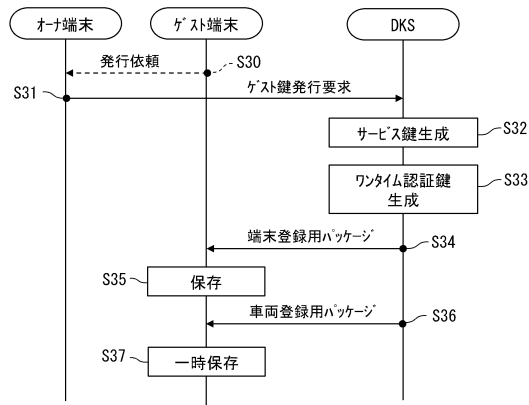


【図 1 6】
図 16



20

【図 1 7】
図 17



【図 1 8】
図 18

要求元情報
対象車両情報
対象ユーザID
有効期限
権限設定
・ゲスト鍵発行
・電源操作
・利用可能ドア

30

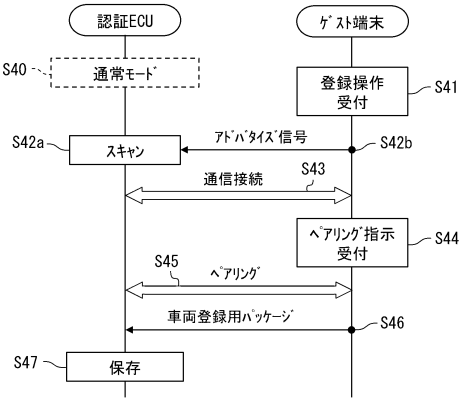
40

50

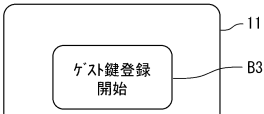
【図 19】
図19

基本情報	サービス鍵
	サービス鍵ID
	ワンタイム認証鍵
	変動コード
ゲスト用 情報	発行元情報
	オーナー鍵ID
	対象車両情報
	有効期限
	権限設定

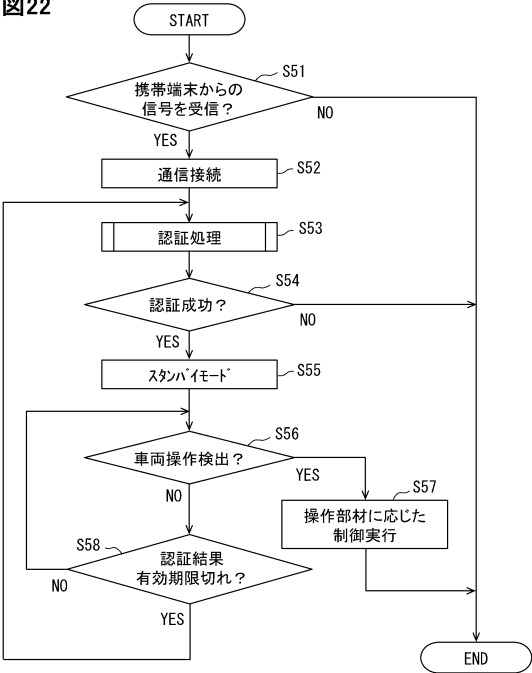
【図 20】
図20



【図 21】
図21



【図 22】
図22



10

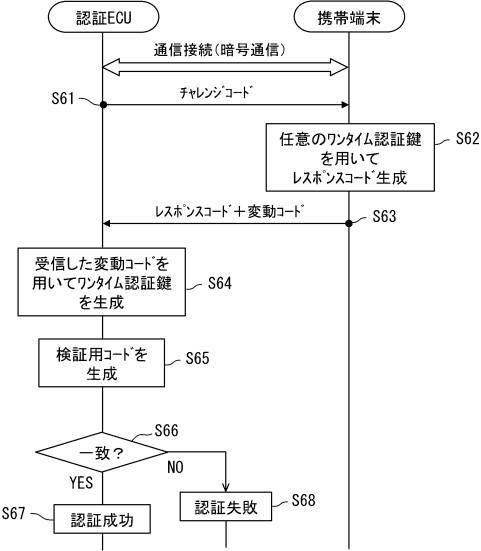
20

30

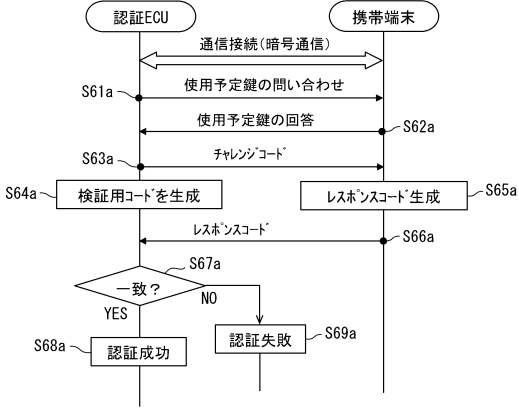
40

50

【図 2 3】
図23

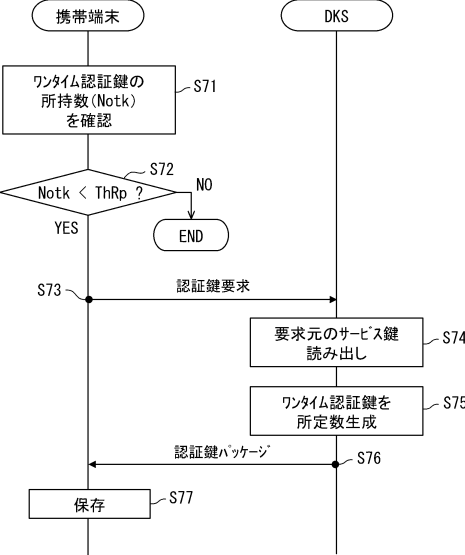


【図 2 4】
図24

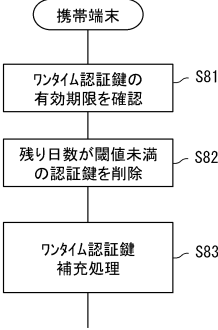


10

【図 2 5】
図25



【図 2 6】
図26



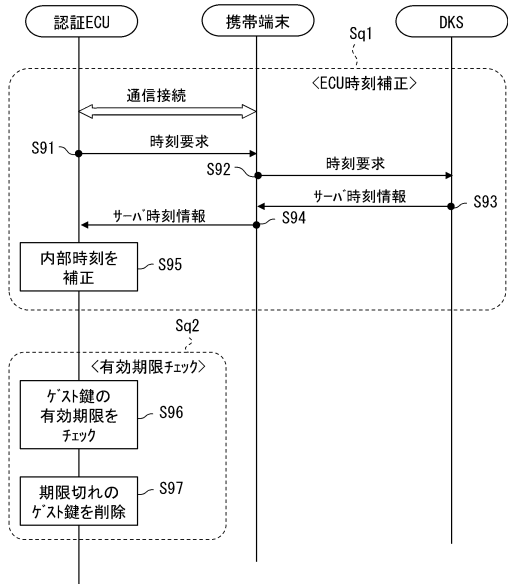
20

30

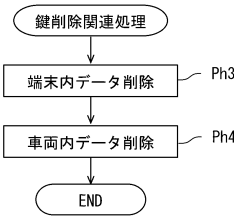
40

50

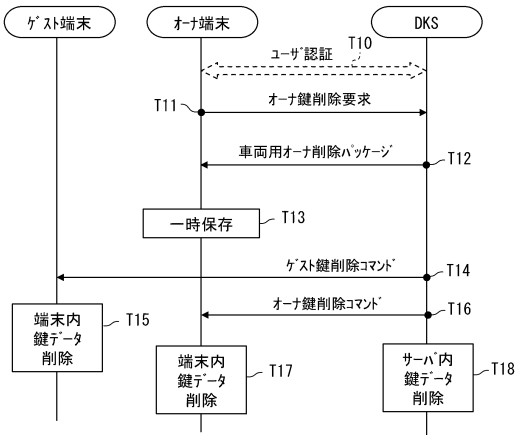
【図 27】
図27



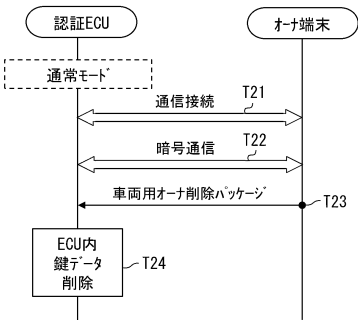
【図 28】
図28



【図 29】
図29



【図 30】
図30



10

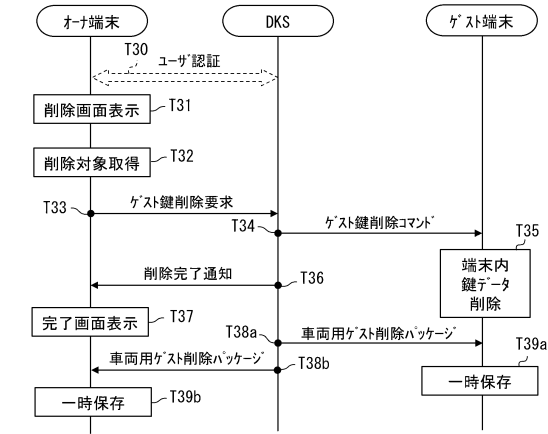
20

30

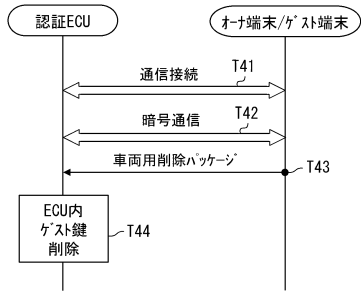
40

50

【図 3 1】
図31

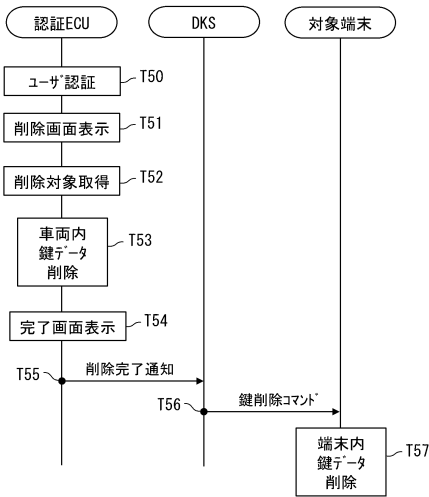


【図 3 2】
図32

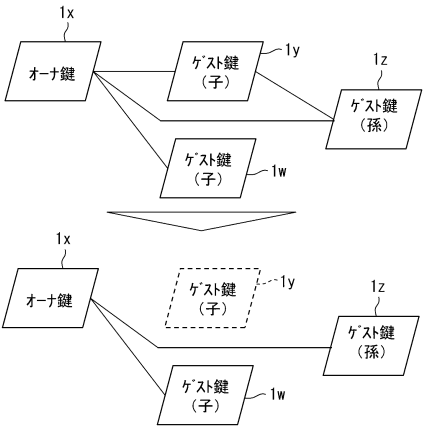


10

【図 3 3】
図33



【図 3 4】
図34



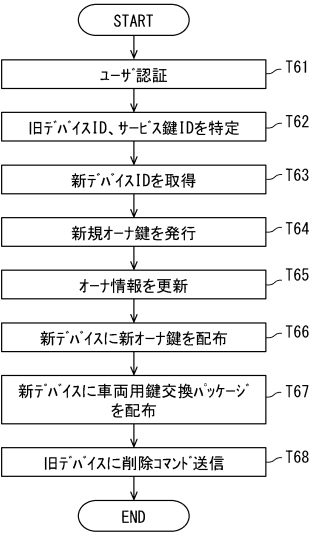
20

30

40

50

【図 3 5】
図35



10

20

30

40

50

フロントページの続き

- 会社デンソー内
- (72)発明者 マレク コチェンスキ
フランス国， 9 2 4 0 0 クルブボア， プラス サミュエル ドゥ シャンプラン 2 アイデミア フ
ランス内
- (72)発明者 ミカエル ワシレフスキ
フランス国， 9 2 4 0 0 クルブボア， プラス サミュエル ドゥ シャンプラン 2 アイデミア フ
ランス内
- (72)発明者 フィリップ ラテル
フランス国， 9 2 4 0 0 クルブボア， プラス サミュエル ドゥ シャンプラン 2 アイデミア フ
ランス内
- (72)発明者 バルトミ レヴィンスキ
フランス国， 9 2 4 0 0 クルブボア， プラス サミュエル ドゥ シャンプラン 2 アイデミア フ
ランス内
- 審査官 辻 勇貴
- (56)参考文献 国際公開第 2 0 2 0 / 1 7 4 5 4 4 (WO， A 1)
特開 2 0 2 0 - 1 9 3 5 1 0 (JP， A)
特開 2 0 1 6 - 1 3 3 9 6 9 (JP， A)
特開 2 0 1 1 - 2 5 6 5 6 1 (JP， A)
- (58)調査した分野 (Int.Cl.， DB名)
G 0 6 F 2 1 / 6 2